N° d'ORDRE : 11/2015-M/MT

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE 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 :ARITHMETIQUE, Codage et Combinatoire :
Algèbre et Théorie des Nombres

par MOUZAÏA Mohamed

Discriminant d'un corps de nombre défini par un $\mathbb{Q}$ -trinôme

Soutenu publiquement le 19/02/2015, devant le jury composé de :

Mme BENFERHAT LEILA, MAITRE DE CONFERENCES / A à l'USTHB, Présidente

Mr BENSBAA BOUALEM, MAITRE DE CONFERENCES / A à l'USTHB, Directeur de Mémoire.

Mr BENCHERIF FARID, PROFESSEUR à l'USTHB, Examinateur

Mr BOUCHENA RACHID MAITRE ASSISTANT/A à l'USTHB, Invité

Mémoire de Magister

17 avril 2015

Remerciements

e tiens tout d'abord à remercier vivement le directeur de ma thèse , monsieur BENSEBA BOUALEM , pour sa disponibilité , ses orientations , ses aides et conseils qui m'ont permis de mener à terme ce travail.

Mes remerciements vont également à l'encontre de madame BENFERHAT LEILA , pour avoir accepté de présider le jury de soutenance de ce mémoire . Que monsieur BENCHERIF FARID et monsieur BOUCHENA RACHID trouvent ici l'expression de mes remerciements pour avoir accepté de faire partie du jury de ce mémoire.

Ce mémoire est le résultat d'un travail de recherche de près de trois ans .

Je veux adresser tous mes remerciements aux personnes avec lesquelles j'ai pu échanger des avis et qui m'ont aidé pour la rédaction de ce mémoire .

Enfin , j'adresse mes plus sincères remerciements à ma famille qui m'a accompagné, aidé, soutenu et encouragé tout au long de la réalisation de ce mémoire .

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 du polynôme$P$ 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 $K-$ automo
$\det(u)$:	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

L'objet de ce mémoire est l'étude de la détermination du discriminant d'un corps de nombre défini engendré sur $\mathbb{Q}$ par une racine d'un polynôme irréductible à coefficients dans l'anneau des entiers rationnels. Cette détermination a été examinée par P. Llorente, E. Nart et N. Vila dans une publication parue dans Acta Arithmetica (1984). Cette publication traite de la notion de polygone de Newton que Ore a expoité pour la détermination de l'indice d'un entier algébrique. Les travaux de Ö. Ore ont permis la généralisation des travaux de Dedekind sur la ramification d'un nombre premier p dans l'anneau des entiers du corps de nombres. Les résultats donnés par Ore et précisés par les auteurs ci- dessus dans une publication parue en 1991 ont été généralisés par S.D. Cohen, A.C. Movahhedi et A. Salinier en 2000 dans une publication parue dans le jounal of Algebra.
Soit $f(X) = X^n + AX^s + B \in \mathbb{Z}[X]$, $(n, s) = 1$ et $1 \leq s < n$, un trinôme irréductible sur $\mathbb{Q}$. Soit $\alpha := \alpha_1, \ldots, \alpha_n$ les différentes racines de f dans une clôture algébrique de $\mathbb{Q}$. On note par $K = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ respectivement le corps de rupture et le corps de décompositions de f sur $\mathbb{Q}$ et soit $\mathcal{O}_K$ l'anneau d'entiers de K.

On note par $i(\alpha) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ l'indice du groupe $\mathbb{Z}[\alpha]$ dans le groupe additif $\mathcal{O}_K$

Le discriminant D_f du trinôme f est donné par :

$$D = (-1)^{n(n-1)2} B^{s-1} \left[n^n B^{n-s} + (-1)^{n-1} (n-s)^{n-s} s^s A^n\right]$$

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

$$D = i(\theta)^2 d.$$

La démarche des auteurs consiste en la détermination de la valuation p-adique $v_p(d_K)$ du discriminant d_K en un nombre premier p divisant le discriminant D_f du trinôme $f(X)$ sachant qu'ils sont liés par la relation

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

où $i(\alpha)$ désigne l'indice de $\mathbb{Z}[\alpha]$ dans le groupe additif de l'anneau $\mathcal{O}_K$ des entiers du corps K. Les auteurs, dans une large partie de leur travail, s'appuient pour cela sur le résultat de Ore donnant la valuation p-adique de l'entier $i(\alpha)$.

Ce mémoire se décline en trois chapitres.

Le premier chapitre est consacré à la revue des résutats de base en théorie algébrique des nombres. Nous évoquerons les différentes notions relatives à l'arithmétique des corps de nombres. Nous donnerons un exposé sur les notions d'anneaux d'entiers, de normes d'un entier et d'un idéal ainsi que la notion de discriminant d'une base d'entiers. Nous donnerons un apperçu sur les anneaux de Dedekind afin de définir la notion de factorisation en produit d'idéaux premiers d'un idéal dans l'anneau $\mathcal{O}_K$ des entiers d'un corps de nombre $\mathcal{O}_K$.

La ramification est un outil très déterminant dans l'étude de l'arithmétique des corps de nombres. Cette connaissance est rendue possible grâce aux corps p-adique, c'est l'objet du second chapitre. Pour exprimer les résultats de l'arithmétique au niveau local (dans les extensions du corps p-adique $\mathbb{Q}_p$) au niveau global (dans les extensions du corps $\mathbb{Q}$), nous donnons un dictionnaire permettant de faire le lien entre les ramifications et les discriminants pour chacun des contextes.

Le chapitre 3 est consacré à la recherche du discriminant d'un corps de nombre $K = \mathbb{Q}(\alpha)$ engendré par une racine d'un trinôme irréductible $f(X) = X^n +$

$AX^s + B$, où n et s sont des entiers premiers entre eux, une étude due à Llorente-Nart et Villa (un article paru en 1984 dans Journal of Number Theory). Par la suite nous donnerons une généralisation du théorème de Ore sur la ramification d'un nombre premier p dans l'anneau des entiers du corps de rupture du trinôme $f(X)$. Cette généralisation est due à S.D. COHEN, A. MOVAHHEDI et A. SALINIER , parue en 2000 dans Journal of Algebra.

Chapitre 1

Extensions de corps de nombres

1.1 Notions d'extensions

1.1.1 Définitions et notations :

Soit K un corps commutatif

Définition 1.1 *:On appelle extension du corps K, tout corps L le contenant. Dans ce cas , on note L/K ou bien $K \subset L$ l'extension de K.*

Exemple 1

1. L'ensemble $\{a + b\sqrt{2}\,;\, a, b \in \mathbb{Q}\}$muni des opérations + et õ ,addition et multiplication,est une extension du corps $\mathbb{Q}$.
2. $\mathbb{R}$ est une extension de $\mathbb{Q}$.
3. $\mathbb{C}$est une extension de $\mathbb{Q}$.
4. $\mathbb{C}$ est une extension de $\mathbb{R}$.

Proposition 1.2 *Une extension L d'un corps K est un K-espace vectoriel*
preuve :K est un sous-corps de L donc L est un K-espace vectoriel.

Définition 1.3 *La dimension de L comme K-espace vectoriel est appelée degré de l'extension L/K qu'on note*$[L : K]$.

On dit que l'extension L/K est finie si$[L : K]$ *est finie.*

- 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

1. Soit L=$\{$a+b$\sqrt{2}$,avec a$\in \mathbb{Q}$ et b$\in\mathbb{Q}\}$.$(1,\sqrt{2})$ est une base de$L$ comme $\mathbb{Q}$-espace vectoriel, alors $[L : \mathbb{Q}] = 2$ et $L/\mathbb{Q}$ est une extension quadratique .

2. $\mathbb{C}/\mathbb{R}$ est une extension quadratique dont une base est $\{1, i\}$ comme $\mathbb{R}$-espace vectoriel , alors $[\mathbb{C} : \mathbb{R}] = 2$.

3. $\mathbb{R}/\mathbb{Q}$ est une extension infinie.

4. $M = \left\{a + b\alpha + c\alpha^2 \,;\, a, b, c \in \mathbb{Q} \text{ et } \alpha = \sqrt[3]{2}\right\}$est un $\mathbb{Q}$-espace vectoriel dont une base est $\{1, \alpha, \alpha^2\}$, c'est donc une extension cubique de $\mathbb{Q}$.

Proposition 1.4 *Soient L/K et M/L deux extensions, alors M/K est une extension de degré fini si et seulement si les extensions L/K et M/L sont de degrés finis et dans ce cas on a :* $[M : K] = [M : L]\,[L : K]$

Preuve : Si L/K et M/L sont de degrés finis, soit $[L : K] = k$ et $[M : L] = m$, alors il existe $\{x_1, \ldots, x_k\}$une K-base de L et $\{y_1, \ldots, y_m\}$ une L-base de M, ce qui entraine que $\forall z \in M, , z = \sum_{i=1}^{m} a_i y_i$, où $a_i \in L$. D'autre part, on a

$a_i = \sum_{j=1}^{k} a_{ji}x_j$, où $a_{ji} \in K$, ce qui donne

$$z = \sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq k}} a_{ji}x_j y_i$$

Ainsi, M est un K-espace vectoriel de dimension finie de base $\{x_j y_i\}$ et donc $[M : K] = km = [M : L]\,[L : K]$.
Réciproquement, supposons que M/K est finie, il en sera de même de L/K, car tout élément de L est un élément de M. D'autre part, M/L est aussi fini, sinon M/K ne le serait pas.

□

Exemple 3

1. Soient $L = \left\{a + b\sqrt{2},\ a, b \in \mathbb{Q}\right\}$et $M = \mathbb{Q}(j) = \{a + bj,\ a, b \in \mathbb{L} \text{ et } j^2 + j + 1 = 0\}$. Alors, $[L : \mathbb{Q}] = 2$ et $[M : L] = 2$ ce qui donne $[M : \mathbb{Q}] = [M : L].[L : \mathbb{Q}] = 4$.M est un $\mathbb{Q}$-espace vectoriel de dimension 4 dont une base est $(1, \sqrt{2}, \text{j}, \text{j}\sqrt{2})$

Remarque 1 *La proposition précédente peut se généraliser à une tour de n extensions de degrés finis :*

Proposition 1.5 *Soit la tour d'extensions $K = K_1 \subset K_2 \subset K_3 \subset \ldots \subset K_n = M$, alors M/K est finie si et seulement si K_{i+1}/K_i , $1 \leq i \leq n-1$, est finie . Dans ces cas, on a*

$$[M : K] = [M : K_{n-1}] \ldots [K_2 : K] = \prod_{i=1}^{n-1} [K_{i+1} : K_i]$$

1.1.2 Extensions algébriques :

Définition 1.6 *SoitL/K une extension de corps .Un élément α de L est dit algébrique sur K s'il existe un polynôme non nul P de K[X] tel que $P(\alpha) = 0$.*

Définition 1.7 *On dit qu'une extension L/K est algébrique si tout élément de L est algébrique sur K c-à-d tout élément de L est racine d'un polynôme à coéfficients dans K .*

Exemple 4 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$*est une extension algébrique.*

Proposition 1.8 *Soit L/K une extension de corps telle que L=K(α),où αde L est algébrique sur K, alors L/K est une extension algébrique, et plus généralement, L = L(A) avec A={α,αalgébrique sur K}*

Preuve : Soit $\alpha \in L$ algébrique sur K de degrén, alors$K(\alpha)$ est un$K$-espace vectoriel de dimension$n$ dont une base est $\{1 , \alpha, \alpha^2,\alpha^3,...,\alpha^{n-1}\}$.
Soit$x \in L$,alors la famille $1, x, x^2, x^3, ..., x^n$ est liée, donc ils existent des $\lambda_i$de K avec $0 \leq i \leq n$ non tous nuls tels que :$\lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n = 0$.
Ce qui montre que tout élément x de L est algébrique sur$K$ et par conséquent,L/K est une extension algébrique.

□

Proposition 1.9 *Toute extension finie L/K est une extension algébrique.*

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

□

Définition 1.10 *On appelle corps de nombres, toute extension finie du corps $\mathbb{Q}$ des nombres rationnels.*

Définition 1.11 *SoientK un corps ,L/K une extension de corps et α un élément deL algébrique surK.*

L'unique polynome unitaireP de $K[X]$ de degré minimal s'annulant en αest appelé polynome minimal de αsurK.On le noteP $= min(\alpha, X, K)$.

Si le degré de Pest n,on dit que α est de degré n sur K

Proposition 1.12 *:Soient K un corps , L/K une extension de corps et α un élément de L algébrique surK de polynôme minimalP surK , alors on a les propriétées suivantes :*

1. Tout polynome de $K[X]$ s'annulant en α est divisible par$P$.
2. Pest irréductible sur K.
3. Si $\beta \in L$ et$P(\beta) = 0$ alors min(β, X, K)=P

Preuve :

□

1. Si$f(X)\in K[X]$ et$f(\alpha) = 0$alors$f(\alpha) \in$ (P) donc$f(X)$ est divisible par$P$.
2. Supposons que P est réductible sur K ,alors$P = UV$ avec$U$et$V$deux polynomes de$K[X]$ tels que$degU \geq 1$et $degV \geq 1$et$U(\alpha)V(\alpha) \neq 0$ sinon$P \neq min(\alpha, X, K)$ d'où$P(\alpha) \neq 0$ce qui est absurde ,par conséquent$P$ est irréductible.
3. Si $\beta \in L$ et$P(\beta) = 0$ alors$P = \lambda min(\beta, X, K)$ avec $\lambda \in K^*$,comme$P$ et min$(\beta, X$,K) sont unitaires alors $\lambda = 1$ donc$P = min(\beta, X, K)$

Exemple 5

1. $X^2-3 \in \mathbb{Q}\left(\sqrt{3}\right)$.$\sqrt{3}$est racine de X^2-3 donc $\sqrt{3}$est algébrique sur$\mathbb{Q}$.D'autre part X^2-3est irréductible sur $\mathbb{Q}$ car $\sqrt{3}$ et$-\sqrt{3} \notin \mathbb{Q}$ donc $min(\sqrt{3}, \mathbb{Q}, X) = X^2 - 3$ et $\sqrt{3}$est de degré 2 sur $\mathbb{Q}$.

2. soit$P = X^2 + 2X + 2 \in \mathbb{R}[X]$de racines $\alpha = -1 - i$ et $\beta = -1 + i.\alpha \notin \mathbb{R}$ et $\beta \notin \mathbb{R}$ donc $X^2 + 2X + 2$ est irréductible sur $\mathbb{R}$ et $\min(\alpha, \mathbb{R}, X) = X^2 + 2X + 2$ et α est de degré 2 sur$\mathbb{R}$.

3. Soit α une racine de $X^3 + 2X + 2 \in \mathbb{Q}[X]$ alors α est algébrique sur $\mathbb{Q}$.Soient $u \in \mathbb{Z}$ et $v \in \mathbb{N}$tel que$(u/v)^3 + 2(u/v) + 2 = 0$ donc$u/v \in \{-2, -1, 1, 2\}$ or -2,-1,1,2 ne sont pas racines de $X^3 + 2X + 2$donc ce polynome est irréductible sur $\mathbb{Q}$.
   Par conséquent Min(α,$\mathbb{Q}$,X)=X^3+2X+2 et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

Le critère d'Eisenstein est utilisé pour décider de l'irréductibilité d'un polynôme

Proposition 1.13 *Soient P(X)=*$a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in \mathbb{Z}$ *et p un nombre premier*

si $p \mid a_i$*pour tout i,*$0 \leq i \leq n-1$ *et* $p \nmid a_n$*et* $p^2 \nmid a_0$*alors P(X) est irréductible sur* $\mathbb{Q}$*.On dit alors que P(X)est d'Eisenstein en p.*

Exemple 6

1. P(X)=$X^3 + 6X^2 - 4X + 2$, on remarque que P(X) est d'eisenstein en p=2 donc P est irréductible sur $\mathbb{Q}$.

2. P(X)=$X^3 + 7X^2 + 5X + 1$, On ne peut appliquer le critère d'Eisenstein(il n'existe pas de p premier divisant 1,5,7).Mais comme Q(X)=P(X-1)=$X^3 + 4X^2 - 6X + 2$ est d'Eisenstein en p=2 alors P est irréductible sur $\mathbb{Q}$

Définition 1.14 *SoitK un corps,on appelle clôture algébrique de K , toute extensionL/K telle que tout polynômeP*$\in L[X]$ *de degré* $\deg P \geq 1$ *admet au moins une racine dansL*

1.1.3 Extensions séparables, extensions normales

Définition 1.15 *SoitK un corps, on dit qu'un polynômef ∈ K[X] de degrén est séparable s'il admet exactementn racines distinctes dans une clôture algébrique deK*

Exemple 7

1. $X^3 - 3$ admet trois racines distinctes dans $\mathbb{C}$, alors $X^3 - 3$est séparable sur $\mathbb{Q}$.

2. Soit p un nombre premier, $K = \mathbb{F}_p[T^p]$ un sous corps du corps des fractions rationnelles $L = \mathbb{F}_p[T]$. Le polynôme $P = X^p - T^p$ est irréductible sur K, mais $P = (X - T)^p$ est décomposé dans L, alors P est non séparable sur K.

La caractérisation des polynômes séparables est donnée par

Proposition 1.16 *SoientK un corps et P un polynôme deK[X] , alors P est séparable sur K si et seulement si P et sa dérivée formelle P′ sont premiers entre eux*

Preuve : [cf. J.Ca, p. 43]

□

Corollaire 1.17 *Soient K un corps de caractéristique 0, P un polynôme non constant et irréductible dans K [X], alors P est séparable sur K.*

Preuve : [cf. J.Ca, p. 43]

□

Exemple 8 *Le polynômeP(X) = X^4 − 3X^2 + 6X + 3 ∈ ℚ[X] est d'Eisenstein en p = 3, alors P est irréductible et séparable sur ℚ*

Corollaire 1.18 *SoientK un corps de caractéristique un nombre premier p et f(X) un polynôme de K[X],degf≥ 1 alors f est inséparable sur K si et seulement si ∃g∈ K [X]tel que f(X)=g(X^p)*

Preuve : [cf. J.Ca, Théorème 324 p. 43]

□

Définition 1.19 *SoientL/K une extension de corps ,α un élément deL algébrique surK. On dit que α est séparable surK si son polynôme minimal irr(α, K, X) est séparable surK*

On dit qu'une extensionL/K est séparable sur$K$ si tout élément de$L$ est séparable sur$K$

Théorème 1.20 *(Théorème de l'élément primitif)*

SoientK un corps ,L/K une extension de degré fini. SiL/K est séparable, alors il existe α ∈ L tel queL = K(α).

Dans ce cas α est appelé élément primitif deL

Preuve : [voir cf J.c p46. }

□

Proposition 1.21 *SoitK ⊂ L ⊂ M une tour d'extensions de corps de degrés finis, alorsM/K est séparable si et seulement siM/L est séparable et L/K est séparable*

Définition 1.22 *SoitL/K une extension de corps .On dit queL est séparable surK si le polynome minimal Irr(α, K, X) de tout élémentα ∈ L est séparable surK.*

Définition 1.23 *On dit qu'une extensionL/K de degré fini est normale surK si et seulement si le polynôme minimal ,Irr(α, K, X) de tout élémentα ∈ L a toutes ses racines dansL*

Exemple 9

1. $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ est une extension de degré 2, normale sur $\mathbb{Q}$ car $\alpha = \sqrt{2}$a pour polynôme minimal $X^2 - 2$ dont les racines sont dans $\mathbb{Q}(\sqrt{2})$.

2. L'extension $\mathbb{Q}(\exp(\frac{2i\Pi}{5}))/\mathbb{Q}$ est une extension normale sur $\mathbb{Q}$ car l'élément α=$exp(\frac{2i\pi}{5})$ a pour polynôme minimal $P(X) = X^4 + X^3 + X^2 + X + 1$ qui a pour racines $\alpha_k = exp(\frac{2ik\pi}{5})$avec $0 \leq k \leq 4$ qui sont toutes dans $\mathbb{Q}(\exp(\frac{2i\pi}{5}))$.

3. L'extension $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ n'est pas normale car le polynôme minimal de $\alpha = \sqrt[3]{3}$est $X^3 - 3$ qui admet pour autres racines les nombres complexes non réels $\alpha j, \alpha j^2$tq j=$\exp(\frac{2i\pi}{3})$ qui ne sont pas dans $\mathbb{Q}(\sqrt[3]{3})$.

1.2 Anneaux d'entiers et discriminants de corps des nombres

1.2.1 normes , traces et discriminant

1.2.1.1 normes

Définition 1.24 *on appelle norme sur un anneau$A$ de $\mathbb{C}$ toute application$N$ de A dans $\mathbb{Z}$, multiplicative càd vérifiant :*$\forall \alpha, \beta \in A : N(\alpha\beta) = N(\alpha)\, N(\beta)$

Exemple 1.1 *soit* $A = \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d}; a, b \epsilon \mathbb{Z}\right\}$ *où*$d \in \mathbb{Z}$*, est sans facteur carré.*
$N : A \longrightarrow \mathbb{Z}$ *tel que*$N(a + b\sqrt{d}) = a^2 - db^2$ *est une norme*

Proposition 1.25 *soit$A$ un sous-anneau de $\mathbb{C}$;$\alpha, \beta \in A$ et$N$ une norme sur$A$.Si αdivise βdans$A$ alors$N(\alpha)$divise $N(\beta)$ dans $\mathbb{Z}$.*

En particulier,si$N(\alpha)$est premier dans $\mathbb{Z}$,alors α est irréductible dans$A$.De plus α est une unité de$A$ si et seulement si$N(\alpha) = \pm 1$.

Preuve : [cf. Z.I. Bo]

□

Exemple 1.2 *1)*$\mathbb{Z}[i]$ *est un anneau euclidien donc factoriel c.à.d tout élèment de* $\mathbb{Z}[i]$ *s'écrit comme produit de facteurs irréductibles de* $\mathbb{Z}[i]$ *et ce de façon unique à l'ordre des facteurs prés.*

2)$\mathbb{Z}[\sqrt{-5}]$*est un anneau non factoriel .*$N(a+b\sqrt{-5}) = a^2+5b^2$*.On a deux factorisations pour 6.*

*6=2*3=(1+*$\sqrt{-5}$*)(1-*$\sqrt{-5}$*) et chacun des nombres 2,3,1+*$\sqrt{-5}$*,1-*$\sqrt{-5}$ *est irrédutible.*

soit$L|K$ une extension de corps séparable, $n = [L : K]$.Ωune clôture algébrique de$K$ et$L$. On note σ_i,$1 \leq i \leq n$ les K-morphismes de$L$ dans Ω .Pour tout $x \in L$, soitm_x l'application$K$-linéaire :$L \longrightarrow L$

tq: $m_x(u) = ux$

Définition 1.26 *On appelle Trace(resp Norme, Polynôme caractéristique) de* $x \in L$ *sur* K *, et on le note*$Tr_{L|K}(x)$*(resp*$N_{L|K}(x)$*,*$P_{L|K}(x)$*), la trace (resp le determinant ,le polynôme caractéristique)de* m_x*.*

On a donc$P_{L|K}(x) = det(xId_L - m_x)$*.*

Remarques :Notons que pour tout $x, y \in L$ *et* $\alpha \in K$ *on a :*$m_x + m_y = m_{x+y}$ *;*$m_x \circ m_y = m_{xy}$ *et* $\alpha m_x = m_{\alpha x}$*.*

Proposition 1.27 *soit* $x \in L$ *, on a :*$P_{L|K}(m_x) = 0$

Preuve : Soit$P_{L|K,x}(X) = a_nX^n+a_{n-1}X^{n-1}+...+a_1X+a_0$*. Par le théoréme de Cayley-Hamilton,* $P_{L|K,x}(m_x) = 0$*. D'autre part par la remarque précédente :*

$$\begin{aligned} P_{L|K,x}(m_x) &= a_n m_x^n + a_{n-1}m_x^{n-1} + ... + a_0 I \\ &= a_n m_{x^n} + a_{n-1}m_{x^{n-1}} + ... + a_0 m_1 \\ &= m_{a_n x^n+...+a_0} = m_{P_{L|K,x}(x)}(x) \end{aligned}$$

Ainsi ,$m_{a_n x^n+...+a_0} = 0$ *d'où*$m_{P_{L|K},x}(x)(1) = 0$

Preuve : [cf. J.P. Es]

□

Proposition 1.28 *Il en résulte que la condition nécessaire et suffisante pour que les polynômes caractéristique et minimal de*$x \in L$ *sur* K *soient égaux est que* x *soit un élément primitif de*$L|K$.

Proposition 1 *L'application trace :*$Tr_{L|K}$ *:*$L \longrightarrow K$ *est une forme linéaire de* K*-espace vectoriel* L *. L'application Norme :*$N_{L|K}$ *:*$L \longrightarrow K$ *induit un morphisme de groupes multiplicatifs de* L^* *vers* K^* *.Pour tout*$x \in K$ *on a :*$Tr_{L|K}(x)$ $=nx$ *et* $N_{L|K}(x) = x^n$

Preuve : On a :$\mathrm{N}_{L|K}(xy)=\det(\mathrm{m}_{xy})=\det(\mathrm{m}_x \circ m_y)=\det(\mathrm{m}_x).\det(\mathrm{m}_y)=\mathrm{N}_{L|K}(x).\mathrm{N}_{L|K}(y)$

□

Proposition 2 *D'autre part si* $x \in K$ *, la matrice de* m_x*dans une base de* K *est* $x\ Id_n$ *, d'où les valeurs de* $Tr_{L|K}(x)$ *et* $N_{L|K}(x)$ *dans ce cas.*

Proposition 1.29 *Soient*$K \subset M \subset L$ *une suite d'extensions de corps ,*$m = [M : K]$ *;*$r = [L : M]et n = [L : K] = mr$ *.Pour tout*$x \epsilon M$ *on a :*$P_{L|K,x}(X) = P_{M|K,x}(X)^r$

Preuve : Soit $(e_1, e_2, ..., e_n)$ une base de L sur$M$ et $(f_1, f_2, ..., f_n)$une base de$M$ sur$K$. En tant que$K$-espace vectoriel , on a :$L = Me_1 \oplus Me_2 \oplus ... \oplus Me_r$ etMe_j a$(f_1e_j, f_2e_j, ..., f_me_j)$pour base sur$K$ .Pour $x \in M$, les sous-K-espaces vectorielsMe_j sont stables par$m_x : L \longrightarrow L, u \longmapsto ux.SoitB$ la matrice de $m_x$dans la base des(f_ie_j)et A la matrice de $\widetilde{m}_x : M \longrightarrow M, u \longmapsto ux$ dans la base $(f_1, f_2, ..., f_m)$alors$B$ est diagonale par blocs avec r blocs diagonaux égaux à A .En prenant les détérminants , on en déduit le résultat.

□

Corollaire 1.30 *Soit L une extension finie de K.Pour tout$x \in K$,le polynôme caractéristique de$x \in K$ est une puissance de son polynôme minimal.*

Preuve : On applique la proposition précédente aux extensions$K \subset K(x) \subset L$.

□

Proposition 1.31 *Soit$L$ une extension finie séparable de$K$ de degré n et $\sigma_i, 1 \leq i \leq n$, les$K-morphismes$ de$L$ dans une clôture algébrique de K et$L$.*

Pour tout $x \in L$, le polynôme caractéristique de x sur K est :$P_{L|K,x}(X) = \prod_{i=1}^{n}(X - \sigma_i(x))$.

Preuve : on a : $K \subset M = K(x) \subset L \subset \Omega$,où$\Omega$ est une clôture algébrique de$L$.

Supposons d'abord $L = K(x)$, les σ_i sont distincts et le polynôme minimal de x sur K est : $\prod_{i=1}^{n}(X - \sigma_i(x))$,qui coincide avec le polynôme caractéristique puisque x est primitif .

□

1.2.2 Discriminant

Définition 1.32 *SoitL/K une extension de corps.Soient $x_1, x_2, ..., x_n$ des éléments de L ,le discriminant $D_{L/K}(x_1, x_2, ..., x_n)$ de ce n-uplet est défini par :*

$D_{L/K}(x_1, x_2,...,x_n)$=$(det(\sigma_i(x_j))^2$.

Exemple 10 *$L = \mathbb{Q}(\sqrt{2})$ et $K = \mathbb{Q}$.$\sigma_1(\sqrt{2}) = \sqrt{2}$ et $\sigma_2(\sqrt{2}) = -\sqrt{2}$.Ainsi $D_{L/K}(1, \sqrt{2})$=$\left(\begin{vmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{vmatrix}\right)^2$=8*

Proposition 1.33 *Pour $(x_1, x_2, ..., x_n) \in L^n$,on a : $D_{L/K}(x_1, x_2, ..., x_n)$=$det(Tr_{L/K}(x_i x_j)$ et $D_{L/K}(x_1, x_2,....,x_n) \in K$.*

Preuve : Soit $A = (\sigma_i(x_j))$,on a :$\det(A^t) = det(A)$ donc $D_{L/K}(x_1, x_2, ..., x_n) = det(A^t A)$ et le coefficient ij de cette matrice est :$\sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)$=$\sum_{k=1}^{n} \sigma_k(x_i x_j) = Tr_{L/K}(x_i x_j) \in K$.

□

Proposition 1.34 *Soit L/K une extension séparable et x un élément primitif de L/K.Soit f le polynôme minimal de x sur K. Alors* $D_{L/K}(1, x, x^2, ..., x^{n-1})$=$(-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_i(x) - \sigma_j(x)) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(x))$

En particulier :$D_{L/K}(1, x, x^2,...,x^{n-1}) \neq 0$

Preuve : Par définition $D_{L/K}(1, x, x^2,...,x^{n-1})$=$(\det(\sigma_i(x^j)))^2 = (det(\sigma_i(x))^j)^2$

$(\sigma_i(x^j))$=$((\sigma_i(x))^j)$ est la matrice de Vandermonde du n-uplet $(\sigma_1(x),\sigma_2(x),...,\sigma_n(x))$ donc $\det(\sigma_i(x^j))$=$\prod_{i<j} (\sigma_i(x) - \sigma_j(x))$ et puis :

$$D_{L/K}(1, x, x^2, ..., x^{n-1}) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\sigma_i(x) - \sigma_j(x)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{j \neq i} (\sigma_i($$

D'autre part , on sait que : $f(X) = \prod_{i=1}^{n} (X - \sigma_i(x))$ pour tout $i : 1 \leq i \leq n$

.

$\sigma_i(f'(x))$=$f'(\sigma_i(x))$=$\prod_{j \neq i} (\sigma_i(x) - \sigma_j(x))$ Par conséquent :$D_{L/K}(1, x, x^2, ..., x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \sigma_i(f'(x))$ =$(-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(x))$

Comme les $\sigma_i(x)$ sont distincts , on a bien $D_{L/K}(1, x, x^2, ..., x^{n-1}) \neq 0$

□

Exemple 11 *$f(x) = x^3 + px + q$ irréductible avec $p, q \in \mathbb{Q}$*

α une racine de $f(x)$, alors $(1, \alpha, \alpha^2)$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\alpha)$. La matrice de $m_{f(\alpha)}$ dans la base $(1, \alpha, \alpha^2)$ est $\begin{pmatrix} p & -3q & 0 \\ 0 & 2p & -3q \\ 3 & 0 & 2p \end{pmatrix}$

Son determinant est :$4p^3+27q^2$ *Par la proposition précédente :*$D_{K/\mathbb{Q}}(1,\alpha,\alpha^2) = -(4p^3+27q^2)$

Lemme 1.35 *Soit L/K une extension séparable de degré n et $x_1, x_2, ..., x_n \in L$*

Si $B = (b_{ik})$ est une matrice $n\times n$ à coefficients dans K et $y_j = \sum_{k=1}^{n} b_{jk}\ x_k$ alors $D_{L/K}(y_1, y_2, ..., y_n) = (det(B))^2 D_{L/K}(x_1, x_2, ..., x_n)$

Preuve : $D_{L/K}(x_1, x_2, ..., x_n) = (det(\sigma_k(x_j)))^2$ et $\sigma_k(y_j) = \sum_{k=1}^{n} b_{ji}\sigma_k(y_i)$

si bien que :$\sigma_k(y_j) = B.(\sigma_k(x_j))$ d'où le résultat

□

Proposition 1.36 *Soit L/K une extension séparable de degré n.*

$y_1, y_2, ..., y_n$ des éléments de L, alors les (y_j) forment une base de L si et seulement si $D_{_{L/K}}(y_1, y_2, ..., y_n) \neq 0$

Preuve : Soit $x \in L$ tel que $L = K(x)$, alors $(1, x, x^2, ..., x^{n-1})$ est une base du $K-$espace vectoriel L .On peut écrire $y_j = \sum_{k=1}^{n} b_{jk}x^{k-1}$avec $b_{jk} \in K$

Et on aura : $D_{L/K}(y_1, y_2, ..., y_n) = (detB)^2 D_{L/K}(1, x, x^2, ..., x^{n-1})$

L/K extension séparable et x élément primitif de L/K. f le polynôme minimal de x sur K alors $D_{L/K}(1, x, x^2, ..., x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(x))$

En particulier $D_{L/K}(1, x, x^2, ..., x^{n-1}) \neq 0$, donc $D_{L/K}(y_1, y_2, ..., y_n) \neq 0$ si et seulement si $detB \neq 0$ soit encore si et seulement si les $y_i$forment une base du $K-$espace vectoriel L.

□

1.2.3 Intégralité :

Définition 1.37 *(entier) Soit L un corps et $A \subset L$ un sous-anneau deL.On dit que $\alpha \in L$ est entier sur A s'il existe $P \in A[X]$ unitaire tel que $P(\alpha) = 0$.*

Exemple 12 *Soit* $\alpha = \frac{\sqrt{3}+\sqrt{7}}{2} \in \mathbb{R}$, *on a :*$\alpha^4 - 5\alpha^2 + 1 = 0$, *donc* α *est entier sur* $\mathbb{Z}$.

Théorème 1.38 *(fondamental) Soit* L *un corps ,*A *un sous-anneau de* L *et* $\alpha \in A$ *. Les conditions suivantes sont équivalentes :*

i)α *est entier sur* A.

ii)L'anneau $A[\alpha]$ *engendré par* A *et* α *est un sous-*A*module de type fini de* L .

iii)Il existe un sous-anneau B *de* L *contenant* α *et* A *qui est un sous -*A*module de type fini de* L.

iv)Il existe un sous-A*module non nul* E *de type fini de* L *tel que* $\alpha E \subset E$.

Preuve : $i) \Longrightarrow ii)$ soit αentier sur A .Il existe $f(x) \in A[X]$ unitaire de degré n tel que $f(\alpha) = 0$.Soit $g(X) \in A[X]$,comme $f(X)$ est unitaire ,on peut effectuer la division

euclidienne par $f(X)$ dans $A[X]$.Ils existent $q(X)$et $r(X)$ avec $deg(r) \leq n-1$ tel que $g(X) = q(X).f(X) + r(X), d'où g(\alpha) = r(\alpha)$ .Ainsi le sous-Amodule $A(\alpha) \subset L$

admet $(1, x, x^2, ..., x^{n-1})$comme système générateur.

$ii) \Longrightarrow iii) \Longrightarrow iv)$ triviales .

$iv) \Longrightarrow i)$supposons qu'il existe un sous-Amodule de type fini non nul E de L tel que $\alpha E \subset E$ engendré par $(e_1, e_2, ..., e_n)$. Les relations $\alpha e_i \in E$ se traduisent

par l'existence d'une matrice $M = (a_{ij})_{1 \leq i,j \leq n}$ à coefficients dans A telle que :$\begin{cases} \overset{\alpha e_1 = a_{11}e_1 + a_{12}e_2 + ... + a_{1n}e_n}{\alpha e_2 = a_{21}e_1 + a_{22}e_2 + ... + a_{2n}e_n} \\ ..... \\ \underset{\alpha e_n = a_{n1}e_1 + a_{n2}e_2 + ... + a_{nn}e_n}{} \end{cases}$

Comme $E \neq 0$,il existe m tel que $e_m \neq 0$ et les formules de Cramer donnent $det(xId_n - M)u_i = 0$. Les u_i n'étant pas tous nuls car $E \neq 0$,on a : $det(x.Id_n - M) = 0$.

En developpant , on aura la relation de dépendance intégrale pour x.

□

Définition 1.39 *(Anneau entier , fini) Soit L un corps et $A \subset B$ deux sous-anneaux de L. On dit que B est entier sur A si tout $y \in B$ est entier sur A.*

On dit que B est fini sur A si c'est un A-module de type fini .

Par le théorème précédent si B est fini sur A , alors il est entier sur A.

Définition 1.40 *(Fermeture et clôture intégrale)*

L'ensemble C des $x \in L$ entiers sur A est la fermeture intégrale de A dans L. Si A est intégre , sa férméture intégrale dans son corps des fractions s'appelle sa clôture intégrale.

Définition 1.41 *(Intégralement clos) :On dit qu'un anneau intégre A est intégralement clos si sa clôture intégrale est A lui même.*

Théorème 1.42 *Soit L un corps et $A \subset L$ un anneau .Soit C la clôture intégrale de A dans L ,alors C est un anneau intégralement clos contenant A .*

Preuve : Soient $x, y \in C$, alors $A[x]$ est fini sur A et$A[x, y] = (A[x])[y]$ est fini sur $A[x]$, donc aussi sur A. Or $x + y$ et xy étant dans $A[x, y]$, ils sont entiers sur A , donc ils appartiennent à C .

Soit $x \in L$ entier dans C , il existe une relation de dépendance intégrale $x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0 = 0$où les $c_i$sont entiers sur A.

Dans la suite d'inclusion :$A \subset A[c_0] \subset A[c_0, c_1] \subset ... \subset A[c_0, c_1, ..., c_{n-1}] \subset A[c_0, c_1, ..., c_{n-1}, x]$.

Chaque anneau est entier sur celui qui le précéde et par application répétée , on aura $A[c_0, c_1, ..., c_{n-1}, x]$est fini sur A, donc $x \in C$.

□

Proposition 1.43 *Soit A un anneau intégralement clos , K son corps des fractions supposé de caractéristique 0 ,L une extension fini de K et B la fermeture intégrale de A dans L ,*

alors :

i)L est le corps des fractions de B.

ii)Il existe un élément primitif de L sur K appartenant à B .

iii)Un élément $z\in$ L est dans B si et seulement si son polynôme caractéristique(respéctivement minimal) est à coéfficients dans A.

Preuve : *i*) soit $y \in L$ de polynôme minimal $f(X) \in K[X]$. En multipliant par un dénominateur commun a des coefficients , la relation $f(y) = 0$

peut s'écrire : $ay^n + a_{n-1}y^{n-1} + ... + a_1y + a_0 = 0$ où les a_i sont dans A .

En posant $b = ay$ et en multipliant par a^{n-1}, on aura : $b^n + a_{n-1}b^{n-1} + ... + a_1a^{n-2}b + a_0a^{n-1} = 0$.

Tout $y \in L$ est de type $y = \frac{b}{a}$, où $a \in A$, $b \in B$ donc L est le corps des fractions de B .

ii) L'extension L/K est séparable car K est de caractéristique 0. Soit y un élément primitif de L sur K , avec les notations précédentes il existe $a \in A$ tel que $b = ay \in B$ et l'élément primitif b est aussi primitif de L sur K .

iii) Puisque L/K est séparable de degré n , il y a exactement n $K-$morphismes de L dans Ω une clôture algébrique de K et L ; notons-les σ_i avec $1 \leq i \leq n$. Si $x \in L$, l'application $K-$linéaire $m_x : L \to L, u \longmapsto ux$ a pour polynôme caractéristique

$p_x(X) = p_{L/K,x}(X) = \prod_{i=1}^{n} (X - \sigma_i(x))$

Soit $x \in L$, si $p_x(X)$ est à coéfficients dans A , alors la relation $p_x(x) = 0$ est une relation de dépendance intégrale de x sur A, donc $x \in B$.

Réciproquement , si $x \in B$, les $\sigma_i(x)$ sont aussi entiers sur A car vérifiant les mêmes relations de dépendance intégrale que x. Les coefficients de $p_x(X)$

sont les fonctions symétriques fondamentales de $\sigma_i(x)$, donc appartiennent à K et sont entiers sur A , donc sont dans A puisque A est intégralement clôs

. Donc pour tout $x \in L$, $p_x(X) \in A[X]$si et seulement si $z \in B$.

L'assertion sur le polynôme minimal résulte de l'application de ce qui précéde au cas où $L = K(x)$.

□

Corollaire 1.44 *Soit A un anneau intégralement clos , K son corps des fractions supposé de caractéristique 0 , L une extension finie de K et B la fermeture intégrale de A dans L . Alors pour tout $\alpha \in B$ et $\alpha_1, \alpha_2, ..., \alpha_n \in B$, on a : $Tr_{L/K}(\alpha)$, $N_{L/K}(\alpha) \in A$ et $D_{L/K}(\alpha_1, \alpha_2, ..., \alpha_n) \in A$.*

Preuve : L'extension L/K est séparable car elle est de caractéristique 0. Les nombres $Tr_{L/K}(\alpha)$,$N_{L/K}(\alpha)$ sont au signe prés des coefficients du polynôme caractéristique de α sur K , que l'on sait être à coefficients dans A , d'où le résultat.

□

Définition 1.45 *SoitK un corps de nombres .Les éléments deK qui sont racines de polynomes unitaires à coefficients dans$\mathbb{Z}$ s'appellent les entiers deK. Ces entiers deK forment l'anneau des entiers deK qu'on note $\mathcal{O}_K$*

Proposition 1.46 *Soit K une extension quadratique de $\mathbb{Q}$. Il existe $d \in \mathbb{Z} \setminus \{0, 1\}$ et d sans facteurs carrés tel que : $K = \mathbb{Q}\left(\sqrt{d}\right)$ (où $\sqrt{d}$ désigne un complexe dont le carré est d) .*

Preuve : Soit u un élément primitif de l'extension $K/\mathbb{Q}$ et $M(X)$=X^2+bX+c son polynôme minimal , avec $b, c \in \mathbb{Q}$.

On a :$M(X) = \left(X + \frac{b}{2}\right)^2 - \frac{b^2-4c}{4}$ donc $\begin{cases} v = 2u + b \\ M(u)=0 \end{cases}$ vérifie $v^2 = b^2 - 4c$

D'où K =$\mathbb{Q}(u) = \mathbb{Q}(v)$. Comme $b^2 - 4c \in \mathbb{Q}$, notons $b^2 - 4c = \frac{r}{s}$ avec $r \in \mathbb{Z}$ et $s \in \mathbb{N}^*$donc $w = sv$ vérifie $w^2 = rs^2$ et $K = \mathbb{Q}(v) = \mathbb{Q}(w)$.

Dans $\mathbb{Z}^*$, rs se décompose ainsi : $rs = m^2 d$ avec d ne possédant pas de facteurs carrés . Donc $K = \mathbb{Q}(w) = \mathbb{Q}\left(\frac{w}{m}\right)$ et comme $d = \left(\frac{w}{m}\right)^2$on aura :

$K = \mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(-\sqrt{d}\right)$et $d \notin \{0,1\}$car $K \neq \mathbb{Q}$.

□

Définition 1.47 . *On dit que* $\mathbb{Q}\left(\sqrt{d}\right)$ *est un corps quadratique réel (resp complexe) si* $d > 0$ *(res* $d < 0$*).*

Théorème 1.48 *-Soit* $d \in \mathbb{Z} \setminus \{0,1\}$ *sans facteurs carrés .Une* $\mathbb{Z}-$*base d'entiers de* $\mathbb{Q}\left(\sqrt{d}\right)$ *est donné par* $\left(1, \sqrt{d}\right)$ *si* $d \equiv 2, 3 mod\,(4)$ *et par* $\left(1, \frac{1+\sqrt{d}}{2}\right)$ *si* $d \equiv 1 mod\,(4)$.

Les discriminants de ces corps sont : $4d$ *si* $d \equiv 2, 3 mod\,(4)$ *et* d *si* $d \equiv 1 mod\,(4)$.

Preuve : Posons $K = \mathbb{Q}\left(\sqrt{d}\right)$. Les deux isomorphismes de K sont : l'identité et $\sigma : a + b\sqrt{d} \longmapsto a - b\sqrt{d}$ (qui est un automorphisme puisque $K/\mathbb{Q}$est normale).Soit $x = a + b\sqrt{d} \in \mathcal{O}_K$, avec $a, b \in \mathbb{Q}$.On a donc , d'aprés le corollaire 47 :

$Tr_{K/\mathbb{Q}}(x) = x + \sigma(x) = 2a \in \mathbb{Z}$ et $N_{K/\mathbb{Q}}(x) = x\sigma(x) = a^2 - db^2 \in \mathbb{Z}$.

Réciproquement : Si $Tr_{K/\mathbb{Q}}(x), N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$, alors la relation de dépendance intégralepour $x$est : $x^2 + Tr_{K/\mathbb{Q}}(x)\, x + N_{K/\mathbb{Q}}(x)$=0.

Distinguons deux possibilités :

i)On suppose $a \in \mathbb{Z}$,donc $db^2 \in \mathbb{Z}$.Posons $b = \frac{u}{v}$avec u et v entiers premiers entre eux ,on aura : $db^2 = d\frac{u^2}{v^2}$ d'où $v^2 \mid d$ et $v = \pm 1$puisque d est sans facteurs carrés .Donc $b \in \mathbb{Z}$.Comme la réciproque est évidente , le cas i)donne les éléments de $\mathbb{Z}\left[\sqrt{d}\right]$.

ii) On suppose $a \notin \mathbb{Z}$, on a donc $a = \frac{\alpha}{2}$ avec α entier impair .Mais $a^2 - db^2 = \frac{\alpha^2 - 4db^2}{4}$ d'où $\alpha^2 - 4db^2 \in 4\mathbb{Z}$.

On a donc $4db^2 = d(2b)^2 \in \mathbb{Z}$ et comme ci-dessus , on en déduit que : $2b \in \mathbb{Z}$ d'où $b = \frac{\beta}{2}$ avec $\beta \in \mathbb{Z}$.

Pour la réciproque distinguons deux cas selon les valeurs de d $modulo 4$.

iia)$Sid \equiv 2$, $3 mod(4)$ alors $\alpha^2 - 4db^2 = \alpha^2 - d\beta^2 \in 4\mathbb{Z}$, comme $\alpha^2 \equiv 1 mod\,(4)$et $\beta^2 \equiv 0 mod\,(4)$on aura $\alpha^2 - db^2 \equiv 1$, 2 ou 3 $mod\,(4)$

ce qui est absurde , donc dans ce cas , il n'est pas possible que $a \notin \mathbb{Z}$et i)donne tous les entiers possibles .

iib)Si $d \equiv 1 mod\,(4)$alors $\alpha^2 - d\beta^2 \equiv 1 - \beta^2 mod\,(4)$ d"où β *impair* et $x = \left(\alpha + \beta\sqrt{d}\right)/2$ avec α , β impairs .

Réciproquement , un tel $x$est entier car il est racine du polnôme $X^2 - \alpha X + \frac{\alpha^2 - d\beta^2}{4} \in \mathbb{Z}[X]$.

On peut écrire dans ce cas : $x = \frac{\alpha-\beta}{2} + \beta\frac{1+\sqrt{d}}{2} = \gamma + \beta\frac{1+\sqrt{d}}{2}$ avec $\gamma, \beta \in \mathbb{Z}$.

Comme $\frac{1+\sqrt{d}}{2}$est entier (prendre le polynôme ci-dessus avec $\alpha = \beta = 1$), le résul tat est démontré .Il reste à calculer les discriminants .

Si $d \equiv 2, 3 (resp 1) mod\,(4)$ alors $D = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$, respectivement $D = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & -\frac{1+\sqrt{d}}{2} \end{vmatrix}^2 = d.$

□

Remarque 2 *Si $d \equiv 1 mod\,(4)$ alors $\mathcal{O}_K = \{\frac{\alpha+\beta\sqrt{d}}{2}$, αet β de même parité$\}$ .En particulier $\mathcal{O}_K \subset \{\alpha + \beta\sqrt{d}$ avec $\alpha, \beta \in \mathbb{Z}\}$*

L'anneau des entiers de $\mathbb{Q}\left(\sqrt{-3}\right)$ est $\mathbb{Z}[w]$ avec $w = e^{\frac{i\pi}{3}}$ et non $\mathbb{Z}\left[\sqrt{-3}\right]$ puisque -3$\equiv 1\ mod\,(4)$.

Remarque 3 *Si $d > 0$, l'anneau $\mathcal{O}_K$est dense dans $\mathbb{R}$ car ce n'est pas un sous-groupe additif monogène .*

Si $d < 0$, l'anneau $\mathcal{O}_K$ est un réseau du plan complexe .

Si $d < 0$ et $d \equiv 2, 3 mod\,(4)$, une base de ce réseau est $\left(1, \sqrt{d}\right)$.Ces deux vecteurs sont orthogonaux , car $\sqrt{d}$ est immaginaire pur et les mailles de ce réseau sont des rectangles .

Si $d < 0$ et $d \equiv 1 mod\,(4)$, alors une base de ce réseau $(1, \alpha)$où $\alpha = \frac{1+\sqrt{d}}{2}$. Mais $\alpha + \overline{\alpha} = 1$, donc $(\alpha, \overline{\alpha})$ est aussi une base de ce réseau dont les mailles sont donc des losanges .

Détérminons le groupe des unités de l'anneau des entiers d'un corps quadratique immaginaire .

Proposition 1.49 *Soit $d<0$ un entier sans facteurs carrés et $K=\mathbb{Q}\left(\sqrt{d}\right)$. Alors $\mathcal{O}_K^{\times}=\{-1,+1\}$sauf dans les deux cas suivants :*

i) $d=-1$ donc $\mathcal{O}_K=\mathbb{Z}\left[\sqrt{-1}\right]$et alors $\mathcal{O}_K^{\times}=\{-1,+1,i,-i\}$.

ii) d=-3 , donc $\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ et alors $\mathcal{O}_K^{\times}=\{w^k,0\leq k\leq 5\}$ où $w=e^{\frac{i\pi}{3}}$

.

Preuve : *i)* $d\equiv 2,3 mod\,(4)$, dans ce cas $\mathcal{O}_K=\mathbb{Z}\left[\sqrt{d}\right]$

i) $d\equiv 2,3 mod\,(4)$. Dans ce cas $\mathcal{O}_K=\mathbb{Z}\left[\sqrt{d}\right]$.

Soit $\varepsilon=\alpha+\beta\sqrt{d}\in\mathcal{O}_K$, alors $N_{K/\mathbb{Q}}(\varepsilon)=\alpha^2-b\beta^2$. On a :

$\varepsilon\in\mathcal{O}_K^{\times}\Leftrightarrow\alpha^2-d\beta^2=1\Leftrightarrow\begin{cases}\alpha^2=1\\-d\beta^2=0\end{cases}\quad ou\begin{cases}\alpha^2=0\\-d\beta^2=1\end{cases}$

Le premier système conduit à $(\alpha=\pm1,\beta=0)$ et le second à $(\alpha=0,d=-1,\beta=\pm1)$d'où les unités sont ±1, $\pm\sqrt{-1}$de $\mathbb{Z}\left[\sqrt{-1}\right]$.

ii)$d\equiv 1 mod\,(4)$, dans ce cas $\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Soit $\varepsilon=\frac{\alpha+\beta\sqrt{d}}{2}\in\mathcal{O}_K$ avec α,β de même parité , alors $N_{K/\mathbb{Q}}(\varepsilon)=\frac{\alpha^2-d\beta^2}{4}$ .Supposons α,βpairs, on aura :

$\varepsilon\in\mathcal{O}_K^{\times}\Longleftrightarrow\alpha^2-d\beta^2=4\Longleftrightarrow\begin{cases}\alpha^2=4\\-d\beta^2=0\end{cases}\quad ou\begin{cases}\alpha^2=0\\-d\beta^2=4\end{cases}$.

Le premier système conduit à $(\alpha=\pm2,\beta=0)$, le second n'a pas de solution . Donc dans ce cas ,on récupère les unités ±1.Supposons α,β impaires , on aura : $\varepsilon\in\mathcal{O}_K^{\times}\Longleftrightarrow\alpha^2-d\beta^2=4\Longleftrightarrow\begin{cases}\alpha^2=1\\d\beta^2=-3\end{cases}\quad ou\begin{cases}\alpha^2=3\\d\beta^2=-1\end{cases}$.

Le premier système conduit à ($\alpha=\pm1$, $d=-3$, et $\beta=\pm1$) , d'où les unités de $\mathbb{Z}[w]$sont :$\frac{1+\sqrt{-3}}{2}=w$, $\frac{1-\sqrt{-3}}{2}=w^5$,$\frac{-1+\sqrt{-3}}{2}=w^2$ et $\frac{-1-\sqrt{-3}}{2}=w^4$. Le second système n'a pas de solution car $d\equiv 1 mod\,(4)$.

□

1.3 les Idéaux dans un corps de nombres

1.3.1 Structure d'idéaux dans un corps de nombre

Définition 1.50 *(corps de nombres) .On appelle corps de nombres K une extension finie (donc algébrique)de $\mathbb{Q}$. Le degré de K est $[K:\mathbb{Q}]$. On notera $\mathcal{O}_K$ la fermeture intégrale de $\mathbb{Z}$ dans K . Si $\alpha \in K$ est entier sur $\mathbb{Z}$, on parlera plus simplement d'entier s'il n'y a pas de risque de confusion avec les éléments de $\mathbb{Z}$, qu'on appelera entier rationnel .*

Lemme 1.51 *Soit L/K une extension de corps de nombres alors $\mathcal{O}_L \cap K = \mathcal{O}_K$.*

Preuve : $x \in \mathcal{O}_L \cap K$ si et seulement si $x \in K$ et x vérifie la relation de dépendance intégrale sur $\mathbb{Z}$, si et seulement si $x \in K \cap \mathcal{O}_K$.

Or $K \cap \mathcal{O}_K = \mathcal{O}_K$ car $\mathcal{O}_K$est intégralement clos .

□

Proposition 1.52 *Soit $\alpha \in K$. Il existe un $a \in \mathbb{Z}$ tel que $a\alpha \in \mathcal{O}_K$. D'aprés le corollaire 48 appliqué à $A = \mathbb{Z}$, l'anneau $\mathcal{O}_K$ est un $\mathbb{Z}-$module libre de rang n .*

Définition 1.53 *(Base intégrale) : Une $\mathbb{Z}-$base de $\mathcal{O}_K$ en tant que $\mathbb{Z}$-module s'appelle une base intégrale de K .*

En fait tout idéal non nul de $\mathcal{O}_K$ est un $\mathbb{Z}-$module libre de rang n .

Définition 1.54 *(Discriminant d'un idéal) : L'entier ainsi défini qui ne dépend pas de la base de $\mathfrak{b}$ choisie pour le calculer s' appelle le discriminant de $\mathfrak{b}$ et se note $D_{\mathfrak{b}}$. En particulier ,si $\mathfrak{b} = \mathcal{O}_K$, on l'appelle le discriminant de K , et on le notera D_K.*

Proposition 1.55 *soit $(x_1, x_2, ..., x_n)$ des entiers de K formant une base de K . Si le discriminant $D_{K/\mathbb{Q}}(x_1, x_2, ..., x_n)$ est sans facteurs carrés , alors $(x_1, x_2, ..., x_n)$ est une base intégrale de $\mathcal{O}_K$.*

Preuve : Si $(\beta_1, \beta_2, ..., \beta_n)$ *est* une base intégrale de $\mathcal{O}_K$, en écrivant $x_i = \sum_{j=1}^{n} a_{ij}\beta_j$ le lemme 38 montre que :

$D_{K/\mathbb{Q}}(x_1, x_2, ..., x_n) = (det(a_{ij})^2)\, D_{K/\mathbb{Q}}(\beta_1, \beta_2, ..., \beta_n)$ Comme $D_{K/\mathbb{Q}}(x_1, x_2, ..., x_n)$ est sans facteurs carrés alors

$det(a_{ij}) = \pm 1$ et $(x_1, x_2, ..., x_n)$ est une base intégrale de $\mathcal{O}_K$.

□

Exemple 13 *Soit $K = \mathbb{Q}(\alpha)$ où α est une racine du polynôme $x^3 + 2x^2 + 1$ alors $D_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = 59$ or 59 est premier (à fortiori sans facteurs carrés) , donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

Définition 1.56 *Soit K un corps de nombres . Pour $x \in K$, la norme $N_{K/\mathbb{Q}}(x)$ est le déterminant de l'application $\mathbb{Q}-$linéaire $m_x : K \longrightarrow K$,$x \longmapsto ux$ si $x \in \mathcal{O}_K$, alors $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.*

-Soit $\mathfrak{b}$ un idéal non nul de $\mathcal{O}_K$. Le nombre $[\mathcal{O}_K : \mathfrak{b}]$ s'appelle la norme de $\mathfrak{b}$ et se note $N_K(\mathfrak{b})$.

Proposition 1.57 *Soit $\alpha \in \mathcal{O}_K$ non nul et $\mathfrak{b}$=(α). Alors $N_K(\mathfrak{b}) = |N_{K/\mathbb{Q}}(\alpha)|$.*

Preuve : Soit $(\theta_1, \theta_2, ..., \theta_n)$ *une* base intégrale de $\mathcal{O}_K$ adaptée à $\mathfrak{b}$. Il existe donc $q_1, q_{2,...,q_n}$ dans $\mathbb{Z}/\{0\}$ tels que $(q_1\theta_1, q_2\theta_2, ..., q_n\theta_n)$ est une $\mathbb{Z} - base$ de $\mathfrak{b}$, donc : $\mathcal{O}_{K/\natural} = \overset{n}{\underset{i=1}{\oplus}} \mathbb{Z}\theta_i / \overset{n}{\underset{i=1}{\oplus}} \mathbb{Z}q_i\theta_i \simeq \prod_{i=1}^{n} \mathbb{Z}\theta_i/\mathbb{Z}q_i\theta_i \backsimeq \prod_{i=1}^{n} \mathbb{Z}/q_i\mathbb{Z}$.

D'où $N_K(\mathfrak{b}) = [\mathcal{O}_K : \mathfrak{b}] = |q_1...q_n|$. D'autre part en notant $D_K$le discriminant de K,

$D_{K/\mathbb{Q}}(q_1\theta_1, ..., q_n\theta_n) = \det(\sigma_i(q_j\theta_j))^2 = \prod_{j=1}^{n} q_j^2 D_K$.

D'où $D_{K/\mathbb{Q}}(q_1\theta_1, ..., q_n\theta_n) = (N_K(\mathfrak{b}))^2 D_K$ 1.1
Mais $(\alpha\theta_1, ..., \alpha\theta_n)$ *est* une autre $\mathbb{Z}-$base de $\mathfrak{b}$.
donc $D_{K/\mathbb{Q}}(q_1\theta_1, ..., q_n\theta_n) = D_{K/\mathbb{Q}}(\alpha\theta_1, ..., \alpha\theta_n)$ et comme $D_{K/\mathbb{Q}}(\alpha\theta_1, ..., \alpha\theta_n)$=$\det(\sigma_i(\alpha\theta_j))^2$=$\det(\sigma_i(\alpha)\sigma_i(\theta_j$
D'où $N_K(\mathfrak{b})$=$|N_{K/\mathbb{Q}}(\alpha)|$ en comparant avec 1.1 puisque $D_K \neq 0$.

□

Corollaire 1.58 *Soit $\mathfrak{b}$ un idéal non nul de $\mathcal{O}_K$. Alors $D_\mathfrak{b} = (N_K(\mathfrak{b}))^2 D_K$.*

Preuve : Le résultat découle de l'équation 1.1, puisque l'entier $D_\mathfrak{b}$ne dépend pas de la base choisie pour le calculer .

□

Proposition 1.59 *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathcal{O}_K$. Alors $N_K(\mathfrak{ab})$= $N_K(\mathfrak{a}) N_K(\mathfrak{b})$.*

Preuve : [cf. P. Sa]

□

1.4 Anneaux de Dedekind

1.4.1 DEFINITIONS

Définition 1.60 *On dit qu'un anneau A est Noetherien si tout idéal de A est de type fini.*

Nous allons dans ce qui suit caractériser les anneaux Noethériens.

Lemme 1.61 *Soit A un anneau, alors les propositions suivantes sont équivalentes*

1. Tout idéal de A est de type fini

(a) Toute suite croissante d'idéaux de A est stationnaire

(b) Toute famille non vide d'idéaux de A admet un élément maximal

Preuve : Montrons que (1) $\Longrightarrow$ (2)
Soit $(I_n)_{n\geq 0}$ une suite croissante d'idéaux de A, $I_0 \subseteq I_1 \subseteq ....$, alors, $I = \bigcup_{n\geq 0} I_n$ est un idéal de A, donc de type fini. Ainsi, il existe n_0 tel que I_{n_0} contient tous les générateurs qui sont en nombre fini. Par conséquent $I = I_{n_0}$ ce qui montre que pour $n \geq n_0$ on a $I_n = I_{n_0}$.
Montrons que (2) $\Longrightarrow$ (3)
Par l'absurde, supposons qu'un tel élément maximal n'existe pas, alors il existe une suite strictement croissante infinie d'idéaux de A ce qui contredit l'hypothèse (2).
Montrons que (3) $\Longrightarrow$ (1)
Pour tout idéal I de A, considérons l'ensemble S_I des idéaux de A contenu dans I. S_I est non vide car $(0) \subseteq I$, par suite S_I admet un élément maximal qu'on note I_1.
Si $I = I_1$ c'est fini, sinon on considère l'idéal $I_2 = (x_1, I_1)$ avec $x_1 \in I - I_1$, alors $I_2 \in S_I$ et $I_1 \subset I_2$ ce qui contredit la maximalité de I_1.

□

Corollaire 1.62 *L'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres est un anneau Noetherien.*

Preuve : Soit $I = I_0 \subseteq I_1 \subseteq ...$ une suite croissante d'idéaux de $\mathcal{O}_K$, on suppose que $I_0 \neq 0$. Comme $\mathcal{O}_K I$ est fini, alors il exist seulement un nombre fini d'idéaux de $\mathcal{O}_K$ contenant I, en particulier la suite croissante $I = I_0 \subseteq I_1 \subseteq ...$ sera stationnaire, ce qui par le lemme précédent entraine la Noetherianité de A.

□

Définition 1.63 *On appelle dimension (de KRULL) d'un anneau A, le plus grand entier $n \geq 0$ telle qu'il existe une suite croissante $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ d'idéaux premiers $\mathfrak{p}_i$ de A et on note cette dimension* $\dim(A) = n$

Lemme 1.64 *Soit A un anneau intègre, alors*

- $\dim(A) = 0$ si, et seulement si A est un corps

  - $\dim(A) \leq 1$ si, et seulement si tout idéal premier non nul de A est maximal.

Preuve :

□

- $\dim A = 0$ équivaut à dire que tout idéal premier $\mathfrak{p}$ est maximal, ce qui est équivalent à $A\mathfrak{p}$ est un corps.

  - Notons que $\dim A \leq 1 \iff \dim A = 0$ ou $\dim A = 1$.
    Si $\dim A = 1$, alors pour tout idéal premier $\mathfrak{p}$ la longueur de la chaine d'idéaux premiers $(0) \subset \mathfrak{p}$ est maximale, donc $\mathfrak{p}$ est maximal. La réciproque est évidente.
    En combinant avec la première proposition on obtient le résultat voulu

Proposition 1.65 *Soit I un idéal non nul d'un anneau $\mathcal{O}_K$ des entiers de corps de nombres, alors l'anneau quotient $\mathcal{O}_K I$ est fini*

Comme corollaire à la proposition précédente on obtient :

Corollaire 1.66 *Si K est un corps de nombres, alors son anneau d'entiers $\mathcal{O}_K$ est de dimension 1*

Preuve : Comme $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, alors $\mathcal{O}_K$ n'est pas un corps. Ainsi, par le lemme précédent, $\dim \mathcal{O}_K = 1 \iff$ tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est maximal. Etant donné que $\mathcal{O}_K$ est intègre, alors $\mathcal{O}_K\mathfrak{p}$ est fini et est donc un corps, ce qui montre que $\mathfrak{p}$ est maximal.

□

Définition 1.67 *Un anneau A est dit de Dedekind s'il est intègre, Noetherien, intégralement clos et de dimension 1.*

De cette définition résulte

Théorème 1.68 *Si K est un corps de nombres, alors son anneau d'entiers $\mathcal{O}_K$ est de Dedekind.*

Soient I et J deux idéaux d'un anneau A , on définit le produit IJ comme étant le plus petit idéal contenant tous les produits xy avec $x \in I$ et $y \in J$.
Si $I = (a_i)_{-1 \leq i \leq m}$ et $J = (b_j)_{1 \leq j \leq n}$, alors

$$IJ = \{a_i b_j / \, 1 \leq i \leq m \, ; \, 1 \leq j \leq n\}$$

Définition 1.69 *On dit qu'un anneau A est factoriel si tout idéal propre de A se décompose de manière unique en produit d'idéaux premiers.*

Exemple 14 *Nous allons illustrer par des exemples la notion de factorialité.*

1. Considérons l'anneau $\mathbb{Z}\left[\sqrt{-5}\right]$ et examinons la factorisation de l'entier 6 dans cet anneau :

   $$6 = 2 \times 3 = \left(1 - \sqrt{-5}\right)\left(1 + \sqrt{-5}\right)$$

   On vérifie que chacun des nombres 2, 3, $1 - \sqrt{-5}$ et $1 + \sqrt{-5}$ est irréductible, ceci en utilisant la norme définie sur cet anneau.s
   En effet, examinons la situation pour le nombre 2. Si $x = a + b\sqrt{-5}$ divise

2 dans $\mathbb{Z}\left[\sqrt{-5}\right]$, alors $\mathrm{N}(x)$ divise $\mathrm{N}(2)$ =4 . Ainsi, les valeurs possibles de $\mathrm{N}(x)$ sont 1, 2 et 4.
En premier lieu, $\mathrm{N}(x) = a^2 + 5b^2 = 2$ n'a pas de soluton dans $\mathbb{Z}$, et donc 2 n'a pas de diviseur propre
D'autre part, $\mathrm{N}(x) = 1$ ou 4 entraine que x est soit une unité, soit il est associé avec 2.
Par conséquent, il n'y a pas d'unicité de la décomposition en facteurs irréductibles. Par contre, et Kummer y a pensé, il y unicité de la décomposition en facteurs d'idéaux premiers Pour cela, considérons les idéaux suivants :

$$\mathfrak{p}_1 = \left(2, 1+\sqrt{-5}\right), \quad \mathfrak{p}_2 = \left(3, 1-\sqrt{-5}\right) \text{ et } \mathfrak{p}_3 = \left(3, 1+\sqrt{-5}\right)$$

Comme 2 et $1+\sqrt{-5} \in \mathfrak{p}_1$, alors $1-\sqrt{-5} \in \mathfrak{p}_1$ et on peut écrire $\mathfrak{p}_1 = \left(2, 1-\sqrt{-5}\right)$ et on aura

$$\mathfrak{p}_1^2 = \left(4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6\right)$$

D'autre part, $(2) = \left(2, 1-\sqrt{-5}\right)\left(2, 1+\sqrt{-5}\right)$ et $2 = 4-6 \in \mathfrak{p}_1^2$, alors $(2) = \mathfrak{p}_1^2$.
Par le même procédé on trouve $(3) = \mathfrak{p}_2\mathfrak{p}_3$, ce qui entraine $6 = \mathfrak{p}_1\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

(a) Considérons la factorisation en facteurs irréductibles de 4 dans l'anneau $\mathbb{Z}\left[\sqrt{-3}\right]$:

$$4 = 2 \times 2 = \left(1-\sqrt{-3}\right)\left(1+\sqrt{-3}\right)$$

où on montre, par le même procédé ci-dessus, que 2, $1-\sqrt{-3}$ et $1+\sqrt{-3}$ sont irréductibles dans $\mathbb{Z}\left[\sqrt{-3}\right]$.
Pour exprimer cette factorisation en terme d'idéaux premiers, po-

sons $\mathfrak{q} = \left(2, 1+\sqrt{-3}\right)$, alors on aura

$$\mathfrak{q}^2 = \left(4, 2+2\sqrt{-3}, -2+2\sqrt{-3}\right) = \left(4, 2+2\sqrt{-3}\right) = 2\mathfrak{q}$$

puisque $-2+2\sqrt{-3} = 4-\left(2+2\sqrt{-3}\right)$ et, contrairement à l'exemple précédent, $1+\sqrt{-3} \notin (2)$ qui donne$\mathfrak{q} \neq (2)$. Ainsi, on a exhibé un défaut de factorisation unique en produit d'idéaux premiers dans $\mathbb{Z}\left[\sqrt{-3}\right]$. Remarquons que dans l'anneau $\mathbb{Z}\left[\dfrac{-1+\sqrt{-3}}{2}\right]$ on a $1+\sqrt{-3} \in (2)$ et donc $(2) = \left(2, 1+\sqrt{-3}\right)$, ce qui corrige le défaut précédent puisque cet anneau, et on le verra juste après, est l'anneau des entiers d'un corps de nombres

Théorème 1.70 *Tout anneauA de Dedekind est factoriel.*

Preuve : [Cf. S. La]

□

Pour démontrer ce théorème nous aurons besoin de quelques résultats intermédiaires.

Lemme 1.71 *Soient $I_1, \ldots, I_n$ des idéaux d'un anneau A et $\mathfrak{p}$ un idéal premier de cet anneau. Si $I_1 I_2 \ldots I_n \subseteq \mathfrak{p}$, alors il existe j, $1 \leq j \leq n$, tel que $I_j \subseteq \mathfrak{p}$.*

Preuve : Supposons que $\forall j$, $1 \leq j \leq n$, $I_j \not\subseteq \mathfrak{p}$, alors $\exists \alpha_j \in I_j$ tels que $\alpha_j \notin \mathfrak{p}_j$. D'autre part, $\alpha_1 ... \alpha_n \in I_1 \ldots I_n \subseteq \mathfrak{p}$, et comme $\mathfrak{p}$ est premier, entraine l'existence d'un $\alpha_i \in \mathfrak{p}$, $1 \leq i \leq n$, ce qui est absurde.

□

Lemme 1.72 *Soit A un anneau Noetherien, alors pour tout idéal non nul I il existe des idéaux premiers non nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ de A tels que $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I$.*

Preuve : Soit S l'ensemble des idéaux de I qui ne vérifient pas la propriété précédente.

Si $S \neq \emptyset$ et A est Noetherien, alors S admet un élément maximal J et, par définition de S, J n'est pas premier, ce qui montre que $\exists x, y \in A$ tels que $xy \in J$ avec $x, y \notin J$. Considérons les idéaux de A suivants

$$\mathfrak{a} = (a, J) \text{ et } \mathfrak{b} = (b, J)$$

où on a $J \subset \mathfrak{a}$ et $J \subset \mathfrak{b}$. Par maximalité de J on aura

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{a}, \quad \mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{b}$$

où $\mathfrak{p}_i$ et $\mathfrak{q}_j$ sont des idéaux premiers non nuls de A.
Comme $\mathfrak{ab} \subseteq J$, alors $\mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{q}_1 \dots \mathfrak{q}_s \subset J$ ce qui est contradictoire, et par conséquent $S = \emptyset$

□

Soit A un anneau d'entier de corps de fractions K, et soit I un idéal non nul de cet anneau.
On définit la partie de K notée I^{-1} donnée par

$$I^{-1} = \{x \in K / \, xI \subset A\}.$$

I^{-1} est un sous-A-module de K et on a $A \subseteq I^{-1}$, et si $I = (x)$ est principal alors $I^{-1} = Ra^{-1}$.

Proposition 1.73 *Soit A un anneau de Dedekind et I un idéal non nul de A. Pour tout idéal premier non nul $\mathfrak{p}$ on a $\mathfrak{p}^{-1}I \neq I$.*

Preuve : [Cf. P. Sa, p58]

□

Corollaire 1.74 *Soit A un anneau de Dedekind et $\mathfrak{p}$ un idéal premier non nul de A, alors $\mathfrak{p}^{-1}\mathfrak{p} = A$*

Preuve : Par définition on a $x\mathfrak{p} \in A$, $\forall x \in \mathfrak{p}^{-1}$ et comme $A \subseteq \mathfrak{p}^{-1}$, alors $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq A$.
Sachant que A est de diemnsion 1, alors $\mathfrak{p}^{-1}\mathfrak{p} = A$.

□

Théorème 1.75 *Tout anneau de Dedekind est factoriel*

Preuve : Soit A un anneau de Dedekind, nous savons que tout idéal de A se factorise de façon unique en produit d'idéaux premiers.
Commençons par montrer l'unicité d'une telle décomposition si elle existe. Considérons les deux décompositions suivantes

$$I = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$$

Alors $\mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s \subseteq \mathfrak{q}_1$, et comme $\mathfrak{q}_1$ est premier i exite i, $1 \leq i \leq r$, te ue $\mathfrak{p}_i \subseteq \mathfrak{q}_1$. En changeant de numérotation, on suppose que $\mathfrak{p}_1 \subset \mathfrak{q}_1$, avec $\mathfrak{p}_1$ maximal, puisque A est de dimension 1, alors $\mathfrak{p}_1 = \mathfrak{q}_1$. En multipiant les deux membre de l'égalité précédente par $\mathfrak{q}_1^{-1}$ on aboutit à l'équation suivante

$$\mathfrak{p}_2...\mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$$

puis on réitère le raisonnement précédent et de proche en proche on montre que $\mathfrak{p}_i = \mathfrak{q}_i$ et $r = s$.
Pour montrer l'unicité d'une telle décompoition, on considère l'ensemble S des idéaux de A qui ne se décomposent pas de la façon ci-dessus. Comme A est Noetherien, alors S contient un élément maximal J qui sera contenu dans un idéal maximal $\mathfrak{p}$. Comme $A \subseteq \mathfrak{p}^{-1}$, on aura

$$J \subseteq J\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A.$$

Par la propoition 75 on a $J\mathfrak{p}^{-1} \neq \mathfrak{p}$ et du fait de la maximalité de J on tire que $J\mathfrak{p}^{-1} = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_r$, ce ui entraine que $J = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_r\mathfrak{p}$ ce qui montre que S

est vide.

□

Théorème 1.76 *Soient A un anneau de Dedekind, K son corps des fractions , L une extension de degré fini de K et A' la fermeture intégrale de A dans L .*

On suppose K de caractéristique 0. Alors A' est un anneau de Dedekind et un A-module de type fini.

Preuve : En effet A' est intégralement clos par construction , noethérien et A-module de type fini.Reste à montrer que tout idéal premier $\mathfrak{p}' \neq (\mathfrak{o})$ de A' est maximal . Or prenons un élément $x \neq 0$ de $\mathfrak{p}'$ et

une équation de dépendance intégrale de x sur A, de degré minimum :

1) $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$ ...$(a_i \in A)$

On a $a_0 \neq 0$, sinon on simplifierait par x , et on obtiendrait une équation de dépendance intégrale de degré $n-1$ .Par (1)on a , $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$; On a donc $\mathfrak{p}' \cap A \neq (0)$ .Or $\mathfrak{p}' \cap A$ est un idéal

premier de A. Alors $\mathfrak{p}' \cap A$ est un idéal maximal de A, car A est un anneau de Dedekind, et donc $A/\mathfrak{p}' \cap A$ est un corps. Mais $A/\mathfrak{p}' \cap A$ s'identifie à un sous-anneau de $A'/\mathfrak{p}'$, $A'/\mathfrak{p}'$ est entier sur $A'/\mathfrak{p}' \cap A$ car A' est entier sur A. Comme $A/\mathfrak{p}' \cap A$ est un corps et $A'/\mathfrak{p}'$ est un corps si, et seulement si, $A/\mathfrak{p}' \cap A$ est un corps, alors$\mathfrak{p}'$ est maximal.

□

Exemple 15 *Considérons l'anneau des entiers $A = \mathbb{Z}\left[\sqrt{-5}\right]$ de $\mathbb{Q}\left[\sqrt{-5}\right]$, on a*

2) $\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = 2.3$

Les normes des quatres facteurs sont respectivement 6,6,4 et 9 ; or $1+\sqrt{-5}$ ne peut avoir de diviseur non trivial dans A , car la norme d'un tel diviseur devrait être un diviseur non trivial de 6, et que les équations

$a^2 + 5b^2 = 2$ *et* $a^2 + 5b^2 = 3$

n'ont pas de solutions dans $\mathbb{Z}$*.Si* A *était principal , l'élément* $1 + \sqrt{-5}$*, qui divise le produit 2.3 par* (1)*, devrait diviser l'un de ses facteurs ;Mais , en prenant les normes 6 diviserait 4 ou 9, ce qui n'est pas.*

Théorème 1.77 *Soient* A *un anneau de Dedekind , P l'ensemble des idéaux premiers non nuls de* A*.*

a)Tout idéal fractionnaire non nul $\mathfrak{b}$ *de* A *s'écrit , d'une façon et d'une seule , sous la forme*

4. $\mathfrak{b} = \prod_{\mathfrak{p} \in p} \mathfrak{p}^{np(\mathfrak{b})}$

où les $n_{\mathfrak{p}}(\mathfrak{b})$ *sont les entiers relatifs , presque tous nuls .*

b) Le monoide des idéaux fractionnaires non nuls de A *est un groupe .*

Preuve : [Cf. P. Sa. théorème 3 p61]

□

1.4.2 Décomposition d'un idéal premier dans une extension

On désigne par A un anneau de Dedekind de caractéristique 0, par K son corps des fractions, par L une extension de degré fini n de K, et par B la

fermeture intégrale de A dans L. On rappelle que B est un anneau de Dedekind .

Soit $\mathfrak{p}$un idéal premier non nul de A. Alors $B\mathfrak{p}$ est un idéal de B dont on a une décomposition

1. $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_{\mathfrak{i}}^{\mathfrak{e}_{\mathfrak{i}}}$

où les $\mathfrak{P}_{\mathfrak{i}}$ sont des idéaux premiers de B, deux à deux distincts, et où les e_i sont des entiers ≥ 1 .

Proposition 1.78 *Les* $\mathfrak{P}_{\mathfrak{i}}$*sont exactement les idéaux premiers* $\mathfrak{D}$ *de* B *tels que* $\mathfrak{D} \cap A = \mathfrak{p}$*.*

Preuve : En effet, pour un idéal premier $\mathfrak{D}$ de $\mathbf{B}$, la relation $\mathfrak{D} \cap A = \mathfrak{p}$ équivaut à $\mathfrak{D} \supset \mathfrak{p}B$ ($\Rightarrow$ *évident* ; $\Leftarrow$car $\mathfrak{D} \cap A$ est un idéal premier de A et que $\mathfrak{p}$est maximal).

Ainsi $A/\mathfrak{p}$ s'identifie à un sous-anneau de $B/\mathfrak{P}_i$. Ces deux anneaux sont des corps . Comme B est un A-module de type fini , $B/\mathfrak{P}_i$ est un espace vectoriel de dimension finie sur $A/\mathfrak{p}$; nous noterons f_i

cette dimension, et l'appellerons le degré résiduel de $\mathfrak{P}_i$sur A. L'exposant e_i dans (1) s'appelle l'indice de ramification de $\mathfrak{P}_i$sur A. Notons enfin qu'on a

$B\mathfrak{p} \cap A = \mathfrak{p}$ ($\supset$évidente ; $\subset$résulte de $\mathfrak{P}_i \cap A = \mathfrak{p}$), de sorte que $B/B\mathfrak{p}$ est un espace vectoriel sur $A/\mathfrak{p}$ de dimension finie comme ci-dessus.

□

Théorème 1.79 *Avec les notations précédentes on a*

$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n$

Preuve : La premiere égalité est facile. Considérons la suite d'idéaux

$B \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset ... \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supset ... \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \supset ... \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}...\mathfrak{P}_q^{e_q} = B\mathfrak{p}$.

Deux termes consécutifs sont de la forme $\mathfrak{B}$ et $\mathfrak{B}\mathfrak{P}_i$; or, comme il n'y a pas d'idéaux strictement compris entre $\mathfrak{B}$ et $\mathfrak{B}\mathfrak{P}_i$, $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ est un espace vectoriel de dimension 1 sur $B/\mathfrak{P}_i$; c'est donc un

espace vectoriel de dimension f_i sur $A/\mathfrak{p}$.

Or, dans la suite ci-dessus il ya e_i quotients de termes consécutifs de la forme $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ avec i donné . Au total la dimension $[B/B\mathfrak{p} : A/\mathfrak{p}]$ est égale à la somme des dimmensions de ces quotients, donc à $\sum_{i=1}^{q} e_i f_i$

La seconde égalité est facile dans le cas où B est un A-module libre , en particulier lorsque A est principal : en effet une base $(x_1, x_2, ..., x_n)$ du A-module B donne, par réduction mod.

$B\mathfrak{p}$, une base de $B/B\mathfrak{p}$ sur $A/\mathfrak{p}$. Nous allons nous ramener à ce cas en considérant la partie multiplicativement stable $S = A - \mathfrak{p}$ de A et les anneaux de fractions $A' = S^{-1}A$ et $B' = S^{-1}B$.

On sait que A' est un anneau principal dont $\mathfrak{p}A'$ est le seul idéal maximal , et que B' est la fermeture intégrale de A' dans L . Par le cas principal , on a donc $[B'/\mathfrak{p}\mathfrak{B}' : A'/\mathfrak{p}A'] = n$.Considérons alors

la décomposition de l'idéal $\mathfrak{p}B'$ dans l'anneau de Dedekind B' : de $\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{P}_{\mathfrak{i}}^{\mathfrak{e}_{\mathfrak{i}}}$ on déduit $\mathfrak{p}B' = \prod_{i=1}^{q} (B'\mathfrak{P}_{\mathfrak{i}})^{e_i}$ .Comme $\mathfrak{P}_{\mathfrak{i}} \cap A = \mathfrak{p}$, on a $\mathfrak{P}_{\mathfrak{i}} \cap S = \emptyset$ et $B'\mathfrak{P}_{\mathfrak{i}}$ est un idéal premier non nul de B'.

La premiere partie de la démonstration nous donne donc

$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i \left[B'/B'\mathfrak{P}_{\mathfrak{i}} : A'/\mathfrak{p}A'\right]$. Or, on a $A'/\mathfrak{p}A' \simeq A/\mathfrak{p}$ et $B'/B'\mathfrak{P}_{\mathfrak{i}} \simeq B/\mathfrak{P}_{\mathfrak{i}}$. D'où en combinisant nos égalités, $n = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i f_i$.

□

Proposition 1.80 *Avec les mêmes notations, l'anneau $B/B\mathfrak{p}$ est isomorphe à $\prod_{i=1}^{q} B/\mathfrak{P}_{\mathfrak{i}}^{\mathfrak{e}_{\mathfrak{i}}}$.*

Preuve : En effet, comme $\mathfrak{P}_{\mathfrak{i}}$ est le seul idéal maximal de B qui contient $\mathfrak{P}_{\mathfrak{i}}^{\mathfrak{e}_{\mathfrak{i}}}$, alors on a $\mathfrak{P}_{\mathfrak{i}}^{\mathfrak{e}_{\mathfrak{i}}} + \mathfrak{P}_{\mathfrak{j}}^{\mathfrak{e}_{\mathfrak{j}}} = B$ pour $i \neq j$ .On applique (1)et le lemme1(page 22 de samuel).

Exemples des corps cyclotomiques .

Soient p un nombre premier, et $z \in \mathbb{C}$ une racine primitive $p^r - ème$ de l'unité. Les racines $p^r - ème$ de l'unité, dans $\mathbb{C}$, sont alors les $z^j (f = 1, 2, ..., p^r)$; parmi elles les racines primitives sont les z^j telles que j ne soit multiple de p, et sont donc au nombre de : $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$

Ces racines $p^r - èmes$ de l'unité sont les racines du polynôme cyclotomique

3. $F(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + ... + X^{p^{r-1}} + 1$

Nous nous proposons de redémontrer ici qu'on a $[\mathbb{Q}[z] : \mathbb{Q}] = p^{r-1}(p-1)$, c'est -à-dire que $F(X)$ est irréductible .(Samuel p50)

Posons $e = p^{r-1}(p-1)$, et soient $z_1, z_2, ..., z_e$ les racines primitives p^r-ème de l'unité . Comme le terme constant de $F(X+1)$ est p, on a

$\prod_{j=1}^{e}(z_j-1)=\pm p$.

Soit B l'anneau des entiers de $\mathbb{Q}[z]$; on a évidemment $z_j\in B$, et aussi $(z_j-1)\in B(z_k-1)$pour tous j,k car $z_j$est une puisance z_k^q de z_k

et qu'on a $z_k^q-1=(z_k-1)\left(z_k^{q-1}+...+z_k+1\right)$; ainsi tous les idéaux $B(z_k-1)$sont égaux .on a donc $Bp=B(z_1-1)^e$.

Or écrivons $Bp=\prod_{i=1}^{q}\mathfrak{P}_i^{\mathfrak{e}_i}$ où les $\mathfrak{P}_i$sont les idéaux premiers de B.Les e_i sont donc tous les multiples de e.Mais on a $e\geq[\mathbb{Q}[\sqrt{z}]:\mathbb{Q}]$ (par (3)), d'où

$e\geq\prod_{i=1}^{q}e_if_i$. DE ces inégalités en sens contraire on déduit que $q=1,e=e_1,[\mathbb{Q}[z]:\mathbb{Q}]=e$. En résumé :

a)$[\mathbb{Q}[z]:\mathbb{Q}]=e=p^{r-1}(p-1)$

b)$B(z_1-1)$est un idéal premier de B,de degré résiduel 1

c)$Bp=B(z_1-1)^e$

□

1.4.3 Discriminant et ramification

Avec les notations précédentes (soit$B\mathfrak{p}=\prod_{i=1}^{q}\mathfrak{P}_i^{\mathfrak{e}_i}$) on dit qu'un idéal premier $\mathfrak{p}$ de A se ramifie dans B (ou dans L)

si l'un des indices de ramifications

si on prend les classes de B modulo $B\mathfrak{p}$, on voit , dans le second cas ,que $a+b\left(\frac{1+\sqrt{d}}{2}\right)$(avec b impair) est congru à $a+(b+p)\left(\frac{1+\sqrt{d}}{2}\right)$,

qui est élément de $\mathbb{Z}+\mathbb{Z}\sqrt{d}$. Donc, dans tous les cas , on a

$$B/Bp\simeq\left(\mathbb{Z}+\mathbb{Z}\sqrt{d}\right)/(p).$$

Or $\mathbb{Z}+\mathbb{Z}\sqrt{d}\simeq\mathbb{Z}[X]/(X^2-d)$ .D'où

$B/Bp\simeq\mathbb{Z}[X]/(p,X^2-d)\simeq(\mathbb{Z}[X]/(p))/(X^2-d)\simeq F_p[X]/\left(X^2-\bar{d}\right)$,

où $\bar{d}$ désigne la classe de d modulo p . Or l'assertion que p est décomposé (resp.est inerte, se ramifie) dans B signifie que B/Bpest produit de deux corps (res.est un corps, a des éléments nilpotents) ;

ceci signifie donc que , dans $F_p[X]$, le polynôme $X^2 - \bar{d}$ est produit de deux facteurs distincts du premier degré (resp.est irréductible, est un carré) ; or ceci se produit si $\bar{d}$ est un carré non nul dans F_p

(resp. n'est pas un carré dans F_p, est nul dans F_p).Lorsque $\bar{d}$ est un carré non nul dans F_p(resp.n'est pas un carré dans F_p), on dit que d est*un* résidu quadratique (resp.un non résidu) modulo p.

Traitons maintenant le cas $p = 2$. Si $d \equiv 2, 3\,(mod 4)$, on a $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, d'où, comme plus haut $B/2B \simeq F_2[X] / \left(X^2 - \bar{d}\right)$; or, $X^2 - \bar{d}$ vaut X^2ou $X^2 + 1 = (X+1)^2$, et est donc un carré ;

ainsi 2 se ramifie dans B . Si $d \equiv 1(mod 4)$, $\frac{1+\sqrt{d}}{2}$ admet $X^2 - X - \frac{d-1}{4}$ pour polynôme minimal , d'où , comme plus haut, $B/2B \simeq F_2[X]/(X^2 - X - \delta)$où δ est la classe mod.2 de $\frac{d-1}{4}$; pour

$d \equiv 1\ (mod.8)$on a $\delta = 0$ et $X^2 - X - \delta = X(X-1)$, de sorte que 2 est décomposé ; pour $d \equiv 5\,(mod.8)$, on a $\delta = 1$ et $X^2 - X - \delta = X^2 + X + 1$ est irréductible dans $F_2[X]$, de sorte que 2 est inerte .

En résumé , on a démontré les résultats suivants

Proposition 1.81 *Soit $L = \mathbb{Q}\left[\sqrt{d}\right]$ un corps quadratique, où $d \in \mathbb{Z}$ est sans facteurs carrés .*

a)Sont décomposés dans L, les nombres premiers impairs p tels que d soit résidu quadratique mod.p, et 2 si $d \equiv 1\,(mod.8)$;

b)Sont inertes dans L, les nombres premiers impairs p tels que d soit non résidu mod.p, et 2 si $d \equiv 5\,(mod.8)$;

c)Se ramifient dans L,les diviseurs premiers impairs de d , et 2 si $d \equiv 2ou3\,(mod.4)$

Preuve : [Cf. P. Sam, Proposition 1, p91]

□

Chapitre 2

Corps de nombres p-adiques

2.1 Anneaux de valutions

Proposition 2.1 *L'ensemble $\mathcal{E}$ des suites de cauchy , 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 et l'anneau quotient $\frac{\mathcal{E}}{I}$ vérifie :*

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

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

Preuve : (Cf. E. Ha, p 74)

□

2.2 Extensions et completion

Proposition 2.2 *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'injectent.
L'déal I formé des suites de Cauchy tendant vers 0 est maximal dans A. Le complété de K pour $|\ |$ est le corps $\frac{A}{I}$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 2.3 *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 $\left[\frac{B}{\mathfrak{M}} : \frac{A}{\mathfrak{m}}\right] = f$ où $ef = [L : K]$.

Preuve : [Cf. J.P. Se]

□

Proposition 2.4 *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 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 2.5 *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 nombre rationnels pour la valuation p-adique.

Proposition 2.6 *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 : [Cf. Y. Am]

□

Théorème 2.7 *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 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 2.8 *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.

Soty $\alpha \in A_K$ 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

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

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

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

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

Proposition 2.9 *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 et l'ensembles 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* $e_{\mathfrak{p}} f_{\mathfrak{p}}$.

Preuve : [Cf. E. Ha]

□

Examinons de façon précise le cas d'un corps de nombres algébrique K engendré par une racine d'un polynôme unitaire irréductible sur $\mathbb{Q}$.
Soit $f(X) \in \mathbb{Z}$ 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 2.10 *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 morphisme 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 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 2.11 *(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

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

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

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

Corollaire 2.12 *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 $\mathbb{Z}_p[X]$.

2.5.1 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 ramificaction de l'extension $E/\mathbb{Q}_p$. Le degré résiduel f est donné par

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

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

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

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 de l'anneau $\mathcal{O}_L$ des entiers de L sur K.

Définition 2.14 *On appelle groupe d'inertie de $\wp$ dans L, le sous groupe G_0 du groupe de Galois G donné par*

$$G_0 = \{\sigma \in G,\, \sigma(x) \equiv x \, mod \, \wp\}.$$

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

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

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 2.15 *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.

Preuve : [Cf. N. Na]

□

Corollaire 2.16 *Si L/K est non ramifiée, alors le groupe de Galois est cyclique d'ordre $f(L/K)$.*

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

Théorème 2.17 *(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

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

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 f_i.

Preuve : [Cf. E. Ha]

□

Théorème 2.18

Proposition 2.19 *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 16 *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 disciminat 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-Dedekindlegroupe 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 d 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 2.20 *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 .

Preuve : [Cf. J.P. Se]

□

Remarque 4 *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

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

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

Commençons par l'isomorphisme suivant

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

Du point de vue des dimension, on aura

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

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

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

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

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

ce qui assure le passage du local au global.

Exemple 17 *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

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

Connclusions :

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

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

  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.

Chapitre 3

Discriminant de corps de nombres

3.1 Motivations

Dans cette section nous exposerons le travail de Lorente, Nart et Villa [LNV] autour de la question de la détermination du discriminant d_K d'un corps de nombres $K = \mathbb{Q}(\alpha)$, de degré n, engendré par une racine α d'un trinôme irréductible $f \in \mathbb{Z}[X]$.
La démarche des auteurs consiste en la détermination de la valuation p-adique $v_p(d_K)$ du discriminant d_K en un nombre premier p divisant le discriminant D_f du trinôme $f(X)$ sachant qu'ils sont liés par la relation

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

où $i(\alpha)$ désigne l'indice de $\mathbb{Z}[\alpha]$ dans le groupe additif de l'anneau $\mathcal{O}_K$ des entiers du corps K. Les auteurs, dans une large partie de leur travail, s'appuient pour cela sur le résultat de Ore donnant la valuation p-adique de l'entier $i(\alpha)$. Dans la dernière partie de ce chapitre nous utiliserons ces résultats pour déterminer dans certains cas le groupe de Galois.

3.1.1 Notations

Soit $f(X) = X^n + AX^s + B \in \mathbb{Z}[X]$, $(n, s) = 1$ et $1 \leq s < n$, un trinôme irréductible sur $\mathbb{Q}$. Soit $\alpha := \alpha_1, \ldots, \alpha_n$ les différentes racines de f dans une clôture algébrique de $\mathbb{Q}$. On note par $K = \mathbb{Q}(\alpha)$ et $N = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ respectivement le corps de rupture et le corps de décompositions de f sur $\mathbb{Q}$ et soit $\mathcal{O}_K$ l'anneau d'entiers de K.

On note par $i(\alpha) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ l'indice du groupe $\mathbb{Z}[\alpha]$ dans le groupe additif $\mathcal{O}_K$

Le discriminant D_f du trinôme f est donné par :

$$D = (-1)^{n(n-1)2} B^{s-1} \left[n^n B^{n-s} + (-1)^{n-1} (n-s)^{n-s} s^s A^n\right]$$

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

$$D = i(\theta)^2 d.$$

Nous allons examiner dans ce qui suit la valuation p-adique $v_p(d_K)$ du discriminant du corps K pour un diviseur premier p du discriminant D_f du trinôme f.

Notons que les diviseurs premiers de D_f sont soit de B, soit de $D_0 = n^n B^{n-s} + (-1)^{n-1} (n-s)^{n-s} s^s A^n$.

Remarque 5 *On suppose que p ne divise pas B.*
si p divise A et ne divise pas n, ou si p ne divise pas A et divise n, alors p ne divise pas D_0, par conséquent p ne divise pas D_f. Sachant que les diviseurs de d_K sont parmi ceux de D_f, alors $v_p(d_K) = 0$.

- On pose :

$$A_p = Ap^{v_p(A)}\,,\; B_p = Bp^{v_p(B)}\,,\; a_p = (n, v_p(B))\,;\; b_p = (n-s\,,\; v_p(A))\,,$$

$$c_p = (s\,,\, v_p(B) - v_p(A))\,,\; M_p = (n-s)v_p\,(B) - nv_p(A)$$

3.1.2 Calcul de $v_p\,(d_K)$ si $p \nmid AB$

Dans ce cas nous étudierons la valuation proposée selon que p divise ou ne divise pas $ns\,(n-s)$).

1. Si $p \mid ns\,(n-s)$ et comme n et s sont premiers entre eux, alors p divise exclusisement que l'un des nombres n, s ou $(n-s)$, ce qui entraine que p ne divise pas D_0 et donc ne divise pas D_f. Par conséquent p ne divise pas d et donc $v_p\,(d_k) = 0$

   - $v_p\,(d) = 0$
   - alors $v_p\,(D) = 0$

2. Si $p \nmid ns\,(n-s)$, alors nous supposerons que $p \neq 2$. Comme $p \nmid n\,(n-s)$, alors $f'\,(X) = X^{s-1}\,(nX^{n-s} + sA)\,(\mathrm{mod}p)$ n'admet pas de racine multiple, par suite $f\,(X)\,(\mathrm{mod}\ p)$ admet des racines au plus d'ordre 2. Soit α l'une de ces racines multiples, alors on a

   $$\alpha^{n-s} = -sAn$$

   ce qui entraine

   $$\alpha^s = \frac{-nB}{(n-s)\,A}$$

   et implique que $\alpha \in \mathbb{Z}p\mathbb{Z}$. D'autre part, si β est une autre racine multiple de f, alors on aura

   $$\left(\frac{\alpha}{\beta}\right)^s = \left(\frac{\alpha}{\beta}\right)^{n-s}$$

   ce qui entraine $\alpha = \beta$, puisque s et $(n-s)$ sont premiers entre eux. Par conséquent, f admet au plus une racine multiple α, d'ordre au plus égal

2, ce qui qui donne la factorisation de $f(X) \pmod p$ suivante

$$f(X) = (X-\alpha)^2 \varphi_1(X) \dots \varphi_r(X).$$

Par le lemme de Hensel, cette factorisation de $f(X) \pmod p$ coorespond à la factorisation suivante en idéaux premiers de $p\mathcal{O}_K$

$$p = \mathfrak{a}\mathfrak{p}_1 \dots \mathfrak{p}_r$$

où $\mathfrak{a}$ est un idéal de $\mathcal{O}_K$ et les $\mathfrak{p}_i$, $1 \leq i \leq r$, sont des idéaux premiers de $\mathcal{O}_K$ de normes

$$N_{K/\mathbb{Q}}(\mathfrak{a}) = p^2 \text{ et } N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{\deg \varphi_i}.$$

Cette décomposition permet de conclure que si $p \mid d$, alors p est ramifié dans K et on aura $\mathfrak{a} = \mathfrak{p}^2$, où $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$.
En combinant les résultats ci-dessus on obtient

Théorème 3.1 *Soit $f(X) = X^n + AX^s + B \in \mathbb{Z}[X]$ un polynôme irréductible sur $\mathbb{Q}$ de degré n, où n et s sont des entiers premiers entre eux avec $1 \leq s < n$. soit p un nombre premier ne divisant pas AB, alors la valuation p-adique $v_p(d_K)$ du discriminant du corps K est*

$$v_p(d) = \begin{cases} 0 & \text{si } v_p(D) \text{ est paire} \\ 1 & \text{sinon} \end{cases}$$

3.1.3 Calcul de $v_p(d_K)$ lorsque p divise à la fois A et B

Dans ce paragraphe on se donne un nombre premier p divisant à la fois A et B et tel que $p \mid A$ et B. Dans ce cas nous étudierons la valuation p-adique $v_p(d_K)$ du corps K selon les valeurs prises par l'entier M_p défini précédemment.

1. On supposera pour commencer que $M_p = 0$. Dans ce cas nous aurons

$$(n-s)\, v_p(B) = n v_p(A)$$

ce qui entraine que $v_p(A) = (n-s)$ et $v_p(B) = n$, puisque n et $(n-s)$ sont premiers entre eux. On considère alors le polynôme $g \in \mathbb{Q}[X]$ défini par

$$g(X) = \frac{1}{p^n} f(pX) = X^n + B_p X^s + A_p,$$

et on note D' son discriminant. Alors $\beta = \alpha p$ est une racine de $g(X)$ et engendre sur $\mathbb{Q}$ le même corps K .
Par ce qui précède, comme p ne divise pas $A_p B_p$, on aura le résultat suivant :

Théorème 3.2 *La valuation p-adique du discriminant d_K du corps K est donné par*

$$v_p(d_K) = \begin{cases} 0 & \text{si } v_p(D') \text{ est paire} \\ 1 & \text{sinon} \end{cases}$$

2. Dans ce qui suivra nous supposerons que $M_p \neq 0$. Nous aurons besoin d'introduire la notion de polygone de Newton associé à un polynôme relatif à un nombre premier p.
Soit $g(X) = X^n + \sum_{i=1}^{n-1} a_i X^{n-i} + a_n X^n \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers.

Définition 3.3 *On appelle polygone de Newton associé au polynôme $g(X)$ et relatif au nombre premier p, l'enveloppe convexe supérieure de l'ensemble des points suivants $\{(i, v_p(a_i)),\ 1 \leq i \leq n\}$.*

On note $\epsilon_i = pgcd(\ell_i, h_i)$ *et* $\lambda_i = \ell_i/\epsilon_i$.

Si S_i *commence par le point* $(r, v_p(a_r))$ *, on pose* $r_j = r + j\lambda_i$, *et on considère les entiers* b_j *suivants :*

$$b_j = \begin{cases} a_{rj}/p^{v_p(a_{rj})} si (r_j, v_p(a_{rj})) \in s_i \\ 0 \quad sinon \end{cases}$$

On appelle polynôme associé au côté S_i, le polynôme g_i défini par les coefficients b_j donnés par

$$g_i(Y) = b_0 Y^{\epsilon_i} + \cdots + b_{\epsilon_i}$$

On dit que $g_{i\sum}$ est régulier si p ne divise aucun des discriminants des g_i.

Cette notion permet d'exprimer la valuation $v_p(i(\theta))$ de l'indice $i(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]$ du groupe monogène $\mathbb{Z}[\theta]$ dans le groupe additif de l'anneau $\mathcal{O}_K$ des entiers du corps $K = \mathbb{Q}(\theta)$.Ore montre le résultat suivant :

Théorème 3.4 *(Théorème de l'indice) Soit* $f(X) = X^n + \sum_{1 \le i \le n} a_i X^{n-i} \in \mathbb{Z}[X]$ *un polynôme irréductible. Soit* θ *une racine de* f *dans* $\overline{\mathbb{Q}}$ *et* $K = \mathbb{Q}(\theta)$ *et* p *un nombre premier*
Alors la valuation p-adique $v_p(i(\theta))$ *de l'indice de* θ *est*

$$v_p(i\theta) = \sum_{j=2}^{k} \ell_i \left(\sum_{s=1}^{j-1} h_s \right) + \frac{1}{2} \sum_{i=1}^{k} [\ell_i (h_i - 1) - h_i + \epsilon_i]$$

Selon les valeurs de l'entier M_p et en utilisant le théorème de Ore ci-dessus, nous déterminerons dans ce qui suit la valuation p-adique $v_p(i(\theta))$ de l'indice $i(\theta)$. Cette valeur sera donnée, comme indiquée dans ce théorème, suivant le nombre de côtés du polygone de Newton de $X^n + AX^s + B$ sous la condition que les entiers A et B vérifient $M_p = nv_p(A) - (n-s)v_p(B) \neq 0$. En effet, nous aurons à examiner les cas selon que $M_p < 0$ ou $M_p > 0$ ce qui précisera,

comme on le verra, le polygone de Newton associé au polynôme f et relatif au nombre premier p.
En premier, déterminons l'ensemble des points qui définiront l'enveleoppe convexe supérieur de ce polygone de Newton. Cet ensemble sera formé des points suivants

$$(0,0), \quad ((n-s), v_p(A)) \text{ et } (n, v_p(B))$$

et l'enveloppe convexe supérieure sera déterminée selon l'ordre sur les pentes des segments formés par, d'un côté le segment reliant les points $(0,0)$ et $((n-s), v_p(A))$ et de l'autre côté celui reliant les points $(0,0)$ et $(n, v_p(B))$ de pentes respectivement égales à $v_p(A)n - s$ et $v_p(B)n$. Ainsi le polygone de Newton associé à $f(X)$ relativement au nombre premier p est formé d'un côté ou de deux côtés selon que $v_p(B)n < v_p(A)n - s$ ou non, ce qui correspond à $M_p < 0$ ou $M_p > 0$.
On suppose que $M_p < 0$, alors le polygone de Newton relatif à p est formé d'un côté S_1 reliant les points $(0,0)$ et $(n, v_p(B))$ de pente $v_p(B)n$, ainsi $\epsilon_1 = \text{pgcd}(v_p(B), n)$ et $\lambda_1 = \dfrac{n}{\epsilon_1}$. Sachant que ce côté contient seulement les points $(0,0)$ et $(n, v_p(B))$ et qu'il démarre du point $(0,0)$, alors les seuls coefficients b_j définissant le polynôme associé sont $b_0 = 1$ et b_{ϵ_1}. Dans ce cas, le polynôme associé au côté S_1 et relatif au premier p est $g_1(Y) = Y^{b_p} + B_p$ de discriminant $\pm b_p^{b_p} B_p^{b_p - 1} \neq 0 \pmod p$, ce qui montre que f est p-régulier.

Proposition 3.5 *Soientt $f(X) = X^n + AX^s + B \in \mathbb{Z}[X]$ un polynôme irréductible et p un nombre premier tel que p divise à la fois les entiers A et B dont les valuations p-adiques vérifient $(n-s)v_p(B) - nv_p(A) < 0$. Soit θ une racine de f dans une clôture algébrique de $\mathbb{Q}$ et $K = \mathbb{Q}(\theta)$ le corps de rupture de f sur $\mathbb{Q}$. Alors la valuation p-adique $v_p(i(\theta))$, de l'indice $i(\theta)$ de $\mathbb{Z}[\theta]$ dans l'anneau $\mathcal{O}_K$ des entier de K , est égale à $v_p(i(\theta)) = \dfrac{1}{2}[(n-1)v_p(B) - n + b_p]$*

Preuve : Comme indiqué précédemment, le polygome associé à f et relatif à p est formé d'un coté reliant les points $(0,0)$ et $(n, v_p(B))$ et sous les hypothèse

de la proposition le théorème de Ore sur l'indice entraine que

$$v_p\left(i(\theta)\right) = \frac{1}{2}\left[n\left(v_p(B)-1\right) - v_p\left(B\right) + b_p\right]$$

ce qui entraine

$$v_p\left(i(\theta)\right) = \frac{1}{2}\left[(n-1)\, v_p(B) - n + b_p\right]$$

□

On suppose maintenant que $M_p > 0$, alors le polygone de Newton relatif à p est formé de 2 côtés : S_1 reliant les points $(0,0)$ et $(n-s\,,\, v_p\left(A\right))$ et S_2 reliant les points $(n-s\,,\, v_p(A))$ et $(n\,,\, v_p\left(B\right))$.
Pour le côté S_1, sa pente est $v_p(A)n - s$ avec $\epsilon_1 = \text{pgcd}\left(n-s\,,\, v_p(A)\right)$ et $\lambda_1 = \dfrac{n-s}{\epsilon_1}$ et sachant qu'il démarre du point $(0,0)$ et qu'il ne contient en plus que le point $(n-s\,,\, v_p(A))$, alors le polynôme associé à ce côté est $Y^{a_p} + A_p$ qui est régulier puisque son discriminant est $\pm a_p^{a_p} A^{a_p - 1}$ n'est pas divisibe par p.
Pour le côté S_2, sa pente est $v_p(B) - v_p(A)s$ avec $\epsilon_2 = \text{pgcd}\left(s\,,\, v_p(B) - v_p(A)\right)$ et $\lambda_2 = \dfrac{s}{\epsilon_2}$ et sachant qu'il démarre du point $(n-s\,,\, v_p(A))$ et qu'il ne contient en plus que le point $(s\,,\, v_p(B) - v_p(A))$, alors le polynôme associé à ce côté est $A_p Y^{c_p} + B_p$. Comme ce polynôme est de discriminant $\pm c_p^{c_p} A_p B_p^{c_p}$, alors il est régulier en p.

Proposition 3.6 *Soientt $f\left(X\right) = X^n + AX^s + B \in \mathbb{Z}\left[X\right]$ un polynôme irréductible et p un nombre premier tel que p divise à la fois les entiers A et B dont les valuations p-adiques vérifient $(n-s)v_p(B) - nv_p(A) > 0$. Soit θ une racine de f dans une clôture algébrique de $\mathbb{Q}$ et $K = \mathbb{Q}\left(\theta\right)$ le corps de rupture de f sur $\mathbb{Q}$. Alors la valuation p-adique $v_p\left(i(\theta)\right)$, de l'indice $i\left(\theta\right)$ de $\mathbb{Z}\left[\theta\right]$ dans l'anneau $\mathcal{O}_K$ des entier de K , est égale à $v_p\left(i(\theta)\right) = \dfrac{1}{2}\left[n\left(v_p(A)-1\right) - (s-1)v_p\left(B\right) + a_p + c_p\right]$.*

Preuve : Sous les hypothèses de la proposition, le théorème de Ore sur l'indice donne

$$\begin{aligned} v_p\left(i\left(\theta\right)\right) &= sv_p(A) + \frac{1}{2}\left[\left(n-s\right)\left(v_p(A)-1\right) - v_p(A) + \left(s-1\right)\left(v_p(B)-v_p(A)\right) - s + a_p + c_p\right] \\ &= \frac{1}{2}\left[n\left(v_p(A)-1\right) + \left(s-1\right)v_p(B) + a_p + c_p\right] \end{aligned}$$

□

De la relation $D = i\left(\theta\right)^2 d_K$ on tire la valuation $v_p\left(d_K\right)$

$$v_p\left(d_K\right) = v_p\left(D\right) - 2v_p\left(i(\theta)\right) \tag{3.1}$$

ce qui nous permet de déterminer la valeur de d_K en connaissant sa valuation p-adique en un diviseur prmier p du discriminant D_f du trinôme f.
La section précédente nous a permis de déterminer la valuation p-adique $v_p\left(i(\theta)\right)$ de l'indice $i\left(\theta\right)$ dont la valeur est donnée selon le polygone de newton associé au polynôme f et relatif au nombre premier p . Ainsi,

$$2v_p\left(i\left(\theta\right)\right) = \begin{cases} n\left(v_p\left(B\right)-1\right) - v_p\left(B\right) - b_p & \text{si } M_p < 0 \\ nv_p\left(A\right) + \left(s-1\right)v_p\left(B\right) - n + a_p + c_p & \text{si } M_p > 0 \end{cases} \tag{3.2}$$

D'autre part, comme le discriminant D_f du trinôme f est donné par

$$D_f = \left(-1\right)^{n(n-1)2} B^{s-1}\left[n^n B^{n-s} + \left(-\right)^{n-1}\left(n-s\right)^{n-s} s^s A^n\right]$$

alors sa valuation p-adique $v_p\left(D_f\right)$ est donnée par

$$v_p\left(D\right) = \left(s-1\right)v_p\left(B\right) + \inf\left\{nv_p\left(n\right) + \left(n-s\right)v_p\left(B\right)\ ;\ sv_p\left(s\right) + \left(n-s\right)v_p\left(n-s\right) + nv_p\left(A\right)\right\}$$

cette valuation est précisée selon que le polygone de Newton est formé d'un ou de 2 côtéq. En effet, si $M_p < 0$, donc $-M_p > 0$, alors on aura

$$\inf\{nv_p(n)+(n-s)v_p(B)\ ;\ sv_p(s)+(n-s)v_p(n-s)+nv_p(A)\} = (n-s)v_p(B)+\inf\{nv_p(n), sv_p(s)+(n-$$

Par contre, si $M_p > 0$ on aura

$$\inf\{nv_p(n)+(n-s)v_p(B)\ ;\ sv_p(s)+(n-s)v_p(n-s)+nv_p(A)\} = nv_p(A)+\inf\{M_p, \max\{sv_p(s); (n-s)v_p$$

En combinant les dernière égalités on tire

$$v_p(D_f) = \begin{cases} (n-1)v_p(B)+\inf\{nv_p(n), sv_p(s)+(n-s)v_p(n-s)-M_p\} & \text{si} M_p<0 \\ \quad +\inf\{M_p\,;\,\max\{sv_p(s)\,;\,(n-s)v_p(n-s)\}\} & \text{si } M_p>0 \end{cases}$$

ce qui permet de déterminer la valuation $v_p(d_K)$ du discriminant du corps de nombres K suivant la relation (1) et (2) on aura

$$v_p(d) = \begin{cases} n-b_p-\inf\{-M_p, nv_p(n)\} & \text{si} M_p<0 \\ n-l-m+\inf\{M_p\,;\,\max\{sv_p(s)\,;\,(n-s)v_p(n-s)\}\} & \text{si } M_p>0 \end{cases}$$

Exemples

Nous donnerons dans ce qui suit des éxemples qui illustrent la déterminantion du discriminant d'un corps de nombre par l'utilisation du théorème de Ore sur l'indice d'un entier algébrique qui engendre ce corps de nombres.

1. On considère le trinôme $f(X) = X^5+5X+5$. Soit α une racine de f dans $\overline{\mathbb{Q}}$, $K = \mathbb{Q}(\alpha)$ et N la clôture normale de K sur $\mathbb{Q}$.
   Le discriminant du trinôme est $D = 5^5 \times 881$. Nous allons déterminer la valuation p-adique du discriminant d_K du corps de nombre K suivant les diviseurs premiers p de D.
   Pour $p = 5$, le polygone de Newton associé au trinôme f et relatif au nombre premier $p = 5$ est formé d' un côté reliant les points $(0,0)$ et $(5,1)$

Par conséquent, le polynôme associé à ce côté et relatif à$p = 5$ est $Y + 1$, qui esr régulier.
D'autre part on a $M_5 = -1 < 0$, alors $v_5(d) = 5$.
Pour $p = 881$, on a $v_{881}(d) = 1$
Comme $v_{881}(d) = 1$, alors le groupe de Galois $G(f)$ contient une transposition, c'est donc S_5.

2. On considère le trinôme $f(X) = X^5 + 5X + 25$. Soit α une racine de f dans $\overline{\mathbb{Q}}$, $K = \mathbb{Q}(\alpha)$ et N la cloture normale de K sur $\mathbb{Q}$.
Le discriminant : $D = 5^5 \times 17 \times 22993$
Pour $p = 5$, $M_5 = 3 > 0$, le polygone de Newton est formé de 2 côtés : le côté reliant les points $(0, 0)$ et $(4, 1)$; et le côté reliant les points $(4, 1)$ et $(5, 2)$.
Ainsi, les polynômes associés respectivement à chacun des côtés du polygone de Newton sont : $Y + 1$ et $Y + 1$ et sont réguliers.
La formule de la valuation $v_p(d_K)$ du discriminant d_K du corps K pour $p = 5$ donne $v_5(d) = 3$.
Pour $p = 17$ou $p = 22993$, $p \nmid 5$ et $p \nmid 4$ et comme $v_p(D) = 1$ et impaire, alors $v_p(d_K) = 1$.
Par conséquent, $d = 5^3 \times 17 \times 22993$

3.2 Théorème de Ore et ramification

Soit K un corps de nombre, A_K son anneau d'entiers et $\mathrm{disc}(K)$ son discriminant absolu.
La détermination de la décomposition en idéaux premiers dans A_K d'un nombre premier, le calcul de $\mathrm{disc}(K)$ et la construction d'une base de A_K comme $\mathbb{Z}-$module sont trois problèmes intimement liés en théorie algébrique des nombres.
Après les travaux de Hensel, les trois questions peuvent être réduites dans le

cas local, mais plus que cela, une solution effctive en terme d'équation définie pour K peut être donnée de façon algorithmique.
Parmi les procédures directes de résolution de ces problèmes, notons la réponse très partielle donnée par le célèbre théorème de Dedekind, qui est une version plus soft du résultat de Kummer.
Soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire irréductible, θ une racine de $f(X)$, et $\operatorname{ind}(\theta) = (A_K : \mathbb{Z}[\theta])$ l'indic de $f(X)$, alors

$$\operatorname{disc}(f) = \operatorname{ind}(\theta)^2 \operatorname{disc}(K).$$

Soit $p \in \mathbb{Z}$ un nombre premier et soit $\overline{f}(X)$ le polynôme de $\mathbb{F}_p[X]$ obtenu de $f(X)$ par réduction modulo$p$ de ses coefficients. Soit

$$\overline{f}(X) = \varphi_1(X)^{e_1} \dots \varphi_r(X)^{e_r} \tag{3.3}$$

sa factorisation dans $\mathbb{F}_p[X]$ en produit de puissances de polynômes irréductibles. de KUMMER
On suppose que $p \nmid \operatorname{disc}(f)$, dans ce cas $e_1 = \dots = e_r = 1$. Alors

$$pA_K = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

où, $\forall i$ $\mathfrak{p}_i = pA_K + \varphi_i(\theta) A_K$ est un idéal premier de A_K au dessus de p de degré résiduel $f(\mathfrak{p}_i/p) = \deg \varphi_i(X)$.

de DEDEKIND
On suppose que $p \nmid \operatorname{ind}(\theta)$, alors

$$pA_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

où, $\forall i$, $\mathfrak{p}_i = pA_K + \varphi_i(\theta) A_K$ est un idéal premier de A_k au dessus de p d'indice de ramification $e(\mathfrak{p}_i/p) = e_i$ et de degré résiduel $f(\mathfrak{p}_i/p) = f_i = \deg \varphi_i(X)$.

Pour appliquer ce résultat de façon effective, nous aurons besoin d'un

critère permettant de savoir lorsque la condition $p \nmid \operatorname{ind}(f)$ est satisfaite. Ceci est donné par le critère de DEDEKIND avec les notations ci-dessus, soit $g_1(X), \ldots, g_r(X)$ des polynômes unitaires arbitraires de $\mathbb{Z}[X]$ tels que $\overline{g_i}(X) = \varphi(X)$ et soit

$$g(X) = \frac{1}{p}\left(f(X) - g_1(X)^{e_1} \ldots g_r(X)^{e_r}\right).$$

Alors $p \nmid \operatorname{ind}(f)$ si et seulement si $\forall i,\ e_i = 1$ ou bien $\varphi_i(X) \nmid \overline{g}(X)$ dans $\mathbb{F}_p[X]$.

Un résultat qui n'est pas bien connu est le théorème de ORE qui constitue très grande généralisation de ces résultats. Par le lemme de HENSEL, nous obtenons à partir de (1) la factorisation dans $\mathbb{Z}_p[X]$:

$$f(X) = f_1(X) \ldots f_r(X), \qquad \overline{f_i}(X) = \varphi_i(X)^{e_i}.$$

Si $p \nmid \operatorname{ind}(f)$ n'ont pas besoin d'être irréductibles dans $\mathbb{Z}_p[X]$ et le problème est de déterminer une telle décomposition en produit de facteurs irréductibles. Mieux que cela, ce qui reste à trouver, pour chaque facteur irréductible, l'indice de ramification, le degré résiduel, le discriminant et la bas d'entiers de l'extension locale correspondante.
Ore considère à cet effet le polygone de Newton pour chaque i, dont les côtés détermine la factorisation de $f_i(X)$ dans $\mathbb{Z}_p[X]$ et des informations partielles sur les indices de ramification, etc....
De plus, il associe à chaque côté S un polynôme $(f_i)_S(Y) \in \mathbb{F}_{q_i}[Y]$, $q_i = p^{\deg \varphi_i(X)}$, dont la factorisation dans $\mathbb{F}_{q_i}[Y]$ produit une telle décomposition d'un facteur de $f_i(X)$ correspondant à ce côté. Finalement, montre que lorsque ces polynômes $(f_i)_S(Y)$ n'ont pas de facteurs multiples, alors tous ces facteurs de $f_i(X)$ sont irréductibles et l'enveloppe du polygone ainsi que les degrés des facteurs irréductibles de $(f_i)_S(Y)$ donne les données nécessaires pour compléter la connaissance complète de tous les indices de ramification et les degrés

résiduels.
Le but de cet article est de donner une généralisation de ces résultats de Ore dans le même esprit que le théorème de Dédekind généralisant celui de Kummer. Nous trouvons une condition, jouant le même rôle que "$p \nmid \operatorname{ind}(f)$ " qui rend possible l'obtention la décomposition complète de pA_K même si le polynôme $(f_i)_S(Y)$ comporte des facteurs multiples.
La multiplicité de ces facteurs contribue aussi pour les indices de ramification des idéaux premiers au dessus de p. Finalement, nous trouvons aussi un critère analogue à celui de Dedekind, pour décider si la condition est satisfaite.
La méthode de Ore produit une formule explicite pour $\operatorname{ind}(f)$(ainsi que le calcul du discriminant $\mathrm{d}(K)$de K) et permet de construire une base d'entiers. Les mêmes résultats restent valides dans les situation plus générales que nous considérons.

3.3 Les travaux de Ore et les polygones de Newton

FIxons un nombre premier $p \in \mathbb{Z}$, et les clôtures algébriques $\overline{\mathbb{Q}_p}$, $\overline{\mathbb{F}_p}$ de $\mathbb{Q}_p$ et $\mathbb{F}_p$. Pour toute extension finie L de $\mathbb{Q}_p$ nous notons par A_L l'anneau des entiers, $\mathfrak{p}_L$ l'idéal premier de L, v_L la valuation de $\mathbb{Q}_p$ prolongée en une valuation de L, et par $\mathbb{F}_L$ le corps résiduel que nous supponsons injecté dans $\overline{\mathbb{F}_p}$.
Pour tout polynôme irréductible $\psi(X) \in \mathbb{F}_L(X)$ nous fixons une fois pour tout un polynôme unitaire dans $A_L[X]$par réduction de $\psi(X)$ mod $\mathfrak{p}_L$ et on le note par le même symbole $\psi(X)$.
Nous prenons une extension finie K de $\mathbb{Q}_p$ et on note $A = A_K$, $\mathfrak{p} = \mathfrak{p}_K$, $v = v_K$ et $\mathbb{F} = \mathbb{F}_K$. On fixe un élément $\pi \in A$, un polynôme unitaire irréductible $\varphi(X) \in \mathbb{F}[X]$ de degré $m \geq 1$ et une racine $\zeta \in \overline{\mathbb{F}_p}$ de $\varphi(X)$. Soit T l'extension non ramifiée de K de degré m.On a $\mathbb{F}_T = \mathbb{F}(\zeta)$.
Soit $f(X) \in A[X]$ un polynôme de degré $m \geq 1$. Il peut être écrit de façon

unique

$$f(X) = \sum_{i=0}^{[n/m]} a_i(X) .\varphi(X)^i$$

où $a_i(X) \in A[X]$ et $\deg a_i(X) < m$ ou $a_i(X) = 0$. Soit s_i la plus grande puissance telle que π^{s_i} divise tous le coefficients de $a_i(X)$.

Définition 3.7 *Le $\varphi(X)-$polygone de $f(X)$ est l'enveloppe convexe supérieure de l'ensemble des points $(i\,,\, s_i)$.*
Le polygone de Newton classique correspond au cas $\varphi(X) = X$.

L'ensemble des côtés de pentes positives constitue la partie principale de ce polygone. Leur projections sur l'axe OX ont des longueurs égales à la plus grande puissance ℓ telle que $\varphi(X)^\ell$ divise $\overline{f}(X) \in \mathbb{F}[X]$.
Soit S un segment d'origine et d'extrémité (r, s) et $(r + E\,,\, s + H)$, respectivement, à coordonnées entière, où r, s, E et H sont des entiers non négatifs. On dnote

$$d = \text{ppcm}(E, H), \quad e = E/d, \quad h = H/d$$

avec la convention que $e = h = 0$ lorsque $E = H = 0$. On suppose que sur la verticale passant par les points à coordonnées entières appartenant à S il n'ya aucun point du $\varphi(X)-$polygone de $f(X)$ se trouvant endessous de S.
On associe à chacun de ces points un élément de $\mathbb{F}_T$et prenons ces éléments comme les coefficients d'un polynôme $f_S(Y) \in \mathbb{F}_T[Y]$ que nous appellerons polynôme associé à $f(X)$ et S. EN fait, les polynômes

$$b_i(X) = \pi^{s+jh} a_{r+je}(X), \quad 0 \leq j \leq d$$

sont à coefficients entier et on peut définir

$$f_S(Y) = \sum_{j=0}^{d} \overline{b_j}(\zeta).Y^j \in \mathbb{F}_T[Y]$$

Les coefficients non nuls de $f_S(Y)$ correspondent aux points du $\varphi(X)-$polygone de $f(X)$ se trouvant sur S. En particulier, dans le cas considéré par Ore, tel que S est précisemment l'un des côtés du $\varphi(X)-$polygone de $f(X)$, ce polynôme $f_S(Y)$ est de degré exactement d et de terme constant non nul. (**du produit**) Soient $f_1(X), \ldots, f_r(X) \in A[X]$ des polynômes unitaires et posons $f(X) = f_1(X) \ldots f_r(X)$. la partie principale du $\varphi(X)-$polygone de $f(X)$ est formé en joignant tous les côtés de la partie principale de $\varphi(X)-$polygone de tous les $f_i(X)$ dans l'ordre croissant des pentes. De plus, pour chaque côté S de pente positive du $\varphi(X)-$polygone de $f(X)$ on a

$$f_S(Y) = (f_{i_1})_{S_1}(Y) \ldots (f_{i_t})_{S_t}(Y),$$

où $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, r\}$ et $S_1, \ldots, S_t$ sont tous les côtés de même pente que S appartenant à chacun des $\varphi(X)-$polygone de $f_1(X), \ldots, f_r(X)$.

(**du polygone**) Soit $f(X) \in A[X]$ un polynôme unitaire et on suppose que le $\varphi(X)-$polygone est formé de r côtés différents $S_1, \ldots, S_r$ de pentes $h_1/e_1 < h_2/e_2 < \cdots < h_r/e_r$. Alors $f(X)$ admet la factorisation $f(X) = f_1(X) \ldots f_r(X)$ où les $f_i(X)$ son,t des polynômes unitaires dans $A[X]$ dont le $\varphi(X)-$polygone est formé d'un seul côté de même pente que S_i et tel que le polynôme de $\mathbb{F}_T[Y]$ associé à ce côté est égal à $f_{S_i}(Y)$.
De plus, $\forall i$, si θ est une racine de $f_i(X)$ on a $v(\varphi(\theta))\, h_i/e_i$.

(de ORE) Soit $f(X) \in A[X]$ un polynôme unitaire dont le $\varphi(X)-$polygone est formé d'un seul cˆté S et soit e, h comme définis ci-dessus. Soit

$$f_S(Y) = \psi_1(Y)^{e_1} \ldots \psi_t(Y)^{e_t}$$

la factorisation de $f_S(Y)$ en produit de puissances de polynômes unitaires irréductibles de $\mathbb{F}_T[Y]$. Alors $f(X)$ sz factorise sous la forme

$$f(X) = f_1(X) \dots f_r(X),$$

où chaque $f_i(X)$ est un polynôme de $A[X]$ de $\varphi(X)-$polygone formé d'un seul côté S_i de même pente que S et de polynôme associé $(f_i)_{S_i}(Y) = \psi_i(Y)^{e_i}$. De plus, si $e_1 = \dots = e_t = 1$, alors $f_1(X), \dots, f_t(X)$ sont irréductibles et, $\forall i$, si θ est une racine de $f_i(X)$ et $L = K(\theta)$ on a $\mathfrak{p}_L = \left(\varphi(\theta)^b / \pi^c\right) A_L$, où b et c sont des entiers positifs tels que $bh - ce = 1$ et

$$e(L/K) = e, \quad f(L/K) = m.\deg \psi_i(Y)$$

Une généralisation de ce résultt est donné dans [CMS].

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

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

$$f(X) = \sum_{j=O}^{t} p^{\alpha_j} Q_j(X) \phi(X)^{t-j} \tag{3.4}$$

où les polynômes $Q_j(X) \in \mathbb{Z}[X]$ sont de degrés $degQ_j(X) < m$ pour tout j, et t le plus grand entier vérifiant $t \leq \frac{n}{m}$. Dans l'égalité (2.1), les coefficients de $Q_j(X)$ ne divisent pas tous le nombre premier p , sauf si $Q_j = 0$ et dans ce cas le terme correspondant est omis de la somme.
Si $f(X)$ est unitaire, on a $\alpha_0 = 0$.
Le développement donné dans (1.1) est appelé décomposition canonique de $f(X)$.

Le (p, ϕ) polygone de $f(X)$ est défini par :

Définition 3.8 *Le $(p, \phi)-$polygone de $f(X)$ est la frontière de l'enveloppe*

convexe supérieure 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 côtéss 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

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

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

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

Définition 3.9 *On appelle polynôme associé à $f(X)$ et relatif au côté S_i, le polynôme $F_i(X,Y)$ donné par*

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

Par construction, le polynôme $F_i(X,Y)$ dépend du choix de $A_i(X)$, ce qui n'est pas le cas de sa classe modulo l'idéal $(p, \phi(X))$.
La relation entre $(p,\phi)-$polygone et ramification est donnée par [11, Theoreme 1.5] Soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire irréductible tel que $f(X) \mod p$ n'est pas irréductible, et soit θ une racine de $f(X)$ dans une clôture algébrique de $\mathbb{Q}$ fixée. On considère la factorisation modulo p de f(X)

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

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

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

Alors

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

où¿½ $\lambda_i = l_i/\epsilon_i$ 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 18 *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 $\mathbb{Q}^{alg}$ 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¿½ 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 puissances 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* $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}_1} : \mathbb{F}_5\right] = 1$ *et* $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}_2} : \mathbb{F}_5\right] = 2$*, où* $\mathfrak{p}_1$ *et* $\mathfrak{p}_2$ *sont des idéaux distincts puisqu'il sont de normes différentes.*

Bibliographie

[Y. Am] Y. AMICE, "Les nombre p-adiques", Presse Universitaire Française, Collection Sup,1974

[Ben] B. BENSEBAA, "Groupe de Galois de trinômes", Thèse de Doctorat d'Etat, USTHB, Décembre 2008,

[Z.I. Bo] Z. BOREVITCH, "<Théorie des Nombres">, Gauthier Villard, ed. 1967

[C.M.S] S.D. COHEN, A. MOVAHHEDI and A. SALINIER, "Factorization over local fields and the irreductibility of generalized difference polynomials", J.N.T, 2000

[H.En] H. ENGSTROM, "On the common index divisors of an algebraic field,

[J.P.Es] P. ESCOFIER, "Théorie de Galois", DUNOD, second édition, 2000

[E.Ha] E. HALLOUIN, "Parcourt initiatique à travers la théorie des valuations, www.math.univ-toulouse.fr/ hallouin/Documents/eh-valuation.ps

[L.N.V] P. Lorente, E. Nart et N. Villa <Discriminant of number field defined by trinomial">, Acta Arith. XLIII (1984), 367-373

[M.N.] J. MONTES, E. NART, "On a Theorem of ORE", J. of Algebra, Volume 146, Issue 2, March 1992, Pages 318-334

[N.Na] N. NARKIEWICZ, "<Elementary and analytic Theory of algebraic number">, Monogr. Math. 57 (1974)

[J.P.] J. J. PAYAN, "<Sur les extensions cubiques non galoisiennes des rationnel et leur clôture galoisienne">, J. Reine Angew. Math 228(1967), 15-37

[P.Sa] P. SAMUEL, "Théorie algébrique des nombres", Herman Paris, deuxième

édition, 1971
[J.P.Se] J.P. SERRE "Cours d'arithmétiques", Springer Verlag, 1996
[J.P.Se2] J.P. SERRE, "Corps locaux", Herman, 3ème édition, 1968
[Tor] L. TORNHEIM, "Minimal basis and inessential discriminant divisors for a cubic field", Pacific J. Math. 5(1955), 623-631