جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES



كلية العلوم ظهر المهراز فاس
FACULTE DES SCIENCES DHAR EL MAHRAZ FES

N° d'ordre : 66/2022

Formation Doctorale : Mathématiques-Applications

Discipline : Mathématique

Spécialité : Algèbre

Laboratoire : LAMA

THESE DE DOCTORAT

Présenté par

BOUGHALEB Omar

On the normality of certain rational algebras

Soutenue le 29/11/2022 devant le jury composé de :

Pr. MOUANIS Hakima	**Faculté des sciences Dhar El Mehraz -Fès**	**Présidente**
Pr. EL FADIL Lhoussain	**Faculté des sciences Dhar El Mehraz –Fès**	**Directeur de thèse**
Pr. Chillali Abdelhakim	**Faculté Polydisciplinaire -Taza**	**Rapporteur**
Pr. Ziane M'hammed	**Faculté des sciences -Oujda**	**Rapporteur**
Pr. KACHA Ali	**Faculté des sciences -Kénitra**	**Rapporteur**
Pr. Sahmoudi Mohammed	**Faculté des sciences -Meknès**	**Examinateur**
Pr. Tamekkante Mohammed	**Faculté des sciences -Meknès**	**Examinateur**
Pr. E. CHARKANI Mohammed	**Faculté des sciences Dhar EL Mehraz-Fès**	**Invité**

Année universitaire : 2022-2023

On the normality of certain rational algebras

January 27, 2023

Acknowledgements

I would like to express my sincere gratitude to my thesis supervisors Mr. M. E. Charkani and Mr. Lhoussain El Fadil for their patience, enthusiasm, co-operations and suggestions made me present this research work to produce in the present form. Their brilliant, skillful supervision enriched this study higher than my expectation. This research work would not be possible without their stimulation inspiration and cooperation.

Thank you to my committee members, Pr. Mouanis Hakima, Pr. Chillali Abdelhakim, Pr. Ziane M'hammed and Pr. Kacha Ali. Your encouraging words and thoughtful, detailed feedback have been very important to me. Thank you to Pr. Sahmoudi Mohammed and Pr. Tamekkante Mohammed, examiners of this report, for all of the kind words and assistance you have provided. Thank you to my partner, Pr. Soullami Abderazak, for constantly listening to me rant and talk things out.

Further, yet importantly, sense of respect goes to my father , mother and my family for their strong support and regular encouragement in every step to make me in present stage. Similarly other relatives are also subjects to special thanks for their inspiration and cooperation in my study.

Résumé

Soient R un anneau de Dedekind et K son corps de fraction. Soient $L = K(\alpha)$ une extension finie séparable de K avec $\alpha \in O_L$ l'anneau des entiers de K. dans cette thèse nous utilisons l'application norme et la notion de polynômes pures, que nous généralisons à un anneau de valuation discrète arbitraire pour étudier les éléments d'une base intégrale de O_L, cela nous permet de donner une condition suffisante pour que $R[\alpha]$ ne soit pas intégralement clôs. Nous considérons également le problème d'existence d'une base triangulaire de O_L sur un anneau principal arbitraire tel que la suite de ses dénominateurs est suite factorielle et nous donnons plus de précision sur l'indice idéal et les coefficients dominants. Améliorant significativement un résultat dans cette direction par M. Hall pour les corps de nombres cubiques (1937) [30] qui est dérivé comme un cas particulier d'un résultat plus général prouvé ici. La preuve est basée sur une nouvelle version du théorème de structure bien connu des modules sur (PID). Plus précisément, nous exprimons explicitement l'indice idéal comme un produit de dénominateurs d'une base triangulaire monique et établissons ainsi une décomposition intéressante de l'indice sur (PID). Ensuite, nous étudions quelques conditions nécessaires et suffisantes pour l'existence d'une base intégrale d'extensions relatives en utilisant une version récente du critère de Dedekind, quelques exemples illustratifs sont donnés en utilisant le logiciel de calculMaple. Enfin, lorsque α satisfait le polynôme irréductible $P(X) = X^p - a$, on donne une formule explicite du discriminant $D_{L/K}$ de L sur K. A titre d'illustration, on calcule le discriminant $D_{L/K}$ d'une famille de corps purs septiques et quintiques sur des sous-corps quadratiques.

Abstract

Let R be a Dedekind ring and K its fraction field. Let L/K be a finite separable extension of K and let O_L denote the ring of the integral elements of K. Let $\alpha \in O_L$ be an algebraic integer over R such that $L = K(\alpha)$. in this thesis we use the map norm and the notion of hight isoline polynomials, which we extend to arbitrary discrete valuation ring to study the elements of an integral basis of O_L, this allows us to give a sufficient condition for $R[\alpha]$ to be not integrally closed. We also consider the problem of existence of triangular basis of O_L over arbitrary principal ideal domain such that the sequence of its denominators is a factorial sequence and we give more precision on ideal index and leading coefficients. Improving significantly a result in this direction by M. Hall for Cubic numbers fields (1937) [30] which is derived as a special case of a more general result proved here. The proof is based on a new version of the well-known structure Theorem of finitely generated modules over a (PID). More precisely, we express explicitly the ideal index as a product of denominators of a monic triangular basis and hence establish an interesting decomposition of the index over (PID). Then we investigate some necessary and sufficient conditions for the existence of power integral basis of relative extensions using a recent version of Dedekind criterion, some illustrative examples are given using Maple software. Finally, when α satisfies the monic irreducible polynomial $P(X) = X^p - a$ of prime degree , we give an explicit formula for the discriminant $D_{L/K}$ of L over K. As an illustration, we compute the discriminant $D_{L/K}$ of a family of septic and quintic pure fields over quadratic subfields.

Contents

Introduction **5**

1 Generality **10**
1.1 The υ-norm $\overline{\upsilon}$ . . . 10
1.2 The map υ^* . . . 12
1.3 The map $\upsilon^\star$ and the notion of isoline polynomials . . . 14
1.4 Factorization of polynomials via Newton polygons . . . 17
1.5 Hight isoline polynomials . . . 19
1.6 Extension of valuations . . . 24
1.6.1 Extension of valuation to finite extension . . . 25
1.6.2 Transcendental extension of valuation and generalized Ore's Theorem . . . 29

2 Triangular basis and index over Principal ideal domains **35**
2.1 Preliminaries . . . 35
2.1.1 Triangular family relative to a basis . . . 35
2.1.2 Modules over principal ideal domain . . . 35
2.2 Triangular basis over (PID) . . . 38
2.3 Factorial divisors of the Index over (PID) . . . 43
2.4 Applications . . . 44

3 On the normality of a monogenic algebra **47**
3.1 Definitions and some preliminary results . . . 47
3.2 Dedekind criterion . . . 48
3.2.1 Dedekind criterion over (DVR) . . . 49
3.2.2 Monogenicity of relative prime-power pure extensions . . . 51
3.3 Monogenicity of relative prime-power pure extensions-local case . . . 53
3.4 Monogenicity of relative prime-power pure extensions, Dedekind case . . . 55
3.5 Illustration . . . 56

3.5.1 Relative power integral basis of a family of number fields defined By $X^{p^n} + a\,X^{p^s} - b$ 60
3.6 Some preliminary results 61
3.7 Monogeneity of relative non-pure extension, local case 62
3.8 Monogeneity of relative non-pure extension, Dedekind case 64
3.9 Illustrations 65

4 On the Discriminant of some relative pure extensions 70
4.1 Introduction 70
4.2 Preliminary results 71
4.3 Proof of Theorem 4.1.1 73
4.4 Illustration 75
4.4.1 Relative pure septic extension 75
4.4.2 Relative pure quintic extension 76

Notations

Symbols	Descriptions
$\mathbb{N}$	natural numbers set.
$\mathbb{Z}$	integer numbers set.
$\mathbb{Q}$	rational numbers set.
$\mathbb{Q}_p$	the field of p-adic number.
$\cap$	intersection symbol .
R	commutative unitary ring or a Dedekind ring.
$R[X]$	the set of all polynomials with coefficients in R.
$Fr(R)$	fraction field of R.
K	number field .
k_υ	the residue field of a valuation υ.
O_K	the ring of integers of K.
$M_n(R)$	set $n \times n$ matrices with entries in R.
$\mathcal{W}$	the set of valuations extending a valution υ.
G_υ	the value group of a valuation υ.
$Z(P)$	the set of all root of a polynomial P.
υ_G	the Gaussian valution of the field $K(x)$.
$\widehat{K}$	the completion of K.
K_υ	the separable closure of K in $\widehat{K}$.
K^h	the henselization of K.
$\overline{K}$	the algebraic closure of K.
$Ind_R(\alpha)$	the index ideal of α.
$disc_R(P)$	the discriminant of a polynomial P.
$N_{L/K}(x)$	the norm of an element x of L over K.
$G(M/N)$	set of R-automorphisms of M.
$\oplus_{i=1}^n M_i$	direct sum of M_i.
$\otimes_{i=1}^n M_i$	tensor product M_i.
$det(A)$	determinant of the matrix A.
$\prod_{i=1}^n a_i$	product of the elements a_i
$Res(f(X), g(X))$	resultant of the polynomials $f(X)$ and $g(X)$.
$a\|b$	a divides b.
$gcd(a, b) = d$	d is the gcd of a and b.
$Gal(L/K)$	the galois group of L over K.
$Tr_{L/K}(x)$	the trace of an element x of L over K.

$D_{L/K}$	the relative discriminant ideal of L over K.
$N_g^{\upsilon_G}$	the g-Newton polygon of P with respect to υ_G.
$N_{\mathfrak{p}}$	the cardinality of the residual field $R/\mathfrak{p}$.
S_p	the set of prime $\mathfrak{p}$ such that $\mathfrak{p}^2$ divides $disc_R(P)$.
$Fib_R(p)$	the set of all non zero primes ideals in R lie above p.
$\delta_{i,j}$	the Kronecker Symbol.
$[x]$	the largest integer not exceeding x.

Introduction

The problems of existence and construction of integral bases (or normalization) is a fundamental problem in number theory, commutative algebra and algebraic geometry, and is related to the computation of the discriminant and the ideal index which are two intimately connected problems in in algebraic number theory. Several number theorists were interested in and attracted by this problem (see [5, 4, 13, 14, 53, 64]). Especially for the problem of computing triangular bases of integral closures, H. D. Stainsby [64] constructs a reduced triangular basis of integral closures of one-dimensional local rings using a simple procedure to find some polynomials $g_i \in R[x]$ of degree i with maximal valuation amongst all monic polynomials in $R[x]$ of the same degree called optimal polynomials and hence the global triangular basis is obtained by the patching process based on the Chinese remainder theorem. When R is a principal ideal domain (PID), L/K is a finite separable extension of degree n over K and O_L denote the ring of the integral elements of K. We are interested in the existence of a triangular integral basis of L over K, in other word an integral basis $\mathcal{B} = \{x_1, x_2, ...x_n\}$ of O_L such that $x_1 = 1$ and $x_i = \frac{g_i(\alpha)}{\lambda_i}$ such that for all $2 \leq i \leq n$ the polynomial $g_i \in R[X]$ is monic of degree $i-1$ and $\lambda_i \in R$. Early in 1937, M. Hall gives a nice decomposition of the ideal index of cubic fields (see [30]). we generalized the Hall's Result for cubic fields to arbitrary extension of a fraction field of principal ideal domain. More precisely we express explicitly the ideal index as a product of denominators of a monic triangular basis and hence establish an interesting decomposition of the index over (PID). Some useful examples are also given.

The question of the existence of a power basis was originally examined by Dedekind [17]. Many number theorists were also attracted by this problem and noticed the advantages of working with monogenic number fields. It is called a problem of Hasse to characterize whether the ring of integers in an algebraic number field has a power integral basis or does not. In this thesis we deal with the analogous problem for arbitrary Dedekind domains. Let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n and let O_L denote the ring of the integral elements of K. We say that L/K is *monogenic* if L possess a relative *monogenic* integral basis (RMIB for short), or equivalently, $\{1, \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$ is an integral

basis of L/K for some α in O_L, in other words $O_L = R[\alpha]$ (In this one may say that α is monogenic or equivalently the irreducible polynomial of α is monogenic). Indeed, testing whether L/K has a RMIB is a hard open problem, worse still, we don't even know if the integral closure O_L of R in L is necessarily a free R-module despite that every fractional ideals of L is finitely generated and torsion-free R-module.

In the following, we recall some of the most important works carried out in this context:

For cubic relative extension, [65] give relative integral basis (RIB) for L/K when L is a normal closure of K. This (RIB) simplifies and completes the one given by [27] (1986). For quartic extension L with quadratic subfield K. The authors of [62] give a necessary and sufficient condition for L to have a relative integral basis (RIB) over K and an explicit relative integral basis when it exists. For relative extensions of degree greater than 4 there is few results on relative integral basis and almost published works deal with decomposable extensions (which are composite of two pure subfields). There is no known work for relative abelian indecomposable extension L/K of higher degree (i.e., which is not a composite at last of two " pure" subfields).

Examples of quadratic extensions of imaginary quadratic number fields for which there exists no relative integral basis and by using a theorem of Artin were given by [25, 46]. Washington [67] gives necessary and sufficient conditions for certain quadratic extensions of imaginary quadratic fields to have relative integral bases. Here after, [9, 56], studies monogeneity in general quadratic cases.

Recently H.Smith [60] gives necessary and sufficient conditions for a radical extension $K(\sqrt[n]{\alpha})$ to be monogenic over L where L is a number field, he also gives sufficient conditions for a Kummer extension of the form $\mathbb{Q}(\zeta, \sqrt[n]{\alpha})$ to be non-monogenic over $\mathbb{Q}$ and establishes a general criterion relating ramification and relative monogeneity. For relative cubic-power pure extensions L the authors of [58] gives a necessary and sufficient conditions to study the monogeneity of $L = K(\sqrt[p^3]{\alpha})$ over K , where K is a number field and construct an integral basis of a family of number field of degree equal to 2.3^n for a positive integer n. In [61] we studied the relative monogeneity of a family of number field arising from some Trinomials and construct an integral basis for a family of extension $L/\mathbb{Q}$, such that $[L : \mathbb{Q}] = 2.3^n$ $(n \in \mathbb{N}^*)$.

This thesis is organized as follows:

In chapter 1 we recall some well known results on v-norm and and its relationship with prolongation of valuation to a finite separable extension of a valued field (K, v), this allows us to give a nice cracterization of the element of O_L the integral closure of L in R when R is a discrete valuation

ring. We also use the maps υ^* appeared in 1978 in the Thèse d'Etat of Ford ([22]) and also in series of papers (see [21, 23, 29]) to study the notion of isoline polynomials which play a crucial role in different domains, for example in the computation of integral closure over a discrete valuation ring, called polynomials satisfied the υ^*-test ([28]). Or in the study of irreducibility over $\mathbb{Q}_p$ ([23]). More recently, the notion of hight isoline polynomials appeared in the work of K. Khanduja and M. Kumar in series of papers ([38, 41, 40]), For example, when υ is a valuation of arbitrary rank of a field K and $L = K(\alpha)$ is a finite extension of K, where $\alpha \in O_L$ the integral closure of the valuation ring R of υ in L, the authors of [38] used this polynomials to describe all the extensions w of υ to L. More precisely, Let $\overline{P} = \overline{g}_1^{e_1}.....\overline{g}_r^{e_r}$ be the factorization of P the minimal polynomials of α over K into a product of powers of distinct monic irreducible polynomials over R/m the residue field of υ, where $\overline{P}$ the polynomial over k obtained on replacing each coefficient of P by its residue modulo m. Then its was shown in [38] that when P is g_i-hight isoline (see Definition 1.5.1), and the order of $\upsilon^*_{g_i}(P)$ modulo the value group of υ is l_i for any $1 \leq i \leq r$, then there exist exactly r prolongation of υ to L (see [38], Theorem 1.1). Among other things, A. Deajim and El. Fadil used also this notion, called polynomials satisfies the (Hyp λ) to a give a improvement of the result of K. Khanduja and K. Kumar in the context of number fields ([16]). Then we define the maps υ^*_g where g is monic polynomial belonging to $R[X]$. It may pointed out that the maps υ^*_g coincide with the maps υ^* defined in ([21, 23, 29]) when $g(X) = X$ and $\upsilon_{\overline{X}}(\overline{P}) = \deg P$. In Section 1.3 we introduce the notion of isoline polynomials and we give some background information about this notion. In particular we prove that the polynomial P is isoline if and only if $\overline{v}(\alpha_i) = \overline{v}(\alpha_j)$ for any i, j, where $\alpha_1, \alpha_2, ...\alpha_n$ are the roots of P in some fixed algebraic closure $\overline{K}$ of K and $\overline{v}$ is a fixed prolongation of the valuation υ defined on K to $\overline{K}$. In Section 1.5 we extend the notion of isoline polynomials defined in Section 1.3 to g-hight isoline polynomials over discrete valued fields and prove similar results Generalizing some classical results for algebraic number fields. In particular when L is a finite separable extension of K of degree n and α is a primitive element of L which is integral over R. We use the map υ^*_g below to give a sufficient condition for $R[\alpha]$ to be not integrally closed.

In chapter 2, we show the existence of a global triangular integral basis $\mathcal{B} = \{x_1, x_2, ..., x_n\}$ of O_L such that $x_1 = 1$ and $x_{i+1} = \frac{g_i(\alpha)}{\lambda_i}$ where the polynomials $g_i \in R_i[X]$ are monic of degree i and the sequence of its denominators $(\lambda_k)_{1 \leq k \leq n-1} \in R$ is a factorial sequence (i.e., $\lambda_k \lambda_l$ divides λ_{k+l} for any index k, l such that $k + l < n$, in other words, if where υ_p is the p-adic discrete valuation associated to the non zero prime ideal $\mathfrak{p} = pR$ then the function $k \to \upsilon_p(\lambda_k)$ is superlative, see [36] and [55]). This result allows us to give a nice and explicit decomposition of the index ideal of $R[\alpha]$ in O_L obtained from certain triangular integral basis of L over K.

Our description of triangular integral basis is new and different and uses only module theoretical considerations. More precisely our approach gives more precisions on index ideal and

leading coefficients. It involves standard techniques with modules over a PID. In Section 4.2, after introducing some concepts and notations relevant to the work, we will deal with the above problem in a more general situation, when M is a free R-module of finite rank $n \geq 2$ and N is a free submodule of M of finite rank $m = n$. Then we prove that there exists a triangular basis $\mathcal{B}' = \{x_1, ..., x_n\}$ of N relative to $\mathcal{B}$ (see Theorem 2.1.3), which gives yet a better generalization of the well-known structure theorem of finitely generated modules over a PID when $\mathrm{rk}_R M = \mathrm{rk}_R N$ (see [[59] Theorem 1 p.26]). This allows us to prove Theorem 2.2.1 which ensures that there exists a triangular integral basis $\mathcal{B} = \{1, \frac{g_1(\alpha)}{\lambda_1}, \frac{g_2(\alpha)}{\lambda_2}, \cdots, \frac{g_{n-1}(\alpha)}{\lambda_{n-1}}\}$ of O_L over R such that $(\lambda_k)_{1 \leq k \leq n-1}$ is a factorial sequence (i.e., $\lambda_k \lambda_l$ divides λ_{k+l} for any index k, l such that $k + l < n$). Moreover using the divisibility relation among the denominators of the elements of $\mathcal{B}$ we prove in Section 3 that there exists a unique (mod Units) sequence $(k_1, k_2, ..., k_{n-1})$ of elements of R such that $\mathrm{Ind}_R(\alpha) = \left(k_1 k_2^2 ... k_{n-3}^{n-3} k_{n-2}^{n-2} k_{n-1}^{\frac{n(n-1)}{2}}\right) R$ which extends the result of M. Hall for cubic numbers (see [30]) to the case when $L = K(\alpha)$ is a finite relative algebraic extension of K of degree n and R is a principal ideal domain (see Remark 2.3.1). In Section 4, we use our main result in context of pure number fields to show that we can also read off the index ideal only from the Ascending Power Decomposition (APD) of α^p where where α is a root of an irreducible polynomial $P(X) = X^p - a$ belonging to $\mathbb{Z}[X]$.

In chapter 3, we address our attention to problem of monogenity. We investigate some necessary and sufficient conditions for the existence of power integral basis of relative extensions using recent version of dedekind criterion, some illustrative examples are given using Maple software. More precisely, let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n and let O_L denote the ring of the integral elements of K. Let $disc_R(P)$ denotes the discriminant of the polynomial $P(X)$ and $D_{L/K}$ denotes the discriminant of the number field L over K. The purpose of this chapter is the study the relative monogeneity of $L = K(\alpha)$ over its subfield where α is a root of a monic irreducible polynomial of the forms

$$P(X) = X^{p^n} - \beta \in O_K[X], \ n \in \mathbb{N}^*. \tag{1}$$

And

$$P(X) = X^{p^n} + a\, X^{p^s} - b \in O_K[X], \ with\ n > s\ and\ (n, s) \in \mathbb{N}^2. \tag{2}$$

This allow to construct an integral basis for a family of extensions $L/\mathbb{Q}$, such that $[L : \mathbb{Q}] = 2.p^n$ ($n \in \mathbb{N}^*$). As a consequence, we compute the discriminant $D_{L/\mathbb{Q}}$ using the tower-discriminant formula:

$$D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K})\,(D_{K/\mathbb{Q}})^{[L:K]}, \tag{3}$$

where $N_{K/\mathbb{Q}}$ denote the norm from K to $\mathbb{Q}$ (see [50, Corollary 10. 2] and [24]).

Another crucial topic is to search the discriminant of the ring of integral elements in a field wich is in general a difficult task. In 2010 Del Corso and Rossi [15] provided a formula for the discriminant of Kummer cyclic extension of number fields. For pure algebraic number fields Jakhar and Khanduja [32] gave a formula for the discriminant of pure number fields having square free degree. In 2020 the authors of [33] gave a formula for the discriminant of n-th degree fields of the type $\mathbb{Q}(\sqrt[n]{a})$ using Newton polygon techniques. Let L be a relative pure extension, in other word an algebraic field of the type $L = K(\sqrt[p]{a})$, where K is an algebraic number field and the polynomial $X^p - a$ of prime degree belonging to $K[X]$ is irreducible over the field K. In chapter 4, our aim is to give an explicit formula for the discriminant $d_{L/K}$ of O_L the ring of integer of L in terms of the set of primes $\mathfrak{p}$ in O_K (denoted by $Spec(O_K)$) with $p = \mathfrak{p} \cap O_K$ and such that $aO_K \subseteq \mathfrak{p}$. As a consequence, using the tower formula stated below (4.2), we compute the discriminant $d_{L/\mathbb{Q}}$ for two family of septic and quintic pure fields L, such that $[L, \mathbb{Q}] = 10$ and $[L, \mathbb{Q}] = 14$ respectively.

Chapter 1

Generality

1.1 The υ-norm $\overline{\upsilon}$

Let $(K,\ \upsilon)$ be a valued field with υ a real valuation, R the ring of valuation of υ, m the maximal ideal and $k_\upsilon = R/m$ the residue field of υ. Let L be a finite separable extension of K of degree n and $\alpha \in\ L$. Let $\overline{K}$ be a fixed algebraic closure of the field K and $\widetilde{\upsilon}$ is a fixed prolongation of the valuation υ defined on K to $\overline{K}$. We denote by $\mathcal{W}$ the set of valuations of L extending υ.

Definition 1.1.1. *A υ-norm on L is a mapping $w:\ L \longrightarrow\ \mathbb{Q} \cup \{\infty\}$ that satisfies:*

1. $w(x+y) \geq \min(w(x), w(y)), \forall x, y \in L$.
2. $w(ax) = \upsilon(a) + w(x)$, *for all* $a \in\ K$ *and* $x \in\ L$.
3. $w(x) = \infty$ *if and only if* $x = 0$.

In other words, a υ-norm is an extension of the valuation υ to L having all properties of a valuation except the product law.

Proposition 1.1.1. *With the above assumptions and notations. Let $x \in L$. The application $\overline{\upsilon}$ defined on L by :*

$$\overline{\upsilon}(x)\ =\ min\{w(x), w \in \mathcal{W}\}$$

is a υ-norm on L.

Proof.

Let $x \in L$, it is clear that $\overline{\upsilon}(x) = \infty$ if and only if $x = 0$. Let $x, y \in L$, we prove first that $\overline{\upsilon}(x+y) \geq \min(\overline{\upsilon}(x), \overline{\upsilon}(y))$. Assume that $\overline{\upsilon}(x) \leq \overline{\upsilon}(y)$, then by the definition of $\overline{\upsilon}$ we have $\overline{\upsilon}(x) \leq w(y)$ for any $w \in \mathcal{W}$. Let $w_M \in \mathcal{W}$ such that

$$min\{w(x+y), w \in \mathcal{W}\} = w_M(x+y).$$

Hence $\overline{v}(x+y) = min\{w(x+y), w \in \mathcal{W}\} = w_M(x+y) \geq min(w_M(x), w_M(y) \geq \overline{v}(x) = min(\overline{v}(x), \overline{v}(y))$. Similarly, by the same way we can prove the triangle law for $\overline{v}$ when $\overline{v}(y) \leq \overline{v}(x)$. On the other hand we have $\overline{v}(xy) = min\{w(xy), w \in \mathcal{W}\} = w_{M'}(xy) = w_{M'}(x) + w_{M'}(y) \geq \overline{v}(x) + \overline{v}(y)$, which prove the product law for $\overline{v}$, in particular $\overline{v}(ax) \geq \upsilon(a) + \overline{v}(x)$, for all $a \in K$ and $x \in L$, so the proposition is proved as soon as we show that $\overline{v}(ax) \leq \upsilon(a) + \overline{v}(x)$. Observe that $\overline{v}(ax) \leq w(ax) = w(a) + w(x)$, $\forall w \in \mathcal{W}$ and hence $\overline{v}(ax) \leq \upsilon(a) + w(x)$, $\forall w \in \mathcal{W}$, this prove that $\overline{v}(ax) \leq \upsilon(a) + \overline{v}(x)$. ∎

Remark 1.1.1. *By the proof of the above proposition we see that application $\overline{v}$ is a semi-valuation on L (for more detail see [[29], p.219]).*

Corollary 1.1.1. *Let $(R, \pi R, k)$ be a discrete valuation ring, π a uniformizer of R, $\mathfrak{p} = \pi R$ the prime ideal of R. Let K be the quotient field of R, L a finite separable extension of K of degree n. Let O_L be its ring of integers and $x, y \in L$. Then*

1. *$\overline{v}(x^k) = k\overline{v}(x)$ for every $k \in \mathbb{N}$.*
2. *$\overline{v}(x+y) = min(\overline{v}(x), \overline{v}(y))$ when $\overline{v}(x) \neq \overline{v}(y)$.*
3. *$O_L = \{x \in L \mid \overline{v}(x) \geq 0\}$.*

Proof. Let $k \in \mathbb{N}$ and $x \in L$. In view of proposition 1.1.1 we have $\overline{v}(x^k) \geq k\overline{v}(x)$. Now using the fact that $\overline{v}(x^k) \leq w(x^k)$ for any prolongment w of $\upsilon_{\mathfrak{p}}$ to L, we see that

$\forall w \in \mathcal{W}$, $\overline{v}(x^k) \leq kw(x)$.

Consequently $\overline{v}(x^k) \leq k\overline{v}(x)$. Let $x, y \in L$ such that $\overline{v}(x) \neq \overline{v}(y)$. Assume for example that $\overline{v}(x) < \overline{v}(y)$, then by virtue of proposition 1.1.1 we see that $\overline{v}(x) \leq \overline{v}(x+y)$. It remains to be shown that $\overline{v}(x) \geq \overline{v}(x+y)$, as $\overline{v}(x) < \overline{v}(y)$ we see immediately $\overline{v}(x) = \overline{v}(x+y-y) \geq \min(\overline{v}(x+y), \overline{v}(y)) = \overline{v}(x+y)$. To show (3), it is enough to use the fact that $O_L = \cap_{w \in \mathcal{W}} R_w$. ∎

Proposition 1.1.2. *With notations as in Corollary 1.1.1. Let $\overline{v}$ be the semi-valuation defined above and let $\mathcal{B} = \{x_1, x_2, ..., x_n\}$ be a basis of O_L over R, then $\overline{v}(x_i) < 1$ for any index i.*

Proof. Suppose to the contrary that exist i such that $\overline{v}(x_i) \geqslant 1$. Set $[\overline{v}(x_i)] = s$ and $\lambda = \pi^s$. Observe that $\overline{v}(\frac{x_i}{\lambda}) = \overline{v}(x_i) - s \geq 0$ and using the fact that $O_L = \{\alpha \in L \mid \overline{v}(\alpha) \geq 0\}$, we conclude immediately that $\frac{x_i}{\lambda} \in O_L$. Write

$$\frac{x_i}{\lambda} = \sum_{j=1}^{n} a_j x_j,$$

where $a_1, ...a_n \in R$, it follows that $a_j\lambda = 0$ for $j \neq i$ and $a_i\lambda = 1$. This contradiction complete the proof of Lemma 1.1.2. ∎

Proposition 1.1.3. *With the above assumptions and notations. Let $x \in L$ such that $\overline{v}(x) = w(x)$ for any $w \in \mathcal{W}$. Then $\overline{v}(xy) = \overline{v}(x) + \overline{v}(y)$ for any $y \in L$.*

Proof. In view of the Proposition 1.1.1 the Proposition 1.1.3 is proved once we show that $\overline{v}(xy) \leq \overline{v}(x) + \overline{v}(y)$. Let $y \in L$ and assume that $\overline{v}(y) = w(y)$ where $w \in \mathcal{W}$. Using the hypothesis and the definition of $\overline{v}$, we see that $\overline{v}(xy) \leq w(xy) = w(x) + w(\beta) = \overline{v}(x) + w(\beta)$ for any $w \in \mathcal{W}$. It follows that $\overline{v}(xy) \leq \overline{v}(x) + \overline{v}(y)$ as desired. ∎

Proposition 1.1.4. *With the above assumptions and notations. Let P be the minimal irreducible polynomial of α over K. Le v be an extension of v to $\overline{K}$. Let $\alpha_1, \alpha_2, ...\alpha_n$ be the roots of P in $\overline{K}$ of K. Then*

$$\overline{v}(\alpha) = \min\{v(\alpha_i)\, 1 \leq i \leq n\}$$

Proof. (See [[28], Chapter 4, p.79]))

1.2 The map v^*

Definition 1.2.1. *Let $P = a_0 + a_1X + a_2X^2 + ...+ a_{n-1}X^{n-1} + a_nX^n \in K[X]$ be a polynomial over K. Then we define the v^*-semi valuation of P by :*

$$v^*(P) = min\left\{\frac{v(a_i)}{n-i},\ |\ 0 \leq i \leq n-1 \ \text{and}\ a_i \neq 0\right\} + v(a_n).$$

If the polynomial $P = a \in K^*$ is a constant polynomial then we put $v^*(P) = v(a)$. Note that if P is monic then $v^*(P)$ is the slope of the initial segment of the Newton polygon of P.

Let $\overline{P}$ the image of P in $k_v[X]$. If P is monic and $v^*(P) > 0$ then $\overline{P} = \overline{X}^n$ and hence P is an Eisenstein polynomial.

The following lemma which is an immediate consequence of a well known result (see [28]). For the sake of reader's convenience, it is proved here.

Lemma 1.2.1. *Let $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ be a polynomial in $R[X]$ such that $v_{\overline{X}}(\overline{P}) = \deg P$. Let $\alpha_1, \alpha_2, ...\alpha_n$ be the roots of P in some fixed algebraic closure $\overline{K}$ of K and $\overline{v}$ is a fixed prolongation of v to $\overline{K}$. Then*

$$v^*(P) = \min\{\overline{v}(\alpha_j) \mid 1 \leq j \leq n\}.$$

Proof. Let $\alpha \in \overline{K}$ be a root of P, we show first that $\overline{v}(\alpha) \geqslant v^*(P)$. Suppose to the contrary that $\overline{v}(\alpha) < v^*(P)$. Hence for $0 \leqslant i \leqslant n-1$, we have $\overline{v}(a_i) = v(a_i) > \overline{v}(\alpha)(n-i)$, and consequentely

$$\overline{v}(a_i\alpha^i) = \overline{v}(a_i) + i\overline{v}(\alpha^i) > \overline{v}(\alpha)(n-i) + i\overline{v}(\alpha) = \overline{v}(\alpha^n).$$

We conclude that $\overline{v}(\alpha^n) = \overline{v}\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) \geqslant \min_{0\leqslant i\leqslant n-1} \overline{v}(a_i\alpha^i) > \overline{v}(\alpha^n)$. This contradiction proves the desired inequality.

Set $\overline{v}(\alpha_{j_0}) = \min\{\overline{v}(\alpha_j) \mid 1 \leq j \leq n\}$. Conversely using the symmetric formulas relating the roots and coefficients of P we prove that $v(a_i) \geq (n-i)\overline{v}(\alpha_{j_0})$ for $0 \leq i \leq n-1$. For simplicity of notation, we prove it for $i = 1$. By the same argument above a_1 can be expressed as (see proposition 1.4.1) p.15)

$$a_1 = (-1)^{n-1} \sum_{i=1}^{n} \prod_{i\neq j} \alpha_j$$

Consequently

$$v(a_1) = \overline{v}\left((-1)^{n-1} \sum_{i=1}^{n} \prod_{i\neq j} \alpha_j\right) \geq \min_{1\leq i\leq n}\left\{\overline{v}\left(\prod_{i\neq j}\alpha_j\right)\right\} = \min_{1\leq i\leq n}\left\{\left(\sum_{i\neq j}\overline{v}(\alpha_j)\right)\right\}.$$

Hence the lemma follows from the above inequality and the definition of $v^*(P)$. ∎

Proposition 1.2.1. *With the above assumptions and notations. Let $\alpha \in L$ and P its minimal irreducible polynomial over K. Then*

$$\overline{v}(\alpha) = v^*(P)$$

Proof. Use Lemma 1.2.1+ Proposition 1.1.4. ∎

For P a polynomial over K and $\lambda \in K^* = K - \{0\}$. We consider the transformation $\widetilde{\lambda}(P) := \frac{1}{\lambda^n}P(\lambda X)$ where $n = deg\, P$. Observe that when P is the minimal irreducible polynomial of α over K, then $\widetilde{\lambda}(P)$ is the minimal irreducible polynomial of $\frac{\alpha}{\lambda}$ over K.

With the above notations, we prove

Proposition 1.2.2. *Let (K, v) be a valued field with v a real valuation, R the ring of the valuation v. Let P be a polynomial over K. Then $v^*(\widetilde{\lambda}(P)) = v^*(P) - v(\lambda)$. If P is monic then $\widetilde{\lambda}(P) \in R[X]$ if and only if $v(\lambda) \leq v^*(P)$.*

Proof. Assume that $P = \sum_{i=0}^{n} a_i X^i$, then $\widetilde{\lambda}(P) = \sum_{i=0}^{n} a_i\lambda^{i-n}X^i$. As $\frac{v(a_i\lambda^{i-n})}{n-i} = \frac{v(a_i)}{n-i} - v(\lambda)$, the desired equality follows directly from the definition of $v^*(P)$. Now suppose that P is monic, then $\widetilde{\lambda}(P) \in R[X]$ if and only if $v(a_i\lambda^{i-n}) \geq 0$ if and only if $v(a_i) \geq (n-i)v(\lambda)$ if and only if $v(\lambda) \leq v^*(P)$ as desired. ∎

Corollary 1.2.1. *Let $(R, \pi R, k)$ be a discrete valuation ring, π a uniformizer of R, $\mathfrak{p} = \pi R$ the prime ideal of R. Let K be the quotient field of R, L a finite separable extension of K of degree n. Let O_L be its ring of integers and $\alpha \in O_L$. Then*

$$[\overline{v}(\alpha)] = max\{s \in \mathbb{N} \mid \frac{\alpha}{\pi^s} \in O_L\}.$$

Proof. Let $s \in \mathbb{N}$. It is clear that $\frac{\alpha}{\pi^s} \in O_L$ if only if $\widetilde{\lambda}(P) \in R[X]$, which hold by Proposition 1.2.1 if and only if $\overline{v}(\alpha) \geq s$, it follows that $max\{s \in \mathbb{N} \mid \frac{\alpha}{\pi^s} \in O_L\} = [\overline{v}(\alpha)]$ as desired. ∎

1.3 The map $\upsilon^\star$ and the notion of isoline polynomials

Throughout this section, unless specifically stated otherwise, let (K, υ) be a valued field with υ a rank-one discrete valuation, R the ring of valuation of υ, m the maximal ideal, and $k_\upsilon = R/m$ the residue field of υ. $\overline{\upsilon}$ will stand for a fixed prolongation of the valuation υ defined on K to an algebraic closure $\overline{K}$ of K.

Definition 1.3.1. *Let $P = a_0 + a_1X + a_2X^2 + ... + a_{n-1}X^{n-1} + X^n \in R[X]$ be a monic polynomial and set $l = \min\{0 \leqslant i \leqslant n \mid \upsilon(a_i) = 0\}$. We may denote $\min\limits_{0 \leq i \leq l-1} \left\{\frac{\upsilon(a_i)}{l-i}\right\}$ by $\upsilon^*(P)$ and we say that the polynomial P is isoline if $\upsilon_g^*(P) = \dfrac{\upsilon(a_0)}{l}$.*

Proposition 1.3.1. *Let $P = X^l + a_{l-1}X^{l-1} + ... + a_0$ and $Q = X^s + b_{s-1}X^{s-1} + ... + b_0$ two polynomials in $R[X]$ such that $\upsilon_{\overline{X}}(\overline{P}) = l$, $\upsilon_{\overline{X}}(\overline{Q}) = s$ and $\upsilon^*(P) = \upsilon^*(Q)$, then the product PQ is isoline if and only if the polynomials P and Q are isolines.*

Proof. Suppose that the polynomials P and Q are isolines and $\upsilon^*(P) = \upsilon^*(Q)$. The expansion of the product PQ in $R[X]$ is given by $PQ = \sum\limits_{i=0}^{l+s} c_iX^i$. Now using the fact that $\upsilon_{\overline{X}}(\overline{P}) = l$ and $\upsilon_{\overline{X}}(\overline{Q}) = s$, we see immediatly that $\upsilon_{\overline{X}}(PQ) = l + s$ and $c_0 = a_0b_0$. Therefore $\upsilon(c_0) = \upsilon(a_0) + \upsilon(b_0) = (l + s)\upsilon^*(P)$, hence $\upsilon^*(P) = \frac{\upsilon(c_0)}{l+s}$. Now to prove that PQ is isoline, it enough to show that

$$\upsilon^*(PQ) = \upsilon^*(P).$$

Observe that if $i > l$ then $a_i = 0$ and hence $\upsilon(a_i) = \infty$ in this case. consequently for $0 \leq i \leq l+s-1$ we have $c_i = \sum_{k=0}^{i} a_k b_{i-k}$, it follows that

$$\begin{aligned} \upsilon(c_i) = \upsilon\left(\sum_{k=0}^{i} a_k b_{i-k}\right) &\geqslant \min_{0\leqslant k\leqslant i}(\upsilon(a_k b_{i-k})) \\ &\geqslant \min_{0\leqslant k\leqslant i}((l-k)\upsilon^*(P) + (s-i+k)\upsilon^*(P)) \\ &\geqslant \upsilon^*(P)(l+s-i). \end{aligned}$$

Consequently $\frac{\upsilon(c_i)}{l+s-i} \geqslant \upsilon^*(P) = \frac{\upsilon(c_0)}{l+s}$ and PQ is isoline as desired.

Conversely suppose that PQ is isoline. We show first that

$$\upsilon^*(PQ) = \upsilon^*(P) = \upsilon^*(Q).$$

Let $i_0 = \min_{0\leqslant i\leqslant l-1}\{\upsilon(a_i) = (l-i)\upsilon^*(P)\}$ and $j_0 = \min_{0\leqslant j\leqslant s-1}\{\upsilon(b_j) = (s-j)\upsilon^*(Q)\}$. Consider $c_{i_0+j_0} = a_0 b_{i_0+j_0} + ... + a_{i_0} b_{j_0} + ... + a_{i_0+j_0} b_0$. Note that for any $(i,j) \neq (i_0, j_0)$ such that $i + j = i_0 + j_0$ we have $i < i_0$ or $j < j_0$, then it follows that for any i, j

$$\upsilon(a_i b_j) = \upsilon(a_i) + \upsilon(b_j) > (l-i)\upsilon^*(P) + (s-j)\upsilon^*(P).$$

Now using the fact that $i + j = i_0 + j_0$, we see immediyatly that

$$\upsilon(a_i b_j) > \upsilon(a_{i_0}) + \upsilon(b_{j_0}) = \upsilon(a_{i_0} b_{j_0}).$$

We conclude that $\upsilon(c_{i_0+j_0}) = \upsilon(a_{i_0} b_{j_0}) = (l-i_0)\upsilon^*(P) + (s-j_0)\upsilon^*(P) = (l+s-(i_0+j_0))\upsilon^*(P)$. Using the hypothesis that PQ is an isoline polynomial we see that $\upsilon(c_{i_0+j_0}) \geqslant (l+s-(i_0+j_0))\upsilon^*(PQ)$, consequently $\upsilon^*(PQ) \leqslant \upsilon^*(P)$. Now Using hypothesis and the definition of υ^* we see that

$$(l+s)\upsilon^*(PQ) = \upsilon(c_0) = \upsilon(a_0) + \upsilon(b_0) \geqslant l\upsilon^*(P) + s\upsilon^*(Q) = (l+s)\upsilon^*(P),$$

which proves the desired equality.

In view of the fact that $\upsilon(a_0) + \upsilon(b_0) = \upsilon(c_0) = (l+s)\upsilon^*(PQ) = l\upsilon^*(P) + s\upsilon^*(Q)$ and since $\upsilon(a_0) \geqslant l\upsilon^*(P)$ and $\upsilon(b_0) \geqslant s\upsilon^*(Q)$. We conclude that $\upsilon(a_0) = l\upsilon^*(P)$ and $\upsilon(b_0) = s\upsilon^*(Q)$ which prove that the polynomials P and Q are isolines as desired. ∎

Proposition 1.3.2. *Let $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ and $Q = X^m + b_{m-1}X^{m-1} + ... + b_0$ in $R[X]$ two polynomials such that $\upsilon(b_0) = 0$, then P is an isoline polynomial if and only if PQ is*

isoline.

Proof. Suppose first that P is isoline. We show that PQ is isoline. Observe that since $v(b_0) = 0$, then $v_{\overline{X}}(\overline{Q}) = 0$ and hence $v_{\overline{X}}(\overline{PQ}) = v_{\overline{X}}(\overline{P}) = l$. Let $PQ = \sum_{i=0}^{n+m} c_i X^{n+m}$ be the expansion of the product PQ in $R[X]$. So it remains to be shown that

$$v^*(PQ) = \frac{v(c_0)}{l}.$$

For $1 \leq i \leq l-1$, we see that
$v(c_i) = v\left(\sum_{k=0}^{i} a_k b_{i-k}\right) \geqslant \min_{0\leqslant k\leqslant i}\{v(a_k b_{i-k}) \geqslant \min_{0\leqslant k\leqslant i}\{v(a_k)\} \geqslant \min_{0\leqslant k\leqslant i}\{v^*(P)(l-k)\}$ and since $\min_{0\leqslant k\leqslant i}\{v^*(P)(l-k)\} = v^*(P)(l-i)$, we conclude that $v(c_i) \geqslant v^*(P)(l-i)$. Using the hypothesis that $v(b_0) = 0$, it follows that for $0 \leqslant i \leqslant l-1$

$$v^*(PQ) = \frac{v(c_i)}{l-i} \geqslant v^*(P) = \frac{v(a_0)}{l} = \frac{v(c_0)}{l}.$$

Conversely assume that the polynomial PQ is isoline, we show that $v^*(P) = \frac{v(a_0)}{l}$. Suppose to the contrary that $v^*(P) < \frac{v(a_0)}{l}$ and let i_0 the minimum index such that $\frac{v(a_{i_0})}{l-i_0} < \frac{v(a_0)}{l}$. Consider $c_{i_0} = \sum_{i=0}^{i_0} a_i b_{i_0-i} = a_{i_0}b_0 + \sum_{i=0}^{i_0-1} a_i b_{i_0-i}$ and keeping in mind that $v(b_0) = 0$, then we see that for $i < i_0$

$$v(a_i b_{i_0-i}) \geqslant v(a_i) \geqslant (l-i)\frac{v(a_0)}{l} > (l-i_0)\frac{v(a_0)}{l} > v(a_{i_0}b_0).$$

It follows that $v(c_{i_0}) = v(a_{i_0}b_0) < (\frac{v(a_0)}{l})(l-i_0)$, consequently $\frac{v(c_{i_0})}{l-i_0} < \frac{v(a_0)}{l}$, which prove that $v^*(PQ) = \frac{v(c_0)}{l} \leqslant \frac{v(c_{i_0})}{l-i_0} < \frac{v(a_0)}{l}$. Moreover we have $v(a_0) = v(c_0)$. This contradiction proves that $v^*(P) = \frac{v(a_0)}{l}$ and hence the proposition. ∎

Proposition 1.3.3. *Let $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ be a polynomial in $R[X]$ such that $v_{\overline{X}}(\overline{P}) = \deg P$. Let $\alpha_1, \alpha_2, ...\alpha_n$ be the roots of P in some fixed algebraic closure $\overline{K}$ of K and $\overline{v}$ is a fixed prolongation of v to $\overline{K}$. Then P is an isoline polynomial if and only if $\overline{v}(\alpha_i) = \overline{v}(\alpha_j)$ for any i, j.*

Proof (proposition 1.3.3). Assume first that $\overline{v}(\alpha_i) = \overline{v}(\alpha_j)$ for any i, j. Using the fact that $\prod_{i=1}^{n} \alpha_i = (-1)^n a_0$, we immediately conclude that $\overline{v}(\alpha_i) = \frac{v(a_0)}{n}$ for $1 \leq i \leq n$, on applying Lemma 1.2.1 the last equality clearly show that P is an isoline polynomial.

Conversely suppose that P is isoline. We show that $\overline{v}(\alpha_i) = v^*(P)$ for $1 \leq i \leq n$. Let $\alpha \in \overline{K}$ be a root of P, in view of Lemma 1.2.1 we have $\overline{v}(\alpha) \geq v^*(P)$. If $\overline{v}(\alpha^n) > v(a_0)$, then for any i,

we have

$$\overline{v}(a_i\alpha^i) = \overline{v}(a_i) + i\overline{v}(\alpha) \geq \left(\frac{n-i}{n}\right)\overline{v}(a_0) + i\overline{v}(\alpha) > v(a_0).$$

We conclude that $v(a_0) = \overline{v}\left(\sum_{i=1}^{n} a_i\alpha^i\right) \geqslant \min_{1\leqslant i\leqslant n} \overline{v}(a_i\alpha^i) > v(a_0)$, which is impossible. This prove that $\overline{v}(\alpha^n) = v(a_0)$ and completes the proof of the proposition. ∎

1.4 Factorization of polynomials via Newton polygons

Definition 1.4.1. *The Newton polygon of a polynomial $P = a_0+a_1x+a_2x^2+.....+a_nx^n$, $a_0a_n \neq 0$ with respect to v is the polygon formed by the lower edges along the convex hull of the points*

$$\{(i, v_G(a_i) \mid 0 \leq i \leq n, a_i \neq 0\},$$

with the slopes of edges increasing when calculated from right to left.

Proposition 1.4.1. *Let be $P(x) = a_0+a_1x+a_2x^2+.....+a_nx^n$, $a_0a_n \neq 0$ be a polynomial over the valued field (K, v) and w an extension to the splitting field L of P. If $(r, v(a_r)) < -- > (s, v(a_s))$ is a line segment of slope $-\lambda$ occurring in the Newton polygon of P then $P(x)$ has precisely $s-r$ roots $\alpha_1, ...\alpha_{s-r}$ of value*

$$w(\alpha_1) = ... = w(\alpha_{s-r}) = \lambda.$$

Proof. Dividing by a_n only shifts the polygon up or down. Thus we may assume that $a_n = 1$. We number the roots $\alpha_1, ...\alpha_n \in L$ of f in such a way that :

$$\begin{aligned} w(\alpha_1) = ... = w(\alpha_{s_1}) &= \lambda_1, \\ w(\alpha_{s_1+1}) = ... = w(\alpha_{s_2}) &= \lambda_2, \\ ..... = ... = ... &= ..... \\ w(\alpha_{s_t+1}) = ... = w(\alpha_{s_n}) &= \lambda_{t+1}, \end{aligned}$$

where $\lambda_1 < \lambda_2 < ..... < \lambda_{t+1}$. Viewing the coefficients a_i as elementary symmetric functions of

the roots α_i, we see immediately that

$$\begin{aligned} \upsilon(a_n) &= \upsilon(1) = 0, \\ \upsilon(a_{n-1}) &\geqslant min_i\{w(\alpha_i)\} = \lambda_1, \\ \upsilon(a_{n-2}) &\geqslant min_{i,j}\{w(\alpha_i\alpha_j)\} = 2\lambda_1, \\ \ldots\ldots\ldots\ldots &\geqslant \ldots\ldots\ldots\ldots\ldots\ldots = \ldots\ldots\ldots\ldots, \\ \upsilon(a_{n-s_1}) &= min_{i_1,\ldots\ldots i_{s_1}}\{w(\alpha_{i_1}\ldots\ldots\alpha_{i_{s_1}})\} = s\lambda_1, \end{aligned}$$

the latter because the value of the term $\alpha_1\ldots\ldots\alpha_{s_1}$ is smaller than that of all the others,

$$\begin{aligned} \upsilon(a_{n-s_1-1}) &\geqslant min_{i_1,\ldots i_{s_1+1}}\{w(\alpha_{i_1}\ldots\ldots\alpha_{i_{s_1+1}}\} = s_1\lambda_1 + \lambda_2, \\ \upsilon(a_{n-s_1-2}) &\geqslant min_{i_1,\ldots i_{s_1+2}}\{w(\alpha_{i_1}\ldots\ldots\alpha_{i_{s_1+2}}\} = s_1\lambda_1 + 2\lambda_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots &\geqslant \ldots\ldots\ldots\ldots\ldots\ldots\ldots = \ldots\ldots\ldots\ldots\ldots\ldots;, \\ \upsilon(a_{n-s_2}) &\geqslant min_{i_1,\ldots i_{s_2}}\{w(\alpha_{i_1}\ldots\ldots\alpha_{i_{s_2}}\} = s_1\lambda_1 + (s_2 - s_1)\lambda_2, \end{aligned}$$

And so on. From this result one concludes that the vertices of the Newton polygon, from right to left, are given by $(n, 0), (n - s_1, s_1\lambda_1), (n - s_2, s_1m_1 + (s_2 - s_1)\lambda_2), \ldots\ldots\ldots\ldots$ The slope of the extreme right-hand segment is

$$\frac{0 - s_1\lambda_1}{n - (n - s_1)} = -m_1,$$

and, proceeding further to the left,

$$\frac{(s_1\lambda_1 + \ldots\ldots + ((s_j - s_{j-1})\lambda_j)) - (s_1\lambda_1 + \ldots\ldots + ((s_{j+1} - s_j)\lambda_{j+1}))}{(n - s_j) - (n - s_{j+1})} = -\lambda_{j+1}$$

We emphasize that, according to the preceding proposition, the Newton polygon consists of precisely one segment if only if the roots $\alpha_1, \ldots\ldots, \alpha_n$ of f have all the same value.

Definition 1.4.2. *Let G_υ be the value group of υ, we will say that P is λ-pure or isoline if the value of all roots of P are equal to λ for some $\lambda \in G_\upsilon$.*

Corollary 1.4.1. *Let $Z(P) = \{\alpha_1, \alpha_2, \ldots\ldots\alpha_m\}$ be the set of all root of P in L, let $\lambda_1, \lambda_2, \ldots\ldots\lambda_m$ be the value of all roots of P (i. e., : $\lambda_i = w(\alpha_i)$, for any index i). Then P factors into a product according to the $-\lambda_r < \ldots\ldots\ldots < -\lambda_1$,*

$$P = a_n \prod_{i=1}^{m} P_i,$$

where

$$P_i = \prod_{\lambda_i = w(\alpha_i)} (x - \alpha_i).$$

Corollary 1.4.2. *Assume that P is λ-pure, then P factors into a product*

$$P = a_n \prod_{\lambda = w(\alpha_i)} (x - \alpha_i).$$

In this Section we extend the notion of isoline polynomials defined in Chapter 1 to g-hight isoline polynomials over discrete valued fields and prove similar results Generalizing a some classical results for algebraic number fields. In particular when L is a finite separable extension of K of degree n and α is a primitive element of L which is integral over R. We use the map v_g^* defined below to give a sufficient condition for $R[\alpha]$ to be not integrally closed. we give also a reformulation of the K-Khanduja theorem in term of isoline polynomials

1.5 Hight isoline polynomials

Throughout v is a discrete valuation of a field K with value group $G_v = \mathbb{Z}$, valuation ring R, maximal ideal m and residue field R/m. Let π be a prime element of $R$and $g \in R[X]$ be a fixed monic polynomial. For a polynomial with coefficients in the valuation ring $R$of v, $\overline{P}$ will have its usual meaning. In this section we extend the notions of isoline polynomials in Definition 1.3.1 to g-hight isoline polynomials over discrete valued field and prove similar results. It may be pointed out that the two notions are the same if we take $g(X) = X$.

Definition 1.5.1. *Let $P \in R[X]$ and g be a monic polynomial with coefficients in R such that $\overline{g}$ divides $\overline{P}$. Let $P = \sum_{i=0}^{s} a_i g^i$ be the g-expansion of P and $l = v_{\overline{g}}(\overline{P})$ the highest power of $\overline{g}$ dividing $\overline{P}$. We may denote $\min_{0 \le i \le l-1} \left\{ \frac{v_G(a_i)}{l-i} \right\}$ by $v_g^*(P)$ and we say that P is a g-hight isoline polynomial if $v^*(P) = \dfrac{v_G(a_0)}{l}$, where v_G the Gaussian valuation of the field $K(x)$ extending v.*

With the above notations, we prove

Theorem 1.5.1. *Let P and Q two monic polynomials with coefficients in Rsuch that $\bar{P} = \bar{g}^l$ with g an irreducible polynomial such that $\overline{g}$ does not divides $\overline{Q}$, then P is a g-hight isoline polynomial if and only if PQ is a g-hight isoline polynomial.*

Before tackling the proof, we need the following lemma.

Lemma 1.5.1. *Keep the notations, assuptions, and terminology as above. Let* $P = \sum_{i=0}^{l} a_i g^i$ *and* $Q = \sum_{i=0}^{s} b_i g^i$ *be the g-expansion of* P *and* Q *respectively. Set* $\alpha_k = \sum_{i=0}^{k} a_i b_{k-i}$ *and* $c_k = r_k + q_{k-1}$ *where* r_k, q_k *are respectively the quotient and the remainder of the Euclidean division of* α_k *by* g*. Then the g-expansion of the product* PQ *in* $R[X]$ *is given by*

$$PQ = r_0 + \sum_{i=1}^{l+s+1} c_i g^i.$$

Proof. It is clear that the expansion of the product PQ in $R[X]$ is given by

$$PQ = \sum_{k=0}^{l+s} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) g^k = \sum_{k=0}^{l+s} \alpha_k g^k,$$

where $a_i = 0$ for $i > l$ and $b_j = 0$ for $j > s$. By the Euclidean division of α_k by g one can write

$$\alpha_k = \sum_{i=0}^{k} a_i b_{k-i} = q_k g + r_k,$$

where $r_k = 0$ or $\deg r_k < \deg g$, it follows that

$$\begin{aligned} PQ = \sum_{k=0}^{l+s} \alpha_k g^k = \sum_{k=0}^{l+s} (q_k g + r_k) g^k &= \sum_{k=0}^{l+s} q_k g^{k+1} + \sum_{k=0}^{l+s} r_k g^k \\ &= \sum_{t=1}^{l+s+1} q_{t-1} g^t + \sum_{t=1}^{l+s+1} r_t g^t + r_0 \\ &= r_0 + \sum_{t=1}^{l+s+1} (r_t + q_{t-1}) g^t. \end{aligned}$$

Which completes the proof of the lemma. ∎

Proof (theorem 1.5.1). Suppose first that P is a g-hight isoline polynomial. We now show that PQ is g-hight polynomial. Using the hypothesis that $\bar{P} = \bar{g}^l$, we see that the g-expansion of P has the form

$$P = g^l + a_{l-1} g^{l-1} + ... + a_0.$$

Let $Q = b_0 + b_1 g + b_2 g^2 + ... + b_s g^s$ be the g-expansion of Q, then we conclude immediately that $\alpha_{l+s} = b_s$ and hence $\deg(\alpha_{l+s}) = \deg(b_s) < \deg g$, which prove that $c_{l+s+1} = q_{l+s} = 0$. Keeping in mind this and using Lemma 2.1.1, we see that the g-expansion of the product PQ has the form

$$PQ = c_0 + c_1 g + c_2 g^2 + ... + c_{l+s} g^{l+s}.$$

Now since $\overline{g}$ does not divides $\overline{Q}$, then

$$\min\{0 \leqslant i \leqslant l+s \mid v_G(c_i)=0\} = v_{\overline{g}}(\overline{PQ}) = v_{\overline{g}}(\overline{P}) + v_{\overline{g}}(\overline{Q}) = l.$$

It remains to be shown that

$$v_g^*(PQ) = \frac{v_G(c_0)}{l}.$$

For $0 \leqslant i \leqslant l-1$, we have

$$\begin{aligned} v_G(\alpha_i) = v_G\left(\sum_{k=0}^{i} a_k b_{i-k}\right) \geqslant \min_{0\leqslant k\leqslant i}\{v_G(a_k)\} &\geqslant \min_{0\leqslant k\leqslant i}\{v_g^*(P)(l-k)\} \\ &= v_g^*(P)(l-i) \end{aligned}$$

we conclude that $v_G(\alpha_i) \geqslant v_g^*(P)(l-i)$ for $0 \leqslant i \leqslant l-1$.

Since q_k and r_k are respectively the quotient and the remainder resulting from the Euclidian division of α_k by a monic polynomial, then by [16], we have

$$v_G(\alpha_i) = \min\{v_G(q_i), v_G(r_i)\} \geqslant v_g^*(P)(l-i).$$

Then $v_G(c_i) \geqslant v_g^*(P)(l-i)$, it follows that for $0 \leqslant i \leqslant l-1$

$$\frac{v_G(c_i)}{l-i} \geqslant v_g^*(P) = \frac{v_G(a_0)}{l}.$$

So to complete the proof it is enough to show that

$$v_g^*(P) = \frac{v_G(c_0)}{l}.$$

Observe that $\alpha_0 = a_0 b_0$ and using that the fact that $\overline{g}$ does not divides $\overline{Q}$, we see that $v_G(\alpha_0) = v_G(a_0)$, it remains to be shown that $v_G(c_0) = v_G(\alpha_0)$. Set $v_G(\alpha_0) = s$, then we have the following equality

$$\frac{\alpha_0}{\pi^s} = g\frac{q_0}{\pi^s} + \frac{r_0}{\pi^s}.$$

Now suppose to the contrary that $v_G(r_0) > s$, it follows from the above equality that $\overline{g}$ divides $\overline{\frac{\alpha_0}{\pi^s}}$ which is impossible as $\deg a_0 < \deg g$, $\deg b_0 < \deg g$ and g irreducible. This prove that $v_G(c_0) = v_G(r_0) = s$.

Conversely assume that PQ is a g-convex polynomial, we show that $v_g^*(P) = \frac{v_G(a_0)}{l}$. Suppose to the contrary that $v_g^*(P) < \frac{v_G(a_0)}{l}$ and let i_0 the minimum index such that $\frac{v_G(a_{i_0})}{l-i_0} < \frac{v_G(a_0)}{l}$, then

we can write

$$\alpha_{i_0} = \sum_{i=0}^{i_0} a_i b_{i_0-i} = a_{i_0}b_0 + \sum_{i=0}^{i_0-1} a_i b_{i_0-i}.$$

Now it is clear that $\upsilon_G(a_{i_0}b_0) = \upsilon_G(a_{i_0})$ and for $0 \leqslant i \leqslant i_0 - 1$, we have

$$\upsilon_G(a_i b_{i_0-i}) \geq \upsilon_G(a_i) \geq (l-i)\frac{\upsilon_G(a_0)}{l} > (l-i_0)\frac{\upsilon_G(a_0)}{l} > \upsilon_G(a_{i_0}).$$

It follows that $\upsilon_G(\alpha_{i_0}) = \upsilon_G(a_{i_0}) < (\frac{\upsilon_G(a_0)}{l})(l-i_0)$. Set $\upsilon_G(a_{i_0}) = t$. Then one cane write

$$\frac{\overline{\alpha_{i_0}}}{\pi^t} = \frac{\overline{a_{i_0}b_0}}{\pi^t} = \overline{g}\frac{\overline{q_{i_0}}}{\pi^t} + \frac{\overline{r_{i_0}}}{\pi^t}.$$

Now by the same argument as above we conclude immediately that $\upsilon_G(\alpha_{i_0}) = \upsilon_G(r_{i_0})$ since $\deg a_{i_0} < \deg g$, $\deg b_0 < \deg g$ and g irreducible. Now using the fact that for $i < i_0$, we have

$$\upsilon_G(q_{i_0-1}) \geq \upsilon_G(\alpha_{i_0-1}) \geq \upsilon_G(a_i b_{i_0-i}) > t.$$

This prove that $\upsilon_G(c_{i_0}) = \upsilon_G(r_{i_0})$ and hence $\frac{\upsilon_G(c_{i_0})}{l-i_0} < \frac{\upsilon_G(a_0)}{l}$ then $\upsilon_g^*(PQ) = \frac{\upsilon_G(c_0)}{l} \leqslant \frac{\upsilon_G(c_{i_0})}{l-i_0} < \frac{\upsilon_G(a_0)}{l}$. Moreover we have $\alpha_0 = a_0b_0 = gq_0 + c_0$ then $\upsilon_G(a_0) = \upsilon_G(\alpha_0) \leqslant \upsilon_G(c_0)$ contradiction hence P is a g-hight isoline polynomial.

∎

Proposition 1.5.1. *Let $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ and $Q = X^m + b_{m-1}X^{m-1} + ... + b_0$ be two polynomials in $R[X]$ such that $\upsilon_g^*(P) = \upsilon_g^*(Q)$, then the product PQ is a g-hight isoline polynomial if and only if P and Q are a g-hight isoline polynomials.*

Proof. Suppose that the polynomials P and Q are g-hight isoline such that $\upsilon_g^*(P) = \upsilon_g^*(Q)$. By Lemma 2.1.1 we see that the g-expansion of the product PQ in $R[X]$ is given by

$$PQ = \sum_{i=0}^{n+m+1} c_i g^i.$$

Assume that $\upsilon_{\overline{g}}(\overline{P}) = l$ and $\upsilon_{\overline{g}}(\overline{Q}) = s$, then it is clear that $\upsilon_{\overline{g}}(PQ) = l + s$ and $\alpha_0 = a_0b_0$, Therefore, $\upsilon_G(\alpha_0) = \upsilon(a_0) + \upsilon(b_0) = (l+s)\upsilon_g^*(P)$, hence $\upsilon_g^*(P) = \frac{\upsilon(\alpha_0)}{l+s} = \frac{\upsilon(c_0)}{l+s}$ as $\upsilon(c_0) = \upsilon_G(\alpha_0)$ see the proof of Theorem 1.5.1. Now to prove that PQ is g-hight isoline polynomial, it enough to show that

$$\upsilon_g^*(PQ) = \upsilon_g^*(P).$$

Observe first that $\alpha_i = \sum_{k=0}^{i} a_k b_{i-k}$, it follows that

$$\begin{aligned} \upsilon_G(\alpha_i) = \upsilon_G\left(\sum_{k=0}^{i} a_k b_{i-k}\right) &\geqslant \min_{0\leqslant k\leqslant i}(\upsilon(a_k b_{i-k})) \\ &\geqslant \min_{0\leqslant k\leqslant i}((l-k)\upsilon_g^*(P) + (s-i+k)\upsilon_g^*(P)) \\ &\geqslant \upsilon_g^*(P)(l+s-i) \end{aligned}$$

Keeping in mind the fact that $\upsilon_G(\alpha_i) = \min\{\upsilon_G(q_i), \upsilon_G(r_i)\}$, we see immediately that for $0 \leqslant i \leqslant l+s-1$

$$\frac{\upsilon_G(c_i)}{l+s-i} \geqslant \upsilon_g^*(P) = \frac{\upsilon_G(c_0)}{l+s}.$$

and PQ is a g-hight isoline polynomial as desired.

Conversely suppose that PQ is a g-hight isoline polynomial. We show first that

$$\upsilon_g^*(PQ) = \upsilon_g^*(P).$$

Let $i_0 = \min_{0\leqslant i\leqslant l-1}\{\upsilon(a_i) = (l-i)\upsilon_g^*(P)\}$ and $j_0 = \min_{0\leqslant j\leqslant s-1}\{\upsilon(b_j) = (s-j)\upsilon_g^*(Q)\}$. Consider $\alpha_{i_0+j_0} = a_0 b_{i_0+j_0} + ... + a_{i_0} b_{j_0} + ... + a_{i_0+j_0} b_0$. Then by the same steps as in Theorem 1.5.1 one can show easily

$$\upsilon(\alpha_{i_0+j_0}) = (l+s-(i_0+j_0))\upsilon_g^*(P).$$

Now we conclude that

$$\upsilon(c_{i_0+j_0}) = \upsilon(r_{i_0+j_0}) = (l+s-(i_0+j_0))\upsilon_g^*(P).$$

Using the hypothesis that PQ is a g-hight isoline polynomial we see that $\upsilon(c_{i_0+j_0}) \geqslant (l+s-(i_0+j_0))\upsilon_g^*(PQ)$, consequently $\upsilon_g^*(PQ) \leqslant \upsilon_g^*(P)$. Now Using hypothesis and the definition of υ_g^* we see that

$$(l+s)\upsilon_g^*(PQ) = \upsilon(c_0) = \upsilon(\alpha_0) = \upsilon(a_0) + \upsilon(b_0) \geqslant l\upsilon_g^*(P) + s\upsilon_g^*(Q) = (l+s)\upsilon_g^*(P)$$

which proves the desired inequality.

In view of the fact that $\upsilon(a_0) + \upsilon(b_0) = \upsilon(\alpha_0) = \upsilon(c_0) = (l+s)\upsilon_g^*(PQ) = l\upsilon_g^*(P) + s\upsilon_g^*(Q)$ and since $\upsilon(a_0) \geqslant l\upsilon_g^*(P)$ and $\upsilon(b_0) \geqslant \upsilon_g^*(Q)$. We conclude that $\upsilon(a_0) = l\upsilon_g^*(P)$ and $\upsilon(b_0) = s\upsilon_g^*(Q)$ which prove that P and Q are a g-hight isoline polynomials as desired. ∎

we prove the following theorem, which give a sufficient condition for $R[\alpha]$ to be not integrally

closed, when L is a finite separable extension of K of degree n and α is a primitive element of L which is integral over R, and which is also of independent interest as well.

Theorem 1.5.2. *Let $(R, \pi R, k)$ be a discrete valuation ring, $\mathfrak{p} = \pi R$ the prime ideal of R, and $k = R/\mathfrak{p}$ its residue field. Let K the quotient field of R and $L = K(\alpha)$ is a finite extension of K with α in the integral closure of the valuation ring R. Let P be the minimal polynomial of α over K. Suppose that $\bar{P} = \bar{g}^l$ where g is a monic polynomial whose reduction modulo p is irreducible, let $P = \sum_{i=0}^{l} a_i g^i$ the g-expansion of P. Suppose that $v_g^*(P) > 0$ then $R[\alpha]$ is not integrally closed.*

Proof. Suppose that $v_g^*(P) > 0$ and set $\lambda = \frac{g(\alpha)}{\pi^{\left[v_g^*(P)\right]}}$; we show that λ is a element of $O_L - R[\alpha]$ and, thus, $R[\alpha]$ is not integrally closed. Since g is monic it is clear that $\lambda \notin R[\alpha]$. To show that $\lambda \in O_L$ it is enough to show that λ is integral over $R[\alpha]$. Since The g-expansion of P has the form $P = g^l + a_{l-1}g^{l-1} + ... + a_1 g + a_0$ then

$$\frac{P(\alpha)}{\pi^{l\left[v_g^*(P)\right]}} = \sum_{i=0}^{l} \frac{a_i(\alpha) g^i(\alpha)}{\pi^{l\left[v_g^*(P)\right]}} = \sum_{i=0}^{l} \left(\frac{a_i(\alpha)}{\pi^{\left[v_g^*(P)\right](l-i)}} \right) \left(\frac{g(\alpha)}{\pi^{\left[v_g^*(P)\right]}} \right)^i = 0.$$

So to complete the proof it is enough to show that each $\frac{a_i(\alpha)}{\pi^{\left[v_g^*(P)\right](l-i)}} \in R[\alpha]$ $(0 \leq i < l)$.We have $a_i \in R[X]$ then $a_i = \pi^{v_G(a_i)} u$ and $u \notin \pi R[X]$ so $a_i(\alpha) = \pi^{v_G(a_i)} u(\alpha)$ and hence $\frac{a_i(\alpha)}{\pi^{\left[v_g^*(P)\right](l-i)}} = \pi^{v_G(a_i)} \frac{u(\alpha)}{\pi^{\left[v_g^*(P)\right](l-i)}} = \pi^{v_G(a_i) - \left[v_g^*(P)\right](l-i)} u(\alpha)$ and since $\frac{v_G(a_i)}{l-i} \geqslant v_g^*(P) \geqslant \left[v_g^*(P)\right]$ then $v_G(a_i) - \left[v_g^*(P)\right](l-i) \geqslant 0$ this complete the proof of the theorem. ∎

1.6 Extension of valuations

Let K be a field which is complete with respect to a nonarchimedean valuation v. Let R be the corresponding valuation ring with maximal ideal m and residue class field $k_v = R/m$.

Lemma 1.6.1. *(Hensel's Lemma) With notations as above . Let $P(x) \in R[x]$ such that : $P(x) \not\equiv 0 \mod m$, let $P \equiv \bar{G}\bar{H} \mod m$ be the factorization into relatively prime polynomials $\bar{G}$, $\bar{H} \in k[x]$, then P admits a factorisation $P = GH$ into polynomials $G, H \in R[x]$ such that : $\deg(G) = \deg(\bar{G})$ and $G \equiv \bar{G} \mod m$ and $H \equiv \bar{H} \mod m$.*

Let (K, v) be a nonarchimedean valued field and $(\hat{K}, \hat{v})$ its completion and let K_v be the separable closure of K in $\hat{K}$, this extension will be called the henselization of the field K with respect to v and offers the advantage of being itself an algebraic extension of K.

Definition 1.6.1. *A henselian field is a field with a nonarchimedean valuation whose valuation ring Rsatisfies Hensel's Lemma (see Lemma 1.6.1).*

Theorem 1.6.1. *A nonarchimedean valued field (K, υ) is henselian if and only if the valuation υ can be uniquely extended to any algebraic extension.*

If K is a henselian field, then the proof that υ admet one and only one extension to any given algebraic extension L/K is the same as in the case of complete field (see [50]).

Now the fact that the unique extendability also characterizes henselian fields is related to factorization of polynomials over K, more precisely we appeal to a method wich allows us to express the valuation of the roots of a polynomial in terms of the valuations of the coefficients. It relies on the notion of Newton polygon,. (for more detail see [50]).

1.6.1 Extension of valuation to finite extension

In this section we will study the question of how an arbitrary archimedean or nonarchimedean valuation υ of a field K extends to an algebraic extension in general. In what follows, for any valued field (K, υ), $(\hat{K}, \hat{\upsilon})$ will denote its completion, A the algebraic closure of $\hat{K}$ with respect to υ. The following result gives us a complete description of the possible extension of υ to L where L is an algebraic extension of K. (see (8.1) Extension Theorem [50]))

Theorem 1.6.2. *Let L/K be an algebraic field extension and υ a valuation of K. Then one has :*

1. *Every extension w of the valuation υ arises as the composite $w = \bar{\upsilon} \circ \tau$ for some K-embedding $\tau : L \longrightarrow A$.*

2. *Two extension $w = \bar{\upsilon} \circ \tau$ and $w = \bar{\upsilon} \circ \tau'$ are equal if and only if τ and τ' are conjugate over $\hat{K}$.*

Remark 1.6.1. *Every K-embedding $\tau : L \longrightarrow \hat{K}$ gave us an extension $w = \bar{\upsilon} \circ \tau$ of υ. For every automorphism $\sigma \in G(A/\hat{K})$ of A over $\hat{K}$, we obtain with the composite*

$$L \underset{\rightarrow}{\tau} A \underset{\rightarrow}{\sigma} A$$

a new K-embedding $\tau' = \sigma \circ \tau$ of L. It will ba said to be conjugate to τ over $\hat{K}$.

Let (K, υ) be a valued field and $L = K(\alpha)$ be a finite separable extension of K with α in the integral closure O_L of R in L. Suppose that the minimal polynomial P of α over K has the factorization $P = \prod_{i=1}^{s} P_i$ into monic irreducible polynomials over $\hat{K}$. The K-embedding $\tau : L \longrightarrow A$ are then given by the zero α_i of P which lie in A. $\tau : L \longrightarrow A$, $\tau(\alpha) = \alpha_i$. Two embeddings τ and τ' are conjugate over A if they are zeroes of the same irreducible factor P_i, this gives the following result (see (8.2) proposition [50]))

Proposition 1.6.1. *Let (K, υ) be a valued field and $L = K(\alpha)$ be a finite separable extension of K with α in the integral closure O_L of R in L. Suppose that the minimal polynomial P of α over K has the factorization $P = \prod_{i=1}^{s} P_i$ into monic irreducible polynomials over $\hat{K}$. Then there are exactly s prolongations of υ to L. Let α_i be a root of P_i and w_i be the prolongation of υ to L defined by*

$$w_i\left(\sum_j a_j\alpha^j\right) = \hat{\upsilon}\left(\sum_j a_j\alpha_i^j\right), \quad a_j \in K.$$

are the prolongations of υ to L.

In the case of a valuation of arbitrary rank the following theorem show that there is one-to-one correspondence between the irreducible factors obtained by factorization of P over a fixed henselization of K and the extension of υ to K (see Theorem 2.D [38])

Theorem 1.6.3. *Let υ be a valuation of arbitrary rank of a field K and $L = K(\alpha)$ be a finite extension of K with α in the integral closure O_L of Rin L. Let $\prod_{i=1}^{s} P_i$ be the factorization of the minimal polynomial P of α over K into a product of distinct monic irreducible polynomials over a fixed henselization K^h of (K, υ). Then there are exactly s prolongations of υ to L. Let α_i be a root of P_i, the valuations $\omega_1, ..., \omega_s$ of L defined by*

$$\omega_i\left(\sum_j a_j\alpha^j\right) = \upsilon^h\left(\sum_j a_j\alpha_i^j\right)$$

are the prolongations of υ to L.

Assume that υ is a valuation of arbitrary rank of a field K and $L = K(\alpha)$ is a finite extension of K with α in the integral closure of the valuation ring R of υ. Let P be the minimal polynomial of α over K. Let $\prod_{i=1}^{r} \overline{P}_i^{l_i}$ be the factorization of the polynomial $\overline{P}$ into powers of distinct irreducible polynomials over the residue field k_υ of υ. Then the authors of [38] (see Theorem 1.6.4 below) gives a sufficent condition to be satisfied by P which ensures that there are exactly r prolongations $w_1, ..., w_r$ of υ to L, moreover the index of ramification and the residual degree of w_i/υ eaqual l_i, $\deg \bar{g}_i$ respectively for $1 \leqslant i \leqslant r$

Let $g \in R[X]$ be a monic polynomial whose reduction modulo m is irreducible then each $P \in R_v[X]$ can be uniquely represented as a finite sum

$$P = a_m g^m + a_{m-1}g^{m-1} + ... + a_0$$

(where $i = 0....m$, $a_i \in R[X]$ and $dga_i < dgg$), this representation of P will be referred to as the g-expansion of P. If $\bar{P} = \bar{g}^l$ then the g-expansion of P has the form $P = g^l + a_{l-1}g^{l-1} + ... + a_0$

and we have $l = \inf\{i \mid v_G(a_i) \neq 0\}$ and $a_l = 1$ where v_G the Gaussian valuation of the field $K(X)$ which extends v. It is defined on $K[X]$ by $v_G(\sum a_i X^i) = \min_i\{v(a_i)\}$.

Theorem 1.6.4. *(2010)(S.K. Khanduja and M.Kumar condition)*
Let v be a Krull valuation of arbitrary rank of a field K with valuation ring R, residue field k and value group G. Let $L = K(\alpha)$ be a finite extension of K with α in the integral closure of R in L and P be the minimal polynomial of α over K. Let $\prod_{i=1}^{r} \overline{P}_i^{l_i}$ be the factorization of the polynomial $\overline{P}$ into powers of distinct irreducible polynomials over k, with each P_i monic. Suppose that for $1 \leq i \leq r$ the P_i-expansion of P given by :

$$P(x) = \sum_{j \geq 0} a_{ij}(x) P_i(x)^j$$

Satisfies $\frac{v_G(a_{ij})}{l_i - j} \geq \frac{v_G(a_{i0})}{l_i}$ when $1 \leq j \leq l_i - 1$ and that the order of $\frac{v_G(a_{i0})}{e_i}$ modulo G is l_i. Then there are exactly r valuations $w_1, ...w_r$ of L which extend υ and l_i, $\deg \overline{P}_i$ are respectively the index of ramification and the residual degree of w_i/υ.

Remark 1.6.2. *Due to a well-known Theorem of Hensel, the problems of determining the prime ideal factorization in O_K is directly related to the factorization of P in $\mathbb{Q}_p[X]$, which in turn is related to the extensions of υ_p to K where υ_p the discrete valuation associated to p.*

Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with α in the ring O_K of algebraic integers of K and P be the minimal polynomial of α over the field $\mathbb{Q}$ of rational numbers. One of the most important problems in algebraic number theory is determining the prime ideal factorization in O_K for a rational prime p . Let $\overline{P} = \overline{P_1}^{l_1} ... \overline{P_r}^{l_r}$ be the factorization of the polynomial $\overline{P}$ obtained by remplacing each coefficient of P modulo p in a product of distinct irreducible polynomials over $\mathbb{Z}p\mathbb{Z}$ with P_i monic. In 1878, Dedekind proved that if p does not divide $[O_K : \mathbb{Z}[\alpha]]$, then $pO_K = \mathcal{P}_1^{l_1} ... \mathcal{P}_r^{l_r}$, where $\mathcal{P}_1, ..., \mathcal{P}_r$ are distinct prime ideals of O_K satisfying :

1. $\mathcal{P}_i = pO_K + P_i(\alpha)O_K$,
2. The residual degree of $\mathcal{P}_i$ over p is $\deg \overline{P_i}$.

Dedekind also gave a criterion (see chapter 3) to verify when p does not divide $[O_K : \mathbb{Z}[\alpha]]$, the following theorem (see 1.6.4 Corollary 1.2)give a weaker condition than that of Dedekind Criterion which guarantees that if $\overline{P}$ has a factorization $\overline{P_1}^{l_1} ... \overline{P_r}^{l_r}$ into irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, then $pO_K = \mathcal{P}_1^{l_1} ... \mathcal{P}_r^{l_r}$ for some prime ideal $\mathcal{P}_1, ..., \mathcal{P}_r$ of O_K with residual degree of $\mathcal{P}_i$ over p is $\deg \overline{P_i}$.

Theorem 1.6.5. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with α in the ring O_K of algebraic integers of K and P be the minimal polynomial of α over the field $\mathbb{Q}$ of rational numbers. For a rational prime p . Let $\overline{P} = \overline{P_1}^{l_1}...\overline{P_r}^{l_r}$ be the factorization of the polynomial $\overline{P}$ obtained by remplacing each coefficient of P modulo p in a product of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with P_i monic. Suppose that for $1 \leq i \leq r$, the P_i-expension of P given by $P = \sum_{j\geq 0} a_{ij}P_i^j$ satisfies :*

1. $\frac{\upsilon_G(a_{ij})}{l_i - j} \geq \frac{\upsilon_G(a_{i0})}{l_i}$ *when* $1 \leq j \leq l_i - 1$,
2. $(l_i, \upsilon_G(a_{i0})) = 1$.

Then pO_K factors into prime ideals as $\mathcal{P}_1^{l_1}...\mathcal{P}_r^{l_r}$ with residual of $\mathcal{P}_i/p$ equal to $\deg P_i$. *In other words $\mid Fib_K p \mid = \mid Fib_{\mathbb{Q}} p \mid = r$.*

In 2019 Abulaziz Deajim and Lhoussain El fadil gives an improvement of Thoerem 1.6.4 in the context of number field (see Theorem 2.1 [16]). It may pointed out that this result relaxes the linearity of $F_{g_i}(Y)$ (defined below) required in K-K's result (see Theorem 1.6.7).

Let p be a rational prime and $\mathbb{Z}_p$ the ring of p-adic integers, $\mathbb{Q}_p$ the fraction field of $\mathbb{Z}_p$. Let υ_p be the discrete p-adic valuation associated to p. Extend υ_p to a discrete valuation υ_G of $\mathbb{Q}_p(X)$ by letting it act in the following way in polynomials

$$\upsilon_G\left(\sum_i a_i X^i\right) = \min_i \upsilon_p(a_i).$$

Let $\mathbb{Z}_{\mathbb{Q}_{\upsilon_p}} = \overline{\mathbb{Z}_{(p)}}^{\mathbb{Q}_{\upsilon_p}}$ be the integral closure of $\mathbb{Z}_{(p)}$ in the henselization $\mathbb{Q}_{\upsilon_p}$ of $(\mathbb{Q}, \upsilon_p)$. Let $P \in \mathbb{Z}_{\mathbb{Q}_{\upsilon_p}}[X]$ be a monic polynomial, and $\overline{g} \in \mathbb{F}_p[X]$ a monic and irreducible divisor of $\overline{P}$. For a fixed monic lifting $g \in \mathbb{Z}_{\mathbb{Q}_{\upsilon_p}}[X]$ of $\overline{g}$, consider the finite field $\mathbb{F}_g = \mathbb{Z}_{\mathbb{Q}_{\upsilon_p}}[X]/(p, g)$, and let $\psi : \mathbb{Z}_{\mathbb{Q}_{\upsilon_p}}[X] \longrightarrow \mathbb{F}_g$ the homomorphisms of reduction modulo modulo (p, g). Let

$$P = a_0 + a_1 g + a_2 g^2 + ... + a_s g^s,$$

be the g-adic expansion of P in $\mathbb{Z}_{\mathbb{Q}_{\upsilon_p}}[X]$. So $a_i \in \mathbb{Z}_{\mathbb{Q}_{\upsilon_p}}[X]$ and $\deg a_i < \deg g$ for each i. To any coefficient a_i, we attach $u_i = \upsilon_G(a_i)$. If $u_i < \infty$, then let P_i be the point in the Euclidean plane defined by (i, u_i).

Definition 1.6.2. *The g-Newton polygon of P is the lower convex envelope of the set of points $P_i = (i, u_i)$, $u_i < \infty$, in the Euclidean plane. This open polygon is denoted by $N_g^{\upsilon_G}$. Let $N_g^{\upsilon_G}$ the Newton polygon of P with respect to υ_G. The Newton polygon is the union of different sides. The principal part of $N_g^{\upsilon_G}$, denoted by $N_g^{\upsilon_G^+}$ is the polygon determined by the sides of positive slope.*

Let $l = \inf\{0 \leq i \leq s / v_G(a_i) = 0\}$. As $\bar{g}$ divides $\bar{P}$ then $l > 0$, let $\lambda = \frac{v_G(a_0)}{l}$. Note that $-\lambda$ is the slope of the line joining the two points$(l, 0)$ and$(0, v_G(a_0))$. We say that P satisfies the hypothesis (Hyp λ) if $\frac{v_G(a_i)}{l-i} \geq \lambda$ for $i = 1, ..., l-1$, it may pointed out that P satisfies the hypothesis (Hyp λ) if and only if $N_g^{v_G^+}$ is a signle-sided of length l and slope $-\lambda$. Let $d = (v_G(a_0), l)$, $e = \frac{l}{d}$ et $h = \frac{v_G(a_0)}{d}$ then $\lambda = \frac{h}{e}$ with$(h, e) = 1$. if P satisfies the hypothesis (Hyp λ), let $t_j^* = \psi(\frac{a_j}{p^{|(l-j)\lambda|}})$ $j = 0, ..., l-1$. Since $(l-j)\lambda \in \mathbb{Z}$ if only if $(l-j) \in e\mathbb{Z}$, let $t_i = \psi(\frac{a_{l-ei}}{p^{ih}})$ where $i = 0, ..., d$. We define the g-residual polynomial attached to P by $F_g(Y) = \sum_{i=0}^{d} t_i Y^{d-i} \in \mathbb{F}_g[Y]$. Note that $t_i \neq 0$ if only if $v_G(l - ei) = ih$. In particular, $t_0 \neq 0$ and thus $\deg F_g(Y) = d$. Let $P(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial, α a complex root of F, $K = \mathbb{Q}(\alpha)$, $\mathbb{Z}_K$ the ring of integers of K, p a rational prime, and $P(X) = \prod_{i=1}^{r} \overline{g}_i^{l_i}(X)$ modulo p, where $\overline{g}_i(X)$ are all monic irreducible. For each $i = 1, ..., r$, let $P(X) = \sum_{j=0}^{s_i} a_{i,j}(X) g_i^j$ the g_i-adic expansion of $F(x)$ in $\mathbb{Z}[X]$ where $g_i(X) \in \mathbb{Z}[X]$ is a monic lift of $\overline{g}_i(X)$. Let $l_i = \inf\{j = 0, ..., s_i \mid v_G(a_{i,j}) = 0\}$, $m_i = \deg(g_i)$ and $d_i = gcd(v_G(a_{i,j}), l_i)$.

Given the above notations, assumptions, and terminology, K-K's result, can be reformulated as follows :

Theorem 1.6.6. *If for every $i = 1, ...r$ P satisfies the hypothesis (Hyp λ) and the g_i-residual polynomial attached to P is linear then there are exactly r valuation $w_1, ..., w_r$ of K extending v_p. Furthermore their ramification indices and residue degrees are respectively given by $e(w_i) = l_i$ and $f(w_i) = m_i$*

With the above notation, we have the following theorem :

Theorem 1.6.7. *For $i = 1, ...r$, suppose that either*

1. *$l_i = 1$*
2. *$l_i \geq 2$, and $N_{g_i}^{v_G^+}$ is only one side and $F_{g_i}(Y)$ is irreducible*

then there are exactly r valuation $w_1, ...w_r$ of K extending v_π Furthermore their ramification indices and residue degrees are respectively given by $e(w_i) = \frac{l_i}{d_i}$ and $f(w_i) = m_i d_i$

1.6.2 Transcendental extension of valuation and generalized Ore's Theorem

In what follows, v is a valuation of arbitrary rank of a field K with value group G_v, valuation ring R, maximal ideal m, residue field $\bar{K} = R/m$ and $\tilde{v}$ is a fixed prolongation of v to the algebraic

closure $\tilde{K}$ of K with value group $G_{\tilde{v}}$. By the degree of an element $\alpha \in \tilde{K}$, we shall mean the degree of the extension $K(\alpha)/K$ which will be denoted by $\deg \alpha$. For an element α belonging to the the valuation ring of $\tilde{v}$, $\bar{\xi}$ will denote its $\tilde{v}$-residue, i.e., the image of ξ under the canonical homomorphism from the valuation ring of $\tilde{v}$ onto its residue field and for a polynomial $g(x) \in R_{\tilde{v}}[x]$ $\bar{g}(x)$ will stand for the polynomial over the residue field of $\tilde{v}$ obtained by remplacing each coefficient of $g(x)$ by its $\tilde{v}$-residue. For any subfield L of $\tilde{K}$, $\bar{L}$ will denote the residue field of the valuation of L with is restriction of $\tilde{v}$.

Definition 1.6.1. *With the above notations. A pair (α, δ) belonging to $\tilde{K} \times G_{\tilde{v}}$ is said to be a minimal pair (more precisely (K, v)-minimal pair) if whenever β belongs to K with $\deg \beta < \deg \alpha$, then $\tilde{v}(\alpha - \beta) < \delta$.*

Example 3.1. For example if $g(x)$ is a monic polynomial with coefficients in the valuation ring R such that $\bar{g}(x)$ is irreducible over the residue field $\overline{K}$ of v and α is a root of $g(x)$, then (α, δ) is a minimal pair for each positive δ in $G_{\tilde{v}}$, because whenever β belonging to K has degree less than $m = \deg g(x)$, then $\tilde{v}(\alpha - \beta) \leq 0$, for otherwise $\bar{\alpha} = \bar{\beta}$, which in view of the fundamental inequalit [[18], Theorem 3.3.] would lead to $[K(\beta) : K] \geqslant [\bar{K}(\bar{\beta}) : k_v] = m$.

Definition 1.6.2. *Let $(K, v), (\tilde{K}, \tilde{v})$ be as above and (α, δ) belonging to $\tilde{K} \times G_{\tilde{v}}$ be a minimal pair. The valuation $\tilde{w}_{\alpha,\delta}$ of $\tilde{K}(x)$ defined on $\tilde{K}[x]$ by*

$$\tilde{w}_{\alpha,\delta}\left(\sum_i c_i(x-\alpha)^i\right) = min_i\left\{\tilde{v}(c_i) + i\delta\right\},$$

will be referred to as the valuation with respect to the minimal pair (α, δ).

A different formula for the valuation of $K(x)$ obtained by restricting $\tilde{w}_{\alpha,\delta}$ is given by the following already known theorem whose proof is omitted (see [[3], Theorem 2.1]), [[43], Theorem 1.4]).

Theorem 1.6.1. *Let $\tilde{w}_{\alpha,\delta}$ be the valuation of $\tilde{K}(x)$ with respect to a minimal pair (α, δ)defined above and let $w_{\alpha,\delta}$ be the restriction of $\tilde{w}_{\alpha,\delta}$ to $K(x)$. If $g(x)$ is the minimal polynomial of α over K and $w_{\alpha,\delta}(g(x)) = \lambda$, then for any polynomial $Q(x)$ belonging to K[x] with g-expansion $\sum_i a_i g^i, \deg a_i(x) < m$, one has*

$$w_{\alpha,\delta}(Q) = \min_i\left\{a_i(\alpha) + i\lambda\right\}.$$

Lemma 1.6.2. *Let $\tilde{w}_{\alpha,\delta}$ be as above. If $Q(x) \in K[x]$ is a non-zero polynomial of degree less than $\deg \alpha$, then $\tilde{w}_{\alpha,\delta}\left(\frac{Q(x)}{Q(\alpha)} - 1\right) > 0$.*

Proof. Write $Q(x) = c\prod_i(x-\beta_i)$. Then

$$\frac{Q(x)}{Q(\alpha)} = \prod_i \frac{(x-\beta_i)}{(\alpha-\beta_i)} = \prod_i \left(1 + \frac{x-\alpha}{\alpha-\beta_i}\right).$$

Now since $\tilde{w}_{\alpha,\delta}\left(\frac{x-\alpha}{\alpha-\beta_i}\right) = -\tilde{v}(\alpha-\beta_i)+\delta > 0$, $\deg Q(x) < \deg \alpha$, we see immediately that $\tilde{w}_{\alpha,\delta}\left(\frac{Q(x)}{Q(\alpha)} - 1\right) > 0$. ∎

Lemma 1.6.3. *Let $\tilde{w}_{\alpha,\delta}$ be as above and $g(x)$ as in Theorem 1.6.1. Let $a(x), b(x) \in K[x]$ be polynomials each of degree less that $\deg g(x)$. Lzt $q(x)$, $r(x)$ denote respectively the quotient and the remainder when $a(x)b(x)$ is divided by $g(x)$. Then*

$$\tilde{v}(q(\alpha)) + \tilde{w}_{\alpha,\delta}(g(x)) > \tilde{v}(r(\alpha))$$

Proof. Putting $x = \alpha$ in $a(x)b(x) = q(x)g(x) + r(x)$, we obtain $a(\alpha)b(\alpha) = r(\alpha)$. So on dividing by $r(\alpha)$, the above equation can be rewritten as

$$\frac{a(x)b(x)}{a(\alpha)b(\alpha)} = \frac{q(x)g(x)}{r(\alpha)} + \frac{r(x)}{r(\alpha)}.$$

Since the $\tilde{w}_{\alpha,\delta}$-residue of each of $\frac{a(x)}{a(\alpha)}$, $\frac{b(x)}{b(\alpha)}$
and $\frac{r(x)}{r(\alpha)}$ is $\overline{1}$ by Lemma 1.6.2, it follows from the equation above that the $\tilde{w}_{\alpha,\delta}$-residue of $\frac{q(x)g(x)}{r(\alpha)}$ is $\overline{0}$ and hence

$$\tilde{w}_{\alpha,\delta}(q(x)g(x)) > \tilde{v}(r(\alpha))).$$

Now as $\deg q(x) < \deg g(x)$, the desired inequality follows from Theorem 1.6.1 and the above equation. ∎

Lemma 1.6.4. *With notations as above. Let $\beta \in \tilde{K}$ and $g(x) \in R[x]$ the minimal polynomial of β over K with $\bar{g}(x)$ irreducible over the residue field of υ. Assume that $\deg \beta = \deg \overline{\beta}$. Then $\overline{K(\beta)} = \overline{K}(\overline{\beta})$.*

Observe first that $\overline{\beta} \in \overline{K(\beta)}$, then $\overline{K} \subseteq \overline{K}(\overline{\beta}) \subseteq \overline{K(\beta)}$, hence $\left[\overline{K}(\overline{\beta}) : \overline{K}\right] \geqslant \left[\overline{K}(\overline{\beta}) : \overline{K}\right]$. Now in view of the fundamental inequality [[18], Theorem 3.3.4] we see immediately that $[K(\beta) : K] = \left[\overline{K}(\overline{\beta}) : \overline{K}\right] \geqslant \left[\overline{K}(\overline{\beta}) : \overline{K}\right]$. This prove that $\left[\overline{K}(\overline{\beta}) : \overline{K}\right] = \left[\overline{K}(\overline{\beta}) : \overline{K}\right]$ and hence $\overline{K(\beta)} = \overline{K}(\overline{\beta})$.

Let (K, v) be a henselian valued field of arbitrary rank with valuation ring R, maximal ideal m, residue field $\overline{K} = R/m$ and $\tilde{v}$ be the unique prolongation of v to the algebraic closure $\tilde{K}$ of K with value group $G_{\tilde{v}}$.

Theorem 1.6.8. *With notations as above. Let $g(x)$ be the minimal polynomial of α over K of degree m with $w_{\alpha,\delta}(g) = \lambda$. Then the following hold:*

1. *For any polynomial $Q(x)$ belonging to K[x] with g-expansion $\sum_i a_i g^i, \deg a_i(x) < m$, one has $w_{\alpha,\delta}(Q) = \min_i \{a_i(\alpha) + i\lambda\}$.*

2. *If $h(x)$ belonging to K[x] is a polynomial of degree less than m, then the $w_{\alpha,\gamma}$-residue of $h(x)/h(\alpha)$ equals 1.*

3. *Let e be the smallest positive integer such that $e\lambda \in G(K(\alpha))$, and $h(x)$ belonging to $K[x]$ be a polynomial of degree less than m with $\tilde{v}(h(\alpha)) = e\lambda$, then the w -residue Z of $\frac{g(x)^e}{h(x)}$ is transcendental over $\overline{K(\alpha)}$ and the residue field of $w_{\alpha,\gamma}$ is $\overline{K(\alpha)}(Z)$.*

The following theorem gives an analogue of Theorem 1.6.8 when R is a discrete valuation ring.

Theorem 1.6.9. *Let (K, v) be a henselian valued field and g, α, γ be as above. Let m denote the degree of g and (say) $w_{\alpha,\gamma}(g) = \lambda$. Then the following hold:*

1. *For any polynomial $Q(x)$ belonging to K[x] with g-expansion $\sum_i a_i g^i, \deg a_i(x) < m$, one has $w_{\alpha,\gamma}(Q) = \min_i \{a_i(\alpha) + i\lambda\}$*

2. *If $A(x)$ belonging to K[x] is a polynomial of degree less than m, then the $w_{\alpha,\gamma}$-residue of $A(x)/A(\alpha)$ equals 1.*

3. *Let e be the smallest positive integer such that $e\lambda \in \mathbb{Z}$, then the w -residue Z of $\frac{g(x)^e}{\pi^{\lambda e}}$ is transcendental over $\overline{K(\alpha)}$ and the residue field of $w_{\alpha,\gamma}$ is $\overline{K(\alpha)}(Z)$*

Definition 1.6.3. *For a (K, v)-minimal pair (α, δ), let $g(x), m, , e$ and $h(x)$ be as in Theorem 1.6.8. A monic polynomial $F(x)$ belonging to $K[x]$ is said to be a lifting of a monic polynomial $T(Y)$ belonging to $K(\alpha)[Y]$ having degree $t \geqslant 1$ with respect to (α, δ) (more precisely with respect to (α, δ) and $h(x)$ if the following three conditions are satisfied:*

1. $\deg F(x) = etm$,

2. $w_{\alpha,\delta}(F(x)) = w_{\alpha,\delta}(h(x)^t) = et\lambda$,

3. *the $w_{\alpha,\delta}$-residue of $\frac{F(x)}{h(x)^t}$ is $T\left(\overline{\frac{g(x)^e}{h(x)}}\right)$*

Theorem 1.6.2. *Let (K, v) be a complete rank-1 valued field with valuation ring R, value group G_v, residue field $\overline{K} = R/m$ and let $(\tilde{K})$ be as above. Let $g(x) \in R[x]$ be a monic polynomial of degree m having a root β with $\overline{g}(x)$ irreducible over $\overline{K}$. Let $P(x)$ belonging to $R[x]$ be a monic polynomial with g(x)-expansion $\sum_{i=0}^{s} a_i(x)g(x)^i$, $a_i(x) \neq 0$ such that $P(x) \equiv g(x)^s \mod m$. Suppose that the g-Newton polygon of $P(x)$ has k sides $S_1, ..., S_k$ having slopes $\lambda_1, ..., \lambda_k$. Then the following hold:*

1. *$P(x) = P_1(x)P_k(x)$, where each $P_i(x)$ belonging to $R[x]$ is a monic polynomial of degree ml_i whose g-Newton polygon has a single side which is a translate of S_i and l_i is the length of the horizontal projection of S_i.*

2. *If θ_i is a root of $P_i(x)$, then $\tilde{v}(g(\theta_i)) = \lambda_i$. The index $[G(K(\theta_i)) : G_v]$ is divisible by e_i, where e_i is the smallest positive integer such that $e_i\lambda_i \in G_v$ and the degree $[K(\theta_i) : K]$ is divisible by m.*

3. *$P_i(x)$ is a lifting of $T_i(Y) \in K(\beta)[Y]$ not divisible by Y of degree $\frac{l_i}{e_i}$ with respect to $g(x), \lambda_i$.*

4. *If $U_{i1}(Y)^{a_{i1}}....U_{in_i}(Y)^{ain_i}$ is the factorization of $T_i(Y)$ in to powers of distinct monic irreducible polynomials over $K(\beta)$, then $P_i(x)$ factors as $P_{i1}(x)F_{in_i}(x)$ over K, each $F_{ij}(x)$ is a lifting of $U_{ij}(Y)^{a_{ij}}$ with respect to $g(x), \lambda_i$ and has degree $me_ia_{ij} \deg U_{ij}$. If some $a_{ij} = 1$, then $F_{ij}(x)$ is irreducible over K and for any root ${}_{ij}$ of $F_{ij}(x)$, the index $[G(K(\theta_{ij})) : G_v] = e_i$ and the degree $[K(\theta_{ij}) : K] = m \deg U_{ij}$ in this case.*

The following Theorem gives an analogue of Ores Theorem for Dedekind domains similar to the one in the classical case as well as a refinement of Dedekinds Theorem regarding factorization of prime ideals (see [39]).

Theorem 1.6.3. *Let R be a Dedekind domain with quotient field K and $L = K(\alpha)$ be a finite separable extension of K with α in the integral closure O_L of R in L. Let $P(x)$ be the minimal polynomial of α over K and $\mathfrak{p}$ be a non-zero prime ideal of R. Suppose that $P(x) \equiv g_1(x)^{l_1}....g_r(x)^{l_r} \mod \mathfrak{p}$, where $g_i(x) \in R[x]$ are monic polynomials which are distinct and irreducible $\mod \mathfrak{p}$. Let m_i denote the degree of $g_i(x)$ and let β_i be one of its roots, then $\mathfrak{p}O_L = \mathfrak{b}_1....\mathfrak{b}_r$ where $\mathfrak{b}_1, ..., \mathfrak{b}_r$ are coprime ideals of L and $N_{L/K}(\mathfrak{b}_i) = \mathfrak{p}^{m_i l_i}$. Let υ denote the valuation of K with valuation ring $R_\mathfrak{p}$ and value group $\mathbb{Z}$. Suppose that the g_i -Newton polygon of $P(x)$ with respect to υ has k_i sides $S_{i1}, ..., S_{ik_i}$ of negative slopes $\lambda_{i1}, ..., \lambda_{ik_i}$. Let e_{ij} denote the smallest positive integer for which $e_{ijij} \in \mathbb{Z}$ and v_{ij} the length of the horizontal projection of S_{ij}. Then, over the completion $(\widehat{K}, \widehat{\upsilon})$ of (K, υ), $P(x)$ factors as $\prod_{i=1}^{r} \prod_{i=1}^{k_i} P_{ij}(x)$, where $P_{ij}(x) \in R_{\widehat{\upsilon}}[x]$ is a monic polynomial of degree m_iv_{ij} , which is a lifting of a polynomial $T_{ij}(Y) \in K(\beta_i)[Y]$ having degree v_{ij}/e_{ij} with respect to $g_i, |ambda_{ij}$. If $U_{i1}(Y)^{a_{i1}}....U_{in_i}(Y)^{ain_i}$ is the factorization of $T_{ij}(Y)$, into a product of powers e of distinct monic irreducible polynomials over $K(\beta_i)$, then $\mathfrak{b}_i = \prod_{j=1}^{k_i} \left(\prod_{l=1}^{n_{ij}} \mathfrak{a}_{ijl}\right)^{e_{ij}}$ where $\mathfrak{a}$ are coprime ideals of O_L for $1 \leqslant j \leqslant k_i, 1 \leqslant l \leqslant n_{ij}$ and $N_{L/K}(\mathfrak{a}_{ijl}) = \mathfrak{p}^{m_i a_{ijl} \deg U_{ijl}}$. If some $a_{ijl} = 1$, then a_{ijl} is a prime ideal of O_L.*

Corollary 1.6.1. *Let R, K, L, O_L, $P(x) \equiv g_1(x)^{l_1}...g_r(x)^{l_r} \mod \mathfrak{p}$ and υ be as in the above theorem. Let $P(x) = \sum_j a_{ij}g(x)^i$ be the $g_i(x)$-expansion of $P(x)$. Assume that*

$$\frac{v_G(a_{ij}(x))}{j} \geqslant v_G(a_{i0}(x)), \quad 1 \leqslant j \leqslant l_i - 1, \quad \gcd(v_G(a_{i0}(x)), li) = 1, 1 \leqslant i \leqslant r$$

Then $\mathfrak{p}O_L = \mathfrak{b}_1^{l_1}...\mathfrak{b}_r^{l_r}$, *where* $\mathfrak{b}_1, ..., \mathfrak{b}_r$ *are distinct prime ideals of* O_L *and the residual degree of* $\mathfrak{b}_i/\mathfrak{p}$ *is* $\deg g(x)$ *for each* i.

Chapter 2

Triangular basis and index over Principal ideal domains

2.1 Preliminaries

2.1.1 Triangular family relative to a basis

Let R be a commutative ring. We will say that the matrix $M = (a_{ij})_{1\leq j\leq n}^{1\leq i\leq n} \in \mathcal{M}_n(R)$ is a lower triangular matrix if $a_{ij} = 0$ for all $i < j$ (see [[**?**], p.50 and [45], p. 493]).

Let M be a free R-module of finite rank $n \geq 2$ and $\mathcal{B} = \{e_1, e_2, ..., e_n\}$ a basis of M. A family $\mathcal{S} = \{x_1, x_2, ..., x_n\}$ of M is said a triangular family of M relative to $\mathcal{B}$ if there exists an upper triangular $n \times n$ square matrix $W = (a_{ij})$ such that W^{-1} is the passage matrix between the basis $\mathcal{B} = \{e_1, e_2, ..., e_n\}$ and the family $\mathcal{S}$. In other words:

$$x_j = \sum_{i=1}^{j} a_{ij}e_i$$

for any index j such that $1 \leq j \leq n$. Let $\mathcal{B}^* = \{e_1^*, ..., e_n^*\}$ be the dual basis of $\mathcal{B}$. Then a family $\mathcal{S} = \{x_1, x_2, ..., x_n\}$ of M is triangular family of M relative to $\mathcal{B}$ if for every index $1 \leq k \leq n-1$, one has $e_j^*(x_k) = 0$, for all index $j \geq k+1$.

2.1.2 Modules over principal ideal domain

Let R be a principal ideal domain (PID). Let M be a free R-module of finite rank $n \geq 2$. Let N be a submodule of M. The Theorem of aligned bases (see Theorem 2.1.1) states that there exist a basis $\mathcal{B} = \{e_1, ..., e_n\}$ of M, an integer $q \leq n$, a sequence of non zero elements a_1, ..., a_q of R

such that $\{a_1e_1, ..., a_qe_q\}$ is a basis of N and a_i divides a_{i+1} or any index $1 \leq i \leq q-1$. (see [[45]Theorem 2.7 p. 539], [[7]Theorem 1 AVII p.17] and [[59]Theorem 1 p.26]).

Theorem 2.1.1 (Theorem of aligned bases)**.** *Let R be a principal ideal domain (PID). Let K be the quotient field of R. Let M be a free R-module of finite rank $n \geq 2$. Let N be a submodule of M. Then:*

1. *N is a free submodule of M of finite rank $m \leq n$*
2. *There exist a basis $\mathcal{B} = \{e_1, ..., e_n\}$ of M, an integer $q \leq n$, a sequence of non zero elements $a_1, ..., a_q$ de R such that $\mathcal{B}' = \{a_1e_1, ..., a_qe_q\}$ is a basis of N and a_i divides a_{i+1} or any index $1 \leq i \leq q-1$.*

The pair of bases $\mathcal{B}$ and basis $\mathcal{B}'$ is called a pair of aligned bases. Note that if R is a principal ideal domain then an R-module M is torsion free if and only if M is an R-module free ([[**?**] Theorem 5 p. 442]).

Corollary 2.1.1. *Let R be a principal ideal domain. Then every torsion free R-module is a free R-module.*

Theorem 2.1.2 (HNF-Basis)**.** *(see [14], Theorem 4.7.3, p. 189) Let M be a free $\mathbb{Z}$-module of rank $n \geq 2$. Let $\alpha_1, ..., \alpha_n$ be a $\mathbb{Z}$-basis of M. Then for any $\mathbb{Z}$-submodule N of M, there exists a unique basis (modulo invertible matrix) $\omega_1, ..., \omega_n$ of N such that if we write*

$$\omega_j = \frac{1}{d}\left(\sum_{i=1}^{n} \omega_{ij}\alpha_i\right),$$

where d is the denominator of M with respect to N, then the $n \times m$ matrix $W = (\omega_{ij})$ satisfies the following conditions:

1. *For all i and j the $w_{i,j} \in R$ are in $\mathbb{Z}$.*
2. *W is an upper triangular matrix, i.e., $\omega_{ij} = 0$ if $i > j$.*
3. *For every i, we have $\omega_{ii} > 0$.*
4. *For every $j > i$ we have $0 \leq \omega_{ij} < \omega_{ii}$.*

Remark 2.1.1. *Let R be a commutative principal ideal domain, M be a free R-module of rank $n \geq 2$ and N be a submodule of M. Let $\mathcal{B} = \{e_1, ..., e_n\}$ be a free basis of M and $u \in M^* = Hom_R(M, R)$. Then, $u(M)$ is an ideal of R. Moreover, if $u = e_n^*$ then $M = Ker(u) \bigoplus Re_n$.*

Then, $\mathcal{B}_0 = \{e_1, ..., e_{n-1}\}$ is a free basis of $Ker(u)$ which is a free R-module of rank $n-1$. Then, $N \cap Ker(u)$ is a direct summand of N. For any $1 \leq k \leq n$, we put $N_k = N \cap (\bigoplus_{i=1}^{k} Re_i)$. In particular, we have $N_1 = N \cap Re_1$, $N_n = N$ and $N_{n-1} = N \cap Ker(e_n^*)$.

Notice that $e_j^*(N_k) = 0$ for every index j such that $k+1 \leq j \leq n$.

Lemma 2.1.1. *Let R be a commutative principal ideal domain, M be a free R-module of rank n and N be a submodule of M. Let $u \in M^*$. Then, there is $x \in N$ such that $N = Rx \bigoplus (N \cap Ker(u))$ and $u(N) = u(x)R$.*

Proof. Let $a_u \in R$ such that $u(N) = a_u R$. Let $x \in N$ such that $u(x) = a_u$ and $y \in N$, then there exists $\lambda \in R$ such that $u(y) = \lambda a_u = \lambda u(x)$. Namely, $y - \lambda x \in Ker(u)$ with $y = \lambda x + (y - \lambda x)$. Therefore, $N = Rx + (N \cap Ker(u))$. On the other hand, If $y \in Rx \cap (N \cap Ker(u))$, then $y = \lambda x$ for $\lambda \in R$, as well $u(y) = u(\lambda x) = \lambda a_u = 0$ thus $\lambda = 0$ and $y = 0$.

With the above notation, we shall prove the following theorem which gives a slightly simple proof of the existence of triangular basis $\mathcal{B}$ of submodules of a finitely generated free module over a principal ideal domain.

Theorem 2.1.3. *Let R be a principal ideal domain, let M be a free R-module of finite rank $n \geq 2$ and N a free submodule of M such that $rk_R N = rk_R M$. Let $\mathcal{B} = \{e_1, ..., e_n\}$ be a basis of M. Let $N_k := N \cap (\oplus_{i=1}^{k} R\, e_i)$. Then there exists a basis $\mathcal{B}' = \{x_1, ..., x_n\}$ of N such that for every index $1 \leq k \leq n$, one has*

1. *$N_k = \oplus_{i=1}^{k} R\, x_i$,*
2. *$e_k^*(N_k) = e_k^*(x_k)R$.*

The following lemma is already known. Its proof is omitted (see [26], Theorem 6.1, p.336, [**?**], Theorem 6.2, p.143).

Lemma 2.1.2. *Let R be a principal ideal domain, let M be a free R-module of finite rank $n \geq 2$ and N be a submodule of M. Then N is a free R-module of finite rank $m \leq n$.*

Proof. (Theorem 2.1.3) We use induction on n the rank of M. We start with our base case, $n = 2$. Since R is a PID there exists $x_1 \in N_1$ such that $e_1^*(N_1) = e_1^*(x_1)R$. It is clear that $Rx_1 \subseteq N_1$. Conversely let $y \in N_1$, hence there exists $\lambda, \lambda' \in R$ such that $y = \lambda e_1$ and $e_1^*(y) = \lambda = \lambda' e_1^*(x_1)$, consequently $y = \lambda' e_1^*(x_1)e_1 = \lambda' x_1$, this shows that $N_1 = Rx_1$. Now by applying Lemma 2.1.1 with $f = e_2^*$, we see that there exists $x_2 \in N$ such that $N = Rx_2 \oplus (N \cap \ker e_2^*)$

and $e_2^*(N) = e_2^*(x_2)R$. Keeping this in mind and using the fact that $\ker e_2^* = Re_1$, we see immediately that $N \cap ker\, e_2^* = N \cap R\, e_1 = N_1$, in other words $N = Rx_2 \oplus N_1 = Rx_2 \oplus Rx_1$, so the base case holds. Assume, by induction, that theorem holds for all modules whose free rank n' is at most $n-1$. Set $M' = ker(e_n^*)$ and $N' = N \cap ker(e_n^*)$. Observe first that since $ker\, e_n^* = \oplus_{i=1}^{n-1} R\, e_i$, we have $N' = N \cap ker\, e_n^* = N_{n-1}$. Now by Lemma 2.1.1 there exist $x \in N$ such that $N = Rx \oplus N_{n-1} = Rx \oplus N'$. By lemma 2.1.2 N' is a free R-module of finite rank $m \leq n$. As $rk_R\, N = n$ then x is non zero, for otherwise $N = N' \subseteq M'$, which is impossible as $rk_R\, M' = n-1$. This prove that $rk_R N' = n-1$ as $rk_R\, N' + 1 = rk_R\, N = n$. Then on applying the inductive hypothesis to the free R-module M' and its submodule N', we see that there exist $\mathcal{B}'' = \{x_1, ..., x_{n-1}\}$ a basis of N' such that for every index $1 \leq k \leq n-2$, one has $e_j^*(x_k) = 0$, for all index $j \geq k+1$ (e.i., $\mathcal{B}''$ is a triangular basis of N' relative to $\mathcal{B}_0' = \{e_1, e_2, ..., e_{n-1}\}$). As $N = Rx \oplus N'$ and $N' = \oplus_{i=1}^{n-1} R\, x_i$ then $N = \oplus_{i=1}^{n} R\, x_i$ where $x_n = x$. Now using the fact that x is non zero, we see that $\mathcal{B}' = \{x_1, ..., x_n\}$ is a triangular basis of N relative to $\mathcal{B}$. This completes the proof of Theorem 2.1.3. ∎

Let R be a commutative ring, $M,\ N$ be two free R-modules of the same rank n such that $N \subseteq M$. Then there exists a homomorphism of R-modules, f such that $N = f(M)$, (if $N = \oplus_{i=1}^{n} y_i R$, $M = \oplus_{i=1}^{n} x_i R$ and $y_j = \sum_{i=1}^{n} a_{ij} x_i$, where $a_{ij} \in R$, then we set $f(x_i) = y_i$). The principal ideal $\det(f)\, R$ solely depends on N and M (is independent of the choice of the homomorphism of R-modules f). Then we put $[M : N]_R = \det(f)\, R$. This ideal $[M : N]_R$ of R is called the index ideal of N in M (for details on the index ideal, see [[8] p. 10), [[24] Theorem 13, p.95] and [11]). It is clear that $[M : N]_R M \subseteq N$.

The index ideal $[O_L : R[\alpha]]_R$ of R is called the index of α over R and may also be denoted by $\mathrm{Ind}_R(\alpha)$. It is clear that if R is a principal ideal domain then there exists $d \in R$ such that $[O_L : R[\alpha]]_R = d\, R$. In particular $d\, M \subseteq N$.

2.2 Triangular basis over (PID)

Let R be a principal ideal domain (PID). Let K be the quotient field of R, L a finite separable extension of K of degree $n \geq 2$. In this section we consider the problem of existence of triangular basis of O_L the integral closure of R in L. It may pointed out that our description of triangular integral basis is different and using only module theoretical considerations.

Definition 2.2.1. *A triangular integral basis of L over K is an integral basis $\mathcal{B} = \{x_1, x_2, ...x_n\}$ of O_L such that $x_1 = 1$ and $x_{i+1} = \frac{g_i(\alpha)}{\lambda_i}$ such that for all $1 \leq i \leq n-1$ the polynomial $g_i \in R[X]$ is monic of degree i and $\lambda_i \in R$.*

Let R be a commutative ring, M, N be two free R-modules of the same rank n such that $N \subseteq M$. Then there exists a homomorphism of R-modules, f such that $N = f(M)$, (if $N = \oplus_{i=1}^{n} y_i R$, $M = \oplus_{i=1}^{n} x_i R$ and $y_j = \sum_{i=1}^{n} a_{ij} x_i$, where $a_{ij} \in R$, then we set $f(x_i) = y_i$). The principal ideal $\det(f)\, R$ solely depends on N and M (is independent of the choice of the homomorphism of R-modules f). Then we put $[M : N]_R = \det(f)\, R$. This ideal $[M : N]_R$ of R is called the index ideal of N in M (for details on the index ideal, see [[8] p. 10), [[24] Theorem 13, p.95] and [11]). It is clear that $[M : N]_R M \subseteq N$.

The index ideal $[O_L : R[\alpha]]_R$ of R is called the index of α over R and may also be denoted by $\mathrm{Ind}_R(\alpha)$. It is clear that if R is a principal ideal domain then there exists $d \in R$ such that $[O_L : R[\alpha]]_R = d\, R$. In particular $d\, M \subseteq N$.

We prove the following theorem which gives a nice divisibility relation among the denominators of the elements of integral basis which allow us in the next section to express explicitly the index as a product of denominators of a monic triangular basis.

Theorem 2.2.1. *Let R be a principal ideal domain (PID). Let K be the quotient field of R, L a finite separable extension of K of degree $n \geq 2$, O_L the integral closure of R in L, $\alpha \in O_L$ a primitive element of L. Then there exists a sequence of monic polynomials $g_i \in R[X]$ and a unique (mod Units) sequence $(\lambda_1, \lambda_2, ..., \lambda_{n-1})$ of elements of R such that*

$$\mathcal{B} = \left\{1, \frac{g_1(\alpha)}{\lambda_1}, \frac{g_2(\alpha)}{\lambda_2}, \cdots, \frac{g_{n-1}(\alpha)}{\lambda_{n-1}}\right\},$$

is an integral basis of O_L over R. Further :

1. *$g_0 = 1$ and $\deg(g_k) = k$ for any index k such that $1 \leq k \leq n-1$,*
2. *$\lambda_k \lambda_l$ divides λ_{k+l} for any k, l such that $k + l < n$. In particular λ_1^k divides λ_k for all $k < n$.*

With notations as in Theorem 2.2.1. Let $d \in R$ such that $Ind_R(\alpha) = dR$. Then $O_L \subseteq \frac{1}{d} R[\alpha]$ (see [11] and [35]). We will apply Theorem 2.1.3 to $M = \frac{1}{d} R[\alpha]$ and $N = O_L \subseteq M = \frac{1}{d} R[\alpha]$. It is clear that $\mathcal{B}_0 = \{\frac{1}{d}, \frac{\alpha}{d}, ..., \frac{\alpha^{n-1}}{d}\}$ is a basis of M. Let $e_i := \frac{\alpha^{i-1}}{d}$ and $\mathcal{B}_0^* = \{e_1^*, ..., e_n^*\}$ the dual basis of $\mathcal{B}_0$. Then $e_i^*(\alpha^{j-1}) = d\delta_{i,j}$. In particular $e_1^*(1) = d$.

Remark 2.2.1. *With notations as above. Let $\mathcal{B} = \{x_1, ..., x_n\}$ be a triangular basis of O_L relatively to $\mathcal{B}_0^* = \{e_1^*, ..., e_n^*\}$, then by Theorem 2.1.3 and the fact that $\alpha^{i-1} \in N_i := O_L \cap (\oplus_{j=1}^{i} R\, e_j)$, we see immediately that $d = e_i^*(\alpha^{i-1}) \in e_i^*(x_i)R$, hence $e_i^*(x_i)$ divides d, for any index i.*

Notation 2.2.1. *In the following we consider $d_k = e_{k+1}^*(x_{k+1})$ and $\lambda_k \in R$ such that $d = \lambda_k\, d_k$, for any index $1 \leq k \leq n-1$.*

Remark 2.2.2. *With notations as above. It may be pointed out that for any index k, $1 \leq k \leq n$, there exists $T_k \in R[X]$ of degree less than $k-1$ such that*

$$x_k = \frac{d_{k-1}\alpha^{k-1} + T_k(\alpha)}{d}.$$

Lemma 2.2.1. *With notations as in Theorem 2.2.1. Let d_k, λ_k be as in Notation 2.2.1. Let $\mathcal{B} = \{x_1, ..., x_n\}$ be a triangular basis of O_L relatively to $\mathcal{B}_0^* = \{e_1^*, ..., e_n^*\}$ the dual basis of $\mathcal{B}_0 = \{\frac{1}{d}, \frac{\alpha}{d}, ..., \frac{\alpha^{n-1}}{d}\}$. Then for any k, l such that $k + l < n$, there exists $z_{kl} \in R$ such that $\lambda_{k+l} = \lambda_k \lambda_l \, z_{kl}$. In particular if $z_i := z_{i1}$, then $\lambda_k = \lambda_1^k \prod_{i=1}^{k-1} z_i$, for any index $2 \leq k \leq n-1$.*

Proof. By Remarks 2.2.2 there exists $U \in R[X]$ of degree less than $k+l$ such that

$$x_{k+1}x_{l+1} = \frac{d_k d_l \alpha^{k+l} + U(\alpha)}{d^2}.$$

Now using the fact that $x_{k+1}x_{l+1} \in N_{k+l+1}$, we see by Theorem 2.1.3 that there exists $z_{kl} \in R$ such that $e_{k+l+1}(x_{k+1}x_{l+1}) = d_{k+l}z_{kl}$, therefore

$$\frac{d_k d_l}{d^2} = \frac{1}{\lambda_k \lambda_l} = \frac{d_{k+l}z_{kl}}{d} = \frac{z_{kl}}{\lambda_{k+l}}.$$

This proves that $\lambda_{k+l} = \lambda_k \lambda_l z_{kl}$.

To show that $\lambda_k = \lambda_1^k \prod_{i=1}^{k-1} z_i$ we use induction on k, for $k = 2$, it is clear that $\lambda_2 = \lambda_1^2 z_1$. Assume by induction that $\lambda_k = \lambda_1^k \prod_{i=1}^{k-1} z_i$, then $\lambda_{k+1} = \lambda_k \lambda_1 z_k = \lambda_1^k \prod_{i=1}^{k-1} z_i \lambda_1 z_k = \lambda_1^{k+1} \prod_{i=1}^{k} z_i$. This completes the proof of the lemma. ∎

Proof. (Theorem 2.2.1) In view of Theorem 2.1.3 there exists a triangular basis $\mathcal{B} = \{x_1, ..., x_n\}$ of O_L such that for every index $1 \leq k \leq n$, one has

$$x_k = \sum_{i=1}^{k} e_i^*(x_k) e_i = \sum_{i=1}^{k} \frac{e_i^*(x_k)}{d} \alpha^{i-1}.$$

Observe first that $e_1^*(N_1) = dR$ and using the fact that $d = e_1^*(1)$, we see immediatly by virtue of Theorem 2.1.3 that $x_1 = 1$. Now by Remark 2.2.1 we have $d = d_k \lambda_k$ for every index $2 \leq k \leq n$. It remains to be shown that for every index $2 \leq k \leq n$, there exist a monic polynomial g_{k-1} belonging to $R[X]$ such that

$$x_k = \frac{g_{k-1}(\alpha)}{\lambda_{k-1}}.$$

We use induction on k, for $k = 2$, we have

$$x_2 = \frac{e_1^*(x_2)}{d} + \frac{e_2^*(x_2)\alpha}{d} = \frac{e_1^*(x_2)}{\lambda_1 d_1} + \frac{\alpha}{\lambda_1}.$$

Keeping in mind this and using the fact that $\lambda_1 x_2 - \alpha = \frac{e_1^*(x_2)}{d_1} \in R$, we see that there exists $t_1 \in R$ such that

$$x_2 = \frac{d_1 t_1}{\lambda_1 d_1} + \frac{\alpha}{\lambda_1} = \frac{\alpha + t_1}{\lambda_1} = \frac{g_1(\alpha)}{\lambda_1}.$$

Assume, by induction, that the result holds for k such that $k < n$. Then we conclude immediately that for every index $k < n$, there exists a monic polynomial g_{k-1} belonging to $R[X]$ such that

$$x_k = \frac{g_{k-1}(\alpha)}{\lambda_{k-1}}.$$

Consequently there exists a polynomial $Q_1 \in R[X]$ of degree less than k such that

$$\alpha x_k = \frac{\alpha g_{k-1}(\alpha)}{\lambda_{k-1}} = \frac{\alpha^k + Q_1(\alpha)}{\lambda_{k-1}}.$$

Now using the fact that $\alpha x_k \in N_{k+1}$, one can write

$$\alpha x_k = \frac{e_{k+1}^*(\alpha x_k)\alpha^k + Q_2(\alpha)}{d},$$

where the polynomial $Q_2 \in R[X]$ such that $\deg Q_2 < k$, and using Theorem 2.1.3, we see that there exists $\varepsilon \in R$ such that $e_{k+1}^*(\alpha x_k) = \varepsilon d_k$ and by comparing coefficients of αx_k, we find $d = \varepsilon d_k \lambda_{k-1}$, hence $\lambda_k = \varepsilon \lambda_{k-1}$. Now by virtue of Lemma 2.2.1, we have $\lambda_k = \lambda_1 \lambda_{k-1} z_{k-1}$, this prove that $\varepsilon = \lambda_1 z_{k-1}$. Therefore

$$\begin{aligned}
\lambda_1 z_{k-1} x_{k+1} - \alpha x_k &= \frac{d_k \alpha^k + \sum_{i=1}^k e_i^*(x_{k+1})\alpha^{i-1}}{\lambda_{k-1} d_k} - \frac{\lambda_1 z_{k-1} d_k \alpha^k + Q_2(\alpha)}{d} \\
&= \frac{\lambda_1 z_{k-1} \sum_{i=1}^k e_i^*(x_{k+1})\alpha^{i-1} - Q_2(\alpha)}{d} \\
&= \frac{Q_3(\alpha)}{d},
\end{aligned}$$

where $Q_3 \in R[X]$ such that $\deg Q_3 < k$. Then by inductive hypothesis and Lemma 2.2.1, we see that there exists $a_1, ...a_k \in R$ and a polynomial $Q_4 \in R[X]$ such that

$$\lambda_1 z_{k-1} x_{k+1} - \alpha x_k = \sum_{i=1}^{k} a_i \frac{g_{i-1}(\alpha)}{\lambda_{i-1}} = \sum_{i=1}^{k} a_i \frac{g_{i-1}(\alpha)}{\lambda_1^{i-1} \prod_{t=1}^{i-2} z_t} = \frac{Q_4(\alpha)}{\lambda_{k-1}}.$$

Then in view of the Lemma 2.2.1 and the above equality one can write

$$x_{k+1} = \frac{\alpha x_k}{\lambda_1 z_{k-1}} + \frac{Q_4(\alpha)}{\lambda_{k-1}\lambda_1 z_{k-1}} = \frac{\alpha^k + Q_1(\alpha)}{\lambda_{k-1}\lambda_1 z_{k-1}} + \frac{Q_4(\alpha)}{\lambda_{k-1}\lambda_1 z_{k-1}} = \frac{\alpha^k + Q_1(\alpha) + Q_4(\alpha)}{\lambda_k} = \frac{g_k(\alpha)}{\lambda_k}.$$

This proves that

$$\mathcal{B} = \left\{1, \frac{g_1(\alpha)}{\lambda_1}, \frac{g_2(\alpha)}{\lambda_2}, \cdots, \frac{g_{n-1}(\alpha)}{\lambda_{n-1}}\right\},$$

is a integral basis of O_L over R. Now by virtue of Lemma 2.2.1 there exist z_{kl} such that $\lambda_{k+l} = \lambda_k \lambda_l z_{kl}$ and $\lambda_k = \lambda_1^k \prod_{i=1}^{k-1} z_i$, for any index $2 \leq k \leq n-1$, this prove that for any index $2 \leq k \leq n-1$, λ_1^k divides λ_k in R and hence

1. $g_0 = 1$ and $\deg(g_k) = k$ for any index k such that $1 \leq k \leq n-1$,

2. $\lambda_k \lambda_l$ divides λ_{k+l} for any k, l such that $k + l < n$. In particular λ_1^k divides λ_k for all $k < n$.

Example 3.1. Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field where m is cubic free and $m \neq \pm 1$. Write $m = ab^2$ with a and b square free, coprime. Let α be the cube root of m belonging to K and $\mathbb{Z}_K$ the integral closure of $\mathbb{Z}$ in K. Assume that $a^2 \equiv b^2$ modulo 9. Then by [[14], Theorem 6.4.13, p.346]. We have $(1, \alpha, \frac{\alpha^2 + ab^2\alpha + b^2}{3b})$ is a triangular integral basis of $\mathbb{Z}_K$. Consequently in view of Theorem 2.2.1 we see immediately that $\lambda_1 = 1, \lambda_2 = 3b, n = 3$.

Example 3.2. Let K be a quintic number field defined by an irreducible trinomial $f(X) = X^5 + aX^2 + b \in \mathbb{Z}[X]$, $\mathbb{Z}_K$ its ring of integers, α a complex root of $f(X)$. Assume that $p = 2$, $v_2(b) = 2k \geq 4$, $v_2(a) = 2$ and $a_2 + b_2 \equiv 2 \mod 4$. Then by [[19], Theorem 2.3]. We have $(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2}, \frac{\alpha^4 + a\alpha}{2^{k+1}})$ is a 2-integral basis of K. Now using Theorem 2.2.1 we conclude that $n = 5$, $\lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_3 = 4$, $\lambda_4 = 2^{k+1}$ in this case as well.

Example 3.3. By [[20], Table 4, p.13], the family $\mathcal{B} = (1, \frac{w}{4}, \frac{w}{16}, \frac{w^3}{64})$ is a 2-integral basis of the quartic number field K generated by the irreducible polynomial $f(X) = X^4 + aX^2 + bX + c \in \mathbb{Z}[X]$. Set $\lambda = 4$ and $\mu_1 = \mu_2 = 1$, then it clear that $\mathcal{B} = (1, \frac{w}{\lambda}, \frac{w}{\lambda^2 \mu_1}, \frac{w^3}{\lambda^3 \mu_2})$ which give a approvement of Theorem 2.2.1.

2.3 Factorial divisors of the Index over (PID)

Theorem 2.2.1 ensures that there exists a triangular integral basis $\mathcal{B} = \{1, \frac{g_1(\alpha)}{\lambda_1}, \frac{g_2(\alpha)}{\lambda_2}, \cdots, \frac{g_{n-1}(\alpha)}{\lambda_{n-1}}\}$ of O_L over R such that $\lambda_k\lambda_l$ divides λ_{k+l} for any index k, l such that $k + l < n$. Now using this divisibility relation among the denominators of the elements of $\mathcal{B}$ we prove i that there exists a unique (mod Units) sequence $(k_1, k_2, ..., k_{n-1})$ of elements of R such that $\mathrm{Ind}_R(\alpha) = \left(k_1k_2^2....k_{n-3}^{n-3}k_{n-2}^{n-2}k_{n-1}^{\frac{n(n-1)}{2}}\right) R$ which extend the result of M. Hall for cubic numbers (see [30]) to the case when $L = K(\alpha)$ is a finite relative algebraic extension of K of degree n and R is a principal ideal domain (see Remark 2.3.1). Precisely stated, we prove:

Theorem 2.3.1. *Let R be a principal ideal domain (PID). Let K be the quotient field of R, L a finite separable extension of K of degree $n \geq 2$, O_L the integral closure of R in L, $\alpha \in O_L$ a primitive element of L. Then there exists a unique (mod Units) sequence $(k_1, k_2, ..., k_{n-1})$ of elements of R such that*

$$\mathrm{Ind}_R(\alpha) = \left(k_1k_2^2....k_{n-3}^{n-3}k_{n-2}^{n-2}k_{n-1}^{\frac{n(n-1)}{2}}\right) R.$$

Proof.

By Theorem 2.2.1 the set

$$\mathcal{B} = \left\{1, \frac{g_1(\alpha)}{\lambda_1}, \frac{g_2(\alpha)}{\lambda_2}, \cdots, \frac{g_{n-1}(\alpha)}{\lambda_{n-1}}\right\}.$$

is a integral basis of O_L over R. Now using the definition of $\mathrm{Ind}_R(\alpha) = [O_L : R[\alpha]]_R$ (See Section 4.2) we see that $\mathrm{Ind}_R(\alpha) = \det M$ where $M = Mat(\mathcal{B}', \mathcal{B})$ is the passage matrix of $\mathcal{B}' = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ to $\mathcal{B}$ hence

$$\mathrm{Ind}_R(\alpha) = \left(\prod_{i=1}^{n-1} \lambda_i\right) R,$$

such that λ_1^k divides λ_k for all $k < n$ and there exist z_i in R such that $\lambda_k = \lambda_1^k \prod_{i=1}^{k-1} z_i$, for any index $2 \leq k \leq n-1$ in view of Lemma 2.2.1. Consequently

$$\begin{aligned}
\mathrm{Ind}_R(\alpha) = \left(\prod_{i=1}^{n-1} \lambda_i\right) R &= \left(\lambda_1\lambda_1^2z_1\lambda_1^3z_1z_2....\lambda_1^{n-1}z_1z_2....z_{n-1}\right) R, \\
&= \lambda_1^{\frac{n(n-1)}{2}} \prod_{i=2}^{n-1} \left(\prod_{t=1}^{i-1} z_t\right) R, \\
&= \left(\lambda_1^{\frac{n(n-1)}{2}} z_1^{n-2}z_2^{n-3}.....z_{n-3}^2z_{n-2}\right) R.
\end{aligned}$$

Set $k_{n-1} = \lambda_1$ and $k_{n-(i+1)} = z_i$ for $1 \leqslant i \leqslant n-2$ then we see immediatly that

$$\mathrm{Ind}_R(\alpha) = \left(k_1 k_2^2 .... k_{n-3}^{n-3} k_{n-2}^{n-2} k_{n-1}^{\frac{n(n-1)}{2}} \right) R.$$

∎

Remarks 2.3.1. *1. With notations as above. Let $d_k = e^*_{k+1}(x_{k+1})$ and $\lambda_k \in R$ such that $\lambda_k\, d_k = d$, for any index k. Then by Lemma 2.2.1 there exists $\varepsilon_n \in R$ such that $\lambda_n = \lambda_1^n\, \varepsilon_n$ and hence $d = \lambda_1^n\, \varepsilon_n\, d_n$. In particular if $n = 3$ then $d = \lambda_1^3\, \varepsilon_3$ since in this case $d_3 = 1$ (see [Lemma p. 105 in [30]]).*

2. Theorem 2.2.1 gives a slight simple proof of the existence of triangular basis $\mathcal{B}$ of submodules of a finitely generated free module over principal ideal domain (PID). It may pointed out that the proof is novel and use only module theoretical considerations. For $R = \mathbb{Z}$, the existence of triangular integral basis of O_L over R is already known and apparently somewhat classical (see [5]).

2.4 Applications

Being able to read off the index of certain element from the triangular integral basis is a nice proprerty, Using our main result, we are going now to prove the following theorem which allow us to read off the ideal index only from the ascending Power Decomposition (APD) of α^p where where α is a root of an irreducible polynomial $P(x) = x^p - a$ belonging to $\mathbb{Z}[X]$.

Theorem 2.4.1. *Let p be a prime number and $K = \mathbb{Q}(\alpha)$ be an algebraic number field, where α is a root of an irreducible polynomial $P(x) = x^p - a$ belonging to $\mathbb{Z}[X]$. Assume that a is p^{th} power free which is expressed as $t_1 t_2^2 .... t_{p-2}^{p-2} t_{p-1}^{p-1}$ with each t_i squarefree and t_i, t_j coprime for $i \neq j$.. Assume that $p^2 \nmid (a^{p-1} - 1)$ and set $z_i = t_{p-i}^{\frac{p-1}{2}}$, then the ideal index $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$ is given by*

$$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = z_1^{p-2} z_2^{p-3} .... z_{p-3}^2 z_{p-2}.$$

The following simple lemma is already known. Its proof is omitted (see [[32],Lemma 4.A]).

Lemma 2.4.1. *Le p a prime number and $N_{i,j}$ denote the largest integer not exceeding $\frac{ij}{p}$, $1 \leq i, j \leq p-1$, then for $1 \leq j \leq p-1$, we have*

$$\sum_{i=1}^{p-1} \left[\frac{ij}{p} \right] = \frac{(p-1)(j-1)}{2}.$$

Proof. Let λ_i denote the element $t_1^{\left[\frac{i}{p}\right]}t_2^{\left[\frac{2i}{p}\right]}....t_{p-2}^{\left[\frac{i(p-2)}{p}\right]}t_{p-1}^{\left[\frac{i(p-1)}{p}\right]}$ of K, where $\left[\frac{ij}{p}\right]$ stands for the largest integer not exceeding $\frac{ij}{p}$, then by Theorem 1.2 [32] the set

$$\left\{1, \frac{\alpha}{\lambda_1}, \frac{\alpha^2}{\lambda_2}, ..., \frac{\alpha^{p-1}}{\lambda_{p-1}}\right\},$$

is an integral basis of K. Now using our main result one can write

$$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = \prod_{i=1}^{p-1}\lambda_i = \prod_{i=1}^{p-1}\left(t_1^{\left[\frac{i}{p}\right]}t_2^{\left[\frac{2i}{p}\right]}....t_{p-2}^{\left[\frac{i(p-2)}{p}\right]}t_{p-1}^{\left[\frac{i(p-1)}{p}\right]}\right) = t_1^{\sum_{i=1}^{p-1}\left[\frac{i}{p}\right]}t_2^{\sum_{i=1}^{p-1}\left[\frac{2i}{p}\right]}....t_{p-2}^{\sum_{i=1}^{p-1}\left[\frac{(p-2)i}{p}\right]}t_{p-1}^{\sum_{i=1}^{p-1}\left[\frac{(p-1)i}{p}\right]}.$$

Now using the fact for $1 \leq i, j \leq p-1$, we have $\sum_{i=1}^{p-1}\left[\frac{ij}{p}\right] = \frac{(p-1)(j-1)}{2}$ (see Lemma 2.4.1), we see immediately that

$$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = t_2^{\frac{p-1}{2}}t_3^{p-1}....t_{p-2}^{\frac{(p-1)(p-3)}{2}}t_{p-1}^{\frac{(p-1)(p-2)}{2}} = t_2^{\frac{p-1}{2}}\left(t_3^{\frac{p-1}{2}}\right)^2....\left(t_{p-2}^{\frac{(p-1)}{2}}\right)^{p-3}\left(t_{p-1}^{\frac{(p-1)}{2}}\right)^{p-2}.$$

Since $\sum_{i=1}^{p-1}\left[\frac{i}{p}\right] = 0$, then $z_{p-1} = 1$. Set $z_i = t_{p-i}^{\frac{p-1}{2}}$, then the ideal index $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$ is given by

$$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = z_1^{p-2}z_2^{p-3}....z_{p-3}^2z_{p-2}.$$

We are going in table 1 to schematizes our results for $p = 3, 5, 7, 11$.

Table 2.1: The ideal index $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$

p	(APD) of a	The ideal index $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$
p=3	$a = t_1t_2^2$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = z_1 = t_2$
p=5	$a = t_1t_2^2t_3^3t_4^4$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = z_1^3z_2^2z_3 = \left(t_2t_3^2t_4^3\right)^2$
p=7	$a = t_1t_2^2t_3^3t_4^4t_5^5t_6^6$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = z_1^5z_2^4z_3^3z_4^2z_5 = \left(t_2t_3^2t_4^3t_5^4t_6^5\right)^3$
p=11	$a = t_1t_2^2t_3^3t_4^4t_5^5t_6^6t_7^7t_8^8t_9^9t_{10}^{10}$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha) = z_1^9z_2^8z_3^7z_4^6z_5^5z_6^4z_7^3z_8^2z_9 = \left(t_2t_3t_4t_5t_6t_7t_8t_9t_{10}\right)^5$

Table 1 above show that we can calculte the $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$ for pure number fields directly from The ascending Power Decomposition (APD) of a we give here some useful exemples for $p = 3, 5, 7, 11$. Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field, where α is a root of an irreducible polynomial $P(x) = x^p - a$ belonging to $\mathbb{Z}[X]$.

Table 2.2: The ideal index $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$ for pure number fields

p	a	(APD) of a	The ideal index $\mathrm{Ind}_{\mathbb{Z}}(\alpha)$
$p=3$	13475	$11.35^2.$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha)=35$
$p=5$	11466000	$13.21^2.5^3.2^4$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha)=17640000$
$p=7$	5244319080000	$13.11^2.7^3.5^4.3^5.2^6$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha)=185427026509824000000000$
p=11	5576850000	$17.2^4.5^5.3^8$	$\mathrm{Ind}_{\mathbb{Z}}(\alpha)=15634857843437408437500000000000000000$

Chapter 3

On the normality of a monogenic algebra

3.1 Definitions and some preliminary results

Let R be a commutative ring. An R-algebra B is said to be monogenic if there exist a monic polynomial $P \in R[X]$ such that $B = R[X]/(P)$, which is the same as saying that there exist an element α such that $B = R[\alpha]$. In this case, the element $\alpha = X \mod P$ is called a monogenic element of B over R and the family $\{1, \alpha, \alpha^2 .....\alpha^{n-1}\}$ is indeed a basis of B over R.

Definition 3.1.1. *A commutative ring R is called normal if for every prime p the localization R_p is integrally closed.*

Proposition 3.1.1. *Let R be an integral domain. Then the following are equivalent :*

1. *R is integrally closed,*
2. *$R_{\mathfrak{p}}$ is integrally closed, for each prime ideal $\mathfrak{p}$,*
3. *$R_{\mathfrak{p}}$ is integrally closed, for each maximal ideal $\mathfrak{p}$.*

Proposition 3.1.2. *Let R be an integral domain. Then R is normal if and only if R is integrally closed.*

Proof. If R is integrally closed then R is normal in view of Proposition 3.1.1. Assume now that R is normal and let $x \in K$ the fraction field of R, then $x \in R_{\mathfrak{p}}$ for any prime ideal $R_{\mathfrak{p}}$ of R and using the fact that $R = \bigcap^{\mathfrak{p}} R_{\mathfrak{p}}$, we see immediatly that $x \in R$. ∎

Remark 3.1.1. *It may pointed out that in the case of an integral domain the notion of being normal and integrally closed are the same.(see Proposition 3.1.2 above.)*

Let R be a commutative ring with a unit, $P \in R[X]$ a monic polynomial, and $B = R[X]/(P)$ the monogenic R-algebra associated to P. For an ideal I in R, it can be easily checked that

$$B/IB \simeq R[X]/(IR[X] + PR[X]).$$

When R is integrally closed, it can be shown that $B \cong R[\alpha]$, where α is integral over R and $P = \mathrm{Irrd}(\alpha, R)$. Then using the ideas of Kummer's Theorem ([35, p. 38]) one can show the following.

Proposition 3.1.3. *Let R be an integrally closed domain, K its quotient field, $\mathfrak{m}$ a maximal ideal of R, and $k = R/\mathfrak{m}$. Let $P \in R[X]$ be a monic irreducible polynomial and $\overline{P}(X) = \prod_{i=1}^{r} \overline{P}_i^{e_i}(X)$ the decomposition of $\overline{P}(X)$ into monic irreducible factors in $k[X]$. If we let α be a root of P in an algebraic closure of K, then the only prime ideals of $R[\alpha]$ which contain $\mathfrak{m}$ are the ideals*

$$\mathfrak{m}_1,\ \mathfrak{m}_2, \cdots, \mathfrak{m}_r,$$

where $\mathfrak{m}_i = P_i(\alpha) R[\alpha] + \mathfrak{m}R[\alpha]$ and P_i is a monic lift of $\overline{P}_i$ in $R[X]$. Furthermore, the $\mathfrak{m}_i$ are maximal.

Theorem 3.1.1. *([47], Theorem 11.4, p.81) Let R be a Notherian integral domain, and P a non-zero prime ideal of R, If P is inversible then $htP = 1$ and R_p is DVR.*

The following theorem is an immediate consequence of Proposition 3.1.1 and Theorem 3.1.1.

Theorem 3.1.2. *Let R be a Notherian integral domain of krull dimension 1, Then R is normal if and only if all non-zero prime ideals of R are inversibles.*

3.2 Dedekind criterion

Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with α an algebraic integer and P be the minimal polynomial of α over the field $\mathbb{Q}$ of rational numbers. Let O_K denote the ring of algebraic integers of K. The dermination of the prime ideal decomposition in O_K of any rational prime p is one of the major problems in Algebraic Number Theory and is related to the decomposition of the polynomial $\overline{P}$ obtained by replacing each coefficient of P by its residue modulo p. In 1878 Dedekind proved the following result in this direction.

Theorem 3.2.1. *Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with P as the minimal polynomial of the algebraic integer α over $\mathbb{Q}$. Let p be a rational prime. Let $\overline{P} = \overline{P_1}^{l_1} ... \overline{P_r}^{l_r}$ be the factorization of*

$\overline{P}$ as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, with P_i monic polynomials belonging to $\mathbb{Z}[X]$. Suppose that p does not divide the index of the subgroup $\mathbb{Z}[X]$ in O_K; then $pO_K = \mathfrak{P}_1^{l_1}....\mathfrak{P}_\mathfrak{r}^{l_\mathfrak{r}}$, where $\mathfrak{P}_1...\mathfrak{P}_\mathfrak{r}$ are distinct prime ideals of O_K, $\mathfrak{P}_\mathfrak{i} = pO_K + P_i(\alpha)O_K$ with residual degree $f(\mathfrak{P}_\mathfrak{i}/p) = \deg \overline{P_i}$ for all i.

Dedekind also gave a criterion to verify when the condition p does not divide $[O_K : \mathbb{Z}[\alpha]]$ is satisfied.

Theorem 3.2.2. *Let $K = \mathbb{Q}(\alpha)$, P and $P_1.....P_r$ be as in the above theorem. Let G denote the polynomial $\frac{1}{p}\left(P - P_1^{l_1}...P_r^{l_r}\right)$ with coefficients from $\mathbb{Z}$. Then p does not divide $[O_K : \mathbb{Z}[\alpha]]$ if and only if for each i, we have either $l_i = 1$ or $\overline{P_i}$ does not divide $\overline{G}$.*

In 2006, Ershov formulated and proved a generalization of Dedekind Criterion when the base field is a general valued field. In 2010 S. K. Khanduja and M. Kumar also generalize this criterion to general valuation rings of Krull valuations by reducing the problem to henselian valuation rings. In 2020 A. JAKHAR and S.K. KHANDUJA give a simple proof of of Generalized Dedekind Criterion using elementary valuation theory.

3.2.1 Dedekind criterion over (DVR)

Let $(R, \pi R, k)$ a discrete valuation ring, $\mathfrak{p} = \pi R$ the prime ideal of R, and k its residue field. Let K the quotient field of R, L a finite extention of K, O_L the integral closure of R in L, $\alpha \in O_L$ a primitive element of L, $P = Irr(\alpha, K) \in R[X]$. The knowledge of a monogenic element of O_L (over R) permits us to compute what we want. The family $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is indeed a basis of B over R. Moreover, by Kummer's theorem, we know that the factorization modulo π of the minimal polynomial of α over K gives the factorization of π in O_L. More precisely, if $\overline{P} = \prod_{i=1}^{r} \overline{P_i}^{e_i}$ is is the primary decomposition of P modulo π then O_L has exactly r maximal ideals: $\mathfrak{p}_\mathfrak{i} = (p, p_i(\alpha))$, $1 \leq i \leq r$ for the residual degree of π equals $\deg(P_i)$, and the factorization of π is $\mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}$. Therefore we have to study monogeneity in details. Given a primitive element $\alpha \in O_L$ of L over K, we need an effective criterion to know if $O_L = R[\alpha]$. To show this equality, it is necessary and suffcient to show that $R[\alpha]$ is integrally closed. As P is irreducible, it is also equivalent to the fact that $R[\alpha]$ is a normal ring. The well known Dedekind criterion, which we recall now, permits us to decide whether $R[\alpha]$ is normal (see [14],Chapter 6, Theorem 6.1.4 page 299, or [48], Creterion of Dedekind, page 319 for $R = \mathbb{Z}$, [54], Chap 4, page 295 for discrete valuation ring).

Theorem 3.2.3. *(Dedekind Criterion) Let $(R, \pi R, k)$ be a discrete valuation ring, $\mathfrak{p} = \pi R$ the prime ideal of R, and k its residue field. Let K the quotient field of R, L a finite extention of K, O_L the integral closure of R in L, $\alpha \in O_L$ a primitive element of L, $P = Irr(\alpha, K) \in R[X]$,*

and let $P_1, ..., P_r \in R[X]$ *be arbitrary monic liftings of irreducible divisors of* P *modulo* π. *We introduce* $T \in R[X]$ *such that* $P = P_1^{l_1}, ..., P_r^{l_r} + \pi T$ *then the* R*-algebra* $R[X]/(P)$ *is normal if only if* $\gcd(\overline{P}_i, \overline{T}) = 1$ *where* $i = 1, ..., r$, $l_i \geq 2$.

Before talking the proof we need the following lemma.

Lemma 3.2.1. *Let* $(R,\ \mathfrak{p} = \pi\, R,\ k)$ *be a discrete valuation ring,* π *a uniformizer of* R, $\mathfrak{p} = \pi R$ *its maximal ideal, and* k *its residue field. Let* α *be an integral element over* R *and* $P(X) \in R[X]$ *its monic irreducible polynomial in* $R[X]$. *Let* $G, H, T \in R[X]$ *be such that* G *is monic and* $P = GH + \pi T$. *Consider the ideal* $I = \pi R[\alpha] + G(\alpha) R[\alpha] =< \pi, g(\alpha) >$ *and denote by* I^{-1} *the ideal* $\{y \in K[\alpha] \mid\ yI \subseteq\ R[\alpha]\}$. *Then*

(1) $I^{-1} = R[\alpha] + \dfrac{H(\alpha)}{\pi} R[\alpha]$.

(2) *The ideal* I *is invertible if and only if* $\left(\overline{G}, \overline{H}, \overline{T}\right) = \overline{1}$ *modulo* $\mathfrak{p}$.

Proof.

(1) Let $y \in I^{-1}$, then $\pi y \in R[\alpha]$ and $yG(\alpha) \in R[\alpha]$, This prove that

$$y = \frac{Q(\alpha)}{\pi}, \qquad \frac{Q(\alpha)G(\alpha)}{\pi} = W(\alpha),$$

where $Q, W \in R[X]$, hence P divides $QG - \pi W$ and consequently there exist $F \in R[X]$ such that $QG = FP + \pi W$, now using that fact that $\overline{P} = \overline{GH}$, we see that $\overline{Q} = \overline{FH}$ since G is monic, hence $Q = FH + \pi S$ with $S \in R[X]$. This prove that

$$y = \frac{Q(\alpha)}{\pi} = S(\alpha) + \frac{H(\alpha)}{\pi} F(\alpha) \in R[\alpha] + \frac{H(\alpha)}{\pi} R[\alpha].$$

So to complete the proof it is enough to show that $R[\alpha] + \dfrac{H(\alpha)}{\pi} R[\alpha] \subseteq I^{-1}$. Observe first that $\pi \left(R[\alpha] + \dfrac{H(\alpha)}{\pi} R[\alpha] \right) \subseteq R[\alpha]$ and using the fact that

$$\frac{H(\alpha)G(\alpha)}{\pi} = -\pi T(\alpha),$$

we see immediately that $G(\alpha) \left(R[\alpha] + \dfrac{H(\alpha)}{\pi} R[\alpha] \right) \subseteq R[\alpha]$.

(2) Observe first that $II^{-1} = \pi R[\alpha] + G(\alpha)R[\alpha] + H(\alpha)R[\alpha] + T(\alpha)R[\alpha]$ and using the fact that $\overline{P} = \overline{GH}$ we see immediately that The ideal I is invertible if and only if $\left(\overline{G}, \overline{H}, \overline{T}\right) = \overline{1}$ modulo $\mathfrak{p}$.

Proof. (of Theorem 3.2.3)

By Theorem 3.1.2 The R-algebra $R[X]/(P)$ is normal if only if all non-zero prime ideals of $R[X]/(P)$ are inversibles. Now using Proposition 3.1.3 we see that then the only prime ideals of $R[X]/(P)$ are the ideals

$$\mathfrak{P}_1,\ \mathfrak{P}_2, \cdots, \mathfrak{P}_r,$$

where $\mathfrak{P}_i = P_i(\alpha)\, R[\alpha] + \pi R[\alpha]$. Set $\overline{H}_i = \prod_{\substack{j=1 \\ j\neq i}}^{r} \overline{P}_j^{l_j}.\overline{P}_i^{l_i-1}$, for $r = 1, ..., r$. Now using Lemma 3.2.1 and that fact that $\gcd(\overline{P}_i, \overline{H}_i, \overline{T}) = \gcd(\overline{P}_i, \overline{T})$ when $l_i \geq 2$ we see that $R[X]/(P)$ is normal if only if $\gcd(\overline{P}_i, \overline{T}) = 1$ where $i = 1, ...r$, $l_i \geq 2$.

Now we provide a new simple and practicable Criterion characterizing the existence of power integral bases over an arbitrary Dedekind ring by using the Gauss valuation and the index ideal.

Let K be a nonzero commutative field and υ be a valuation on K. Let $P = a_0 + a_1X + ... + a_nX^n \in K[X]$. We put $\upsilon_G(P) = \inf\{\upsilon(a_i) \mid 0 \leq i \leq n\}$. Then υ_G is a valuation on $K[X]$ called the Gauss valuation on $K[X]$ relative to υ. Let first present a new simple version of Dedekind Criterium in global case:

Theorem 3.2.4 (Dedekind Criterium)**.** *Let R be a Dedekind ring, K its fraction field, L be a finite separable extension over K and O_L be the integral closure of R in L. Let $\alpha \in O_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $P = Irrd(\alpha, R) \in R[X]$ be the monic irreducible polynomial of α. Let $\mathfrak{p}$ be a non zero prime ideal in R and $k := R/\mathfrak{p}$ its residual field. Let $\bar{P}$ be the image in $k[X]$ of P and assume that $\bar{P} = \Pi_{i=1}^{r}\bar{P_i}^{l_i}$ is the primary decomposition of $\bar{P}$ in $k[X]$ with $P_i \in R[X]$ a monic lift of the irreducible polynomial $\overline{P_i}$ for $1 \leq i \leq r$. Let $V_i \in R[X]$ be the remainder of Euclidean division of P by P_i. Let $\upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let υ_G be the Gauss valuation on $K[X]$ associated to $\upsilon_{\mathfrak{p}}$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$.*

3.2.2 Monogenicity of relative prime-power pure extensions

Let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n. We let $disc_R(P)$ and $D_{L/K}$ denote the discriminants over R, respectively, of the polynomial $P(X)$ and the number field L over K.

We study the relative monogenicity of $L = K(\alpha)$ over its subfield where α is a root of a monic irreducible polynomial of the form

$$P(X) = X^{p^n} - \beta \in O_K[X],\ n \in \mathbb{N}^*. \tag{3.1}$$

This allow to construct an integral basis for a family of extensions $L/\mathbb{Q}$, such that $[L,\mathbb{Q}] = 2.p^n$ ($n \in \mathbb{N}^*$), and compute the discriminant of L/K. As a consequence, we compute the discriminant $D_{L/\mathbb{Q}}$ given by the tower formula:

$$D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K}).(D_{K/\mathbb{Q}})^{[L:K]}, \tag{3.2}$$

where $N_{K/\mathbb{Q}}$ denote the norm from K to $\mathbb{Q}$ (see [50, Corollary 10. 2] and [24]). We denote by Spec(R), the set of the prime ideals of a commutative ring R. Equipped with the Zariski topology, the closed sets of Spec(R) are the sets:

$$V(\mathfrak{I}) = \{\mathfrak{p} \in Spec\,(R) \mid \mathfrak{I} \subseteq \mathfrak{p}\}$$

Where $\mathfrak{I}$ is an ideal in R. Note also that for any ideal $\mathfrak{I}$ in R and $n \in \mathbb{N}^*$ we have $V(\mathfrak{I}^n) = V(\mathfrak{I})$.

Now, fix a non-zero prime ideal $\mathfrak{p} \in Spec\,(R)$. We are also interested in the set of primes $\mathfrak{q}$ in O_L with $\mathfrak{p} \subseteq \mathfrak{q}$ −or equivalently $\mathfrak{p} = \mathfrak{q} \cap R$− and we call that set for the fibre over $\mathfrak{p}$, denoted by $Fib_R(\mathfrak{p})$.

With the above notation we prove

Theorem 3.2.5. *Let R be a Dedekind ring with finite residual field and K its fraction field. Assume that $charK = 0$ and $L = K(\alpha)$ is a finite separable extension of K. Let $P = X^{p^n} - \beta \in R[X]$ be the monic minimal polynomial of α. Then*

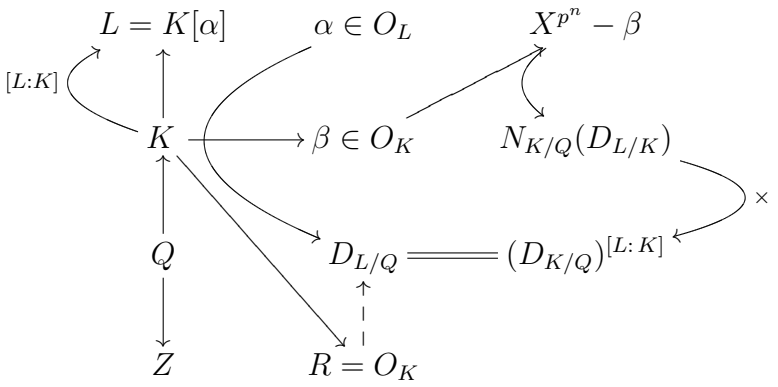
1. *If the $\mathfrak{q}-$adic valuation $v_{\mathfrak{q}}(\beta) \geq 1$ for all primes ideals $\mathfrak{q} \in Fib_R(p)$, then α is a PBG of L over K if and only if β is square free.*

2. *Let $Fib_R(p) - V(\beta R) = \{\mathfrak{p}_1; ...; \mathfrak{p}_h\}$. Let us denote by $(v_i)_{1\leq i\leq h}$ the $\mathfrak{p}_i - adic$ valuation associated to $\mathfrak{p}_i$ and m_i the cardinality of the residual field $R/\mathfrak{p}_i$. Set $m_i = p^{f_i}$ for some integer f_i when the characteristic of $R/\mathfrak{p}_i$ equal to p . Then α is a PBG of L over K if and only if " β is square free" and for all $i \in \{1; ....; h\}$*

$$v_i(\beta^{m_i-1} - 1) = 1 \; if \; f_i \geq n$$

$$v_i(\beta^{m_i^{r_i+1}-1} - 1) = 1 \; if \; f_i < n \; and \; n - r_i f_i \leq f_i$$

Where the optimal value of r_i is the smallest integer satisfying the inequality $n \leq (r_i + 1)f_i$ for all $i \in \{1; ....; h\}$ such that $f_i < n$.



3.3 Monogenicity of relative prime-power pure extensions-local case

In what follows, Let R be a discrete valuation ring with maximal ideal $\mathfrak{p} = \pi R$ and finite residual field k. Let L be a finite separable extension of K, the quotient field of R. Let $\alpha \in L$ be a primitive element of L which be integral over R and $P(X) = X^{p^n} - \beta$ its monic irreducible polynomial in $R[X]$. Let $v_\pi = v_\mathfrak{p}$ be the $\mathfrak{p} - adic$ discrete valuation associated to $\mathfrak{p}$. We denote by c_k the characteristic and m the cardinality of the finite residual field k. In this section, we will prove Theorem when R is the valuation ring of a discrete valuation v of K . Observe first that in this case $Fib_R(p) = \pi R$. It is required to be shown that If $v_\mathfrak{p}(\beta) \geq 1$ then

$$\alpha \text{ is } PBG \text{ of } L/K \text{ if and only if } v_\pi(\beta) = 1.$$

Now using the fa ct that $\overline{P} = \overline{X}^{p^n}$ $modulo$ $\mathfrak{p}$, we see immediately that the remainder of the Euclidean division of P by X is $r(X) = \beta$. This complete the proof in this case.

Assume now that $v_\mathfrak{p}(\beta) = 0$ and $c_k = p$, then we have $m = p^f$ for some integer f. Hence by reducing P modulo the unique prime ideal πR which lies above pR, yields:

$$\begin{aligned} \overline{P(X)} &= \overline{X}^{p^n} - \overline{\beta} \; mod(\pi R) \\ &= \overline{X}^{p^n} - \overline{\beta}^{p^f} mod(\pi R) \; (Since \, \beta^m \equiv \beta \; modulo \, \pi \, .) \end{aligned} \tag{3.3}$$

Hence, We need only consider two cases: $f \geq n$ and $f < n$,

- If $f \geq n$, the formula 3.3 can be written as:

$$\begin{aligned}\overline{P(X)} &\equiv \overline{X}^{p^n} - \overline{\beta}^{p^f} mod(\pi R) \\ &\equiv \left(\overline{X} - \overline{\beta}^{p^{f-n}}\right)^{p^n} mod(\pi R).\end{aligned}$$

  Let us denote by $R_1(X)$, the remainder of the Euclidean division of P by $X - \beta^{p^{f-n}}$. Then, $R_1(X) = P(\beta^{p^{f-n}}) = \left(\beta^{p^{f-n}}\right)^{p^n} - \beta = \beta^{p^f} - \beta$. It follows immediately that α is PBG if and only if $v_\pi(\beta^m - \beta) = 1$.

- If $n > f$, let r be the smallest positif integer such that $n - rf \leq f$ then we have:

$$\begin{aligned}\overline{P(X)} &\equiv \overline{X}^{p^n} - \overline{\beta}\ mod\, \pi R \\ &\equiv \left(\overline{X}^{p^{n-rf}} - \overline{\beta}\right)^{p^{rf}}\ mod\, \pi R \\ &\equiv \left(\overline{X}^{p^{n-rf}} - \overline{\beta}^{p^f}\right)^{p^{rf}}\ mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{\beta}^{p^{f-n+rf}}\right)^{p^{rf}\cdot p^{n-rf}}\ mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{\beta}^{p^{(r+1)f-n}}\right)^{p^n}\ mod\, \pi R.\end{aligned}$$

  Then $R_2 = \beta^{m^{r+1}} - \beta$, is the remainder of the Euclidean division of P by $X - \beta^{p^{(r+1)f-n}}$. So, α is a PBG if and only if $v_\pi(\beta^{m^{r+1}} - \beta) = 1$, which completes the proof, since $v_\pi(\beta) = 0$.

We are going in table 1 to schematizes our results:

Table 3.1: monogeneity in local case

<table>
<tr><td>$v_\mathfrak{p}(\beta) \geq 1$</td><td colspan="3">$\alpha$ is PBG iff $v_\pi(\beta) = 1$</td></tr>
<tr><td rowspan="3">$v_\mathfrak{p}(\beta) = 0$</td><td>$c_k \neq p$</td><td colspan="2">$c_k = p$</td></tr>
<tr><td rowspan="2">α is PBG</td><td>$f \geq n$</td><td>$f < n$ and $n - rf \leq f$</td></tr>
<tr><td>α is a PBG iff
$v_\pi(\beta^{m-1} - 1) = 1$</td><td>$\alpha$ is a PGB iff
$v_\pi(\beta^{m^{r+1}-1} - 1) = 1$</td></tr>
</table>

Remarks 3.3.1. • *In the case of the characteristic of k not equal to p, we can checks that the condition $v_\pi(\beta^m - \beta) = 1$, is equivalent to: β is not a p-power modulo π^2.*

- *If $c_k \neq p$, then from $\beta \in R \setminus \mathfrak{p}$, it follows that P is a separable polynomial. Otherwise, if P has α as a double root, then from $P'(X) = p^n X^{p^n-1}$ we get $\alpha = 0$ which means that $\beta \in \mathfrak{p}$, hence α is PBG of L/K in this case.*

3.4 Monogenicity of relative prime-power pure extensions, Dedekind case

Let R be a Dedekind ring, K its fraction field, L a finite separable extension over K and O_L the integral closure of R in L. Let $\alpha \in O_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $P \in R[X]$ be the monic minimal polynomial of α.

The index of α is defined as the module index $Ind_R(\alpha) := [O_L : O_K[\alpha]]$. Obviously, α is a PBG of L over K if and only if $(O_L)_{\mathfrak{p}} = R_{\mathfrak{p}}[\alpha]$, for all non zero prime ideal $\mathfrak{p}$ in R if and only if $\mathfrak{p}$ doesn't divide the index ideal, $\mathrm{Ind}_R(\alpha)$. Hence, By using the standard Index formula:

$$disc_R(P) = Ind_R^2(\alpha).D_{L/K},$$

α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P ;

$$S_P = \{\, \mathfrak{p} \in specR \mid \mathfrak{p}^2 \ divides \ disc_R(P) \,\}.$$

Our proof starts with the observation that the discriminant of $P(X)$ is $disc_R(P) = D_{L/K} = (p^n)^{p^n}\beta^{p^n-1}$, then the set $S_P = V(\beta\, R) \cup (Fib_R(p) - V(\beta\, R))$ is a disjoint union, return to the introduction of this section, α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P . So, let $\mathfrak{p}$ be a prime in S_P by localization at $\mathfrak{p}$, the ring $R_{\mathfrak{p}}$ is a Discrete valuation ring.

1. Our condition in the first case implies that $S_P = V(\beta\, R)$. Let $\mathfrak{p} \in V(\beta R)$, then by virtue of the result proved in the third section, α is a PBG of L over K if and only if $v_{\mathfrak{p}}(\beta) = 1$ which means that β is square free and complete the proof in this case.

2. Let us first note that $S_P = V(\beta R) \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_h\}$. It is clear that $charR/\mathfrak{p}_i = p$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to p since $pR \subset \mathfrak{p}_i$). According to the the result proved in the third section again, we can conclude that $\mathfrak{p}_i$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $\upsilon_i(\beta^{m_i^{r_i+1}-1} - 1) = 1$ with $r_i = 0$ if $f_i \geq n$. On the other hand, if $\mathfrak{p} \in V(\beta R)$, $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if β is square free.

3.5 Illustration

Let $K = \mathbb{Q}(\sqrt{d})$ is a quadratic extension of the rational number field and d is square free, we recall that the ring of integers

$$t = \begin{cases} \sqrt{d} & if\ d \equiv 2,\ 3\ \text{ modulo }\ 4 \\ \frac{1+\sqrt{d}}{2}, & if\ d \equiv 1\ \text{ modulo }\ 4. \end{cases} \tag{3.4}$$

And the discriminant is given by:

$$D_{K/\mathbb{Q}} = \begin{cases} 4d, & if\ d \equiv 2,\ 3\ \text{ modulo }\ 4 \\ d, & if\ d \equiv 1\ \text{ modulo }\ 4. \end{cases} \tag{3.5}$$

Theorem 3.5.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free $d \equiv 0$ modulo p. Let $L = K(\alpha)$ such that $\alpha^{p^n} = \beta = u\sqrt{d} + v$ ($n \in \mathbb{N}^*$, $u, v \in \mathbb{Z}$), furthermore we assume that $\upsilon_p(u) = \upsilon_p(v) = 0$ and $\upsilon_p(v^{p^n-1} - 1) > 1$, then L/K is monogenic. In this case we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{p^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{p^n-1}\}.$$

is an integral basis of $L/\mathbb{Q}$.

Proof. First of all we note that $pO_K = \mathfrak{p}^2$, it is known that the cardinality of $O_K/\mathfrak{p}$ is p since the residual degree of $\mathfrak{p}$ is $f = 1$ then by Theorem 3.2.5, α is a power basis generator if and only if $\upsilon_{\mathfrak{p}}(\beta^{p^n-1} - 1) = 1$, then we have

$$\begin{aligned} \beta^{p^n-1} - 1 &= \sum_{k=0}^{p^n-1} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k} - 1 \\ &= \sum_{\substack{k=2t \\ t\in\mathbb{N}}} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k} - 1 + \sqrt{d} \left(\sum_{\substack{k=2t+1 \\ t\in\mathbb{N}}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k-1} v^{p^n-1-k} \right) \end{aligned}$$

Now by property of dominance principle, and using the fact that $\upsilon_p(u) = \upsilon_p(v) = 0$, it is easy to check that

$$\upsilon_{\mathfrak{p}} \left(\sum_{\substack{k=2t+1 \\ t\in\mathbb{N}}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k-1} v^{p^n-1-k} \right) = 0,$$

and

$$v_{\mathfrak{p}}\left(\sum_{\substack{k=2t\\ t\in\mathbb{N}^*}}\binom{k}{p^n-1}u^k\left(\sqrt{d}\right)^k v^{p^n-1-k}\right)=2.$$

Keeping this in mind and using the fact that $v_p(v^{p^n-1}-1)>1$, we see immediatly that

$$v_{\mathfrak{p}}\left(\beta^{p^n-1}-1\right)=\min\left(v_{\mathfrak{p}}\left(\sum_{\substack{k=2t\\ t\in\mathbb{N}^*}}\binom{k}{p^n-1}\left(u\sqrt{d}\right)^k v^{p^n-1-k}\right),v_{\mathfrak{p}}((v^{p^n-1}-1)),v_{\mathfrak{p}}(\sqrt{d})\right)=1$$

Satisfying the conditions of Theorem 3.2.5, so that L is monogenic, let denote $\{1;\alpha;\alpha^2;...;\alpha^{3^n-1}\}$ such RMIB. Using [9, Lemma 3.1]it's obvious that

$$\mathfrak{B}=\{1;\alpha;\alpha^2;...;\alpha^{p^n-1};t;t\alpha;t\alpha^2;...;t\alpha^{p^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2\cdot p^n$. ∎

Corollary 3.5.1. *With previous conditions in Theorem 3.5.1, the discriminant $D_{L/\mathbb{Q}}$ is given by:*

$$D_{L/\mathbb{Q}}=\begin{cases}p^{2\times p^n n}(u^2-v^2d)^{p^n-1}(4d)^{p^n} & if\ d\equiv 2,\ 3\ \ modulo\ \ 4\\ p^{2\times p^n n}(d)^{p^n}(u^2-v^2d)^{3^n-1}, & if\ d\equiv 1\ \ modulo\ \ 4.\end{cases}$$

Proof. Since L/K is monogenic we obtain $D_{L/K}=(p^n)^{p^n}\beta^{p^n-1}$, then $N_{K/\mathbb{Q}}(D_{L/K})=p^{2n.p^n}N_{L/K}(\beta)^{p^n-1}$ and the norm of $u\sqrt{d}+v$ is $N_{K/\mathbb{Q}}(\beta)=u^2-v^2d$, by discriminant tower formula 4.2 it follows that:

$$D_{L/\mathbb{Q}}=\begin{cases}p^{2\times p^n n}(u^2-v^2d)^{p^n-1}(4d)^{p^n} & if\ d\equiv 2,\ 3\ \text{modulo}\ \ 4\\ p^{2\times p^n n}(d)^{p^n}(u^2-v^2d)^{3^n-1}, & if\ d\equiv 1\ \text{modulo}\ \ 4.\end{cases}$$

∎

Theorem 3.5.2. *Let $K=\mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free, $5\nmid d$. Let $L=K(\alpha)$ such that $\alpha^{5^n}=\beta=\sqrt{d}+1$ ($n=1,\ 2$), furthermore we assume that the ideal $(\sqrt{d}+1)$ is square free in O_K and $5\mathbb{Z}$ is inert in O_K, then we have :*

- *If $d\equiv\ 2,3,7,12,13,17,18,22,23$ modulo 25, then L/K is monogenic. In this case we note that:*

  $$\mathfrak{B}=\{1;\alpha;\alpha^2;...;\alpha^{5^n-1};t;t\alpha;t\alpha^2;...;t\alpha^{5^n-1}\}.$$

  is an integral basis of $L/\mathbb{Q}$.

- *If $d \equiv 8$ modulo 25 Then α is not monogenic.*

Proof. Observe first that the ideal $5O_K = \mathfrak{p}$ is prime in O_K.
By Theorem 3.2.5 it is known that L/K is monogenic if and only if $v_{\mathfrak{p}}(\beta^{24}-1) = 1$. we already have that $\beta^{24}-1 = \sqrt{d}\,(\beta^2+\beta+1)\,(\beta^{21}+\beta^{18}+\beta^{15}+\beta^{12}+\beta^9+\beta^6+\beta^3+1)$, put $k = \beta^2+\beta+1$, Consequently $v_{\mathfrak{p}}(k) = v_{\mathfrak{p}}(\beta^2+\beta+1) = v_{\mathfrak{p}}(d+3\sqrt{d}+3) = 0$ as $5 \nmid d$. Set now $h = \beta^{21}+\beta^{18}+\beta^{15}+\beta^{12}+\beta^9+\beta^6+\beta^3+1$ and a ssume that $d \equiv a$ modulo 25 where $a \in \{2,7,8,12,13,17,18,22,23\}$ and let k_a be the quotient of h a by $s = d-a$, then we get

$$h = k_a s + u_a + v_a\beta.$$

Now using the fact that $d \equiv a$ modulo 25, we see immediately that $v_{\mathfrak{p}}(h_1 s) = v_{\mathfrak{p}}(h_1) + v_{\mathfrak{p}}(s) \geqslant 2$. Then we have :

1. If $d \equiv 2$ modulo 25, then $h = k_2 s + 17218080 + 41568120\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(17218080+41568120) = 2$ and $v_{\mathfrak{p}}(41568120\sqrt{d}) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

2. If $d \equiv 3$ modulo 25, then $h = k_3 s + 325875485 + 445154190\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(325875485+445154190) = 2$ and $v_{\mathfrak{p}}(445154190\sqrt{d}) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

3. If $d \equiv 7$ modulo 25, then $h = k_7 s + 199236613045 + 121061207890\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(u_7 - 3v_7) = v_{\mathfrak{p}}(199236613045 - 3.121061207890) = 4$ and $v_{\mathfrak{p}}(121061207890(4+\sqrt{d})) = 0$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

4. If $d \equiv 12$ modulo 25, then $h = k_{12} s + 15862082187260 + 6437331720060\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(u_{12} - v_{12}) = v_{\mathfrak{p}}(15862082187260 - 6437331720060) = 2$ and $v_{\mathfrak{p}}(6437331720060(2+\sqrt{d})) = 0$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

5. If $d \equiv 13$ modulo 25, then $h = k_{13} s + 30993885541465 + 11895524262160\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(30993885541465 + 11895524262160) = 3$ and $v_{\mathfrak{p}}(11895524262160\sqrt{d}) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

6. If $d \equiv 17$ modulo 25, then $h = k_{17} s + 303216403752225 + 97095649795380\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(303216403752225) = 2$ and $v_{\mathfrak{p}}(97095649795380\sqrt{d}) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

7. If $d \equiv 18$ modulo 25, then $h = k_{18} s + 496341807039680 + 153083209946520\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(496341807039680 + 153083209946520) = 2$ and $v_{\mathfrak{p}}(153083209946520\sqrt{d}) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24}-1) = 1$, thus L/K is monogenic.

8. If $d \equiv 22$ modulo 25, then $h = k_{22}s + 2851989592814440 + 773025087889600\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(773025087889600) = 2$ and $v_{\mathfrak{p}}(2851989592814440) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

9. If $d \equiv 23$ modulo 25, then $h = k_{23}s + 4216875746193045 + 1111301467484130\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(4216875746193045+1111301467484130) = 2$ and $v_{\mathfrak{p}}(1111301467484130\sqrt{d}) = 1$. This prove that $v_{\mathfrak{p}}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

Let denote $\{1; \alpha; \alpha^2; ...; \alpha^{5^n-1}\}$ such RMIB. Using [9, Lemma 3.1]it's obvious that

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{5^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{5^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2 \cdot 5^n$.

If $d \equiv 8$ modulo 25, then $h = h_1 s + 576421380900 + 315255471300\beta$ and hence $v_{\mathfrak{p}}(h) \geqslant 2$ since $v_{\mathfrak{p}}(576421380900) = v_{\mathfrak{p}}(315255471300) = 2$. This prove that $v_{\mathfrak{p}}(\beta^{24} - 1) \geqslant 2$, thus α is not monogenic. ∎

Corollary 3.5.2. *With previous conditions in Theorem 3.5.2 and $d \not\equiv 8$ modulo 25, the discriminant $D_{L/\mathbb{Q}}$ is given by:*

$$D_{L/\mathbb{Q}} = \begin{cases} 5^{2\times 5^n n}(1-d)^{p^n-1}(4d)^{5^n} & if\ d \equiv 2,\ 3\ \ modulo\ \ 4 \\ 5^{2\times 5^n n}(d)^{5^n}(1-d)^{5^n-1}, & if\ d \equiv 1\ \ modulo\ \ 4. \end{cases}$$

Proof. Since L/K is monogenic we obtain $D_{L/K} = (5^n)^{5^n}\beta^{5^n-1}$, then $N_{K/\mathbb{Q}}(D_{L/K}) = 5^{2n.5^n}N_{L/K}(\beta)^{5^n-1}$ and the norm of $\sqrt{d}+1$ is $N_{K/\mathbb{Q}}(\beta) = 1 - d$, by discriminant tower formula 4.2 it follows that:

$$D_{L/\mathbb{Q}} = \begin{cases} 5^{2\times 5^n n}(1-d)^{5^n-1}(4d)^{5^n} & if\ d \equiv 2,\ 3\ \text{modulo}\ \ 4 \\ 5^{2\times 5^n n}(d)^{5^n}(1-d)^{5^n-1}, & if\ d \equiv 1\ \text{modulo}\ \ 4. \end{cases}$$

∎

Remark 3.5.1. *This work can be generalized to a higher degree of the extension L, knowing that the difficulty of the problem comes from the computation of the relative discriminant. On the other hand, we can be based on the minimal polynomials (see [10]) to study the monogenity.*

3.5.1 Relative power integral basis of a family of number fields defined By $X^{p^n} + a\,X^{p^s} - b$

We study the relative monogeneity of $L = K(\alpha)$ over its subfield where α is a root of a monic irreducible polynomial of the form (see [6]).

$$P(X) = X^{p^n} + a\,X^{p^s} - b \in R[X],\ with\ n > s\ and\ (n,s) \in \mathbb{N}^2. \tag{3.6}$$

This allows to construct an integral basis for a family of extensions L over the field of rationals $\mathbb{Q}$ of degree $2.p^n$ (n is an integer). As a consequence, we compute the discriminant $D_{L/\mathbb{Q}}$ using the tower-discriminant formula:

$$D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K})\,(D_{K/\mathbb{Q}})^{[L:K]}, \tag{3.7}$$

where $N_{K/\mathbb{Q}}$ denotes the norm from K to $\mathbb{Q}$ (see [50, Corollary 10. 2] and [24]).

On the other hand we recall that the index of $\alpha \in O_L$ is defined as the module index $\mathrm{Ind}_R(\alpha) := [O_L : R[\alpha]]$. Obviously, α is a Power Basis Generator (PBG) of L over K if and only if $(O_L)_{\mathfrak{p}} = R_{\mathfrak{p}}[\alpha]$, for all non-zero prime ideals $\mathfrak{p}$ in R if and only if $\mathfrak{p}$ doesn't divide the index ideal, $\mathrm{Ind}_R(\alpha)$. Hence, by using the standard index-discriminant formula:

$$disc_R(P) = \mathrm{Ind}_R^2(\alpha).D_{L/K},$$

α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P defined by:

$$S_P = \{\, \mathfrak{p} \in \mathrm{Spec}(R)\ \ \mathfrak{p}^2\ divides\ disc_R(P)\ \}.$$

We denote by Spec(R) the set of the prime ideals of a commutative ring R. Equipped with the Zariski topology, the closed sets of $\mathrm{Spec}(R)$ are the sets:

$$V(\mathfrak{I}) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{I} \subseteq \mathfrak{p}\},$$

where $\mathfrak{I}$ is an ideal in R. Note also that for any ideal $\mathfrak{I}$ in R, and $n \in \mathbb{N}$ we have $V(\mathfrak{I}^n) = V(\mathfrak{I})$. Now, fix a non-zero prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$. We are also interested in the set of primes $\mathfrak{q}$ in O_L with $\mathfrak{p} \subseteq \mathfrak{q}$ −or equivalently $\mathfrak{p} = \mathfrak{q} \cap R$−, and we call that set the fibre over $\mathfrak{p}$, denoted by $Fib_R(\mathfrak{p})$.

With the above notations we state our main Theorem characterizing monogeneity of an integer $\alpha \in O_L$.

Theorem 3.5.3. *Let R be a Dedekind ring with finite residual fields and K its fraction field.*

Assume that $charK = 0$ *and* $L = K(\alpha)$ *is a finite separable extension of* K. *Let* $P(X) = X^{p^n} + aX^{p^s} - b \in R[X]$ *be the monic minimal polynomial of* α *of degree* p^n. *Assume that* $v_{\mathfrak{p}}(a) \geq 1$ *for all prime ideals* $\mathfrak{p}$ *in* S_P, *where* $v_{\mathfrak{p}}$ *is the* $\mathfrak{p}$*-adic valuation associated to prime ideal* $\mathfrak{p}$ *in* R. *Then:*

1. *If the* $\mathfrak{q}-$*adic valuation* $v_{\mathfrak{q}}(b) \geq 1$ *for all prime ideals* $\mathfrak{q} \in Fib_R(p)$, *then* α *is a PBG of* L *over* K *if and only if* b *is square free.*

2. *Let* $\mathfrak{F}ib_R(p) - V(bR) = \{\mathfrak{p}_1; ...; \mathfrak{p}_h\}$. *Let us denote by* c_i *(resp* $m_i = c_i^{f_i}$*) the characteristic (resp the cardinality) of the finite residual field* $k_i = R/\mathfrak{p}_i$. *Then* α *is a PBG of* L *over* K *if and only if* b *is square free and for all* $i \in \{1; ....; h\}$ *we have:*

$$\begin{aligned} v_{\mathfrak{p}_i}(b^{m_i-1} + ab^{p^{f_i-n+s}-1} - 1) &= 1 \quad if\ f_i \geq n, \\ v_{\mathfrak{p}_i}(b^{m_i^{r_i+1}-1} + ab^{p^{(r_i+1)f_i-n+s}-1} - 1) &= 1 \quad if\ f_i < n, \end{aligned}$$

where the optimal value of r_i *is the smallest integer satisfying the inequality* $n \leq (r_i + 1)f_i$.

3.6 Some preliminary results

With notations as above, for a polynomial P belonging to $R[X]$, $\overline{P}$ will stand for the polynomial over $k[X] = R/\mathfrak{p}[X]$ obtained by replacing each coefficient of P by its residue modulo $\mathfrak{p}$.

Definition 3.6.1. *Let* R *be a Dedekind ring,* K *its fraction field and* v *be a valuation on* K. *Let* $P = a_0 + a_1X + ... + a_nX^n \in K[X]$, *we put:*

$$v_G(P) = \inf\{v(a_i) \mid 0 \leq i \leq n\},$$

then v_G *is a valuation on* $K[X]$ *called the Gauss valuation on* $K[X]$ *relative to* v.

First of all, we recall a criterion which permits us to decide whether a primitive element $\alpha \in O_L$ is a monogenic element of L over K. The well known Dedekind criterion, which we recall now, permits us to find necessary and sufficient conditions for a relative extension to admit a power integral basis (see [57] or [44]).

Dedekind Criterion. Let R be a Dedekind ring, K its fraction field and v be a valuation on K. Let L be a finite separable extension over K and $\alpha \in O_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $P = Irrd(\alpha, R) \in R[X]$ be the monic irreducible polynomial of α. Let $\mathfrak{p}$ be a non zero prime ideal in R and $k := R/\mathfrak{p}$ its residual field. Let $\bar{P}$ be the image in $k[X]$ of P and

assume that $\bar{P} = \Pi_{i=1}^{r} \bar{P_i^{l_i}}$ is the primary decomposition of $\bar{P}$ in $k[X]$ with $P_i \in R[X]$ a monic lift of the irreducible polynomial $\overline{P_i}$ for $1 \leq i \leq r$. Let $T \in R[X]$ satisfying $P = \prod_{i=1}^{r} P_i^{l_i} + \pi T$. Then the element α is PBG of L over $R_{\mathfrak{p}}$ if and only if $gcd\left(\overline{P}_i,\ \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$.

Remark 3.6.1. *It is known that the above condition is equivalent to the simplest one, $v_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$, such that $V_i \in R[X]$ is the remainder of Euclidean division of P by P_i.*

3.7 Monogeneity of relative non-pure extension, local case

Let R be a discrete valuation ring with maximal ideal $\mathfrak{p} = \pi R$ and finite residual field k. Let $L = K(\alpha)$ be a finite separable extension of K the quotient field of R where α is a primitive element of L which is integral over R and $P(X) = X^{p^n} + aX^{p^s} - b$ its monic irreducible polynomial in $R[X]$ such that $n > s$ and $v_{\mathfrak{p}}(a) \geq 1$. Let $v_\pi = v_{\mathfrak{p}}$ be the $\mathfrak{p} - adic$ discrete valuation associated to $\mathfrak{p}$. We denote by c_k (resp. $m = c_k^f$) the characteristic (resp. the cardinality) of the finite residual field k.

1. Assume first that $v_{\mathfrak{p}}(b) \geq 1$, then $\overline{P} = \overline{X}^{p^n}$ *modulo* $\mathfrak{p}$, hence the remainder of the Euclidean division of P by X is $R(X) = -b$. So, α is a PBG *if and only if* $v_\pi(b) = 1$.

2. If $v_{\mathfrak{p}}(b) = 0$, then we have

   (a) If $c_k = p$, then by reducing P modulo the prime ideal πR of R which contains pR, we get:

$$\begin{aligned} \overline{P(X)} &= \overline{X}^{p^n} + a\overline{X}^{p^s} - \overline{b}\ mod\, \pi R \\ &= \overline{X}^{p^n} - \overline{b}^{p^f} mod\, \pi R, since\, b^m \equiv b\, modulo\, \pi\, and\, m = p^f. \end{aligned}$$

   For the rest we must be careful to distinguish two cases:

   - If $f \geq n$ then:

$$\begin{aligned} \overline{P(X)} &\equiv \overline{X}^{p^n} - \overline{b}^{p^f} mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{b}^{p^{f-n}}\right)^{p^n} mod\, \pi R. \end{aligned}$$

   Hence, we can consider the Euclidean division of P by $X - b^{p^{f-n}}$. Then the remainder $R_1(X)$ is given as follows $R_1(X) = P(b^{p^{f-n}}) = \left(b^{p^{f-n}}\right)^{p^n} + a\left(b^{f-n}\right)^{p^s} - b =$

$b^{p^f} + ab^{p^{f-n+s}} - b$. Hence, α is PGB if and only if $v_\pi(b^m + ab^{p^{f-n+s}} - b) = 1$ and by $v_\mathfrak{p}(b) = 0$, the last condition becomes $v_\pi(b^{m-1} + ab^{p^{f-n+s}-1} - 1) = 1$.

- Assume that $n > f$. We denote by r be the smallest positive integer such that $n - rf \leq f$ then we have:

$$\begin{aligned}
\overline{P(X)} &\equiv \overline{X}^{p^n} - \overline{b} \; mod\, \pi R \\
&\equiv \left(\overline{X}^{p^{n-rf}} - \overline{b}\right)^{p^{rf}} \; mod\, \pi R \\
&\equiv \left(\overline{X}^{p^{n-rf}} - \overline{b}^{p^f}\right)^{p^{rf}} \; mod\, \pi R \\
&\equiv \left(\overline{X} - \overline{b}^{p^{f-n+rf}}\right)^{p^{rf}\cdot p^{n-rf}} \; mod\, \pi R \\
&\equiv \left(\overline{X} - \overline{b}^{p^{(r+1)f-n}}\right)^{p^n} \; mod\, \pi R.
\end{aligned}$$

Hence, we can consider the Euclidean division of P by $X - b^{p^{(r+1)f-n}}$. Then the remainder $R_2(X)$ is given as follows $R_2(X) = P(b^{p^{(r+1)f-n}}) = \left(b^{p^{(r+1)f-n}}\right)^{p^n} + a\left(b^{p^{(r+1)f-n}}\right)^{p^s} - b = b^{p^{(r+1)f}} + ab^{p^{(r+1)f-n+s}} - b$. Hence α is PGB if and only if $v_\pi(b^{m^{r+1}} + ab^{p^{(r+1)f-n+s}} - b) = 1$ and by $v_\mathfrak{p}(b) = 0$, the last condition becomes $v_\pi(b^{m^{r+1}-1} + ab^{p^{(r+1)f-n+s}-1} - 1) = 1$.

(b) If $c_k \neq p$, since $b \in R \setminus \mathfrak{p}$, it follows that P is a separable polynomial in the residual field k. Otherwise, if P has α as a double root, then from $P'(X) = p^n\alpha^{p^n-1} = 0$ we get $\alpha \equiv 0 \; mod\, \mathfrak{p}$ which means that $b \in \mathfrak{p}$, this contradiction complete the proof in this case.

We schematize the previous results in Table 1. We denote $T_1 = b^{m-1} + ab^{p^{f-n+s}-1} - 1$ and $T_2 = b^{m^{r+1}-1} + ab^{p^{(r+1)f-n+s}-1} - 1$.

Table 3.2: monogeneity in local case

<table>
<tr><td>$v_{\mathfrak{p}}(b) \geq 1$</td><td colspan="3">$\alpha$ is PBG iff $v_{\pi}(b) = 1$</td></tr>
<tr><td rowspan="3">$v_{\mathfrak{p}}(b) = 0$</td><td>$c_k \neq p$</td><td colspan="2">$c_k = p$</td></tr>
<tr><td rowspan="2">α is PBG</td><td>$f \geq n$</td><td>$f < n$ and $n - rf \leq f$</td></tr>
<tr><td>α is a PBG iff $v_{\pi}(T_1) = 1$</td><td>α is a PGB iff $v_{\pi}(T_2) = 1$</td></tr>
</table>

3.8 Monogeneity of relative non-pure extension, Dedekind case

The following lemma is already known. Its proof is omitted see [65].

Lemma 3.8.1. *Let R be a commutative integral domain containing $\mathbb{Z}$, K its field of fractions of characteristic 0. Consider the polynomial $P(X) = X^m + aX^k + b$ of degree m in $R[X]$, where $m > k > 0$. If $d = (m,\ k)$, then:*

$$disc_R(P) = (-1)^{m(m-1)/2} b^{k-1} [m^{\frac{m}{d}} b^{\frac{m-k}{d}} - (-1)^{\frac{m}{d}} (m-k)^{\frac{m-k}{d}} k^{\frac{k}{d}} a^{\frac{m}{d}}]^d.$$

Corollary 3.8.1. *Consider the particular polynomial $P(X) = X^m + aX^k - b \in R[X]$ of degree $m = p^t k$ with $k = p^s$ and $d = (m,\ k)$. Then,*

$$disc_R(P) = (-1)^{\frac{p^{s+t}(p^{s+t}-1)}{2}} p^{s.p^{s+t}} b^{p^s-1} [\Delta]^{p^s},$$

with $\Delta = p^{t.p^t}.b^{p^t-1} + (p^t-1)^{p^t-1} a^{p^t}$. In particular, If $t = 1$,

$$disc_R(P) = (-1)^{\frac{p^{s+1}(p^{s+1}-1)}{2}} (-b)^{p^s-1} [p^{ps}\, \Delta]^{p^s},$$

with $\Delta = p^p\, b^{p-1} + (p-1)^{p-1}\, a^p$,

Proof. The statement follows immediately from Lemma 3.8.1. ∎

Proof. (Theorem 3.5.3) Our proof starts with the observation that the discriminant of $P(X)$ is

$$disc_R(P) = (-1)^{\frac{p^n(p^n-1)}{2}} p^{s.p^n} b^{p^s-1} [\Delta]^{p^s}.$$

Such that $\Delta = p^{(n-s).p^{n-s}}.b^{p^{n-s}-1} + (p^{n-s}-1)^{p^{n-s}-1}a^{p^{n-s}}$, now by Corollary 3.8.1, the set $S_P = V(b\,R) \cup (Fib_R(p) - V(b.R))$ is a disjoint union, since for each prime ideal $\mathfrak{q}$ containing Δ, this implies that we must have $\mathfrak{q} \in Fib_R(p)$ or $\mathfrak{q} \in V(b\,R)$. Return to the introduction of this section, α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P. So, let $\mathfrak{p}$ be a prime in S_P by localization at $\mathfrak{p}$, the ring $R_{\mathfrak{p}}$ is a discrete valuation ring. We may then use the accomplishment done in the discrete case.

1. Our condition in the first case implies that $S_P = V(b\,R)$. Let $\mathfrak{p} \in V(b\,R)$, therefore, α is a PBG of L over K if and only if $v_{\mathfrak{p}}(b\,R) = 1$ which means that b is square free and completes the proof in this case.

2. Let us first note that $S_P = V(b\,R) \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_h\}$. It is clear that $charR/\mathfrak{p}_i = p$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to p since $pR \subset \mathfrak{p}_i$). According to the second case of the result established in the third section, we can conclude that $\mathfrak{p}_i$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if for all $i \in \{1; ....; h\}$ we have:

$$\begin{aligned} v_{\mathfrak{p}_i}(b^{m_i-1} + ab^{p^{f_i-n+s}-1} - 1) &= 1 \quad if\ f_i \geq n, \\ v_{\mathfrak{p}_i}(b^{m_i^{r_i+1}-1} + ab^{p^{(r_i+1)f_i-n+s}-1} - 1) &= 1 \quad if\ f_i < n, \end{aligned}$$

   where the optimal value of r_i is the smallest integer satisfying the inequality $n \leq (r_i+1)f_i$. On the other hand, if $\mathfrak{p} \in V(b\,R)$, $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if b is square free, which is our claim.

3.9 Illustrations

Throughout this section, we consider the irreducible polynomial $P(X) = X^p + pbrX - b$. The calculations were performed in Maple running under Windows. Hence for a given strictly positive integers b and r such that b is a square free and p does not divide b, we characterize the set of prime divisors of $(p-1)^{p-1}r^pb + 1$ with exponents greater that 2 and we verify that this set is a subset of the set of prime divisors of pbr, once this done, we check if the p-valuation of $b^{p-1} + pbr - 1$ is exactly 1. Since the parameter r enters the discriminant as a high power with exponent p, restriction to $r \leq 30$ would be sufficient. By changing the values of r and b, the software attains the bound values of its functions for $p = 3; 5; 7; 11$, we obtain the following results.

1. For $p = 3$, we vary $1 \leq r \leq 30$ and $1 \leq b \leq 5000$ such that b is square free. We found 2279 values of b and in every case the percentage was between 53.3% and $66,67\%$. In the following table we summarise the first five values of b and the corresponding values of r.

Table 3.3: Monogeneity for $p = 3$

Value of b	Monogeneity cases	Value of r
1	19	1, 2, 4, 5, 7, 8, 10, 13, 14,16, 17, 19, 20, 22, 23, 25, 26, 28, 29
2	18	2, 3, 5, 6, 8, 9, 11, 14, 15, 17, 18, 20, 21, 23, 26, 27, 29, 30
5	20	1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19, 21, 22, 24, 25, 27, 28, 30
7	18	1, 3, 4, 6, 7, 9, 10, 12, 13, 16, 18, 19, 21, 22, 24, 25, 28, 30
10	19	1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 28, 29

2. For $p = 5$, we vary $1 \leq r \leq 30$ and $1 \leq b \leq 3000$ such that b is square free. We found 1520 values of b and in every case the percentage was between 56.67% and 80%. In the following table we summarise the first five values of b and the corresponding values of r.

Table 3.4: Monogeneity for $p = 5$

Value of b	Monogeneity cases	Value of r
1	22	1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 16, 17, 18, 19, 21, 22, 24, 26, 27, 28, 29
2	20	2, 3, 4, 5, 7, 8, 9, 12, 14, 15, 17, 18, 20, 22, 23, 24, 25, 27, 29, 30
3	24	1, 2, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 22, 24, 25, 26, 27, 29, 30
6	22	2, 3, 4, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 27, 28, 29, 30
7	20	1, 2, 3, 4, 6, 7, 9, 11, 12, 13, 16, 18, 19, 21, 22, 23, 24, 27, 28, 29,

3. For $p = 7$, we vary $1 \leq r \leq 30$ and $1 \leq b \leq 103$ such that b is square free. We found 56 values of b and in every case the percentage was between 73.33% and 86.67%. In the following table we summarise the first five values of b and the corresponding values of r.

Table 3.5: Monogeneity for $p = 7$

Value of b	Monogeneity cases	Value of r
1	25	1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 29, 30
2	24	1, 2, 3, 5, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 28, 29, 30
3	25	1, 2, 3, 4, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30
5	26	1, 2, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30
6	22	2, 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 21, 23, 24, 25, 26, 27, 30

4. For $p = 11$, we vary $1 \leq r \leq 3$ and $1 \leq b \leq 100$ such that b is square free. We found 55 values of b and in every case two or three values of r occurs. In the following table we summarise the first five values of b and the corresponding values of r.

Table 3.6: Monogeneity for $p = 11$

Value of b	Monogeneity cases	Value of r
1	3	1, 2, 3
2	2	1, 2
3	3	1, 2, 3
5	2	1, 2
6	2	2, 3

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension of the rational number field and d be a square free integer, we recall that the ring of integers $\mathbb{Z}[t]$ of K is generated by t given by:

$$t = \begin{cases} \sqrt{d} & if\ d \equiv 2,\ 3\ \ \text{modulo}\ \ 4 \\ \frac{1+\sqrt{d}}{2}, & if\ d \equiv 1\ \ \text{modulo}\ \ 4. \end{cases} \tag{3.8}$$

Its discriminant is given by:

$$D_{K/\mathbb{Q}} = \begin{cases} 4d, & if\ d \equiv 2,\ 3\ \ \text{modulo}\ \ 4 \\ d, & if\ d \equiv 1\ \ \text{modulo}\ \ 4. \end{cases} \tag{3.9}$$

Theorem 3.9.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field such that d is square free, $d \equiv 0$ modulo p and $pR = \mathfrak{p}^2$. Let $L = K(\alpha)$ be defined by a root of the monic irreducible polynomial $P(X) = X^{p^n} + aX^{p^s} - b$ $(n > s \geqslant 0)$ such that:*

- *$b = u\sqrt{d} + v$, u, $v \in \mathbb{Z}$ and b is square free.*
- *$\upsilon_{\mathfrak{p}}(u) = \upsilon_{\mathfrak{p}}(v) = 0$ and $\upsilon_{\mathfrak{p}}(v^{p^n-1} - 1) > 1$.*
- *$a \in R = \mathcal{O}_K$ such that $\upsilon_{\mathfrak{p}}(a) > 1$ and $\upsilon_{\mathfrak{q}}(a) \geq 1$ for all $\mathfrak{q} \in S_P$.*

Then L/K is monogenic and we note that:

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{p^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{p^n-1}\}.$$

is an integral basis of $L/\mathbb{Q}$.

Proof. First of all, we note that, if $p\mathcal{O}_K = \mathfrak{p}^2$, it is known that the cardinality of $\mathcal{O}_K/\mathfrak{p}$ is p since the residual degree of $\mathfrak{p}$ is $f = 1$. We should first evaluate the valuation at $\mathfrak{p}$ of $b^{p^n-1} - 1$ for $n \in \mathbb{N}$.

$$\begin{aligned} b^{p^n-1} - 1 &= \sum_{k=0}^{p^n-1} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k} - 1 \\ &= \sum_{\substack{k=2t \\ t\in\mathbb{N}}} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k} - 1 \\ &\quad + \sqrt{d}\left(\sum_{\substack{k=2t+1 \\ t\in\mathbb{N}}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k-1} v^{p^n-1-k}\right) \end{aligned}$$

Now, by the property of dominance principle, and using the fact that $\upsilon_p(u) = \upsilon_p(v) = 0$, it is easy to check that

$$\upsilon_{\mathfrak{p}}\left(\sum_{\substack{k=2t+1 \\ t\in\mathbb{N}}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k-1} v^{p^n-1-k}\right) = 0,$$

and

$$\upsilon_{\mathfrak{p}}\left(\sum_{\substack{k=2t \\ t\in\mathbb{N}^*}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k} v^{p^n-1-k}\right) = 2.$$

Keeping this in mind and using the fact that $\upsilon_{\mathfrak{p}}(v^{p^n-1}-1)>1$, we see immediately that

$$\upsilon_{\mathfrak{p}}\left(b^{p^n-1}-1\right)=\min\left(\upsilon_{\mathfrak{p}}\left(\sum_{\substack{k=2t\\ t\in\mathbb{N}^*}}\binom{k}{p^n-1}\left(u\sqrt{d}\right)^k v^{p^n-1-k}\right),\upsilon_{\mathfrak{p}}((v^{p^n-1}-1)),\upsilon_{\mathfrak{p}}(\sqrt{d})\right)=1$$

According to Theorem 3.5.3, we have to deal with two cases:

- $n=1$. By the above calculation we have that $\upsilon_{\mathfrak{p}}(b^{p-1}-1)=1$ and $\upsilon_{\mathfrak{p}}(ab^{p^{f-n+s}-1})\geq 2$, whence $\upsilon_{\mathfrak{p}}(b^{p-1}+ab^{p^{f-n+s}-1}-1)=1$. Thus L/K is monogenic.
- $n\geq 2$. We have $\upsilon_{\mathfrak{p}}(b^{p^n-1}-1)=1$ and $\upsilon_{\mathfrak{p}}(ab^{p^s-1})\geq 2$, whence $\upsilon_{\mathfrak{p}}(b^{p^n-1}+ab^{p^s-1}-1)=1$. Thus L/K is monogenic.

Hence we conclude that the conditions of Theorem 3.5.3 were satisfied, so that L is monogenic, let denote $\{1;\alpha;\alpha^2;...;\alpha^{3^n-1}\}$ such RMIB. Using [9, Lemma 3.1] it's obvious that

$$\mathfrak{B}=\{1;\alpha;\alpha^2;...;\alpha^{p^n-1};t;t\alpha;t\alpha^2;...;t\alpha^{p^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2\cdot p^n$. ∎

Corollary 3.9.1. *With previous conditions in Theorem 3.9.1 and $a=b$. Set $t=n-s$, then the discriminant $D_{L/\mathbb{Q}}$ is given by:*
$D_{L/\mathbb{Q}}=p^{2s.p^n}(u^2-v^2d)^{p^n-1}(u^2(p^t-1)^{2p^t-2}-(p^{t.p^t}+(p^t-1)^{p^t-1}v)^2d)^{p^s}(4d)^{p^n}$, *if* $d\equiv 2,3$ *modulo* 4.
$D_{L/\mathbb{Q}}=p^{2s.p^n}(u^2-v^2d)^{p^n-1}(u^2(p^t-1)^{2p^t-2}-(p^{t.p^t}+(p^t-1)^{p^t-1}v)^2d)^{p^s}(d)^{p^n}$, *if* $d\equiv 1$ *modulo* 4.

Proof. Since L/K is monogenic we obtain

$$disc_R(P)=(-1)^{\frac{p^n(p^n-1)}{2}}p^{s.p^n}b^{p^n-1}[\Delta]^{p^s},$$

with $\Delta=p^{t.p^t}+(p^t-1)^{p^t-1}b$. $N_{K/\mathbb{Q}}(D_{L/K})=p^{2s.p^n}N_{K/\mathbb{Q}}(b)^{p^n-1}N_{K/\mathbb{Q}}(\Delta)^{p^s}$, the norm of $u\sqrt{d}+v$ is $N_{K/\mathbb{Q}}(b)=u^2-v^2d$ and $N_{K/\mathbb{Q}}(\Delta)=u^2(p^t-1)^{2p^t-2}-(p^{t.p^t}(p^t-1)^{p^t-1}v)^2d$ by discriminant tower formula 4.2 it follows that: $D_{L/\mathbb{Q}}=p^{2s.p^n}(u^2-v^2d)^{p^n-1}(u^2(p^t-1)^{2p^t-2}-(p^{t.p^t}+(p^t-1)^{p^t-1}v)^2d)^{p^s}(4d)^{p^n}$, if $d\equiv 2,3$ modulo 4.
$D_{L/\mathbb{Q}}=p^{2s.p^n}(u^2-v^2d)^{p^n-1}(u^2(p^t-1)^{2p^t-2}-(p^{t.p^t}+(p^t-1)^{p^t-1}v)^2d)^{p^s}(d)^{p^n}$, *if* $d\equiv 1$ modulo 4. ∎

Chapter 4

On the Discriminant of some relative pure extensions

4.1 Introduction

Computation of the discriminant of certain number fields is in general a difficult task and is related to the computation of integral bases which is a classical hard problem in algebraic number theory. Many works are available in this area (cf. [14], [31], [33], [32], [34], [62], [15], [66], and others). In 2010 Del Corso and Rossi [15] provided a formula for the discriminant of Kummer cyclic extension of number fields. For pure algebraic number fields Jakhar and Khanduja [34] gave a formula for the discriminant of pure number fields having square free degree. In 2020 the authors of [32] gave a formula for the discriminant of n-th degree fields of the type $\mathbb{Q}(\sqrt[n]{a})$ using Newton polygon techniques. Let L be a relative pure extension, in other word an algebraic field of the type $L = K(\sqrt[p]{a})$, where K is an algebraic number field and the polynomial $X^p - a$ of prime degree belonging to $K[X]$ is irreducible over the field K. In the present paper, our aim is to give an explicit formula for the discriminant $D_{L/K}$ of O_L the ring of integer of L in terms of the set of primes $\mathfrak{p}$ in O_K (denoted by $Spec(O_K)$) with $p\mathbb{Z} = \mathfrak{p} \cap O_K$ and such that $aO_K \subseteq \mathfrak{p}$. As a consequence, using the tower formula stated below (4.2), we compute the discriminant $D_{L/\mathbb{Q}}$ for two family of septic and quintic pure fields L, such that $[L : \mathbb{Q}] = 10$ and $[L : \mathbb{Q}] = 14$ respectively.

Let R be a Dedekind ring with finite residual fields and containing $\mathbb{Z}$. Let K be its fraction field. Let $\mathfrak{p}$ be a non zero prime ideal in R and $N_{\mathfrak{p}} =\mid R/\mathfrak{p} \mid$ be the cardinality of the residual field $R/\mathfrak{p}$. Let a be a non zero element in R. We will say that a is n^{th} power free in R if $\upsilon_{\mathfrak{p}}(a) \leq n-1$ for any non zero prime ideal $\mathfrak{p}$ in R, where $\upsilon_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let p a prime number. We denote by $Fib_R(p)$ the set of all non zero primes ideals in R which lie above p. It is clear that $\mathfrak{p} \in Fib_R(p)$ if and only if $char(R/\mathfrak{p}) = p$. Note also that if a non zero

element a in K, is n^{th} power free in K then $a \notin K^p$. The converse is false. By theorem 9.1 [[45] p. 331], if K is a field, p an odd prime and $a \in K - \{0\}$ then the polynomial $P = X^p - a$ is irreducible in $K[X]$ if and only if $a \notin K^p$. Hence if a is n^{th} power free in K then the polynomial $P = X^p - a$ is irreducible in $K[X]$. If further R is integrally closed and a is n^{th} power free in R then the polynomial $P = X^p - a$ is irreducible in $R[X]$.

Let L be a finite separable extension of K and O_L the integral closure of R in L. Let $\alpha \in O_L$ such that $L = K(\alpha)$. Assume that $charK = 0$ and $P = X^p - a \in R[X]$ is the monic minimal polynomial of α, where p is an odd prime number and a is p^{th} power free in R. The main result of this paper is Theorem 1.1 which gives the discriminant $D_{L/K}$ of a pure relative cyclic fields of prime degree. Precisely stated, we prove the following result:

Theorem 4.1.1. *With the above assumptions, if* $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$, *for all prime* $\mathfrak{p} \in Fib_R(p)$, *then*

$$D_{L/K} = p^p\, \mathfrak{a}^{p-1},$$

where $\mathfrak{a}$ *is the ideal radical of* aR.

Corollary 4.1.1. *With the above assumptions, if the ideal* aR *is square free and* $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$, *for all prime* $\mathfrak{p} \in Fib_R(p)$, *then* α *is a power basis generator of* L/K.

Proof. indeed if the ideal aR is square free then its radical is aR and hence $D_{L/K} = disc_R P$. ∎

Note the above corollary is approved by Theorem 6.1 in [60]. Indeed $\mathfrak{p}$ satisfies the Wieferich congruence if and only if $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}-1} - 1) \geq 2$ (see [63]).

4.2 Preliminary results

Throughout this article, unless specifically stated otherwise, Let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n, O_L the integral closure of R in L, and $L = K(\alpha)$ for some $\alpha \in O_L$. Let $P \in K[X]$ be the minimal irreducible polynomial of α over K. Since R is integrally closed, $P \in R[X]$ (see [35, p. 7]). Let $\mathrm{disc}_R(P)$ be the principal ideal of R generated by $\mathrm{Res}(P, P')$, where $\mathrm{Res}(P, P')$ denotes the resultant of the two polynomials P and its derivative P', we let $D_{L/K}$ denote the discriminants over R of the number field L over K. It is well known (see [8], [11] or [24]) the following Index-discriminant formula (4.1) and the tower formula (4.2)

$$\mathrm{Disc}_R(P) = \mathrm{Ind}_R(\alpha)^2\, D_{L/K}, \tag{4.1}$$

$$D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K}).(D_{K/\mathbb{Q}})^{[L:K]}. \tag{4.2}$$

where $N_{K/\mathbb{Q}}$ denote the norm from K to $\mathbb{Q}$ (see [57, Corollary 10. 2] and [24]). We denote by $Spec(R)$, the set of the prime ideals of a commutative ring R. Recall that the closed sets of the Zariski topology on $Spec(R)$, are the sets:

$$V(I) = \{\mathfrak{p} \in Spec\,(R) \mid I \subseteq \mathfrak{p}\}$$

where I is an arbitrary ideal in R. Note also that for any non-zero prime ideal $\mathfrak{p}$ in R, we consider the set of prime ideals $\mathfrak{q}$ in O_L such that $\mathfrak{p} = \mathfrak{q} \cap R$. We call this set the fibre of $\mathfrak{p}$ in L and we will denote it by $Fib_L(\mathfrak{p})$.

In view of the previous Index-Discriminant formula (4.1), the element α is a power basis generator (PBG for short) of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $[O_L : R[\alpha]]_R$, for any non zero prime ideal $\mathfrak{p}$ in R, such that $\mathfrak{p}^2$ divides $\mathrm{Disc}_R(P)$. This fact lead us to introduce, for any irreducible polynomial P, the set S_P of prime ideals whose square divides the ideal $disc_R P$. Then:

$$S_P = \{\, \mathfrak{p} \in specR \mid \mathfrak{p}^2 \; divides \; \mathrm{Disc}_R(P) \,\}.$$

It may pointed out that S_P is the set of non zero primes whose may divide the ideal $\mathrm{Ind}_R(\alpha)$. Finally recall that -with notation as above - for a polynomial P belonging to $R[X]$, $\overline{P}$ will stand for the polynomial over $k = R/\mathfrak{p}$ obtained on replacing each coefficient of P by its residue modulo $\mathfrak{p}$. Let denote by $R_{\mathfrak{p}}$ the localization of R at the prime $\mathfrak{p}$.

The following lemma is an immediate consequence of the already known results [1, Proposition 5.12, p. 62]) and [51, property (2), p. 10]), its proof is omitted (cf. [[63], Lemma 3.4]).

Lemma 4.2.1. *Let R be a Dedekind ring, K its fraction field, L a finite separable extension over K and O_L the integral closure of R in L. Let $\alpha \in O_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $\mathfrak{p}$ be a non zero prime ideal in R and B the integral closure of $R_{\mathfrak{p}}$ in L. Then $\mathrm{Ind}_{R_{\mathfrak{p}}}(\alpha) = (\mathrm{Ind}_R(\alpha))_{\mathfrak{p}}$. In particular $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $B = R_{\mathfrak{p}}[\alpha]$.*

Definition 4.2.1. *Let R be a Dedekind ring, K its fraction field and υ be a valuation on K. Let $P = a_0 + a_1X + ... + a_nX^n \in K[X]$, we put:*

$$\upsilon_G(P) = \inf\{\upsilon(a_i) \;\mid\; 0 \leq i \leq n\},$$

then υ_G is a valuation on $K[X]$ called the Gauss valuation on $K[X]$ relative to υ.

The well known Dedekind criterion permits us to decide whether a primitive element $\alpha \in O_L$ is a power basis generator of L over K (PBG for short or a monogenic element of L over K).

Theorem 4.2.1 (Dedekind Criterium)**.** *(see [13],[52], [9], [56], [48], [12], [61]) With notations as above. Let $P = Irrd(\alpha, R) \in R[X]$ be the monic irreducible polynomial of α. Let $\mathfrak{p}$ be a non zero prime ideal in R and $k := R/\mathfrak{p}$ its residual field. Let $\bar{P}$ be the image in $k[X]$ of P and assume that $\bar{P} = \Pi_{i=1}^{r} \bar{P_i}^{l_i}$ is the primary decomposition of $\bar{P}$ in $k[X]$ with $P_i \in R[X]$ a monic lift of the irreducible polynomial $\overline{P_i}$ for $1 \leq i \leq r$. Let $T \in R[X]$ satisfying $P = \prod_{i=1}^{r} P_i^{l_i} + \pi T$. Then α is a PBG of L over $R_{\mathfrak{p}}$ if and only if $gcd\left(\overline{P}_i, \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$.*

Corollary 4.2.1. *With notations as in Theorem 4.2.1. Let $V_i \in R[X]$ be the remainder of Euclidean division of P by P_i. Let $\upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let υ_G be the Gauss valuation on $K[X]$ associated to $\upsilon_{\mathfrak{p}}$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$.*

Proof. Let $T \in R[X]$ satisfying $P = \prod_{i=1}^{r} P_i^{l_i} + \pi T$. Then it can be easily verified that $gcd\left(\overline{P}_i, \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$, where $V_i \in R[X]$ is the remainder of Euclidean division of P by P_i. ∎

4.3 Proof of Theorem 4.1.1

Let R be a Dedekind ring containing $\mathbb{Z}$ and $P = X^p - a$ a monic irreducible polynomial in $R[X]$. Recall that the discriminant of P is equal to $disc_R(P) = p^p\, a^{p-1}R$. As $p \geq 3$, then the set $S_P = Fib_R(p) \cup V(a\,R)$. recall also if $\mathfrak{p}$ is a non zero prime ideal in R then $char(R/\mathfrak{p}) = p$ if and only if $\mathfrak{p} \in Fib_R(p)$.

we shall prove the following two lemmas needed for proving Theorem 4.1.1.

Lemma 4.3.1. *Let R be a Dedekind ring with finite residual fields and K its fraction field. Assume that $charK = 0$ and $L = K(\alpha)$ is a finite separable extension of K. Let $P = X^p - a \in R[X]$ be the monic minimal polynomial of α, where p is an odd prime number. Let $\mathfrak{p}$ be a non zero prime of R and $\upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Assume that $\mathfrak{p} \in V(aR) - Fib_R(p)$. Then $\upsilon_{\mathfrak{p}}(D_{L/K}) = p - 1$.*

Proof. Assume that $\mathfrak{p} \in V(aR) - Fib_R(p)$, by localization at $\mathfrak{p}$ the ring $R_{\mathfrak{p}}$ is a discrete valuation ring, putting $\mathfrak{p} = \pi R$ its maximal ideal, we obtain $P \equiv X^p \mod \pi R$, therefore it is immediate that the remainder of the Euclidean division of P by X is a. Hence if $\upsilon_{\mathfrak{p}}(a) = 1$, then by Dedekind Criterion (Theorem 4.2.1) α is a PBG of L over $R_{\mathfrak{p}}$. Now applying Lemma 4.2.1 we see that $\mathfrak{p}$ does not divide the index ideal $\mathrm{Ind}_R(\alpha)$ and hence by the index-discriminant formula (4.1) we have $\upsilon_{\mathfrak{p}}(D_{L/K}) = p - 1$. Set $\upsilon_{\mathfrak{p}}(a) = s$ and suppose that $s > 1$, let $1 < r < p$ such that $sr \equiv 1[p]$. Set $t = \frac{rs-1}{p}$, then the element $\beta = \frac{\alpha^r}{\pi^t}$ is an algebraic integer satisfies the polynomial $Q = X^p - b$ where $b = \frac{a^r}{\pi^{tp}}$. As the remainder of the Euclidean division of Q by X is b and $\upsilon_{\mathfrak{p}}(b) = rs - tp = 1$,

we see that β is a PBG of L over $R_{\mathfrak{p}}$. Now by index-discriminant formula (4.1) we immediately conclude that

$$p^p b^{p-1} = \mathrm{Ind}_R(\beta)^2 \, D_{L/K}.$$

Since in view of Lemma 4.2.1, $\mathfrak{p}$ does not divide the index $\mathrm{Ind}_R(\beta)$, the above equation shows that the exact power of $\mathfrak{p}$ dividing $D_{L/K}$ is $p-1$.

∎

Lemma 4.3.2. *With notations as in Lemma 4.3.1. Assume that* $\mathfrak{p} \in Fib_R(p) - V(aR)$ *and* $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$. *Then* $\upsilon_{\mathfrak{p}}(D_{L/K}) = p\, e(\mathfrak{p}/p)$.

Proof. Let $\mathfrak{p} \in Fib_R(p) - V(aR)$ and assume that $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$, by localization at $\mathfrak{p}$ the ring $R_{\mathfrak{p}}$ is a discrete valution ring, set $\mathfrak{p} = \pi R$ its maximal ideal, we claim that $\lambda = \alpha - a^{\frac{N_{\mathfrak{p}}}{p}}$ is a PBG of L over $R_{\mathfrak{p}}$, observe first that the element λ is an algebraic integer satisfies the polynomial

$$P_\lambda = \left(X + a^{\frac{N_{\mathfrak{p}}}{p}}\right)^p - a = \sum_{k=1}^{p} \binom{p}{k} X^k \left(a^{\frac{N_{\mathfrak{p}}}{p}}\right)^{p-k} + a^{N_{\mathfrak{p}}} - a,$$

Since p divide $\binom{p}{k}$ for $1 \leq k \leq p-1$, then we see immediately that $P_\lambda \equiv X^p \mod \pi R$ and hence the the remainder of the Euclidean division of P by X is $a^{N_{\mathfrak{p}}} - a$, this prove in view of Dedekind Criterion and the fact that $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$ that λ is a PBG of L over $R_{\mathfrak{p}}$, consequently in view of Lemma 4.2.1 $\mathfrak{p}$ we does not the divide The index $\mathrm{Ind}_R(\lambda) = \mathrm{Ind}_R(\alpha)$. Now by index-discriminant formula (4.1) one can write

$$\mathrm{Disc}_R(P_\lambda) = \mathrm{Disc}_R(P) = p^p a^{p-1} = \mathrm{Ind}_R(\alpha)^2 \, D_{L/K},$$

the above equation shows that the exact power of $\mathfrak{p}$ dividing $D_{L/K}$ is $p-1$. ∎

Proof. (Theorem 4.1.1)

Indeed $pR = \prod_{\mathfrak{p}|\,p} \mathfrak{p}^{e(\mathfrak{p}/p)}$. Let $\mathfrak{c} := p^p \, \mathfrak{b}^{p-1}$. It suffice to show that $\upsilon_{\mathfrak{p}}(D_{L/K}) = \upsilon_{\mathfrak{p}}(\mathfrak{c})$ for all prime $\mathfrak{p} \in S_P$. Let $\mathfrak{p} \in S_P$. It is clear first that

$$\begin{aligned} \upsilon_{\mathfrak{p}}(\mathfrak{c}) &= \upsilon_{\mathfrak{p}}(p) + (p-1)\upsilon_{\mathfrak{p}}(\mathfrak{b}), \\ &= \begin{cases} p\, e(\mathfrak{p}/p) \, + (p-1) & if \ \upsilon_{\mathfrak{p}}(a) \geqslant 1, \\ p\, e(\mathfrak{p}/p)\,, & if \ \upsilon_{\mathfrak{p}}(a) = 0, \end{cases} \end{aligned}$$

If $\upsilon_{\mathfrak{p}}(a) = 0$, then $\mathfrak{p} \in Fib_R(p)$ and hence in view of Lemma 4.3.2 $\upsilon_{\mathfrak{p}}(D_{L/K}) = p\, e(\mathfrak{p}/p)$. If $\upsilon_{\mathfrak{p}}(a) \geqslant 1$, then then there is two cases: If $\mathfrak{p} \notin Fib_R(p)$ then $e(\mathfrak{p}/p) = 0$ and in view of Lemma

4.3.2 $\upsilon_{\mathfrak{p}}(D_{L/K}) = \upsilon_{\mathfrak{p}}(\mathfrak{c}) = p-1$. If $\mathfrak{p} \in Fib_R(p)$ then $\upsilon_{\mathfrak{p}}(a) = 1$ as $\upsilon_{\mathfrak{p}}(\, a^{N_{\mathfrak{p}}} - \, a) = 1$ hence $\mathfrak{p}$ does not divide the index $\mathrm{Ind}_R(\alpha)$ and consequently $\upsilon_{\mathfrak{p}}(D_{L/K}) = \upsilon_{\mathfrak{p}}(\mathrm{Disc}_R(P)) = \upsilon_{\mathfrak{p}}(\mathfrak{c}) = p\, e(\mathfrak{p}/p) + p - 1$.

4.4 Illustration

4.4.1 Relative pure septic extension

Theorem 4.4.1. *Let $K = \mathbb{Q}(\sqrt{35})$ be a quadratic extension and O_K its ring of integer. Let $L = K(\alpha)$ be a septic extension of the field K*

where α satisfies an irreducible polynomial $P = X^7 - a_m$ belonging to $O_K[x]$ such that $a_m = \sqrt{35} + m$, $(m \in \mathbb{Z})$, furthermore we assume that $7 \nmid m$ and $m^6 \equiv 1 \mod 49$. Then

$$D_{L/K} = 7^7 \mathfrak{b}_m^6,$$

where $\mathfrak{b}_m$ is the ideal radical of $a_m R$.

Proof. First of all we note that $7O_K = \mathfrak{p}^2$, it is known that the cardinality of $O_K/\mathfrak{p}$ is 7 since the residual degree of $\mathfrak{p}$ is $f = 1$. We claim that $v_{\mathfrak{p}}(a_m^7 - a_m) = 1$, observe first that

$$\begin{aligned} a_m^6 - 1 &= \sum_{k=0}^{6} \binom{6}{k} \left(\sqrt{35}\right)^k m^{6-k} - 1, \\ &= m^6 - 1 + 525m^4 + 18375m^2 + 42875 + \sqrt{35}\left(6m^5 + 700m^3 + 7350m\right). \end{aligned}$$

Now by property of dominance principle, and using the fact that $\upsilon_7(m) = 0$, it is easy to check that

$$v_{\mathfrak{p}}\left(6m^5 + 700m^3 + 7350m\right) = 0,$$

and

$$v_{\mathfrak{p}}\left(525m^4 + 18375m^2 + 42875\right) = 2.$$

Keeping this in mind and using the fact that $m^6 \equiv 1 \mod 49$, we see immediately that

$$v_{\mathfrak{p}}\left(a_m^6 - 1\right) = \min\left(v_{\mathfrak{p}}\left(525m^4 + 18375m^2 + 42875\right), v_{\mathfrak{p}}((m^6 - 1)), v_{\mathfrak{p}}(\sqrt{35})\right) = 1$$

Now it is clear that $v_{\mathfrak{p}}(a_m^7 - a_m) = 1$, as $v_{\mathfrak{p}}(a_m) = 0$ since $7 \nmid m$. Satisfying the conditions of Theorem 4.1.1, so the discriminant of L over K is given by

$$D_{L/K} = 7^7 \mathfrak{b}_m^6,$$

where $\mathfrak{b}_m$ is the ideal radical of $a_m R$. ∎

Corollary 4.4.1. *With notations as in Theorem 4.4.1. The discriminant $D_{L/\mathbb{Q}}$ is given by*

$$D_{L/\mathbb{Q}} = 7^{21}.2^{14}.5^7.N_{K/\mathbb{Q}}(\mathfrak{b}_m)^6.$$

Proof. The proof follow immediately from the fact that Since $D_{K/\mathbb{Q}} = 2^2.5.7$ and the discriminant tower formula (4.2). ∎

Example 4.4.1. *With notations as in Theorem 4.4.1. Putting $m = 1$, then $L = \mathbb{Q}(\sqrt{35}, \sqrt[7]{1+\sqrt{35}})$. Now using the facts that $N_{K/\mathbb{Q}}(\sqrt{35}+1) = 2 \times 17$, $x^2 - 35 \equiv (x+1)^2 \mod 2$, $x^2 - 35 \equiv \mod (x+1)(x+16) \mod 17$, we see that $(\sqrt{35}+1)O_K = \mathfrak{p}_1^2\mathfrak{p}_2$ where $\mathfrak{p}_1 = 2O_K + (\sqrt{35}+1)O_K$ and $\mathfrak{p}_2 \in Fib_{O_K}(17)$. Hence by Theorem 4.4.1 the discriminant of L over K is given by*

$$D_{L/K} = 7^7(\mathfrak{p}_1\mathfrak{p}_2)^6,$$

Using now corollary 4.4.1 we see that

$$D_{L/\mathbb{Q}} = 7^{21}.2^{14}.5^7.N_{K/\mathbb{Q}}(\mathfrak{p}_1)^6 N_{K/\mathbb{Q}}(\mathfrak{p}_2)^6 = 7^{21}.2^{20}.5^7.17^6.$$

4.4.2 Relative pure quintic extension

Theorem 4.4.2. *Let $K = \mathbb{Q}(\sqrt{3})$ be a quadratic extension and O_K its ring of integer. Let $L = K(\alpha)$ be a quintic extension of the field K where α satisfies an irreducible polynomial $P = X^5 - a_m$ belonging to $O_K[x]$ such that $a_m = 5^2 m + \sqrt{3}$, $(m \in \mathbb{Z})$. Then*

$$D_{L/K} = 5^5\mathfrak{b}_m^4,$$

where $\mathfrak{b}_m$ is the ideal radical of $a_m R$.

Proof. Observe first that $O_K = \mathbb{Z}[\sqrt{3}]$ and $5O_K = \mathfrak{p}$ is prime in O_K. We claim that $v_{\mathfrak{p}}(a_m^{25} - a_m) = 1$. It is clear that

$$\begin{aligned} a_m^{24} - 1 &= \sum_{k=0}^{24} \binom{24}{k} \left(\sqrt{3}\right)^k (5^2 m)^{24-k} - 1, \\ &= \left(\sqrt{3}\right)^{24} - 1 + \sum_{k=0}^{23} \binom{24}{k} \left(\sqrt{3}\right)^k (5^2 m)^{24-k}. \end{aligned}$$

Now using the fact that for any $0 \leqslant k \leqslant 23$, we have

$$\upsilon_{\mathfrak{p}}(5^2m)^{24-k} = (24-k)(\upsilon_{\mathfrak{p}}(m)+2).$$

It is easy to check that

$$\upsilon_{\mathfrak{p}}\left(\sum_{k=0}^{23}\binom{24}{k}\left(\sqrt{3}\right)^k(5^2m)^{24-k}\right) > 1.$$

Now sine $\upsilon_{\mathfrak{p}}(\left(\sqrt{3}\right)^{24}-1) = 1$, then by property of dominance principle, it is easy to check that

$$\upsilon_{\mathfrak{p}}(a_m^{24}-1) = \min\left(\upsilon_{\mathfrak{p}}((\sqrt{3})^{24}-1), \upsilon_{\mathfrak{p}}\left(\sum_{k=0}^{23}\binom{24}{k}\left(\sqrt{3}\right)^k(5^2m)^{24-k}\right)\right) = 1.$$

To complete the proof, clearly it is enough to show that $\upsilon_{\mathfrak{p}}(a_m) = 0$. Suppose to the contrary that 5 divide a_m, now since 5 divide 5^2m, then 5 divide $\sqrt{3}$ which is impossible as $\upsilon_5(\sqrt{3}) = 0$, this prove that $\upsilon_{\mathfrak{p}}(a_m) = \upsilon_5(a_m) = 0$. Satisfying the conditions of Theorem 4.1.1, so the discriminant of L over K is given by

$$D_{L/K} = 5^5\mathfrak{b}_m^4,$$

where $\mathfrak{b}_m$ is the ideal radical of a_mR.

∎

Corollary 4.4.2. *With previous conditions in Theorem 4.4.2. The discriminant $D_{L/\mathbb{Q}}$ is given by:*

$$D_{L/\mathbb{Q}} = 5^{10}.2^{10}.3^5N_{K/\mathbb{Q}}(\mathfrak{b}_m)^4.$$

Proof. The proof follow immediately from the fact that Since $D_{K/\mathbb{Q}} = 2^2.3$ and the discriminant tower formula (4.2). ∎

Example 4.4.2. *Assume that $m = 2$, then $L = \mathbb{Q}(\sqrt{3}, \sqrt[5]{50+\sqrt{3}})$ Now using the facts that $N_{K/\mathbb{Q}}(50+\sqrt{3}) = 11.277$ and $x^2-3 \equiv \mod (x+5)(x+6) \mod 11$, $x^2-3 \equiv \mod (x+130)(x+147) \mod 277$, we see that $(50+\sqrt{3})O_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 \in Fib_{O_K}(11)$. and $\mathfrak{p}_2 \in Fib_{O_K}(277)$. Hence by Theorem 4.4.2 we see that*

$$D_{L/K} = 5^5(\mathfrak{p}_1\mathfrak{p}_2)^4.$$

Now using corollary 4.4.2 we that the discriminant of L over $\mathbb{Q}$ is given by

$$D_{L/\mathbb{Q}} = 5^{10}.2^{10}.3^5N_{K/\mathbb{Q}}(\mathfrak{p}_1)^4N_{K/\mathbb{Q}}(\mathfrak{p}_2)^4 = 5^{10}.2^{10}.3^5.11^4.277^{4.}$$

Bibliography

[1] *M. F. Atiyah, I. G. Macdonald*: Introduction to Commutative Algebra. Addison- Wesley, Massachusetts. (1969). (Cited on page 72.)

[2] W. A. Adkins and S. H. Weintraub, *Algebra: an approach via module theory*, Graduate Texts in Mathematics, Vol. 136, Springer-Verlag, New York, (1992). (Cited on page 72.)

[3] V. Alexandr, N. Popescu and A. Zaharescu, *A theorem of characterization of residual transcendental extension of valuation*, J. Math. Kyoto Univ. 28, 579-592(1988). (Cited on page 30.)

[4] J. D. Bauch, *Computation of integral bases*, J.Number Theory 165 (2016) 382-407. (Cited on page 5.)

[5] W. E. H. Berwick , *Integral bases*, Cambridge University Press, (1927). (Cited on pages 5 and 44.)

[6] O. Boughaleb, A. Soullami and M. Sahmoudi, *On relative monogeneity of a family of number fields defined by* $X^{p^n} + aX^{p^s} - b$, Boletín de la Sociedad Matemática Mexicana volume 29, Article number: 5 (2023). (Cited on page 60.)

[7] N. Bourbaki, *Algèbre*, Chapitres 4 à 7, Masson , 1981. (Cited on page 36.)

[8] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London and New york, (1967). (Cited on pages 38, 39, and 71.)

[9] M. E. Charkani and M. Sahmoudi, *Sextic Extension with cubic subfield*, J.P. Journal of Algebra, Number Theory et Applications, **34** (2), 139-150 (2014). (Cited on pages 6, 57, 59, 69, and 73.)

[10] M. E. Charkani and M. Sahmoudi, *Tower Index formula and monogenecity*, Communications in Algebra, vol. 48, no. 1, 139-150, (2021). (Cited on page 59.)

[11] M. E. Charkani and A. Deajim, *Relative index extensions of Dedekind rings*, JP J. Algebra, Number Theory and Appl **27**, 73–84 (2012). (Cited on pages 38, 39, and 71.)

[12] M. E. Charkani and A. Deajim, Generating a Power Basis over a Dedekind Ring. J. Number Theory 132, No. 10, 2267-2276, (2012).Zbl 1293.11101, https://doi.org/10.1016/j.jnt.2012.04.006. (Cited on page 73.)

[13] M. E. Charkani and O. Lahlou, *On Dedekind's criterion and monogenicity over Dedekind rings*, Int. J. of Math. and Math. Sci. **2003**, 4455–4464 (2003). (Cited on pages 5 and 73.)

[14] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 138, Springer Verlag, Berlin, (1996). (Cited on pages 5, 36, 42, 49, and 70.)

[15] I. Corso and IL. Rossi *Normal integral bases for cyvlic Kummer extensions*, Journal of Pure and Applied Algebra, 214(2010) 385391. (Cited on pages 9 and 70.)

[16] A. Deajim and EL. Fadil, *On the extensions of discrete valuations in number fields*, Mathematica Slovaca 69(5), (2019). (Cited on pages 7, 21, and 28.)

[17] R. Dedekend, *Uber den zussamenhang zwischen der theorie der ideals und der theorie der hoheren cyclotimy index*, Abh. Akad. Wiss. Gottingen, Math.-Phys. KL **23** 1-23, (1878). (Cited on page 5.)

bibitemD-F Alg David S. Dummit and Richard M. Foote, *Abstract Algebra (3rd ed.)*, New York: Wiley, 2004.

[18] A. J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, New York (2005). (Cited on pages 30 and 31.)

[19] L. El Fadil and O.Boughaleb, *p-Integral bases and prime ideal factorization in quintec fields*, Gulf Journal of Mathematics Vol 4, Issue 4 (2016)140-154. (Cited on page 42.)

[20] L. El Fadil and J. Montes, E. Nart, *Newton polygons and p-integral bases of quartic number fields* , Journal of Algebra and Its Applications Vol. 11, No. 4 (2012) 1250073. (Cited on page 42.)

[21] D. Ford, *The Construction of maximal orders over a Dedekind Domain*, J.sumbolic computation (1987). (Cited on page 7.)

[22] D. Ford, *On the computation of the maximal order in a Dedekinds domain*, The ohio State University Ph.D, (1978). (Cited on page 7.)

[23] D. Ford, S. Pauli, and X. Roblot, *A fast algorithm for polynomial factorization over Qp*, Journal de théorie des nombres de Bordeaux, Tome 14 no. 1, p. 151-169 (2002). (Cited on page 7.)

[24] A. Fröhlich and M. J. Taylor, *Algebraic number Theory*, Combridge Studies in Advenced Mathematics, **27**, Cambridge University Press, (1993). (Cited on pages 9, 38, 39, 52, 60, 71, and 72.)

[25] G. Fujisaki, *Some examples of number fields without relative integral bases*, J. Fac. Sei. Univ. Tokyo Sect.IA 21, 92-95, (1974). (Cited on page 6.)

[26] P. A. Grillet, *Abstract Algebra*, Graduate Texts in Mathematics, Vol. 242, second edition, (2007). (Cited on page 37.)

[27] M. Haghighi, Relative integral basis for algebraic number fields, International Journal of Mathematics and Mathematical Sciences, **9**, 97-104 (1986) https://doi.org/10.1155/S0161171286000121. (Cited on page 6.)

[28] E. Hallouin, *Calcul de fermeture intégrale en dimension 1 et factorisation*, Thèse de doctorat de l'Université de Poitiers(1998). (Cited on pages 7 and 12.)

[29] E. Hallouin, *Computing Local Integral Closures* , Journal of Symbolic Computation Volume 32, Issue 3, September (2001), Pages 211-230. (Cited on pages 7 and 11.)

[30] M. Hall , *Indices In Cubic Fields*, Bull. Amer. Math. Soc. Volume 43, Number 2, (1937), 104-108. (Cited on pages 1, 5, 8, 43, and 44.)

[31] A. Hameed and Nakahara, *Integral bases and relative monogenity of pure octic fields*, Bull. Math. Soc. Sci. Math. Roumanie Tome, 58(106) No. 4, (2015), 419-433. (Cited on page 70.)

[32] A. Jakhar and N. Sangwan , *Integral basis of pure prime degree number fields*, Indian Journal of Pure andd Applied Mathematics, volume 50, pages 309-314 (2019). (Cited on pages 9, 44, 45, and 70.)

[33] A. Jakhar, S. K. Khanduja and N. Sanagwan, *On integral basis of number fields*, Mathematika 67, (2021), 187195. (Cited on pages 9 and 70.)

[34] A. Jakhar, S. K. Khandujaand N. Sangwan, *Discriminant of pure squarefree degree num- ber fields*, Acta Arith., 181, (2017), 287-296. (Cited on page 70.)

[35] G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, Second Edition (1995). (Cited on pages 39, 48, and 71.)

[36] K. Johnson , *Super-Additive Sequences and Algebra of polynomials*, Proc. Amer. Math. Soc., Volume 139, **10**, October (2011), Pages 3431 - 3443. (Cited on page 7.)

[37] M. Kumar and S. K. Khanduja, *A Generalization of Dedekind Criterion*, Communication in Algebra, **35**, 1479-1486 (2007). (Cited on page 61.)

[38] S. K. Khanduja and S. Kumar, *Prolongations of valuations to finite extensions*, Manus.math.131, (2010), 323-334. (Cited on pages 7 and 26.)

[39] S. K. Khanduja and S. Kumar , *On prolongations of valuations via Newton polygons and liftings of polynomials*, J.Pure Appl. Algebra 216 (2012) 2648-2656. (Cited on page 33.)

[40] S. K. Khanduja and *J. Saha*, *On a generalization of Eisenstein's irreducibility criterion*, Mathematika 44(1997) 37-41. (Cited on page 7.)

[41] S. K. Khanduja and Sanjeev Kumar, *On prolongation of valuation via Newton polygons and liftings of polynomials*, J.Pure Appl.Algebra 216 (2012) 2648-2656. (Cited on page 7.)

[42] S. K. Khanduja and S.Kumar , *A generalization of a theorem of Ore*, Journal of pure and Applied ALgebra 218(7),1206-1218 (2014). (Not cited.)

[43] S. K. Khanduja , *On valuation of K(x)*, Proc.Edinburgh Math. soc. 35, 419-426(1992). (Cited on page 30.)

[44] M. Kumar and S. K. Khanduja, *A Generalization of Dedekind Criterion*, Communication in Algebra, **35**, 1479-1486 (2007). (Cited on page 61.)

[45] S. Lang, *Algebra*, GTM 211, Springer-Verlag New York (2002), 142-146. (Cited on pages 35, 36, and 71.)

[46] R. Mackenzie and J. Scheuneman, *A Number Field Without a Relative Integral Basis*, Amer. Math. Monthly 78, 882-883, (1971). (Cited on page 6.)

[47] H. Matsumura, *Commutative Ring Theory*, Cambridge Univeristy Press, Cambridge, (1986). (Cited on page 48.)

[48] E. Nart and J. Montes, *On a Theorem of Ore*, Journal of Algebra, 146 (1992). (Cited on pages 49 and 73.)

[49] W. Narkizewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Second Edition, (1999). (Not cited.)

[50] G. Neukirch, *Algebraic Number Theory*, Springer-Verlag, New york, (1999). (Cited on pages 9, 25, 52, and 60.)

[51] P. H. C. Nogués and M. J. Taylor, Unités Modulaires et monogénéité d'anneaux d'entiers, In Séminaire de Théeorie des nombres. Paris, france **1986-1987**, **75**, 35-64 (1989). (Cited on page 72.)

[52] P. Schmid: On criteria by Dedekind and Ore for integral ring extensions. Arch. Math. **84** (2005) 304–310. Zbl 1072.13004 (Cited on page 73.)

[53] K. Okutsu, *Construction of Integral Basis. I*, Proceedings of the Japan Academy, 58, Ser. A (1982), 47-49, 87-89. (Cited on page 5.)

[54] M. Pohst and H. Zassznhaus, *Algorithmic algebraic number theory*, Cambridge University Press, (1989). (Cited on page 49.)

[55] R. A. Rosenbaum , *Subadditive functions* , Duke Math. J., 17, (1950), 227-247. (Cited on page 7.)

[56] M. Sahmoudi and A. Soullami, *On Sextic Integral Bases Using Relative Quadratic Extention*, Bol. Soc. Paran. Mat. **38**(4), 175-180 (2020), https://doi.org/10.5269/bspm.v38i4.40042. (Cited on pages 6 and 73.)

[57] M. Sahmoudi, *Explicit integral basis for a family of sextic field*, Gulf Journal of Mathematics, International Colloquium of Algebra, Number Theory. Cryptography and Information Security Taza, Morocco. **4** (4): 217-222 (2016). (Cited on pages 61 and 72.)

[58] M. Sahmoudi and A. Soullami, *On monogenicity of relative cubic-power estensions*, Advances in Mathematics: Scientific Journal 9, no.9, 68176827, (2020). (Cited on page 6.)

[59] P. Samuel, *Théorie algèbrique des nombres*, (1971), Hermann Paris, 2eme edition revue et corrigée. (Cited on pages 8 and 36.)

[60] H. Smith, The monogeneity of radical extensions, Acta Arithmetica 198 313-327, (2021). DOI: 10.4064/aa200811-7-10 (Cited on pages 6 and 71.)

[61] A. Soullami, M. Sahmoudi and O.Boughaleb, *On relative power integral basis of a family of numbers fields*, Rocky Mountain J. Math. 51(4): 1443-1452 (2021). (Cited on pages 6 and 73.)

[62] B. K. Spearman and K. S. Williams, *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., 70,185-192, (1996). (Cited on pages 6 and 70.)

[63] M. Sahmoudi, M. E. Charkani, : Relative monogenity of pure cyclic fields of degree an odd prime number, Mathematica Bohemica, pp. 1-12, (2022). (Cited on pages 71 and 72.)

[64] H. D. Stainsby, *Triangular bases of integral closures*, J. Symbolic Comput.87 (2018) 140-175. (Cited on page 5.)

[65] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12**, 1099-1106 (1962). (Cited on pages 6 and 64.)

[66] *K. Uchida*, *When is* $\mathbb{Z}[\alpha]$ *the ring of the integers?*, Osaka J. Math. **14** (1977), 155–157. (Cited on page 70.)

[67] L.C. Washington, *Relative integral bases*, Proceedings of the American Mathemtical Society, Vol 56, (1976). (Cited on page 6.)