جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITE SIDI MOHAMED BEN ABDALLAH DE FES
كلية العلوم ظهر المهراز فاس
FACULTE DES SCIENCES DHAR EL MEHRAZ FES

N° d'Ordre : **39 /2021**

Formation Doctorale : Mathématiques-Applications

Discipline : Mathématique

Spécialité : Algèbre

Laboratoire : LAMA

THESE DE DOCTORAT

Présentée par

SOULLAMI Abderazak

Galois structure of a number field and Steinitz class

Soutenue le 28 / 07 / 2021 devant le jury composé de :

Pr. Abdelfattah TOUZANI	***Faculté des sciences Dhar El Mehraz -Fés***	***Président***
Pr. Jilali ASSIM	***Faculté des sciences -Meknès***	***Rapporteur***
Pr. Abdelmalek AZIZI	***Faculté des sciences -Oujda***	***Rapporteur***
Pr. Mohammed TAOUS	***Faculté des sciences et techniques -Errachidia***	***Rapporteur***
Pr. Lhoussain EL FADIL	***Faculté des sciences Dhar El Mehraz -Fés***	***Examinateur***
Pr. Karim MOUNIRH	***Faculté des sciences Dhar El Mehraz -Fés***	***Invité***
Pr. Mohammed CHARKANI	***Faculté des sciences Dhar El Mehraz -Fés***	**Directeur de thèse**

Année universitaire : 2020-2021

Galois Structure of a number field and Steinitz Class

Résumé

Soit R un anneau de Dedekind de corps de fraction K et L une extension Galoisienne finie de K de groupe de Galois $G = Gal(L/K)$, on note $\mathcal{O}_L$ l'anneau des entiers de L. Dans cette thèse, on montre que si l'extension L/K est abelienne avec une base intégrale diagonale alors l'ordre associé est égale à l'ordre maximal $\mathcal{S}$ de $K[G]$. D'autre part on calcule l'indice galoisienne d'un élément θ de $\mathcal{O}_L$, et on donne une condition nécessaire et suffisante pour que θ génère une base normal intégrale, et nous donnons une preuve alternative d'un résultat principal de Del Corso et Rossi prouvé en 2010. De plus on construit une extension cyclique finie de dégré premier d'un corps de caractéristique différente de zéro et aucune condition sur les racines de l'unité est posée. Dans ce cas on donne un candidat pour le générateur de la base normale intégrale. Par suite on traite la formule du tour de quelques invariants algébriques (Discriminant et la Classe de Steinitz), en effet on donne des nouvelles preuves pour ces formules, et on présente quelques exemples. Finalement on examine quelques propriétés nécessaires est suffisantes pour l'existence de la base monogène en utilisant une version récente du critère de Dedekind. Quelques exemples illustratifs sont présentés à l'aide du logiciel Maple.

Keywords : Ordre associé, Base normal intégral, Discriminant, Classe de Steinitz, Monogènité.

Abstract

Let R be a Dedekind ring with fraction field K and L be a finite Galois extension of K with Galois group $G = Gal(L/K)$. Let $\mathcal{O}_L$ denote the integer ring of L. In this thesis, we prove that if the extension L/K is abelian with diagonal integral basis then the associated order is equal to the maximal order $\mathcal{S}$ of $K[G]$. Also, we calculate the Galois index of an element θ of $\mathcal{O}_L$, and we give a necessary and sufficient condition on θ to be a normal integral basis generator also we give an alternative proof of the main result of Del Corso and Rossi stated in 2010. Moreover, we construct a finite cyclic extension of prime degree of a field of prime characteristic and no condition on roots of unity is involved. In such a situation we give a candidate of normal integral basis generator. The tower formula of some algebraic invariants (Discriminant and Steinitz class) is treated in this report; indeed, we state new proofs of those formulas and we give some illustrations. Finally, 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.

Keywords : Associated Order, Normal integral basis, Discriminant, Steinitz class, Power integral basis.

Acknowledgements

I would like to express my sincere gratitude to my thesis supervisor Mr. M. E. Charkani, professor at Department of Mathematic. His patience, enthusiasm, co-operations and suggestions made me present this research work to produce in the present form. His brilliant, skillful supervision enriched this study higher than my expectation. This research work would not be possible without hit stimulation inspiration and cooperation.

Thank you to my committee members, Mr Abdelmalek Azizi, Mr Jilali Assim and Mohammed taous. Your encouraging words and thoughtful, detailed feedback have been very important to me.

Thank you to Lhoussain El Fadil and Karim Mounirh, examiners of this report, for all of the kind words and assistance you have provided.

Thank you to my partner, Mohammed Sahmoudi, 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.

Author's papers involved in this thesis:

1. M. E. Charkani and A. Soullami, *Tower Formula For Discriminant*, JP Journal of Algebra, Number Theory et Applications, (**43**), (1), (2019), 13-21.

2. M. Sahmoudi and A. Soullami, *On Sextic Integral Bases Using Relative Quadratic Extension*, Bol. Soc. Paran. Mat., (**38**), (4), (2020), 175-180.

3. M. Sahmoudi and A. Soullami, *On Monogenicity Of Relative Cubic-Power Pure Extensions*, Adv. Math., Sci. J., (**9**), (9), (2020), 6817–6827.

4. M. E. Charkani, M. Sahmoudi and A. Soullami, *Tower Index formula and monogenecity*, Communications in Algebra, (**49**), (6), (2021), 2469-2475.

5. A. Soullami, M. Sahmoudi, and O. Boughaleb, *On relative power integral basis of a family of numbers fields*, to appear in Rocky Mountain Journal Of Mathematics.

Contents

Acknowledgements **1**

Introduction **7**

1 Generality on representation theory and orders **11**

1.1 Group rings 11

1.2 Module over group rings 15

1.3 Character of a $K[G]$-module 16

1.3.1 Character of an abelian group 17

1.3.2 Conjugated characters 19

1.4 Idempotents 20

1.5 Orders And Maximal Order 25

1.5.1 Orders 25

1.5.2 Maximal Orders 26

1.5.3 Maximal Orders in $K[G]$-module 27

2 Galois module structure **30**

2.1 Associated order 30

2.1.1 Leopoldt and Hilbert-Speiser theorems 32

2.2 Normal integral basis 36

2.2.1 Normal basis 36

2.2.2 Gauss sums 39

2.2.3 Galois index ideal 40

2.2.4 Dedekind sums 46

2.2.5 The associated ideals in a Dedekind ring 47

2.2.6 Cyclic Kummer tamely ramified extensions 47

2.2.7 Associated order in abelian extension 48

2.2.8 Cyclic extension ever a fields of prime characteristic 49

3 Discriminant and Steinitz class **52**
3.1 Tower formula of discriminant . . . 52
3.1.1 Introduction . . . 52
3.1.2 Discriminant of bilinear modules . . . 52
3.1.3 Tower formula of discriminants . . . 54
3.1.4 Applications . . . 55
3.2 Tower formula of Steinitz class . . . 56
3.2.1 Steinitz class . . . 56
3.2.2 Steinitz module and index . . . 61
3.2.3 Steinitz class of Kummer extension . . . 63
3.3 Discriminant of compositum of number fields . . . 64

4 Monogenity of relative extension **66**
4.1 Dedekind criterion . . . 66
4.2 Monogenicity of relative cubic-power pure extensions . . . 67
4.2.1 Monogeneity of relative cubic-power pure extension - local case . . . 67
4.2.2 Monogeneity of relative cubic-power pure extension - Dedekind case . . . 69
4.2.3 Illustration . . . 70
4.3 Monogenicity of some relative cubic-power non-pure extensions . . . 73
4.3.1 Monogeneity of relative cubic-power extension - local case . . . 73
4.3.2 Monogeneity of relative cubic-power extension - Dedekind case . . . 75
4.3.3 Illustrations . . . 79

Conclusion and perspectives **82**

Notations

Symbols	Descriptions
$\mathbb{N}$	natural numbers set.
$\mathbb{Z}$	integer numbers set.
$\mathbb{Q}$	rational numbers set.
$\cup$	union symbol.
$\cap$	intersection symbol .
$\zeta_n = e^{\frac{2i\pi}{n}}$	nth root of unity in $\mathbb{C}$.
$\phi(n)$	Euler's totient function.
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 .
$\mathcal{O}_K$	the ring of integers of K.
$M_{m,n}(R)$	set of $m \times n$ matrices with entries in R.
$M_n(R)$	set $n \times n$ matrices with entries in R.
$GL_n(R)$	$n \times n$ invertible matrices with entries in R.
$Aut_R(M)$	set of R-automorphisms of M.
$Hom_R(M, N)$	R-homomorphisms of M in N.
$\oplus_{i=1}^n M_i$	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 $g(X)$.
$dis(P)$	discriminant of the polynomial P.
$Irred(x,\, K)$	minimal polynomial of x over the field K.
$a\|b$	a divides b.
$a \wedge b = d$	d is the gcd of a and b.
$a \vee b = n$	n is the lcm of a and b.
$p^r \|\| n$	p^r divides n and p^{r+1} does not divide n.
$\mathfrak{A}_{L/K}$	the associated order of L/K.
$Gal(L/K)$	the galois group of L over K.
$Tr_{L/K}(x)$	the trace of an element x of L over K.
$N_{L/K}(x)$	the norm of an element x of L over K.
$D_K(L)$	the relative discriminant ideal of L over K.

$\mathfrak{D}_K(L)$	the relative different ideal of L over K.
$S_{L/K}$	the steinitz class of L over K.
$S_R(M)$	the steinitz class of the R-module over M.

Introduction

Let L/K be a finite Galois extension of number fields, with Galois group G, and let $\mathcal{O}_K$ and $\mathcal{O}_L$ denote the integer rings of K and L respectively. The ring $\mathcal{O}_L$ is naturally endowed with the structure of an $\mathcal{O}_K[G]$-module. The normal basis theorem asserts that L is free of rank 1 left module over the group ring $K[G]$ (See [6] for modern proof). A more deep question is concerned with the freeness of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module. In addition, if $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module, then it must be of rank 1, and the conjugates of a generator constitute an $\mathcal{O}_K$ basis called normal integral basis. It is well known that a necessary condition for $\mathcal{O}_L$ to be free over $\mathcal{O}_K[G]$ is for the extension to be at most tamely ramified, however this is not sufficient.

Studying the galois module structure of O_L means the study of the structure $\mathcal{O}_L$ as an $\mathfrak{A}_{L/K}$-module such that:

$$\mathfrak{A}_{L/K} = \{u \in K[G] \mid u\mathcal{O}_L \in \mathcal{O}_L\}.$$

This is a subring of $K[G]$ which contains $\mathcal{O}_K[G]$. It's known that if $\mathcal{O}_L$ is free over an $\mathcal{O}_K$-order H in $K[G]$ then $H = \mathfrak{A}_{L/K}$.

The main contributions of authors on this subject were investigate the following three problems:

1. Give an explicit description of the associated order $\mathfrak{A}_{L/K}$ of $\mathcal{O}_L$ in $K[G]$.
2. Describe the structure of $\mathcal{O}_L$ as an $\mathfrak{A}_{L/K}$-module, and in particular to determine whether $\mathcal{O}_L$ is free over, i.e. is isomorphic to, $\mathfrak{A}_{L/K}$.
3. Give an explicit generator of $\mathcal{O}_L$ over its associated order. If $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

In the following, we recall some of the most important works carried out in this context, hence A. Srivastav and S. Venkataraman [70] gives necessary and sufficient conditions of O_L to be free over $\mathfrak{A}_{L/K}$ when L/K is quadratic extension, S. P. Chan and C.H. Lim [14] consider a tower of cyclotomic extension $\mathbb{Q} \subset K \subset L$ and prove that O_L is free over the associated order $\mathfrak{A}_{L/K.}$ In the paper of W. Bley [5] he put $K = \mathbb{Q}(\zeta_{p^r})$ and $L = \mathbb{Q}_{p^{n+r}}$ with $r \geq 1$ if $p \geq 3$(resp. $r \geq 2$ if $p = 2$) and $m \geq 1$, then the associated order of L/K is the unique maximal order of the group ring $K[G]$ where $G = Gal(L/K)$, moreover $\mathcal{O}_L$ is free over its associated order. This result was partially generalised by N. Byott and G. Lett [9], hence for L abelian over $\mathbb{Q}$ and $K \subset L$ they give an

explicit description of $\mathfrak{A}_{L/K}$ if K is a cyclotomic field, moreover they prove that $\mathcal{O}_L$ is isomorphic to $\mathfrak{A}_{L/K}$. Furthermore they show that if L/K is cyclic and totally wildly ramified extension which is linearly disjoint with $\mathbb{Q}^{(m)} = \mathbb{Q}(\zeta_m)$, where m is the conductor of K, then the associated order is the maximal order. Other general results about $\mathfrak{A}_{L/K}$ has been described by Bergé [4], precisely when $\mathfrak{A}_{L/K}$ viewed as a subring of $End_{\mathcal{O}_K}(\mathcal{O}_L)$ the ring of $\mathcal{O}_K$-endomorphisms of $\mathcal{O}_L$. Therefore the associated order $\mathfrak{A}_{L/K}$ is isomorphic to $End_{\mathcal{O}_K[G]}(\mathcal{O}_L)$ if L/K is abelian. The associated order has not been studied exclusively in the case of extensions of number fields, in fact other kind of relative extension have been investigated. In [13] Chan proved that for an extension of p-adic fields $\mathbb{Q}_p$ the ring of integer $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ if L and K are division fields of Lubin-Tate formal group. Also Aiba [1] construct an example of a wildly ramified abelian extension over K "the field of one variable rational function over a finite field", whose integer ring is not free over it's associated order. In addition, in [2] she consider the field K of the power series over a finite field of characteristic $p > 0$ and L a cyclic extension of K of degree p, she gives a necessary and sufficient condition for $\mathcal{O}_L$ to be free over $\mathfrak{A}_{L/K}$, in this case she construct a free basis explicitly.

Another crucial topic is to search the existence of normal integral basis briefly NIB, we say that an extension L/K has a normal integral basis if there is an element θ in $\mathcal{O}_L$ such that $\{\sigma(\theta)\}_{\sigma\in G}$ is an integral basis $\mathcal{O}_K$-basis of $\mathcal{O}_L$, in this case the associated order explicitly determined as $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$. The most remarkable result in this direction, is the one established by Ayala [3] on the existence criterion for NIB in a kummer extension of prime degree, and he shows how to construct this basis in this case, Ichimura [44] generalised this result for kummer extension of degree $n \in \mathbb{N}$, in 2010 this last result was slightly corrected By Corso and Rossi [24]. If the extension L/K is unramified cyclic extension of degree p and $\zeta_p \in K$, then if L/K has a power integral basis if it has a NIB, the converse is not true in general this was asserted in [43]. For a tame kummer extension Ichimura [42] gives a necessary and sufficient condition to the existence of NIB. Moreover In [45] the author shows that when $K/\mathbb{Q}$ is unramified at p, then any tame cyclic extension L/K of degree p has a normal integral basis if the extension $L(\zeta_p)/K(\zeta_p)$ has a normal integral basis.

We recall that L/K with $L/\mathbb{Q}$ is abelian is said to be Leopoldt if the ring of integer O_L is free over $\mathfrak{A}_{L/K}$, and a number field K is Leopoldt if for every extension L/K such that $L/\mathbb{Q}$ is abelian is Leopoldt. The field of rational number is Leopoldt, Johnston [46] gives other types of fields which are Leopoldt. Hilbert-speiser proved that a finite abelian extension $K/\mathbb{Q}$ has a normal integral basis if and only if it's tamely ramified, this is not generally true, a number field K is characterised to be Hilbert-speiser if each tame extension L/K has normal integral basis. In [37] , Greither, Replogle, Rubin and Srivastav shows that $\mathbb{Q}$ is the only such number field.

This thesis is organized as follows:

In chapter 1 we recall some well known results on group rings and module over group rings, there characters and idempotents and some fundamental theorems such as Wedderburn-Artin, Maschke's Theorem and others. Hereafter an overview on orders and maximal orders, in particular we precise the maximal order of the group algebra $K[G]$ and we express it as a sum of simple algebra using characters and there associated idempotents. Those results were the intrinsic pieces to get deep achievements on the associated order $\mathfrak{A}_{L/K}$.

In chapter 2 we prove that for an abelian extension L/K with a diagonal integral basis (Definition 2.2.3) the associated order is the maximal order. We would note that in this situation no condition on the galois group of $L/\mathbb{Q}$ have been set. Another topic treated in this chapter the problem of the normal integral basis (NIB for short). Hence we note that the theorem of normal basis is considered to be the best possible result of the additive structure of a G-module, it went through several stages before taking its current form. In 1850 Eisenstein [26], established the case where K is a finite prime field and Schönemann [67] for the case of extension of prime degree. For the proof over finite fields the proof is due to Hensel [40]. The final version of the Theorem is due to M. Deuring [25]. We address our attention to the composition of normal basis and normal integral basis, also we give necessary and sufficient condition to the existence of such a basis in distinct situation such as Kummer extensions and extensions over field with a nonzero characteristic, also and we give an alternative proof of the main result of Del Corso and Rossi [24]. To conclude this part of the this report we calculate the galois index of some relative extensions.

In chapter 3, the first section is devoted to study the tower formula of the discriminant, In the case of a number field it's known as a consequence of the tower formula of the different ideal using the fact that for a finite extension of a number field L over K the discriminant ideal is the norm of the different ideal, one can write $D_K(L) = N_{L/K}(\mathfrak{D}_K(L))$, where $\mathfrak{D}_K(L)$ and $D_K(L)$ are the different ideal and the discriminant ideal respectively, in this report one can omit the previous proof, since the given proof overlook the notion of the different ideal. We recall the notion of bilinear module, and we introduce the notion discriminant of bilinear module and we state the conditions of the main result, an accurate proof is given. Finally in the last part of this section, some useful examples are given in order to demonstrate the interest and the use of the tower formula of discriminant. In seconde section we present some classic results on the steinitz class, a result due to C. Khar and D. Prasad [48] shows that the steinitz class of an ideal $S_{L/K}(\mathfrak{a})$ of an ideal of $\mathcal{O}_L$ is the product of its norm and the steinitz class of $\mathcal{O}_L$. Such a result was established using a long proof based on K-theory. In this work we have taken this result and demonstrated it by using the fact that the norm of a ideal is equal to the order. On the other hand, the tower formula of steinitz class has been proved in [31] using the results of the global class field theory. Hence we have presented a simple proof without going through the class field theory, based only on the definition of the steinitz class. We conclude this section by given a candidate of Steinitz

class in Kummer extension.

In chapter 4, we address our attention to problem of monogenity. 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. If R is a principal ideal domain, every finitely generated torsion-free R-module has integral basis. So, any fractional ideal in a number field has an integral basis. The problem of monogenity (more generally existence of an integral basis) is a classical topic of algebraic number theory. It was originally examined by Dedekind [23] and since many number theorists have been attracted (c.f. [11, 12, 20, 62, 34, 35, 36, 56, 57, 68] and others). Indeed, Testing whether L/K has a relative monogenic integral basis (RMIB for short) is a hard open problem, worse still, we don't even know if the integral closure $\mathcal{O}_L$ 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 best case, we recall that L/K is monogenic or α is a PBG of L/K, or equivalently, $\{1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$ for some α of $\mathcal{O}_L$, is a basis for $\mathcal{O}_L$ over R which is denoted more briefly by $\mathcal{O}_L = R[\alpha]$.

The authors of [55, 32], have given examples of quadratic extensions of imaginary quadratic number fields for which there exists no relative integral basis and by using a theorem of Artin, [73] gives necessary and sufficient conditions for certain quadratic extensions of imaginary quadratic fields to have relative integral bases. Hereafter, [20, 62], studies monogenity in general quadratic cases. For cubic relative extension, [68] 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 [38] (1986), but for relative extensions of degree greater than 4, there is few results on RMIB or RIB and almost published works deal with decomposable extensions (which are composite of two pure subfields). 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.

Chapter 1

Generality on representation theory and orders

1.1 Group rings

Let R be ring and G a group, we denote by $R[G]$ the set of formal linear combination defined as $R[G] = \{\sum_{\sigma\in G} a_\sigma\sigma \mid a_\sigma \in R, \sigma \in G \text{ and } a_\sigma = 0 \text{ almost every where}\}$. For two elements $f, g \in R[G]$ defined by $f = \sum_{\sigma\in G} a_\sigma\sigma$ and $g = \sum_{\sigma\in G} b_\sigma\sigma$ respectively, their sum and product are given by:

$$f + g = \sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma.$$

$$fg = \sum_{\sigma,\,\tau\in G} a_\sigma b_\tau \sigma\tau.$$

From these definitions, $R[G]$ is a ring which has a unity if R is a ring with unit. For an element $r \in R$ we can define the product of an element in $R[G]$ by r as:

$$rf = r(\sum_{\sigma\in G} a_\sigma\sigma) = \sum_{\sigma\in G}(ra_\sigma)\sigma.$$

Then we see that $R[G]$ is also a left (right) R-module. The set $R[G]$, with the operations defined above, is called the group ring of G over R. In the case where R is commutative, $R[G]$ is also called the group algebra of G over R.

Theorem 1.1.1 ([33]). *Let G be a group. The group ring $R[G]$ is Noetherian if and only if R is Noetherian and G is finitely generated. If K is a field and G is a finite group then $K[G]$ is artinian.*

Proposition 1.1.1. *Let S be a commutative subring of R, then:*

$$R \otimes_S S[G] \simeq R[G].$$

as R-algebra.

Proof. See proposition 1.5 [49] p. 70 and proposition 6.3 p. 48 [50].

Corollary 1.1.1. *Let R be a commutative ring and H a normal subgroup of G, then :*

$$R[G/H] \otimes_R R[H] \simeq R[G/H][H].$$

Proposition 1.1.2. *Let R be a commutative ring. Let G_1 and G_2 be two abelian groups, then:*

$$R[G_1 \times G_2] \simeq R[G_1] \otimes R[G_2].$$

Proof. See proposition 1.6 [49] and [50].

Remark 1.1.1. *Let G_1 and G_2 be two groups then $R[G_1 \times G_2] = A[G_2]$ where $A = R[G_1]$. (See [33] Theorem 7.1.)*

Let M ba a R-module, then M is said to be simple if $M \neq 0$ and it have no non-zero proper submodule, one can verify that an R-module M is simple if and only if there exist a left maximal ideal I such that $M \simeq R/I$. The module M is said to be semisimple if every submodule is a direct summand.

Theorem 1.1.2. *Let M be an R module. Then the following conditions are equivalent:*

1. *M is semisimple.*
2. *M is a direct sum of simple submodules.*
3. *M is a sum of simple submodules (not necessarily direct).*

Proof. See Theorem 5.3 [66]. ∎

Remark 1.1.2. *A ring R is said to be semisimple if R, viewed as a left module over itself, is semisimple.*

Theorem 1.1.3 (Schur's lemma)**.** *Let M and N be two simple R-modules, then every homomorphism of M into N is either zero or an isomorphism. Hence $Hom_R(M, N)$ is a division ring.*

Proof. See Theorem 5.1 [66]. ∎

Theorem 1.1.4 (Wedderburn-Artin)**.** *A ring R is semisimple if and only if it is a direct sum of matrix algebras over division rings:*

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s)$$

Proof. See Theorem 13 [66]. ∎

Conclusion 1.1.1. *Let R be a semisimple ring then there is only finite number of simple non-isomorphic left ideals: $L_1, L_2, \cdots, L_r$, therefore*

$$R = \oplus_{i=1}^{r} R_i$$

where the R_i is the sum of left ideals of R isomorphic to L_i (one may check the R_i is a minimal two sided ideal of R). Every finitely generated R-module has the form

$$L_1^{m_1} \oplus L_2^{m_2} \oplus \cdots \oplus L_r^{m_r}$$

So that $\{[L_i], i = 1, 2, \cdots, r\}$ is a basis of the Grothendieck group $\mathcal{K}_0(R)$ of R. By Schur's lemma 1.1.3 $D_i = End_{R_i} L_i$ is a division ring, and Wedderburn-Artin 1.1.4 assert that $R_i = M_{n_i}(D_i)$. Note that if $n_i = Dim_{D_i} L_i$ then $Dim_{D_i} R_i = n_i^2$.

The next Theorem gives necessary and sufficient conditions on group ring to be semisimple.

Theorem 1.1.5 (Maschke's Theorem)**.** *Let G be a group. Then the group ring $R[G]$ is semisimple if and only if the following conditions hold:*

1. *R is a semisimple ring;*
2. *G is finite;*
3. *$|G|$ is invertible in R.*

Proof. This is Theorem 3.4.7 of [60]. ∎

In the case where $R = K$ is a field of characteristic p not dividing the order of the finite abelian group G then, Theorem 1.1.5 can be formulated as follows.

Corollary 1.1.2. *Let G be a finite group and K be a field of characteristic p. Then the group ring $K[G]$ is semisimple if and only if $p \nmid |G|$.*

Theorem 1.1.6 (Theorem 3.4.9 [60])**.** *Let G be a finite group and let K be a field such that* $\mathrm{char}(K) \nmid |G|$. *Then:*

1. *$K[G]$ is a direct sum of a finite number of two-sided ideals $\{B_i\}_{1\leq i\leq r}$, the simple components of $K[G]$. Each B_i is a simple ring.*

2. *Any two-sided ideal of $K[G]$ is a direct sum of some of the members of the family $\{B_i\}_{1\leq i\leq r}$*

3. *Each simple component B_i is isomorphic to a full matrix ring of the form $M_{n_i}(D_i)$, where D_i is a division ring containing an isomorphic copy of K in its centre, and the isomorphism*

$$K[G] \overset{\phi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i)$$

is an isomorphism of K -algebras.

4. *In each matrix ring $M_{n_i}(D_i)$, the set*

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ & & \dots & \\ x_{n_i} & 0 & \dots & 0 \end{bmatrix} : x_1, x_2, \dots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

is a minimal left ideal. Given $x \in K[G]$, we consider $\phi(x) = (\alpha_1, \dots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ and define the product of x by an element $m_i \in I_i$ by $xm_i = \alpha_i m_i$ With this definition, I_i becomes a simple $K[G]$-module.

5. *$I_i \neq I_j$ if $i \neq j$*

6. *Any simple $K[G]$-module is isomorphic to some $I_i, 1 \leq i \leq r$*

Corollary 1.1.3. *Let G be a finite group and let K be an algebraically closed field such that* $\mathrm{char}(K) \nmid |G|$. *Then:*

$$K[G] \simeq \oplus_{i=1}^{r} M_{n_i}(K)$$

and $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$

Proof. Since $\mathrm{char}(K) \nmid |G|$, we have that

$$K[G] \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$$

where D_i is a division ring containing a copy of K in its centre. If we compute dimensions over K on both sides of the equation above, we have that

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K]$$

and it follows that each division ring is finite-dimensional over K. As K is algebraically closed, we have that $D_i = K, 1 \leq i \leq r$, and the result follows. ∎

1.2 Module over group rings

Let M be an $R[G]$-module. In this section we present some relevant facts about $R[G]$-module.

Proposition 1.2.1. *Let M be an $R[G]$-module, assume that G is a finite group of order invertible in R and R is semisimple then M is a semisimple $R[G]$-module.*

Proof. It follows from Theorem 1.1.5 and the fact that every module over a semisimple ring is semisimple. ∎

Lemma 1.2.1. *Let G be a finite abelian group and H a normal subgroup of G. Let M be an $R[G]$-module, then M^H is an $R[G/H]$-module. Assume that $R[G]$ is Noetherian and M is finitely generated $R[G]$-module then M^H is finitely generated $R[G/H]$-module.*

Proof. Since G is an abelian group then M^H is a sub-$R[G]$-module of M, as $R[G]$ is Noetherian, then M^H is a finitely generated $R[G]$-module invariant by the action of H, hence M^H is a finitely generated $R[G/H]$-module. ∎

Lemma 1.2.2. *Let G be a finite group and M a finitely generated $R[G]$-module. The action of G on M is trivial if and only if $M^H = M$ for all cyclic subgroups H of G.*

Proof. Straightforward. Indeed, Every $\sigma \in G$ generate a cyclic group.

Proposition 1.2.2. *Let M be an $R[G]$-module and H a normal subgroup of G then M/M^H and M^H are $R[G]$-modules. If M is a finitely generated $R[G]$-module then M/M^H is a finitely generated $R[G]$-module. In particular if $R[G]$ is Noetherian and M is a finitely generated $R[G]$-module then M/M^H and M^H are finitely generated $R[G]$-modules.*

Proof. As H is a normal subgroup of G, then M^H is invariant by the action of G, hence it's an $R[G]$-module. If $R[G]$ is Noetherian and M is a finitely generated $R[G]$-module then we apply Lemma 1.2.1. ∎

Theorem 1.2.1 (Theorem 5.3 [51].)**.** *Let R be a ring, G a group, and M an $R[G]$-module. Suppose that H is a normal subgroup of G having finite index. If M is a Noetherian $R[G]$-module, then M is a Noetherian $R[H]$-module.*

Proposition 1.2.3 (Corollary 5.6 [51])**.** *Let R be a ring, G a group, and H a normal subgroup of G of finite index. If M is a semisimple $R[G]$-module, then M is a semisimple $R[H]$-module.*

Let N be an $R[G]$-module and $Hom_R(M,N)$ denote the group homomorphism from M to N, we note that $Hom_R(M,N)$ is an $R[G]$-module. The following Lemma gives the fixed ring of $Hom_R(M,N)$ by G.

Lemma 1.2.3. *Let M and N be two $R[G]$-modules. Then $Inv_G(Hom_R(M,N)) = Hom_{R[G]}(M,N)$.*

Proof. See [28] page 82. ∎

1.3 Character of a $K[G]$-module

Let M be a finitely generated $K[G]$-module. Hence M is a K-vector space of finite dimension. For all $\sigma \in G$ define the linear endomorphism:

$$\begin{aligned} f_\sigma : M &\to M \\ x &\mapsto \sigma.x \end{aligned}$$

We note that $\forall \sigma, \tau \in G$ we get $f_\sigma \circ f_\tau = f_{\sigma\tau}$, then:

$$\begin{aligned} f : G &\to Aut_K(M) \\ \sigma &\mapsto f_\sigma \end{aligned}$$

is a group homomorphism. A character of M denoted by χ_M is the function defined by:

$$\begin{aligned} \chi_M : G &\to K \\ \sigma &\mapsto \chi_M(\sigma) = Tr(f_\sigma) \end{aligned}$$

A character χ_M is said to be irreducible if M is a simple $K[G]$-module, and the dimension of χ_M denote by $dim_K\chi$ is the dimension of M as a K-vector space, and we have the following Lemma.

Lemma 1.3.1. *Let M, N be two finitely generated $K[G]$-module then:*

1. *If $M \simeq N$ then $\chi_M = \chi_N$.*
2. *$\chi_{M\oplus N} = \chi_M + \chi_N$ and $\chi_{M\otimes N} = \chi_M\chi_N$.*

Proof. See Proposition 1.3 [66].

Lemma 1.3.2. *Let H be a normal subgroup of G, then $K[G/H]$ is a finitely generated $K[G]$-module with character 1_H^G then:*

$$1_H^G = \begin{cases} |G/H| & \text{if } \sigma \in H \\ 0 & \text{if not.} \end{cases} \tag{1.1}$$

Remark 1.3.1. *Let M be a finitely generated $K[G]$-module of character χ_M, then χ_M can be extended by linearity to $K[G]$, hence if $v = \sum_{\sigma\in G} a_\sigma\sigma \in K[G]$ then $\chi_M(v) = \sum_{\sigma\in G} a_\sigma\chi_M(\sigma)$. Let $v \in K[G]$, set*

$$\begin{aligned} f_v : M &\to M \\ x &\mapsto v.x \end{aligned}$$

f_v is an endomorphism of the K-vector space M and $f_v = \sum_{\sigma\in G} a_\sigma f_\sigma$ for $v = \sum_{\sigma\in G} a_\sigma\sigma$, one can easily see that:

$$\chi_M(v) = Tr(f_v).$$

Lemma 1.3.3. *Let L be a finite extension of K. Let N be an $L[G]$-module with character χ_N. Let N_K be the $K[G]$-module defined by considering the natural structure of K-vector space of N, and denote by χ_{N_K} its character. Then*

$$\chi_{N_K} = \mathrm{Tr}_{L/K} \cdot \chi_N$$

Proof. By the transitivity of trace map. See Corollary of Lemma 1 [7] page 114.

1.3.1 Character of an abelian group

Let G be a finite abelian group of order n and L a field containing all n-th roots of unity, which constitute the group μ_n, a character of G is an homomorphism of G in L. We denote by $\widehat{G}$ be the set of character of G, for $\chi \in \widehat{G}$, $\sigma \in G$. We have that $\chi(\sigma)$ is a n-th root of unity. Then $\chi(G) \subseteq \mu_n$ and one may identify $\widehat{G}$ with $Hom(G, \mu_n)$ or to $Hom(G, \mathbb{Q}/\mathbb{Z})$.

Proposition 1.3.1. *Let G, G_1 and G_2 be abelian groups such that the sequence $1 \to G_1 \to G \to G_2 \to 1$ is exact, then $1 \to \widehat{G}_2 \to \widehat{G} \to \widehat{G}_1 \to 1$ is an exact sequence.*

Proof. Indeed, the functor $Hom(\cdot, \mathbb{Q}/\mathbb{Z})$ is an exact contravariant functor since $\mathbb{Q}/\mathbb{Z}$ is a divisible group, thus injective. ∎

Proposition 1.3.2. *Let G_1, G_2 be two finite abelian groups. Then:*

$$\widehat{G_1 \times G_2} \simeq \widehat{G}_1 \times \widehat{G}_2.$$

Proof. Let χ be a character on $G_1 \times G_2$ and let $t_i (i = 1, 2)$ be the injections defined by:

$$\begin{aligned} t_1 : G_1 &\to G_1 \times G_2 \\ \chi &\mapsto (\chi, 1) \end{aligned}$$

and

$$\begin{aligned} t_2 : G_2 &\to G_1 \times G_2 \\ \chi &\mapsto (1, \chi) \end{aligned}$$

Therefore we get the following map:

$$\begin{aligned} \psi : \widehat{G_1 \times G_2} &\to \widehat{G_1} \times \widehat{G_2} \\ \chi &\mapsto (\chi \circ t_1, \chi \circ t_2) \end{aligned}$$

One may check that ψ is a group homomorphism with trivial kernel, and since $|G| = |\widehat{G}|$ then ψ is an isomorphism. ∎

Proposition 1.3.3. *Let G be an abelian, then we have the following assertions:*

1. $\widehat{G} \simeq G$.
2. $\widehat{\widehat{G}} \simeq G$ *canonically.*

Proof.

1. Since G is direct product of cyclic group and by Proposition 1.3.2, it suffices to show that this holds for a cyclic group. Assume that $G =< \sigma >$, then $\chi \in \widehat{G}$ is completely determined by $\chi(\sigma)$, seeing that $\chi(\sigma)$ is n-th root of unity, then $\chi(\sigma)$ and χ have equal orders, thus $\widehat{G} \simeq G$.

2. For $g \in G$, consider

$$\begin{aligned} \hat{g} : \widehat{G} &\to L \\ \chi &\mapsto \chi(g) \end{aligned}$$

it's obvious that $\hat{g} \in \widehat{\widehat{G}}$ then the map :

$$\begin{aligned} \widetilde{g} : G &\to \widehat{\widehat{G}} \\ g &\mapsto \hat{g} \end{aligned}$$

is an injective homomorphism. Since $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$. Then $\widetilde{g}$ is an isomorphism.

∎

Proposition 1.3.4. *Let H be a subgroup of the abelian group G. Then any character of H can be extended to a character of G in $[G : H]$ ways.*

Proof. Indeed the sequence $1 \to \widehat{G/H} \to \widehat{G} \xrightarrow{\widehat{j}} \widehat{H}_1 \to 1$ is exact, for $\chi \in \widehat{H}$ there is ϕ in $\widehat{G}$ such that $\widehat{j}(\phi) = \chi$, hence the extensions of ϕ are $\phi\psi$ such that $\psi \in Ker(\widehat{j})$, since $|Ker(\widehat{j})| = [G : H]$, thus χ can be extended to a character of G in $[G : H]$ ways. ∎

Let H be a subgroup of G put $H^{\perp} = \{\chi \in \widehat{G} \mid H \subseteq Ker\chi\}$, we recall the following results.

Proposition 1.3.5. *Let H, H' be two subgroups of G, then the following statements hold:*

1. $\widehat{H} \simeq \widehat{G}/H^{\perp}$.
2. $(H^{\perp})^{\perp} = H$, *therefore* $H' \subseteq H \Leftrightarrow H^{\perp} \subseteq H'^{\perp}$.
3. $(\widehat{G/H}) \simeq H^{\perp}$.

Proof. See Proposition 3.3 and Proposition 3.4 [72]. ∎

Proposition 1.3.6. *Let G be an abelian group such that $G = G_1G_2$ and assume that $G_1 \cap G_2 = \{e\}$, then:*

$$\widehat{G} = G_1^{\perp}G_2^{\perp}$$

Proof. We see that $G_1^{\perp}G_2^{\perp} \subseteq G$. As $\widehat{G} \simeq \widehat{G_1} \times \widehat{G_2}$ (Proposition 1.3.2), then $|\widehat{G}| = |\widehat{G_1}||\widehat{G_2}| = |G_1^{\perp}||G_2^{\perp}|$, on the other side we have that $G_1^{\perp} \cap G_2^{\perp} = \{e\}$, this yields $\widehat{G} = G_1^{\perp}G_2^{\perp}$ ∎

1.3.2 Conjugated characters

Let G be an abelian finite group of order n, let $\Gamma_n = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. For $\chi \in \widehat{G}$, $\sigma \in G$, it is obvious that $\sigma \circ \chi \in \widehat{G}$. Hence two characters χ and ψ are said to be conjugate if there exist $\sigma \in \Gamma_n$ such that $\psi = \sigma \circ \chi$, then:

$$\begin{aligned} \Gamma_n \times \widehat{G} &\to \widehat{G} \\ (\sigma,\, \chi) &\mapsto \sigma \circ \chi. \end{aligned}$$

is a group action which induces an equivalence relation, and the orbits are the equivalence classes under this relation, those orbits are called conjugacy classes of $\widehat{G}$.

Proposition 1.3.7. *Let χ, $\chi' \in \widehat{G}$, then the following assumptions are equivalent:*

1. *χ and χ' are conjugate.*
2. $Ker\chi = Ker\chi'$.

3. $<\chi>=<\chi'>$*, where* $<\chi>$ *is the subgroup of* $\widehat{G}$ *generated by* χ*.*

Proof. See [16].

1.4 Idempotents

Definition 1.4.1. *Let* R *be a ring. An element* $e \in R$ *is an idempotent if* $e^2 = e$*. A non-zero idempotent* e *is primitive if, whenever* $e = e_1 + e_2$ *is an expression of* e *as a sum of idempotents such that* $e_1e_2 = 0$*, either* $e_1 = 0$ *or* $e_2 = 0$*.*

Proposition 1.4.1. *Let* R *be a ring and* e *a non-zero idempotent such that* $Re = I_1 \oplus I_2 \oplus \cdots \oplus I_r$*, where the* I_i *are non-zero left ideal, then* $e = e_1 + e_2 + \cdots + e_r$ *is the sum of pairwise orthogonal idempotents and* $I_i = Re_i$*. Conversely if* $e_1, e_2, \cdots, e_n$ *are pairwise orthogonal idempotents then* $e = e_1 + e_2 + \cdots + e_r$ *is an idempotent and* $Re = \bigoplus_{i=1}^{r} Re_i$*.*

Proof. We have that $e \in Re$, then $e = e_1 + e_2 + \cdots + e_r$ with $e_i \in I_i$. Since $e_i \in Re$ then $e_i = te$ hence $e_ie = te^2 = te = e_i$. Seeing that $e = e^2 = ee_1 + ee_2 + \cdots + ee_r$ and from the uniqueness of summands of e one gets $ee_i = e_i$. On the other hand $e_i = e_ie = \sum_{j=1}^{n} e_ie_j$, since $e_ie_j \in I_j$ then $e_i - e_i^2 \in \oplus_{i \neq j} I_i$, therefore $e_i - e_i^2 = 0$ and $\sum_{i \neq j} e_ie_j = 0$, which means that $e_ie_j = 0$ for $i \neq j$. finally we obtain $e_ie_j = e_je_i = \delta_{ij}e_i$ and $\{e_1, e_2, \cdots, e_r\}$ is an orthogonal system of idempotents. For the seconde assertion, let $x \in I_i \subseteq Re$ then $x = xe = \sum_{j=1}^{r} xe_j$. Since $xe_j \in I_j$ and by the uniqueness of the summands of x, it follows that $x = xe_i$. Consequently $x \in Re_i$. Thus $I_i = Re_i$.

Conversely, If $e = e_1 + e_2 + \cdots + e_r$ with $e_1, e_2, \cdots, e_r$ are pairwise orthogonal idempotent, then $e^2 = \sum_{i,j=1}^{r} e_ie_j = \sum_{i=1}^{r} e_i^2 = \sum_{i=1}^{r} e_i = e$. Moreover, if $x \in R$ then $xe = \sum_{i=1}^{r} xe_i$ then $Re \subseteq \sum_{i=1}^{r} Re_i$, on the other hand $e_ie_j = e_i$, then $e_i \in Re$, hence $Re_i \subseteq Re$ thus $\sum_{i=1}^{n} Re_i \subseteq Re$ and consequently $\sum_{i=1}^{n} Re_i = Re$. It remains to verify that $\sum_{i=1}^{n} Re_i$ is a direct sum. If $\sum_{j=1}^{r} x_ie_i = 0$ the $0 = 0.e_j = (\sum_{i=1}^{n} x_ie_i)\, e_j = x_je_j$ then $x_ie_i = 0$ for $1 \leq i \leq r$, as desired. ∎

Definition 1.4.2. *Let* $S = \{e_1, e_2, \cdots, e_r\}$*, then* S *is called a complete system of primitive idempotents if* $e_1, e_2, \cdots, e_r$ *are primitive central pairwise orthogonal idempotent and* $1 = \sum_{i=1}^{r} e_i$*.*

Proposition 1.4.2. *If the ring* R *is semisimple, then* R *has only one complete system of primitive idempotents.*

Proof. See Lemma 7.3 page 21 [28]. ∎

Corollary 1.4.1. *Let* R *be a semisimple ring and* G *is a finite group of order invertible in* R *then* $R[G]$ *has only one complete system of primitive idempotents.*

Proof. This follows from Theorem 1.1.5.

Lemma 1.4.1. *Let e_1 and e_2 be two idempotents of R.*

1. *If e_2 is central and e_1 is primitive, then $e_1e_2 = e_1$ or $e_1e_2 = 0$.*

2. *If $e_1 \neq e_2$, and e_i is primitive central then $e_1e_2 = 0$.*

Lemma 1.4.2. *Let R be a ring and $f \in End(R)$, then the image of an idempotent is an idempotent, if two idempotents e_1, e_2 are orthogonal then $f(e_1), f(e_2)$ are orthogonal. If f is an automorphism then the image of a primitive (respectively central) idempotent is primitive (respectively central) idempotent.*

Proof. It's clear that if e is an idempotent of R then $(f(e))^2 = f(e^2) = f(e)$, and if two idempotents e_1, e_2 are orthogonal then $f(e_1)f(e_2) = 0$. ∎

Theorem 1.4.1. *Assume that R has a complete system of primitive central idempotent $S = \{e_1, e_2, \cdots, e_r\}$, then every automorphism σ of R permute the elements of S. Let Δ be a finite subgroup of the group of automorphisms of R. If $\Omega_1, \Omega_2, \cdots, \Omega_s$ are the orbits corresponding to the action of Δ over S then $\widetilde{e}_i = \sum_{e_j \in \Omega_i} e_j \in R^\Delta$ and $\{\widetilde{e}_1, \widetilde{e}_1, \cdots, \widetilde{e}_s\}$ are the central orthogonal idempotents of $R^\Delta \cap Z(R)$.*

Proof. The first assertion follows from Lemma 1.4.2. For the seconde, let e be an idempotent of R^Δ then $e \in R$ and hence it's a finite sum of elements of S *i.e*, $e = \sum_{i=1}^{t} e_i$, since e is fixed by Δ then $e = \sum_{i=1}^{t'} \widetilde{e}_i$. ∎

The following Lemma asserts that every subgroup can be associated to an idempotent.

Lemma 1.4.3. *Let R be a ring with unity and let H be a subgroup of a group G. If $|H|$ is invertible in R, then $e_H = \frac{1}{|H|}\widetilde{H}$ is an idempotent of $R[G]$ (idempotent norm). Moreover, if $H \triangleleft G$ then e_H is central.*

Proof. First, we prove that e_H is an idempotent. So we consider the product:

$$\begin{aligned} e_H e_H &= \frac{1}{|H|^2}\widetilde{H}\widetilde{H} = \frac{1}{|H|^2}\left(\sum_{h\in H} h\right)\widetilde{H} = \frac{1}{|H|^2}\sum_{h\in H}(h\widetilde{H}) \\ &= \frac{1}{|H|^2}\sum_{h\in H}\widetilde{H} = \frac{1}{|H|^2}|H|\widetilde{H} = e_H \end{aligned}$$

We claim that if $H \triangleleft G$ then $\widetilde{H}$ is central, for any $g \in G$ we have that $g^{-1}Hg = H$; therefore $g^{-1}\widetilde{H}g = \sum_{x\in H} g^{-1}xg = \sum_{x\in H} x = \widetilde{H}$. Thus, $\widetilde{H}g = g\widetilde{H}$, for all $g \in G$ which shows that $\widetilde{H}$ is central in G. Consequently, $R[G] \cdot \widetilde{H} = \widetilde{H} \cdot R[G]$ and the result follows. So the centrality of e_H follows immediately. ∎

Let G be a finite abelian group of order n and K be a field such that $Char(K) \nmid n$. The set of irreducible character of G over K is given by $\mathcal{X}_K(G) = \{\chi_M \mid M \text{ is a simple } K[G]\text{-module}\}$, In particular if $K = \mathbb{C}$ or a field which contains μ_n the group of n-th roots of unity then $\mathcal{X}_{\mathbb{C}}(G) = \widehat{G}$. Let $\chi \in \widehat{G}$ be a character of order m and let $K_\chi = K(\chi(G)) = K(\zeta_m)$ and let $H = Gal(K_\chi/K)$, then characters which are conjugate to χ over K are given by $\sigma \circ \chi$ for $\sigma \in H$, henceforth the set of irreducible character of G over K can be seen as

$$\mathcal{X}_K(G) = \{Tr_{K_\chi/K}(\chi) \mid \chi \in \widehat{G}\}. \tag{1.2}$$

For more details about this one can refer for example to [41] V5.15.

The following Theorem asserts that the idempotents of a group algebra is completely determined by the characters of G.

Theorem 1.4.2. *Let K be a field of characteristic 0 and G a finite abelian group of order n. Then, the primitive idempotents of $K[G]$ are given by*

$$e_\chi = \frac{dim_K \chi}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

where $\chi \in \mathcal{X}_K(G)$. In particular, if K is algebraically closed or contain all n-th roots of unity. Then, the primitive idempotents of $K[G]$ are given by

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

where $\chi \in \widehat{G}$.

Proof. See Theorem 5.1.11 [60] ∎

Remark 1.4.1. *Let K be a field of characteristic 0 and G a finite abelian group. According to Theorem 1.4.1 and 1.2 the primitive idempotents can be expressed as:*

$$e_\chi = \sum_{\sigma \in H} e_{\sigma \circ \chi} \in K[G]. \tag{1.3}$$

where $\chi \in \widehat{G}$ and $H = Gal(K_\chi/K)$.

The next lemma expresses how the idempotents behave when we change to a subgroup or a factor group of G, as in Theorem 1.4.2 we denoted by e_χ the idempotent associated to the character χ, if there are more then group, we denote the idempotent associated to χ by $e_{\chi,G}$.

Lemma 1.4.4. *Let $\pi : K[G] \to K[G/H]$ be the K-linear map induced by the canonical projection.*

1. *For $\bar{\psi} = \psi H^{\perp} \in \widehat{H} \simeq \widehat{G}/H^{\perp}$, then $e_{\bar{\psi},H} = \sum_{\chi \in H^{\perp}} e_{\psi\chi,G} \in K[H]$.*
2. *For $\psi \in \widehat{G} \backslash H^{\perp}$ we have $\pi\left(e_{\psi,G}\right) = 0$.*
3. *For $\psi \in H^{\perp}$ we have $e_{\psi,G} = \frac{1}{|G|} \sum_{i \in I} \psi\left(\rho_i^{-1}\right) \rho_i \sum_{\gamma \in H} \gamma$ and $\pi\left(e_{\psi,G}\right) = e_{\psi,G/H}$, where $\{\rho_i \mid i \in I\} \subset G$ is a set of representatives for G/H.*

Proof. It suffice to show 1. For more details see [9].

1. Let $1 \in \{\rho_i \mid i \in I\} \subset G$ be a set of representatives for G/H. Then we obtain

$$\begin{aligned}
\sum_{\chi \in H^{\perp}} e_{\psi\chi,G} &= \frac{1}{|G|} \sum_{\gamma \in H} \sum_{i \in I} \sum_{\chi \in H^{\perp}} \psi\left(\rho_i \gamma\right)^{-1} \chi\left(\rho_i \gamma\right)^{-1} \rho_i \gamma \\
&= \frac{1}{|G|} \sum_{\gamma \in H} \psi(\gamma)^{-1} \gamma \sum_{i \in I} \psi\left(\rho_i\right)^{-1} \rho_i \sum_{\chi \in H^{\perp}} \chi\left(\rho_i\right)^{-1} \\
&= \frac{1}{|G|} \sum_{\gamma \in H} \psi(\gamma)^{-1} \gamma \psi(1)^{-1} |G/H| \\
&= \frac{1}{|H|} \sum_{\gamma \in H} \psi(\gamma)^{-1} \gamma \\
&= e_{\bar{\psi},H}
\end{aligned}$$

∎

Lemma 1.4.5. *Let G be a finite abelian group, $\chi \in \widehat{G}$ and $H = \ker(\chi)$, let $\{\sigma_1, \sigma_2, \cdots, \sigma_r\} \subset G$ be a set of representatives for G/H, then:*

$$e_{\chi} = \frac{e_H}{[G : H]} \sum_{i=1}^{r} \chi(\sigma_i^{-1}) \sigma_i$$

Proof. We have that $e_{\chi} = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1}) \sigma$, expressing G as union $G = \cup_{1 \leq i \leq r} \sigma_i H$. Hence

$$e_{\chi} = \frac{1}{|G|} \sum_{\substack{\tau \in H \\ 1 \leq i \leq r}} \chi((\sigma_i \tau)^{-1}) \sigma_i \tau.$$

since $\chi((\sigma_i\tau)^{-1}) = \chi(\tau^{-1}\sigma_i^{-1}) = \chi(\tau^{-1})\chi(\sigma_i^{-1}) = \chi(\sigma_i^{-1})$ the last equality follows from $\tau \in H =$

$\ker(\chi)$, using this we get

$$\begin{aligned} e_\chi &= \frac{1}{|G|}\left(\sum_{i=1}^{r}\chi(\sigma_i^{-1})\sigma_i\right)\left(\sum_{\tau\in H}\tau\right) \\ &= \frac{1}{|G|}\widetilde{H}\left(\sum_{i=1}^{r}\chi(\sigma_i^{-1})\sigma_i\right) \\ &= \frac{1}{[G:H]}\frac{\widetilde{H}}{|H|}\left(\sum_{i=1}^{r}\chi(\sigma_i^{-1})\sigma_i\right) \\ &= \frac{e_H}{[G:H]}\sum_{i=1}^{r}\chi(\sigma_i^{-1})\sigma_i. \end{aligned}$$

∎

Lemma 1.4.6. *Let K be a field of characteristic 0, G a finite abelian group and $\chi \in \widehat{G}$, then for all $U \in K[G]e_\chi$ there is a unique $P \in K_d[X]$ (i.e. $P \in K[X]$ and $deg(p) < d$) such that $d = |G/Ker(\chi)| = |\overline{\sigma}|$, then:*

$$U = P(\sigma)e_\chi$$

Proof. In fact it follows from the following isomorphism:

$$\begin{aligned} \widetilde{\chi} : K[G]e_\chi &\to K(\zeta_d) \\ ue_\chi &\mapsto \chi(u) \end{aligned}$$

∎

Corollary 1.4.2. *Let G be a finite abelian group, $\chi \in \widehat{G}$ and $H = \ker(\chi)$. Let $G/H = \{\sigma_1 H, \sigma_2 H, \cdots, \sigma_r H\}$, suppose that $H \triangleleft G$. Then*

$$e_\chi = e_H \cdot e_{\overline{\chi}}$$

where

$$\begin{aligned} \overline{\chi} : G/H &\to \mathbb{Q}(\zeta_n) \\ \sigma H &\mapsto \chi(\sigma) \end{aligned}$$

Proof. This follows from Lemma 1.4.5. ∎

Next lemma describes a special behaviour of the idempotents for cyclic Kummer extensions. Assume that $\zeta_n \in K$ and let $L = K(\alpha)$ be a finite extension of K of finite degree n and $\alpha^n = a \in K$.

Denote the (cyclic) Galois group of L/K by Γ. The Kummer character $\chi_a \in \widehat{\Gamma}$ belonging to a is defined by:

$$\begin{aligned} \chi_a :&\Gamma \to \mu_n \\ &\gamma \mapsto \frac{\gamma(\alpha)}{\alpha} \end{aligned}$$

and $\widehat{\Gamma} = \langle \chi_a \rangle$ is generated by χ_a.

Lemma 1.4.7. *For $\psi \in \Gamma^*$ we have $e_{\psi,\Gamma} \cdot \alpha = \begin{cases} \alpha & \text{if } \psi = \chi_a \\ 0 & \text{if } \psi \neq \chi_a \end{cases}$*

Proof. Let $\psi = \chi_a^r$ with $1 \leq r \leq n$. Then

$$e_{\psi,r}\alpha = \frac{1}{n}\sum_{\gamma\in\Gamma} \chi_a(\gamma)^{-r}\gamma(\alpha) = \frac{\alpha^r}{n}\sum_{\gamma\in\Gamma} \gamma\left(\alpha^{1-r}\right) = \begin{cases} \alpha & \text{for } r = 1 \\ 0 & \text{for } 2 \leq r \leq n \end{cases}$$

∎

1.5 Orders And Maximal Order

1.5.1 Orders

Let R be a Noetherian integral domain with quotient field K and V a finite dimensional K space. An *R-lattice* in V is a finitely generated R submodule M in V such that $K.M = V$, where:

$$K.M = \left\{ \sum a_i m_i \mid a_i \in K,\, m_i \in M \right\}.$$

Let S be a finite dimensional K-algebra, then an *R-order* in the K-algebra S is a subring $\mathcal{S}$ of S having the same unity element as S and such that $\mathcal{S}$ is an R-lattice in S.

Examples 1.5.1. *Let R be a dedekind ring with fraction fields K. Here we give some examples of orders.*

1. *Let L/K be a finite extension of number fields, with ring of integers $\mathcal{O}_L$ and R then, $\mathcal{O}_L$ is an R-order in L.*
2. *Let $S = \mathcal{M}_n(K)$ the algebra of square matrices with entries in K, then $\mathcal{S} = \mathcal{M}_n(R)$ is an R-order in S.*
3. *Let a be an element of S integral over R, then $R[a]$ is an R-order in the K-algebra $K[a]$.*

Lemma 1.5.1. *For two R-lattices M and N in V. Then there exists a nonzero $t \in R$ such that $t.N \subseteq M$.*

Proof. M is an R-lattice then it contains a K-basis for V and for each element $x \in M$ one can find a nonzero $t_x \in R$ such that $t_x.x \in M$. Since N is finitely generated as an R-module, say by $x_1; \ldots; x_n$, therefore $t = t_{x_1} \ldots t_{x_n}$ is the desired element. ∎

Definition 1.5.1. *Let M be any R-lattice in V, then we define the order of M in V as:*

$$\mathbf{O}(M, V) = \{x \in V \mid x.M \subseteq M\}$$

Proposition 1.5.1. *Let M be an R-lattice in S, then $\mathbf{O}(M, S)$ is an R order in S.*

Proof. Its clear that $\mathbf{O}(M, S)$ is a subring of S, and $\mathbf{O}(M, S)$. We verify that $\mathbf{O}(M, S)$ is a R-lattice in S. Let $y \in A$, then yM is an R -lattice in the K-vector subspace yS of S. since $M \cap yS$ is an R-lattice in yS, by Lemma 1.5.1 there is $r \in R$ such that $r \cdot yM \subseteq M \cap yS \subseteq M$ hence $ry \in \mathbf{O}(M, S)$, which gives $K \cdot \mathbf{O}(M, S) = S$. Next, there is a nonzero $s \in R$ such that $s \cdot 1_S \in M$. Therefore $\mathcal{S} \cdot (s \cdot 1_S) \subseteq M$, whence $\mathcal{S} \subseteq s^{-1}M$. Since R is Noetherian and $s^{-1}M$ is an R-lattice, this implies that $\mathbf{O}(M, S)$ is finitely generated as an R-module. Therefore $\mathbf{O}(M, S)$ is an R-order in S. ∎

1.5.2 Maximal Orders

Definition 1.5.2. *Let R be a Noetherian integral domain with quotient field K and assume $R \neq K$. Let S be a finite-dimensional K-algebra. Let $\mathcal{S}$ be an R-order in S. We say that $\mathcal{S}$ is maximal if $\mathcal{S}$ is maximal with respect to inclusion.*

Theorem 1.5.1. *Let R be a Dedekind ring with quotient field K, and let R' be an integral domain such that $R \subseteq R' \subseteq K$. Then:*

1. *Every R'-lattice M' contains an R-lattice M such that $M' = R'M$*
2. *Every R'-order $\mathcal{S}'$ (in a finite dimensional K-algebra A) contains an R -order $\mathcal{S}$ in A, such that $\mathcal{S}' = R'\mathcal{S}$.*
3. *Let $\mathcal{S}' = R'\mathcal{S}$, as in (ii). Then every left $\mathcal{S}'$-lattice M' contains a left $\mathcal{S}$-lattice M such that $M' = \mathcal{S}'M = R'M$.*

Proof. See Theorem (8.8) [61].

Corollary 1.5.1 ((10.4) Corollary.)**.** *Every R-order in S is contained in a maximal R-order in A. There exists at least one maximal R-order in A.*

Proof. Let $\mathcal{S}$ be an R-order in S, and let C be the collection of R-orders in S containing $\mathcal{S}$. Then C is non-empty. If $\{\mathcal{S}_i\}$ for $i \in I$ is a chain of orders containing $\mathcal{S}$, let

$$\mathcal{S}' = \sum_{i \in I} \mathcal{S}_i = \bigcup_{i \in I} \mathcal{S}_i$$

then $\mathcal{S}'$ is a subring of S containing R, and $K \cdot \mathcal{S}' = S$. Let $x \in \mathcal{S}'$ then x belongs to $\mathcal{S}_i$, hence is integral over R. It follows from Theorem (10.3) [61] that $\mathcal{S}'$ is an R -order in S. We have now shown that any increasing chain of elements of C has an upper bound in C. By Zorn's Lemma, C has a maximal element $\mathcal{S}_0$, which is then obviously a maximal R-order in S.

It remains to prove that S contains at least one maximal R-order. We know that there exists a full R-lattice M in S. Setting $\mathcal{S} = \mathbf{O}(M, S)$, hence $\mathcal{S}$ is contained in some maximal R-order $\mathcal{S}_0$ in S, by the first part of this proof and the corollary is established. ∎

As illustration of maximal order in group algebra we give the following proposition.

Proposition 1.5.2. *Let K be an arbitrary field and G a finite abelian group. Then maximal R-order of $K[G]$ is given by*

$$\mathcal{S}_{K[G]} = \oplus_{\chi \in \mathcal{X}_K(G)} R[G] \cdot e_\chi.$$

Proof. See remark after Theorem 8.6 [61] ∎

Let S is a separable K-algebra. Now we give a theorem that proves that a decomposition of S into simple components yields a corresponding decomposition of maximal orders.

Theorem 1.5.2. *Let S be a separable K-algebra with simple components $\{S_1, \cdots, S_r\}$, and let R_i be the integral closure of R in the center K_i of S_i. Then*

1. *For each maximal R-order $\mathcal{S}$ in S, we have $\mathcal{S} = \sum_{i=1}^{r} \mathcal{S}e_i$, where the $\{e_i\}$ are the central idempotents of A such that $A_i = Ae_i$. Further, each $\mathcal{S}e_i$ is a maximal R-order in S_i.*
2. *If $\mathcal{S}_i$ is a maximal R-order in S_i, $1 \leqslant i \leqslant r$, then $\sum_{i=1}^{r} \mathcal{S}_i$ is a maximal R-order in S.*
3. *An R-order $\mathcal{S}_i$ in S_i is a maximal R-order if and only if $\mathcal{S}_i$ is a maximal R_i-order.*

Proof. This is Theorem (10.5) of [61]. ∎

1.5.3 Maximal Orders in $K[G]$-module

Let R be a Dedekind ring, K its quotient field. Let G be a finite abelian group and $\Gamma = R[G]$ be the group ring of G over R. The Group algebra $K[G]$ has decomposition into simple component

as

$$K[G] = \oplus_{\chi \in G'} K[G] e_\chi$$

where G'_K is the set of representatives for the classes of characters which are conjugate over K, (note that if $\mu_n \subseteq K$ then $K[G] = \oplus_{\chi \in \widehat{G}} K[G] e_\chi$). The group algebra $K[G]$ contains a unique maximal R-order $\mathcal{S}$, which is the integral closure of R in $K[G]$, this is true because G is abelian. Applying (1) of Theorem 1.5.2 to the former decomposition of $K[G]$ we obtain

$$\mathcal{S} = \oplus_{\chi \in G'} \mathcal{S}_\chi$$

where $\mathcal{S}_\chi$ is the maximal order of $K[G]e_\chi$.

Lemma 1.5.2. *Let R be a Dedekind ring, K its quotient field. Let G be a finite abelian group of order n and $\chi \in \widehat{G}$ be of order m and $d = [K(\zeta_m) : K]$ such that ζ_m is a root of unity of order m.*

1. *Let $\sigma \in G$ with $\chi(\sigma) = \zeta_m$. Then*

$$\mathcal{S}_\chi = \left\{ \sum_{i=0}^{d-1} a_i \sigma^i e_\chi \;\mid\; a_i \in K \text{ such that } \sum_{i=0}^{d-1} a_i \zeta_m^i \in \mathcal{O}_{K(\zeta_m)} \right\}.$$

   In particular $\mathcal{S}_\chi = R[G]\, e_\chi$ if and only if $\mathcal{O}_{K(\zeta_m)} = R[\zeta_m]$.

2. *$\mathcal{O}_{K(\zeta_m)} = \mathcal{O}_K[\zeta_m]$ if and only if $\mathcal{O}_{K(\zeta_m)} = R \otimes_{\mathcal{O}_{K_m}} \mathbb{Z}[\zeta_m]$, where $K_m = K \cap \mathbb{Q}(\zeta_m)$. Thus $\mathcal{S} = \bigoplus_{\chi \in G'_K} R[G]\, e_\chi$ if and only if $\mathcal{O}_{K(\zeta_m)} = R \otimes_{\mathcal{O}_{K_m}} \mathbb{Z}[\zeta_m]$ holds for all $m \in \mathbb{N}$ with $m|n$.*

   In particular, this condition is fulfilled when K is a cyclotomic field.

Proof.

1. There exists a K-linear isomorphism $\varphi : K[G]\, e_\chi \to K(\zeta_m)$, with $\varphi(\sigma\, e_\chi) = \zeta_m$. Thus $\mathcal{S}_\chi = \varphi^{-1}\left(\mathcal{O}_{K(\zeta_m)}\right)$ is the maximal order of $K[G] \cdot e_\chi$, since $\mathcal{O}_{K(\zeta_m)}$ is the maximal order $K(\zeta_m)$, and all claims are obvious.

2. We have $\mathbb{Z}[\zeta_m] = \mathcal{O}_{K(\zeta_m)}[\zeta_m]$, which implies the first claim. The others are also easily verified.

. ∎

Lemma 1.5.3. *1. Let L/K be a finite field extension and $\mathcal{S} \subseteq L[G]$ be the maximal $\mathcal{O}_L$-order. Then $\mathcal{S} \cap K[G]$ is the maximal R-order of $K[G]$.*

2. Let $H \leq G$ be a subgroup, $\mathcal{S} \subseteq K[G]$ be the maximal R-order and $\pi : K[G] \to K[G/H]$ be induced by the projection. Then $\pi(\mathcal{S})$ is the maximal $\mathcal{O}$-order of $K[G/H]$.

Proof.

1. Immediate.
2. By lemma 1.4.4 2)3) either $\pi\left(e_{\chi,K[G]}\right) = 0$ or $\pi\left(e_{\chi,K[G]}\right) = e_{\chi,K[G/H]}$. Using lemma 1.5.2 1, the claim follows. ∎

Chapter 2

Galois module structure

2.1 Associated order

Definition 2.1.1. *Let L/K be a finite galois extension of number field of galois group $G = Gal(L/K)$. The associated order of the extension L/K is given by:*

$$\mathfrak{A}_{L/K} = \{x \in K[G] \mid x\mathcal{O}_L \subseteq \mathcal{O}_L\}$$

Proposition 2.1.1. *Let L/K be a finite galois extension of number field of galois group $G = Gal(L/K)$.*

1. *$R[G] \subseteq \mathfrak{A}_{L/K}$.*
2. *$\mathfrak{A}_{L/K}$ is an R-order in $K[G]$.*
3. *If $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ then it must be of rank 1 and there is an element $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$. such α generates a normal basis of L/K, i.e., $L = K[G].\alpha$.*

Proof.

1. Straightforward, since the conjugate of an integer is an integer
2. According to the normal basis theorem, L is isomorphic to $K[G]$ as $K[G]$-module. By this isomorphism one may identify $\mathcal{O}_L$ to an R-lattice M in $K[G]$. Accordingly, $\mathfrak{A}_{L/K} = \{x \in K[G] \mid xM \subseteq M\}$, then by Proposition 1.5.1 it is an R-order in $K[G]$.
3. If the rank exceed 1, then so is the rank of L over $K[G]$ which contradict the normal basis theorem.

∎

The next two lemmas will show how the associated orders of composite fields and of subfields can be determined under certain additional assumptions.

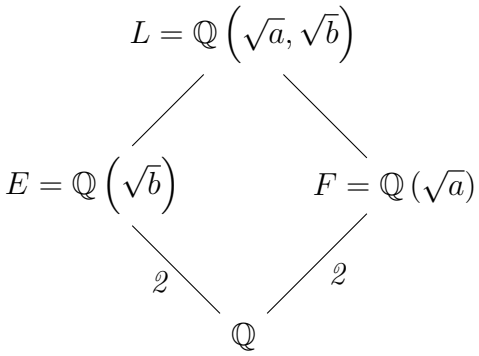
Lemma 2.1.1. *Let E and F be finite Galois extensions of a number field K. Let $L = EF$ and assume that E and F are arithmetically and linearly disjoint over K Then:*

1. *We have $\mathfrak{A}_{L/F} = \mathfrak{A}_{E/K} \otimes_R \mathcal{O}_F$ and $\mathfrak{A}_{L/K} = \mathfrak{A}_{E/K} \otimes_R \mathfrak{A}_{F/K}$.*
2. *If there exists some $\alpha_1 \in \mathcal{O}_E$ with $\mathcal{O}_E = \mathfrak{A}_{E/K} \cdot \alpha_1$, then $\mathcal{O}_L = \mathfrak{A}_{L/F} \cdot (\alpha_1 \otimes 1)$. If there also exists $\alpha_2 \in \mathcal{O}_F$ with $\mathcal{O}_F = \mathfrak{A}_{F/K} \cdot \alpha_2$, then $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot (\alpha_1 \otimes \alpha_2)$.*

Proof. This is Lemma 5 of [9]. ∎

We illustrate the forgoing Lemma by the following example:

Example 2.1.1. *Let a, b be two non-zero square free integers, set two arithmetically disjoint extensions E and F, and let L be their composite. For example, we may choose $b \equiv 2, 3$ [4] and $a \equiv 1$ [4]:*



Let $G = Gal(E/\mathbb{Q}) = \{1, \sigma\}$, we have

$$\mathfrak{A}_{E/\mathbb{Q}} = \mathbb{Z}\left(\frac{1+\sigma}{2}\right) \oplus \mathbb{Z}\left(\frac{1-\sigma}{2}\right).$$

And

$$\mathfrak{A}_{L/F} = \mathcal{O}_F\left(\frac{1+\sigma}{2}\right) \oplus \mathcal{O}_F\left(\frac{1-\sigma}{2}\right).$$

Therefore

$$\mathfrak{A}_{L/F} = \mathfrak{A}_{E/\mathbb{Q}} \otimes_{\mathbb{Z}} \mathcal{O}_F.$$

Lemma 2.1.2. *Let $L \supseteq F \supseteq K$ be a tower of algebraic number field. Assume that all the extensions are Galois and L/F is tamely ramified. Put $G = Gal(L/K)$ and $H = Gal(F/K)$ Let $\pi : K[G] \to K[H]$ denote the K-linear map induced by the projection $\pi : G \to H$. Suppose that $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$ with $\alpha \in \mathcal{O}_L$. Then $\mathfrak{A}_{F/K} = \pi\left(\mathfrak{A}_{L/K}\right)$ and $\mathcal{O}_F = \mathfrak{A}_{F/K} \cdot \alpha'$ with $\alpha' = Tr_{L/F}(\alpha)$.*

Proof. Since L/F is tamely ramified, according to Proposition 2.1.3 it follows that $Tr_{L/F}(\mathcal{O}_L) = \mathcal{O}_F$. Thus we get $\mathcal{O}_F = Tr_{L/F}(\mathfrak{A}_{L/K} \cdot \alpha) = \mathfrak{A}_{L/K} \cdot Tr_{L/F}(\alpha) = \pi\left(\mathfrak{A}_{L/K}\right) \cdot \alpha'$. ∎

Lemma 2.1.3. *Let L/K and E/F both be Galois extensions of number fields. Suppose that E and L are arithmetically disjoint over $\mathbb{Q}$ and that there exist $\alpha_1 \in \mathcal{O}_L$ such that $\mathfrak{A}_{L/K} \cdot \alpha_1 = \mathcal{O}_L$ and $\alpha_2 \in \mathcal{O}_E$ such that $\mathfrak{A}_{E/F} \cdot \alpha_2 = \mathcal{O}_E$. Then $\mathcal{O}_{EL} = \mathfrak{A}_{EL/FK} \cdot (\alpha_1 \otimes \alpha_2)$ and*

$$\mathfrak{A}_{EL/FK} = \left(\mathfrak{A}_{E/F} \otimes_{\mathcal{O}_F} \mathcal{O}_{FK}\right) \otimes_{\mathcal{O}_{FK}} \left(\mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_{FK}\right)$$

Proof. By Lemma 2.1.1 one see that $\mathfrak{A}_{FL/KF} = \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_{KF}$ and $\mathfrak{A}_{EK/KF} = \mathfrak{A}_{E/F} \otimes_{\mathcal{O}_F} \mathcal{O}_{KF}$, hence again by Lemma2.1.1 one gets $\mathfrak{A}_{EL/KF} = \left(\mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_{KF}\right) \otimes_{\mathcal{O}_{KF}} \left(\mathfrak{A}_{E/F} \otimes_{\mathcal{O}_F} \mathcal{O}_{KF}\right)$ ∎

2.1.1 Leopoldt and Hilbert-Speiser theorems

Proposition 2.1.2. *Let $L \supseteq F \supseteq K$ be a tower of algebraic number fields. Assume that all the extensions are Galois. If α generate a normal integral basis of L/K then $Tr_{L/F}(\alpha)$ generate a normal integral basis of F/K.*

Proof. Let $G = Gal(L/K)$, $H = Gal(L/F)$ and $\bar{G} = Gal(F/K) \cong G/H$ Let α be a normal basis generator of L over K and $x \in \mathcal{O}_F$, thus $x = \sum_{\sigma \in G} a_\sigma \sigma(\alpha)$ and $\tau(x) = x$ for every $\tau \in H$ Thus

$$\tau(x) = \sum_{\sigma \in G} a_\sigma \tau\sigma(\alpha) = \sum_{\sigma \in G} a_{\tau^{-1}\sigma} \sigma(\alpha)$$

By uniqueness of the a_σ, we deduce that $a_{\tau^{-1}\sigma} = a_\sigma$ for all $\sigma \in G$ and $\tau \in H$. For each $\theta \in \bar{G}$, fix a lift $\tilde{\theta} \in G$. Then

$$\begin{aligned} x &= \sum_{\sigma \in G} a_\sigma \sigma(\alpha) = \sum_{\theta \in \bar{G}} \sum_{\tau \in H} a_{\tau\tilde{\theta}} \tau\tilde{\theta}(\alpha) = \sum_{\theta \in \bar{G}} a_{\tilde{\theta}} \sum_{\tau \in H} \tau\tilde{\theta}(\alpha) \\ &= \sum_{\theta \in \bar{G}} a_{\tilde{\theta}} \tilde{\theta}\left(Tr_{L/F}(\alpha)\right) = \sum_{\theta \in \bar{G}} a_{\tilde{\theta}} \theta\left(Tr_{L/F}(\alpha)\right) \end{aligned}$$

where the penultimate equality uses that H is normal in G. ∎

Corollary 2.1.1. *If L has a normal integral basis over K then $Tr_{L/F}(\mathcal{O}_L) = \mathcal{O}_F$.*

Proof. Clearly, $Tr_{L/F}(\mathcal{O}_L) \subseteq \mathcal{O}_F$. Let $x \in \mathcal{O}_F$. From the equalities in the proof of Proposition 2.1.2 we have

$$x = \sum_{\theta \in \bar{G}} a_{\tilde{\theta}} \sum_{\tau \in H} \tau\tilde{\theta}(\alpha) = \sum_{\theta \in \bar{G}} a_{\tilde{\theta}} Tr_{L/F}(\tilde{\theta}(\alpha)) = Tr_{L/F}\left(\sum_{\theta \in \bar{G}} a_{\tilde{\theta}} \tilde{\theta}(\alpha)\right)$$

where the last equality uses that $Tr_{L/F}$ is F-linear. Since $\sum_{\theta\in\bar{G}} a_{\tilde{\theta}}\tilde{\theta}(\alpha) \in \mathcal{O}_L$ we now have $x \in Tr_{L/F}(\mathcal{O}_L)$. ∎

Theorem 2.1.1. *Let L be a finite Galois extension of number field K. Then $Tr_{L/K}(\mathcal{O}_L)$ is an ideal of R. Let $\mathfrak{p}$ be a maximal ideal of R, then $\mathfrak{p}$ divides $Tr_{L/K}(\mathcal{O}_L)$ if and only if $\mathfrak{p}$ is wildly ramified.*

Proof. This follows from Lemma 2 in section 5 of [29] and the fact that the extension of residue fields in question is separable. ∎

Proposition 2.1.3. *Let L be a finite Galois extension of a number field K. Then L/K is tamely ramified if and only if $Tr_{L/K}(\mathcal{O}_L) = R$.*

Proof. we have that $Tr_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_K$. Since L/K is tamely ramified then by Theorem 2.1.1, $Tr_{L/K}(\mathcal{O}_L)$ is an ideal of $\mathcal{O}_K$ is not divisible by any maximal ideal of $\mathcal{O}_K$, hence equal to $\mathcal{O}_K$. Conversely, if $Tr_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$, assume that L/K is wildly ramified and $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_L$ and by Theorem 2.1.1, $\mathfrak{p}$ divide $Tr_{L/K}(\mathcal{O}_L)$ then divide $\mathcal{O}_K$. Contradiction. ∎

Proposition 2.1.4. *Let L be a finite Galois extension of a number field K. If L/K has a normal integral basis then L is tamely ramified over K.*

Proof. Since L/K has a normal integral basis, then by Corollary 2.1.1 we obtain $Tr_{L/K}(\mathcal{O}_L) = R$. Using the equivalence from Proposition 2.1.3. Thus L/K is tamely ramified. ∎

Theorem 2.1.2. *Let m and n be two relatively prime numbers. Then*

$$\mathbb{Q}(\zeta_{m.n}) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n).$$

Proof. Indeed $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ lies in $\mathbb{Q}(\zeta_{nm})$, so there composite does too. conversely, a primitive root of unity of order mn can be obtained by multiplying suitable m-th and n-th roots of unity. Hence $\zeta_{mn} \in \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)$ which implies $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)$. Therefore $\mathbb{Q}(\zeta_{m.n}) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$. ∎

Theorem 2.1.3. *Let n be an odd number square free. Then $\mathbb{Q}(\zeta_n)$ has a normal integral basis generated by ζ_n.*

Proof. Let p be a prime number. First we note that $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{n-1}$ are the conjugate of ζ_p. We already know that $\mathbb{Z}[\zeta_p]$ is the ring of integers of $\mathbb{Q}[\zeta_p]$ and $1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{n-1}$ is an integral basis of $\mathbb{Z}[\zeta_p]$ and since ζ_p is invertible, which implies that $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{n-1}$ is a normal integral basis of $\mathbb{Q}(\zeta_p)$.

Now for two primes p, q we have that ζ_p and ζ_q generate a normal integral basis and since the extensions $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$ are arithmetically disjoint over $\mathbb{Q}$, then by Theorem 2.2.2 $\zeta_p\zeta_q$ generates a normal integral basis of $\mathbb{Q}(\zeta_{pq})$. However $\zeta_p\zeta_q$ is a primitive n-th root of unity, hence ζ_{pq} generates a normal integral basis of $\mathbb{Q}(\zeta_{pq})/\mathbb{Q}$. Hence the result follows. ∎

Lemma 2.1.4. *Let L be a finite abelian extension of $\mathbb{Q}$ of conductor n, then the following assertions are equivalent:*

1. *n is odd square free.*
2. *$L/\mathbb{Q}$ is tamely ramified.*
3. *The extension $L/\mathbb{Q}$ has a normal integral basis generated by $\alpha = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n)$.*

Proof.

- $1 \Rightarrow 2$ This is a consequence of Theorem 2.1.3 and Proposition 2.1.2.
- $2 \Rightarrow 3$ Follows from Proposition 2.1.4.
- $3 \Rightarrow 1$ Let p be an odd prime number dividing n, put $n = mp^r$ where p not dividing m. The prime p does not ramify in $\mathbb{Q}(\zeta_m)$ and in fact $N := K \cap \mathbb{Q}(\zeta_m)$ is the maximal subfield of K in which p is unramified. The field N is also the fixed field of the inertia group I_p of any prime of $\mathcal{O}_K$ above p, since $K/\mathbb{Q}$ is tamely ramified, then we have just shown that $p \nmid [K : N] = |I_p|$. Hence K is contained in the fixed field of the p-Sylow subgroup of $Gal(\mathbb{Q}(\zeta_n)/N)$. If $r > 1$ then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{pm})] = p^{r-1}$, so K is contained in $\mathbb{Q}(\zeta_{pm})$ and $p^2 \nmid n$. In the same way, one shows that n is odd (the inertia group of primes above 2 is a 2-group).

∎

Theorem 2.1.4 (Hilbert-Speiser Theorem)**.** *Let L be a finite abelian extension of the field of rational number $\mathbb{Q}$. Then $L/\mathbb{Q}$ has a normal integral basis if and only if $L/\mathbb{Q}$ is tamely ramified.*

Proof. Let n be the conductor of L, then by Proposition 2.1.2 and seeing that $\mathbb{Q}(\zeta_n)$ has a normal basis generated by ζ_n, thus $L/\mathbb{Q}$ has $Tr_{\mathbb{Q}(\zeta_n)/L}(\zeta_n)$ as normal basis generator. Hence by Lemma 2.1.4 the Theorem follows. ∎

Definition 2.1.2. *A number field K is said to be Hilbert-Speiser field if for every tamely ramified abelian extension L, then L/K has a relative normal integral basis.*

Theorem 2.1.5. *The field of rational number is the only Hilbert-Speiser field.*

Proof. This is the main Theorem of [37] ∎

Theorem 2.1.6 (Leopoldt Theorem [53]). *Let K be a finite abelian galois extension of the field of rational number $\mathbb{Q}$. Then R is a free $\mathfrak{A}_{K/\mathbb{Q}}$-module of rank 1 i.e. there is $\alpha \in R$ such that $R = \mathfrak{A}_{L/K} \cdot \alpha$, such α can be explicitly constructed.*

Proof. See [54] for a simplified proof. ∎

Proposition 2.1.5. *Let L/K be a finite abelian extension of a number field K and $G = Gal(L/K)$. If $\mathcal{O}_L$ is a free R-order over $\mathcal{S}$ in $K[G]$ then $\mathfrak{A}_{L/K} = \mathcal{S}$.*

Proof. Assume that $\mathcal{O}_L = \mathcal{S} \cdot \alpha$ is a free $\mathcal{S}$-module of rank one, where $\alpha \in \mathcal{O}_L$, then $L = K[G].\alpha$ is a free $K[G]$-module generated by α. Let $\alpha \in \mathfrak{A}_{L/K}$ then $x\alpha \in \mathcal{O}_L$ hence $x\alpha = y\alpha$ for $y \in \mathcal{S}$, thus $x = y$, finally $\mathfrak{A}_{L/K} \subseteq \mathcal{S}$.
Let $x \in \mathcal{S} \backslash \mathfrak{A}_{L/K}$, then there is $\beta \in \mathcal{O}_L$ such that $x\beta \notin \mathcal{O}_L$. Moreover, $\beta = y\alpha$ for $y \in \mathcal{S}$, then $x\beta = x(y\alpha) = xy\alpha \in \mathcal{S}.\alpha = \mathcal{O}_L$, contradict our assumption. Thus $\mathfrak{A}_{L/K} = \mathcal{S}$. ∎

Definition 2.1.3. *Let L be a finite extension of a number field K. Then L/K is called totally wildly ramified if each intermediate F, the extension F/K is wildly ramified.*

Theorem 2.1.7. *Let L be a finite cyclic extension of a number field K. Assume that L/K is totally wildly ramified and $L/\mathbb{Q}$ is abelian and suppose that L/K and $\mathbb{Q}(\zeta_m)/K$ are linearly disjoint, where m is the conductor of K. Then $\mathfrak{A}_{L/K} = \oplus_{\chi \in \mathcal{X}_K(G)} R[G] \cdot e_\chi$ with $G = Gal(L/K)$.*

Proof. See [9]. ∎

Definition 2.1.4. *Let L be an extension of K and $L/\mathbb{Q}$ is abelian, then L/K is said to be Leopoldt if $\mathcal{O}_L$ is free $\mathfrak{A}_{L/K}$-module. The number field K is said to be Leopoldt if for every extension L of K and $L/\mathbb{Q}$ is abelian is Leopoldt.*

Remark 2.1.1. *The field of rational number is Leopoldt, this is Theorem 2.1.6.*

Theorem 2.1.8 (Theorem A [14]). *Let L and K be two cyclotomic number fields, such that $K \subseteq L$. Then L/K is Leopoldt.*

Theorem 2.1.9 (Theorem 1.2 [46]). *Let r and s be integers such that $r, s \geqslant 1$ and p an odd prime number. Let L be an extension of a number field K such that $[L : K] = p^s$ and $L \subseteq \mathbb{Q}(\zeta_{p^{r+s}})$. Then L/K is Leopoldt.*

Theorem 2.1.10 (Theorem 1.3 [46]). *Let r and s be integers such that $r \geqslant 1$, $s \geqslant 0$ and p an odd prime number. Then $\mathbb{Q}(\zeta_{p^{r+s}}/\mathbb{Q}(\zeta_{p^r})^+$ is Leopoldt, where $\mathbb{Q}(\zeta_{p^r})^+$ is the maximal real subfield of $\mathbb{Q}(\zeta_{p^r})$.*

2.2 Normal integral basis

2.2.1 Normal basis

In this section we recall the well known theorem of normal basis.

Theorem 2.2.1. *Let L be a finite Galois extension of a field K. Then L/K has a normal basis.*

Proof. Put $G = Gal(L/K)$ and $n = |G|$. First we assume that K is infinite, let $G = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$. Since L/K is separable, there is $\alpha \in L$ such that $L = K(\alpha)$. Let $P(X)$ be the minimal polynomial of α and let $\alpha_i = \sigma_i(\alpha)$. Setting

$$Q(X) = \frac{P(X)}{(X-\alpha)P'(\alpha)}$$

and

$$Q_i(X) = \sigma_i(Q(X)) = \frac{P(X)}{(X-\alpha_i)P'(\alpha_i)}$$

Then we have

$$Q_i(X)Q_j(X) \equiv 0 \bmod P(X) \quad \text{For } i \neq j$$

And

$$Q_i(X)^2 \equiv Q_i(X) \bmod P(X)$$

the two last equalities means that $\{Q_1(X), Q_2(X), \cdots, Q_n(X)\}$ are orthogonal idempotent 'mod' $P(X)$. Hence

$$D_G(Q_1(X), Q_2(X), \cdots, Q_n(X)) \equiv 1 \bmod P(X)$$

Since K is infinite, one may found an element $\beta \in K$ such that $D_G(Q_1(\beta), Q_2(\beta), \cdots, Q_n(\beta)) \neq 0$. Using the relation $D_G(Q_1(X), Q_2(X), \cdots, Q_n(X)) = \delta_G(Q(X))^2$, where $\delta_G(Q(X)) = det\,(\sigma\tau(Q(X))_{\tau\in G}^{\sigma\in G}$, and let $\gamma = Q(\beta)$. Then we obtain

$$\delta_G(\gamma) \neq 0$$

which implies that $\{\sigma_1(\gamma), \sigma_2(\gamma), \cdots, \sigma_n(\gamma)\}$ is a normal basis.

Suppose that K is finite, Then G is cyclic, let σ be a generator for G. Let $P(X)$ be the minimal polynomial of σ, then $deg(P(X)) \leq n$, and it's known that $1, \sigma, \sigma^2, \cdots, \sigma^{n-1}$ are linearly independent over L hence over K, then $P(X) = X^n - 1$, then there exist and element $\alpha \in K$ whose images under powers of σ constitute a normal basis of L over K. ∎

The next Theorem gives a necessary and sufficient condition on the existence of normal basis in the composite extension.

Theorem 2.2.2. *Let L be a finite Galois extension with galois group G. Assume that $G = G_1G_2$ and $G_1 \cap G_2 = \{e\}$. Let $L_1 = L^{G_2}$, $L_2 = L^{G_1}$, let $\alpha_1 \in \mathcal{O}_{L_1}$, $\alpha_2 \in \mathcal{O}_{L_2}$ and $\alpha = \alpha_1\alpha_2$.*

1. *Assume that α_i is a normal basis generator for L_i/K for $i = 1, 2$. Then α is a normal basis generator for L/K.*

2. *Assume that α_i is a normal integral basis generator for L_i/K for $i = 1, 2$ and L_1, L_2 are arithmetically disjoint. Then α is a normal integral basis generator for L/K.*

Proof.

1. Indeed, we have that $K[G] \overset{\psi}{\simeq} K[G_1] \otimes_K K[G_2]$, for $\alpha \in L$ put

$$\begin{aligned} \widetilde{\alpha} : K[G] &\to L \\ \sum_{\sigma\in G} a_\sigma\sigma &\mapsto \sum_{\sigma\in G} a_\sigma\sigma(\alpha) \end{aligned}$$

   Recall that if $\widetilde{\alpha}$ is injective then it's an isomorphism hence α is a normal basis generator. Set $\widetilde{\alpha_1}$ and $\widetilde{\alpha_2}$ in the same way. Then we get the following commutative diagram

$$\begin{array}{ccc} K[G_1] \otimes_K K[G_2] & \xrightarrow{\widetilde{\alpha_1}\otimes\widetilde{\alpha_2}} & L_1 \otimes_K L_2 \\ \Big\downarrow{\scriptstyle \Psi} & & \Big\downarrow{\scriptstyle \phi} \\ K[G] & \xrightarrow{\quad\widetilde{\alpha}\quad} & L \end{array}$$

   Hence $\widetilde{\alpha} o \psi = \phi o(\widetilde{\alpha_1} \otimes \widetilde{\alpha_2})$, since α_1 and α_2 are normal basis generators, then so is α.

2. We claim that $R[G] \cdot \alpha \simeq R[G_1] \cdot \alpha_1 \otimes_R R[G_2] \cdot \alpha_2$ as R-module. Put

$$\begin{aligned} \kappa : R[G_1] \cdot \alpha_1 \otimes_R R[G_2] \cdot \alpha_2 &\to R[G].\alpha \\ \sigma.\alpha_1 \otimes \tau.\alpha_2 &\mapsto \sigma\tau(\alpha) \end{aligned}$$

   Since $\{\sigma.\alpha_1 \otimes \tau.\alpha_2 \mid \sigma \in G_1, \tau \in G_2\}$ is a basis of $R[G_1] \cdot \alpha_1 \otimes_R R[G_2] \cdot \alpha_2$ and $\{\delta.\alpha \mid \delta \in G\}$ is a basis of $R[G].\alpha$, then κ in an isomorphism of R-modules. Since L_1 and L_2 are arithmetically disjoint, then α is a normal integral basis generator for L/K.

∎

Let L be a finite Galois extension of a field K and G it's Galois group such that $|G| = n$. Let $\alpha \in L$, then the matrix of $\widetilde{\alpha}$ in the basis $\{\sigma\}_{\sigma\in G}$ and $\{\sigma(\theta)\}_{\sigma\in G}$ where θ is a generator of the

normal basis of L over K, is given as follows: $W_\alpha := (w_{\gamma\tau})_\tau^\gamma$ where γ varies according to the lines and τ following columns. Let $\alpha = \sum_{\gamma\in G} a_\gamma.\gamma(\theta)$ be the expression of α in normal basis. Let $\tau \in G$. Then

$$\widetilde{\alpha}(\tau) := \tau(\alpha) = \sum_{\gamma\in G} a_\gamma.\tau\gamma(\theta) = \sum_{\gamma\in G} a_{\tau^{-1}\gamma}.\gamma(\theta)$$

therefore $w_{\gamma\tau} = a_{\tau^{-1}\gamma}$ for all γ, τ in G.

Remark 2.2.1. *An element α in L is an normal basis generator if and only if $\widetilde{\alpha}$ is injective.*

Proposition 2.2.1. *Under the previous notations, an element α in L is a generator of a normal basis of L over K if and only if $det(W_\alpha) \neq 0$.*

Proof. Indeed W_α is the matrix of $\widetilde{\alpha}$ in the basis $\{\sigma\}_{\sigma\in G}$ and $\{\sigma(\theta)\}_{\sigma\in G}$. ∎

Example 2.2.1. *Let K be a field containing the n-th root of unity, $L = K(\theta)$ where $\theta^n = d$ and d is an integer square-free (then $\theta = \sqrt[n]{d}$). Let ζ a primitive n-th root of 1. Let $\alpha = \sum_{i=0}^{n-1} a_i\theta^i$, written in the K-basis $\{1, \theta, ..., \theta^{n-1}\}$ of L. Then the conjugates of α is expressed as follows, for any $k \in \{1, ..., n-1\}$, $\alpha_k = \sum_{i=0}^{n-1} a_i(\zeta^k\theta)^i$. Therefore*

$$W_\alpha = \begin{pmatrix} a_0 & a_0 & . & . & . & a_0 \\ a_1 & \zeta a_1 & . & . & . & \zeta^{n-1}a_1 \\ . & . & . & . & . & . \\ a_k & \zeta^k a_1 & . & . & . & \zeta^{k(n-1)}a_k \\ . & . & . & . & . & . \\ a_{n-1} & \zeta^{n-1}a_1 & . & . & . & \zeta^{(n-1)^2}a_{n-1} \end{pmatrix}$$

thus

$$det(W_\alpha) = V(1, \zeta, ..., \zeta^{n-1}).(\prod_{i=0}^{n-1} a_i)$$

where $V(1, \zeta, ..., \zeta^{n-1})$ is a Vandermonde determinant.

Lemma 2.2.1. *Let K be a field containing the n-th root of unity, $L = K(\theta)$ where $\theta^n = d$ and d is an integer square-free. The element $\alpha = \sum_{i=0}^{n-1} a_i\theta^i$ is an normal basis generator of L over K if and only if $\prod_{i=0}^{n-1} a_i \neq 0$.*

Example 2.2.2. *Let k be a fixed field, $R = k[X]$ the ring of polynomials and $K = Fr(R)$. Let L/K be a quadratic extension of K, D a square-free polynomial such that $L = K(\sqrt{D})$, then*

$\{1, \sqrt{D}\}$ is a K-basis of L. Let $\alpha = U + V\sqrt{D}$ an element of L, $(U, V) \in K^2$. Note that $G := Gal(L/K) = \{1, \sigma\}$ where $\sigma(\alpha) = U - V\sqrt{D}$, then $W_\alpha = \begin{pmatrix} U & U \\ V & -V \end{pmatrix}$ therefore $det(W_\alpha) = -2UV$.

2.2.2 Gauss sums

Definition 2.2.1. *For L/K a finite abelian extension and $G = Gal(L/K)$, assume that $\mu_n \subseteq K$ where $n = [L : K] = |G|$, then $\mathcal{X}_K(G) = \widehat{G}$. Let $\alpha \in L$ and $\chi \in \widehat{G}$, then gauss sum formula for χ and α is given by:*

$$S(\chi, \alpha) = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\alpha). \tag{2.1}$$

Proposition 2.2.2. *For L/K a finite abelian extension and $G = Gal(L/K)$, assume that $\mu_n \subseteq K$ where $n = [L : K] = |G|$. Let $\alpha \in L$ and $\chi \in \widehat{G}$, then gauss sum formula for χ and α satisfies the following assertions:*

1. *$S(\chi, \alpha + \beta) = S(\chi, \alpha) + S(\chi, \beta)$.*
2. *For $u \in K[G]$, $S(\chi, u(\alpha)) = \chi(u)S(\chi, \alpha)$.*
3. *If $G = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$, let M be the matrix of $\mathcal{M}_n(K)$ defined by: $(M)_{ij} = \chi_i(\sigma_j^{-1})$ for $1 \leq i; j \leq n$. Let $U = (S(\chi_1, \alpha); S(\chi_2, \alpha); \ldots; S(\chi_n, \alpha))$ and $V = (\sigma_1(\alpha); \sigma_2(\alpha); \ldots; \sigma_n(\alpha))$ then:*

   $$U^\intercal = M \cdot V^\intercal.$$

   The matrix M is invertible and has inverse the matrix N, given by: $N = \frac{1}{|G|}\left(\chi_j(\sigma_i^{-1})\right)_{1 \leq j \leq n}^{1 \leq i \leq n}$.
4. *$\sigma(\alpha) = \frac{1}{|G|}\sum_{\chi \in \widehat{G}} \chi(\sigma^{-1})S(\chi, \alpha)$.*

Proof.

1. Indeed, $S(\chi, \alpha + \beta) = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\alpha + \beta) = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\alpha) + \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\beta) = S(\chi, \alpha) + S(\chi, \beta)$.
2. First we note that for an element $a \in K$ we have that:

$$S(\chi, a\alpha) = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(a\alpha) = a\sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\alpha) = aS(\chi, \alpha).$$

Hence, it suffice to prove that $S(\chi, \tau(\alpha)) = \chi(\tau)S(\chi, \alpha)$. Indeed:

$$\begin{aligned} S(\chi, \tau(\alpha)) &= \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\tau(\alpha)) \\ &= \sum_{\tau^{-1}\sigma \in G} \chi(\tau\sigma^{-1})\sigma(\alpha) \\ &= \chi(\tau) \sum_{\tau^{-1}\sigma \in G} \chi(\sigma^{-1})\sigma(\alpha) \\ &= \chi(\tau)S(\chi, \alpha). \end{aligned}$$

Which proves the claim.

3. This follows from the relation of orthogonality of characters.

4. Follows from the previous assertion.

2.2.3 Galois index ideal

Proposition 2.2.3. *Let L be an n-dimensional Galois extension of a field K and $G := \{\sigma_1, ..., \sigma_n\}$ it's Galois group. Let α in L, we put: $D_G(\alpha) := D(\sigma_1(\alpha), ..., \sigma_n(\alpha))$ the discriminant of $(\sigma_1(\alpha), ..., \sigma_n(\alpha))$. If G is an abelian group then:*

$$D_G(\alpha) = \left(\prod_{\chi \in \widehat{G}} S(\chi,\, \alpha) \right)^2 .$$

where $S(\chi, \alpha) = \sum_{\sigma \in G} (\sigma(\alpha).\chi(\sigma^{-1}))$.

Proof. For this we set the function:

$$\begin{array}{rccc} f & : & G & \to & L \\ & & \sigma & \mapsto & f(\sigma) = \sigma(\alpha) \end{array}$$

Hence

$$\sum_{\sigma \in G} f(\sigma^{-1})\chi(\sigma) = \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}(\sigma) = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma(\alpha).$$

Therefore by Lemma 5.26[72] we have that:

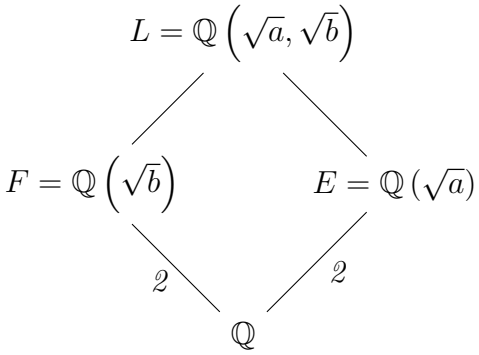
$$\prod_{\chi \in \widehat{G}} \left(\sum_{\sigma \in G} f(\sigma^{-1})\chi(\sigma) \right) = det(f(\sigma^{-1}\tau))_{\sigma \in G}^{\tau \in G} = det(\sigma\tau(\alpha)_{\sigma \in G}^{\tau \in G})$$

Finally we get:

$$D_G(\alpha) = \left(\prod_{\chi \in \widehat{G}} S(\chi, \alpha) \right)^2 .$$

∎

Example 2.2.3. *Let E and F be two quadratic extensions of the field of rational number $\mathbb{Q}$, such that $E = \mathbb{Q}(\sqrt{a})$, $F = \mathbb{Q}(\sqrt{b})$ and a, b are square free. Let $H = Gal(E/\mathbb{Q}) = \{1, \sigma\}$ and $N = Gal(F/\mathbb{Q}) = \{1, \tau\}$, then $G = HN$ is the galois group of $L = EF$ over $\mathbb{Q}$.*



By Proposition 1.3.2 we have that $\widehat{G} = \widehat{H}\widehat{N}$ such that $\widehat{H} = \{1, \chi\}$ and $\widehat{H} = \{1, \phi\}$. The following table gives the values of characters over G:

	1	χ	ϕ	$\chi\phi$
1	*1*	*1*	*1*	*1*
σ	*1*	*-1*	*1*	*-1*
τ	*1*	*1*	*-1*	*-1*
$\sigma\tau$	*1*	*-1*	*-1*	*-1*

Let $\alpha = u + v\sqrt{a} + w\sqrt{b} + t\sqrt{ab}$ be in L, Then

$$S(1, \alpha) = \alpha + \sigma\alpha + \tau\alpha + \sigma\tau\alpha = U + \tau U$$

$$S(\chi, \alpha) = \alpha - \sigma\alpha + \tau\alpha - \sigma\tau\alpha = V + \tau V$$

$$S(\phi, \alpha) = \alpha + \sigma\alpha - \tau\alpha - \sigma\tau\alpha = U - \tau U$$

$$S(\chi\phi, \alpha) = \alpha - \sigma\alpha - \tau\alpha + \sigma\tau\alpha = V - \tau V$$

where $U = \alpha + \sigma\alpha$ and $V = \alpha - \sigma\alpha$, hence

$$\begin{aligned} D_G(\alpha) &= ((U + \tau U)(V + \tau V)(U - \tau U)(V - \tau V))^2 \\ &= (U^2 - (\tau U)^2)^2 (V^2 - (\tau V)^2)^2. \end{aligned}$$

On the other hand we have that $U = 2(u + w\sqrt{b})$ *and* $V = 2(u - w\sqrt{b})$*, hence* $U - \tau(U) = 4w\sqrt{b}$ *and* $U + \tau(U) = 4u$*, which implies* $U^2 - \tau(U)^2 = 16uw\sqrt{b}$*. Also we have that* $V = 2(v\sqrt{a} + t\sqrt{ab})$ *and* $\tau(V) = 2(v\sqrt{a}+t\sqrt{ab})$*, then* $V-\tau(V) = 4t\sqrt{ab}$ *and* $V-\tau(V) = 4v\sqrt{a}$*, therefore* $V^2-\tau(V)^2 = 16vt\sqrt{a}\sqrt{ab}$*. We obtain:*

$$D_G(\alpha) = 2^{16}(uvwt)^2a^2b^2.$$

We conclude that α *is a normal basis generator of* L/K *if and only if the product* $uvwt \neq 0$*.*

For an element α in $\mathcal{O}_L$ we put $I_G(\alpha) := [\mathcal{O}_L : R[G].\alpha]_R$ where $R[G].\alpha = \bigoplus_{\sigma\in G} R.\sigma(\alpha)$.

Proposition 2.2.4. *Let* R *be a Dedekind ring,* K *its quotient field. Let* L/K *be a finite abelian extension of degree* n *and Galois group* G*. Then for any element* α *in* $\mathcal{O}_L$*:*

$$D_R(\mathcal{O}_L).I_G(\alpha)^2 = \left(\prod_{\chi\in\widehat{G}} S(\chi,\, \alpha)\right)^2$$

Proof. Indeed, we use the index-discriminant formula $Disc_R(P) = Ind_R(\alpha)^2 D_R(\mathcal{O}_L)$. Then the result follows from Proposition 2.2.3. ∎

Corollary 2.2.1. *Let* R *be a Dedekind ring,* K *its quotient field. Let* L/K *be a finite abelian extension of degree* n *and Galois group* G*. An element* α *in* $\mathcal{O}_L$ *is a normal integral basis generator of* L *over* K *if and only if* $D_R(\mathcal{O}_L) = \prod_{\chi\in\widehat{G}} S(\chi,\, \alpha)^2$*.*

Proof. Indeed, α is a normal integral basis generator if and only if $I_G(\alpha) = R$, hence the result follows from Proposition 2.2.4. ∎

Theorem 2.2.3. *Let* R *be a Dedekind ring with quotient field* K*. Let* $L = K(\alpha)$ *a pure quadratic extension of* K*, where* α *is a root of a monic irreducible polynomial* $P(X) = X^2 - d \in R[X]$*. Suppose that* $\upsilon_{\mathfrak{p}}(d^2 - d) = 1$ *for all prime divisors* $\mathfrak{p}$ *such that* $\mathfrak{p}/2d$*. Then* $\{1, \alpha\}$ *is an integral basis of* L/K *and* $d_{L/K} = 4dR$*.*

Proof. See [21]. ∎

Example 2.2.4. *With assumptions as in Theorem 2.2.3. Let* $G = Gal(L/K) = \{1, \sigma\}$ *and* $\widehat{G} = \{1, \chi\}$ *then for* $\theta = u + v\alpha \in \mathcal{O}_L$ *we get,* $S(1, \theta) = 2u$ *and* $S(\chi, \theta) = 2v\alpha$*, therefore by Proposition 2.2.3, hence we get* $D_G(\theta) = 4u^2v^2d$*, and according to Proposition 2.2.4 we obtain* $I_G^2(\theta) = 4u^2v^2$*. Thus* θ *generates a normal integral basis if and only if* u, v *and* 2 *are invertible in* $\mathcal{O}_K$*.*

Remark 2.2.2. *In the forgoing Example 2.2.4, we provided a necessary and sufficient condition to the existence of normal integral basis of a relative quadratic extension. The spacial case $K = \mathbb{Q}$ and $d \equiv 2, 3[4]$, one may observe that there is no generator of normal integral basis.*

Proposition 2.2.5. *Let R be a Dedekind ring with quotient field K, let $E = K(\sqrt{a})$ and $F = K(\sqrt{b})$ be two quadratic extensions satisfying the assumptions of Theorem 2.2.3. Let $L = EF$, then L is Galois extension of K with Galois group G, thus the galois index of $\gamma = u + v\sqrt{a} + w\sqrt{b} + w\sqrt{ab} \in \mathcal{O}_L$ is given by:*

$$I_G^2(\alpha) = 2^8(uvwt)^2.$$

Proof. First we note that $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$ is an integral basis of L/K. Thus the discriminant of L/K is:

$$D_{L/K} = 2^8 a^2 b^2.$$

Using the results of Example 2.2.3 we get: $D_G(\alpha) = 2^{16}(uvwt)^2 a^2 b^2$. Finally our claim follows from Proposition 2.2.4. ∎

Definition 2.2.2. *Let R be a dedekind ring and K its fraction field. Let L be a finite Galois extension of K, $G = Gal(L/K)$ and $[L : K] = n$. Let $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a basis of L/K, we will say that $\mathcal{B}$ is a diagonal basis if $\sigma(x_i) = \lambda_{i,\sigma} x_i$, for $\sigma \in G$ and $i = 1, 2, \cdots, n$. In other word the matrix of $\sigma \in G$ over the basis $\mathcal{B}$ is diagonal.*

Remark 2.2.3. *With assumptions as in Definition 2.2.2 we see that field $\mu_n \subseteq K$.*

Proposition 2.2.6. *Let R be a dedekind ring and K its fraction field. Let L be a finite abelian extension of K, $G = Gal(L/K)$ and $[L : K] = n$. If $\mu_n \subset K$, then L/K admit a diagonal basis. More precisely, if α is a normal basis generator of L/K then $\mathcal{B}_1 = \{e_\chi \alpha \mid \chi \in \widehat{G}\}$ is a diagonal basis of L/K.*

Proof. Let $\alpha \in L$ such that α is a normal basis generator of L/K, since $e_\chi \in K[G]$ for all $\chi \in \widehat{G}$ and $1 = \sum_{\chi \in G} e_\chi$, thus $\alpha = \sum_{\chi \in G} e_\chi . \alpha$. As $\sigma(e_\chi) = \chi(\sigma) e_\chi$ then $\sigma(\alpha) = \sum_{\chi \in \widehat{G}} \chi(\sigma) e_\chi . \alpha$, therefore the matrix $\mathcal{M} = (\chi(\sigma))_{\chi \in \widehat{G}}^{\sigma \in G}$ is the passage matrix from $\mathcal{B}_1 = \{e_\chi \alpha \mid \chi \in \widehat{G}\}$ to $\mathcal{B}_2 = \{\sigma(\alpha) \mid \sigma \in G\}$. Since $\mathcal{M}$ is invertible (see Proposition 2.2.2) then L/K has a diagonal basis. ∎

Let R be a dedekind ring and K its fraction field. Let L be a finite abelian extension of K, $G = Gal(L/K)$ and $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a diagonal basis of L/K. Let χ_i be the character defined by:

$$\sigma(x_i) = \chi_i(\sigma) x_i.$$

Since χ_i and χ_j are distinct for $i \neq j$ (if not the elements x_i will not be linearly independent), hence $\widehat{G} = \{\chi_1, \chi_2, \cdots, \chi_n\}$. The following Lemma gives explicitly the value of the Gauss sums.

Lemma 2.2.2. *Let R be a dedekind ring and K its fraction field. Let L be a finite abelian extension of K, $G = Gal(L/K)$ and $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a diagonal basis of L/K. Let $\omega = \sum_{j=1}^{n} \lambda_j x_j$, $\lambda_i \in K$ and $\chi_i \in \widehat{G}$, then:*

$$S(\chi_i, \omega) = |G| \lambda_i x_i.$$

In particular:

$$S(\chi_i,\, x_j) = \begin{cases} |G| x_i & \text{if } \chi_i = \chi_j \\ 0 & \text{if } \chi_i \neq \chi_j. \end{cases} \tag{2.2}$$

Proof. Indeed, $S(\chi_i,\, x_j) = \sum_{\sigma \in G} \chi_i(\sigma^{-1}) \sigma(x_j)$, since $\sigma(x_j) = \chi_j(\sigma) x_j$. then

$$S(\chi_i,\, x_j) = \sum_{\sigma \in G} \chi_i(\sigma^{-1}) \chi_j(\sigma) x_j =< \chi_i, \chi_j > x_i.$$

∎

Lemma 2.2.3. *Let R be a dedekind ring and K its fraction field. Let L be a finite abelian extension of K, $G = Gal(L/K)$ and $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a diagonal basis of L/K. Then*

$$\sigma(S(\chi_i, x_j)) = \chi_i(\sigma) S(\chi_i, x_j), \text{ for } 1 \leq i.j \leq n.$$

Proposition 2.2.7. *Let R be a dedekind ring and K its fraction field. Let L be a finite abelian extension of K, $G = Gal(L/K)$ and $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a diagonal basis of L/K. Let $\omega = \sum_{i=1}^{n} \lambda_i x_i \in L$. Then*

$$D_G(\omega) = \left(\prod_{i=1}^{n} \lambda_i x_i \right)^2 n^{2n} R.$$

Proof. Recall that $D_G(\omega) = \left(\prod_{\chi \in \widehat{G}} S(\chi,\, \omega) \right)^2$ and since $\omega = \sum_{i=1}^{n} \lambda_i \alpha^{i-1}$ then $S(\chi_i, \omega) = \sum_{j=1}^{n} \lambda_j S(\chi_i,\, x_i)$. Consequently $D_G(\omega) = \prod_{\chi \in \widehat{G}} S(\chi,\, \omega)^2 = (\prod_{i=1}^{n} \lambda_i x_i)^2\, n^{2n}$.

∎

In the next corollary we give a particular case of the forgoing result.

Corollary 2.2.2. *Let $L = K(\alpha)$ with $\alpha^n = a$ be a Kummer extension of K of degree n and $G = Gal(L/K)$. Let $\omega = \sum_{i=1}^{n} \lambda_i \alpha^{i-1} \in L$. Then*

$$D_G(\omega) = (\prod_{i=1}^{n} \lambda_i)^2\, a^{n-1} n^{2n} R.$$

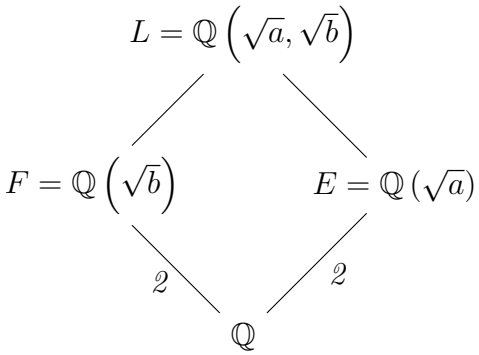
Corollary 2.2.3. *Let R be a dedekind ring and K its fraction field. Let L be a finite abelian extension of K, $G = Gal(L/K)$ and $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a diagonal basis of L/K. Let $\omega = \sum_{i=1}^{n} \lambda_i x_i \in L$. Then ω is a normal basis generator of L/K if and only if $\lambda_i \neq 0$ for all $i = 1, \cdots, n$.*

Corollary 2.2.4. *Let $L = K(\alpha)$ with $\alpha^n = a$ be a Kummer extension of K of degree n and $G = Gal(L/K)$. Let $\omega = \sum_{i=1}^{n} \lambda_i \alpha^{i-1} \in L$. Then ω is a normal basis generator of L/K if and only if $\lambda_i \neq 0$ for all $i = 1, \cdots, n$.*

Proposition 2.2.8. *Let $L = K(\alpha)$ with $\alpha^n = a$ be a Kummer extension of K of degree n and $G = Gal(L/K)$. We assume that L/K is monogenic. Let $\omega = \sum_{i=1}^{n} \lambda_i \alpha^{i-1}$. Then ω is a normal integral basis if and only if $\left(n^n \left(\prod_{i=1}^{n} \lambda_i\right)^2\right) \in U(R)$.*

Proof. In fact, If L/K is monogenic, then its discriminant is $D_R(\mathcal{O}_L) = n^n a^{n-1} R$ and the formula $D_R(\mathcal{O}_L) I_G^2(\omega) = D_G(\omega) = \left(\prod_{i=1}^{n} \lambda_i\right)^2 a^{n-1} n^{2n}$, implies $I_G^2(\omega) = n^n \left(\prod_{i=1}^{n} \lambda_i\right)^2$. Hence the result is attained. ∎

Example 2.2.5. *Let E and F be two quadratic extension of the field of rational number $\mathbb{Q}$, such that $E = \mathbb{Q}(\sqrt{a})$, $F = \mathbb{Q}(\sqrt{b})$ and a, b are square free. Let $H = Gal(E/\mathbb{Q}) = \{1, \sigma\}$ and $N = Gal(F/\mathbb{Q}) = \{1, \tau\}$, then $G = HN$ is the galois group of $L = EF$ over $\mathbb{Q}$.*



The set $\mathcal{B} = \{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$ is a diagonal basis of L/K then for an element $\omega = \lambda_1 + \lambda_2\sqrt{a} + \lambda_3\sqrt{b} + \lambda_4\sqrt{ab}$, and according to Proposition 2.2.7 we get $D_G(\omega) = 4^8 \left(\lambda_1\lambda_2\lambda_3\lambda_4\right)^2 a^2 b^2$.

Proposition 2.2.9. *Let $\mathbb{Q}(\sqrt{a_i})$ be a quadratic extension of the field of rational number $\mathbb{Q}$ for $i = 1, 2, \cdots, n$. Let $L = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_n})$ and $G = Gal(L/\mathbb{Q})$ then L has a diagonal basis $\mathcal{B}$ formed by $\sqrt{a_i}$ over the field of rational number $\mathbb{Q}$. Let $\omega \in L$ and λ_j the coordinate of ω in the basis $\mathcal{B}$, then:*

$$D_G(\omega) = \left(2^{n.2^n} \prod_{i=1}^{2^n} \lambda_i\right)^2 \left(\prod_{i=1}^{n} a_i\right)^{2^{n-1}}.$$

Proof. It suffice to apply Proposition 2.2.7 to the basis $\mathcal{B}$. ∎

Proposition 2.2.10. *Let L_i be a finite extension of degree n_i of $\mathbb{Q}$ for $i = 1, 2, \cdots, r$ and $L = L_1 L_2 \cdots L_r$, if for $i \neq j$ the extensions L_i and L_j are arithmetically disjoint, then:*

$$D_{\mathbb{Q}}(L) = \prod_{i=1}^{r} D_{\mathbb{Q}}(L_i)^{\frac{N}{n_i}}$$

such that $N = n_1 n_2 \cdots n_r$

Proof. We already know that the discriminant of two arithmetically disjoint extensions L_1, L_2 over K is:

$$D_{\mathbb{Q}}(L_1 L_2) = D_{\mathbb{Q}}(L_1)^{[L_2:K]} D_{\mathbb{Q}}(L_2)^{[L_1:K]}$$

Hence the result follows by an inductive argument. ∎

Proposition 2.2.11. *Let $\mathbb{Q}(\sqrt{a_i})$ be a quadratic extension of the field of rational number $\mathbb{Q}$ for $i = 1, 2, \cdots, n$. Let $L = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_n})$ and $G = Gal(L/\mathbb{Q})$, assume that $a_i \equiv 1 \ mod\ 4$ and $\mathbb{Q}(\sqrt{a_i})$ et $\mathbb{Q}(\sqrt{a_j})$ are arithmetically disjoint for $i \neq j$, then:*

$$D_{\mathbb{Q}}(L) = \left(\prod_{i=1}^{n} a_i \right)^{2^{n-1}} R$$

and for an element $\omega \in \mathcal{O}_L$, we obtain:

$$I_G^2(\omega) = \left(2^{n.2^n} \prod_{i=1}^{2^n} \lambda_i \right)^2.$$

Example 2.2.6. *Let $\mathbb{Q}(\sqrt{a_i})$ be a quadratic extension of the field of rational number $\mathbb{Q}$ for $i = 1, 2, \cdots, n$. Let $L = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_n})$ and $G = Gal(L/\mathbb{Q})$, assume that $a_i \equiv 1 \ mod\ 4$ and $\mathbb{Q}(\sqrt{a_i})$ et $\mathbb{Q}(\sqrt{a_j})$ are arithmetically disjoint for $i \neq j$, then $L/\mathbb{Q}$ then the extension $L/\mathbb{Q}$ has no normal integral basis.*

2.2.4 Dedekind sums

Let a and b two non negative integers. Let $C(a, b) := \sum_{t=0}^{a-1} [\frac{bt}{a}]$ where $[t]$ is the integral part of a real number t.

Lemma 2.2.4. *(See [39] and Lemma 1 in [24]) Let a and b are two positive integers. Let $C(a, b) = \sum_{t=0}^{a-1} [\frac{bt}{a}]$. Then*

$$2C(a, b) = ab - a - b + a \wedge b$$

where $a \wedge b$ designs the greater common divisor of a and b.

2.2.5 The associated ideals in a Dedekind ring

Let R be a Dedekind ring, K its quotient field and $\mathfrak{a}$ a non zero ideal of R. The ascending power decomposition of the ideal $\mathfrak{a}$ (abbreviated by APD) is the decomposition

$$\mathfrak{a} := \prod_{k \geq 1} {\mathfrak{a}_k}^k$$

where each $\mathfrak{a}_k$ is a square free ideal of R and the ideals $\mathfrak{a}_k$ are pairwise coprime ideals. The ideal $\mathfrak{a}_k$ is called the k-part of $\mathfrak{a}$.

Let $\mathfrak{a}$ be a non zero ideal of a Dedekind ring R. Then, for any integer k such that $k \in [\![1, n-1]\!]$, the k^{th} associated ideal of $\mathfrak{a}$ is defined by $\mathfrak{b}_k := \prod_{i=1}^{n} {\mathfrak{a}_i}^{[\frac{ik}{n}]}$.

Lemma 2.2.5. *Let R be a Dedekind ring and $\mathfrak{a}$ be a non zero ideal of R. Assume that $\mathfrak{a} := \prod_{k=1}^{n} {\mathfrak{a}_k}^k$ is the ascending power decomposition of the ideal $\mathfrak{a}$ and the ideals $\mathfrak{b}_1$, $\mathfrak{b}_2$, ..., $\mathfrak{b}_{n-1}$ are the associated ideals of the ideal $\mathfrak{a}$. Then*

$$(\prod_{k=1}^{n-1} \mathfrak{b}_k)^2 \prod_{k=1}^{n} {\mathfrak{a}_k}^{n-(n \wedge k)} = \mathfrak{a}^{n-1}.$$

Proof. Indeed $\prod_{k=1}^{n-1} {\mathfrak{b}_k}^2 = \prod_{k=1}^{n-1} (\prod_{i=1}^{n} {\mathfrak{a}_i}^{[\frac{ik}{n}]})^2 = \prod_{i=1}^{n} (\prod_{k=1}^{n-1} {\mathfrak{a}_i}^{[\frac{ik}{n}]})^2 = \prod_{i=1}^{n} {\mathfrak{a}_i}^{2C(i,n)}$. Then $(\prod_{k=1}^{n-1} \mathfrak{b}_k)^2 \prod_{k=1}^{n1} {\mathfrak{a}_k}^{n-(n \wedge k)} = \prod_{k=1}^{n} {\mathfrak{a}_k}^{2C(k,n)} \prod_{k=1}^{n} {\mathfrak{a}_k}^{n-(n \wedge k)} = \prod_{k=1}^{n} {\mathfrak{a}_k}^{(2C(k,n)+n-(n \wedge k))}$. It suffice then to use the Lemma 2.2.4 to see that $2C(k,\, n) + n - (n \wedge k) = k(n-1)$ for any integer k such that $k \in [\![1, n-1]\!]$. ∎

2.2.6 Cyclic Kummer tamely ramified extensions

Let L/K be a cyclic Kummer extension of degree n and $G = Gal(L/K)$. Assume that $L = K(\alpha)$ with $\alpha^n = a$.

Proposition 2.2.12. *(See Corollary 1 in [24]) Let $L = K(\alpha)$ with $\alpha^n = a$ be a Kummer extension of K of degree n and $G = Gal(L/K)$. Assume that the extension L/K is tamely ramified and $aR = \prod_{i=1}^{n} {\mathfrak{a}_k}^k$ is the ascending power decomposition of the ideal aR. Then*

$$D_R(\mathcal{O}_L) = \prod_{k=1}^{n} \mathfrak{a}_k^{n-(n \wedge k)}.$$

Corollary 2.2.5. *Let $L = K(\alpha)$ with $\alpha^n = a$ be a Kummer extension of K of degree n and $G = Gal(L/K)$. Assume that the extension L/K is tamely ramified and $aR = \prod_{i=1}^{n} \mathfrak{a}_k{}^k$ the ascending power decomposition of the ideal aR. Let $\mathfrak{b}_1$, $\mathfrak{b}_2$, ..., $\mathfrak{b}_n$ be the associated ideals of the ideal $\mathfrak{a} = aR$. Then*

$$(\prod_{k=1}^{n} \mathfrak{b}_k)^2 \, D_R(\mathcal{O}_L) = a^{n-1}R.$$

Proof. Indeed $(\prod_{k=1}^{n} \mathfrak{b}_k)^2 \, D_R(\mathcal{O}_L) = (\prod_{k=1}^{n} \mathfrak{b}_k)^2 \prod_{k=1}^{n} \mathfrak{a}_k^{n-(n\wedge k)}$ and it suffice to use the Lemma 2.2.5 to see that $(\prod_{k=1}^{n} \mathfrak{b}_k)^2 \, D_R(\mathcal{O}_L) = a^{n-1}R$. ∎

Let L/K be a cyclic Kummer extension of degree n and $G = Gal(L/K)$. In this section we assume that the extension L/K is tamely ramified and $L = K(\alpha)$ with $\alpha^n = a$.

Assume that the ideal $a\,R := \prod_{k=1}^{n} \mathfrak{a}_k{}^k$ is the ascending power decomposition of the ideal $a\,R$ and the ideals $\mathfrak{b}_1$, $\mathfrak{b}_2$, ..., $\mathfrak{b}_n$ are the associated ideals of the ideal $a\,R$.

Proposition 2.2.13. *Let $L = K(\alpha)$ be a cyclic Kummer extension such that $a = \alpha^n \in R$ and $\alpha \in \mathcal{O}_L$ the ring of integers of L. Let $a\,R := \prod_{k=1}^{n} \mathfrak{a}_k{}^k$ is the ascending power decomposition of the ideal $a\,R$ and the ideals $\mathfrak{b}_1$, $\mathfrak{b}_2$, ..., $\mathfrak{b}_{n-1}$ are the associated ideals of the ideal $a\,R$. Let $\omega = \frac{1}{n}\sum_{i=0}^{n-1} \frac{\alpha^i}{\lambda_i} \in L$. Assume that L/K is tamely ramified. Then ω is normal integral basis generator of L/K if and only if the following conditions are satisfied.*

1. *The ideals $\prod_{i\geq 0} \mathfrak{b}_i = \prod_{i=0}^{n} \lambda_i R$*
2. *The element $\omega \in \mathcal{O}_L$.*

Proof. Indeed, by Proposition 2.2.7 we have that $\left(\prod_{i=0}^{n-1} \lambda_i\right)^2 D_G(\omega) = a^{n-1}$ and according to Lemma 2.2.5 and Proposition 2.2.12 we get $\left(\prod_{i=0}^{n-1} \lambda_i\right)^2 D_R(\mathcal{O}_L) = a^{n-1}$. Therefore

$$D_R(\mathcal{O}_L) = D_G(\omega).$$

If ω is a normal integral basis generator then $D_R(\mathcal{O}_L) = D_G(\omega)$, and by Propositions 2.2.7, 2.2.12 and Lemma 2.2.5 the two assumptions follows. ∎

2.2.7 Associated order in abelian extension

Next we consider an abelian extension, we prove that the associated order of such extension is equal to the maximal order when this extension have a diagonal integral basis.

Definition 2.2.3. *Let R be a dedekind ring and K its fraction field. Let L be a finite Galois extension of K, $G = Gal(L/K)$ and $[L : K] = n$. Let $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be an integral basis of L/K, we will say that $\mathcal{B}$ is a diagonal integral basis if $\sigma(x_i) = \lambda_{i,\sigma} x_i$, for $\sigma \in G$ and $i = 1, 2, \cdots, n$.*

Theorem 2.2.4. *Let R be a dedekind ring with fraction field K. Let $L = K(\alpha)$ be finite abelian extension of degree n of K and let $G = Gal(L/K)$. Suppose that L/K has a diagonal integral basis. Then the associated order $\mathfrak{A}_{L/K}$ of L/K is the maximal R-order of $K[G]$.*

Proof. Let $\mathcal{B} = \{x_1, x_2, \cdots, x_n\}$ be a diagonal integral basis of L/K. By definition $\mathfrak{A}_{L/K} = \{u \in K[G] \mid \ u \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}$, thereby an element $u = \sum_{\sigma \in G} b_\sigma \sigma \in K[G]$ belongs to $\mathfrak{A}_{L/K}$ if and only if $u(x_i) \in \mathcal{O}_L$ for $i = 1, 2, \cdots, n$. Seeing that $u(x_i) = \left(\sum_{\sigma \in G} b_\sigma \chi_i(\sigma)\right)(x_i)$ for $i = 1, 2, \cdots, n$,. Thus $u(x_i) \in \mathcal{O}_L$ if and only if $\sum_{\sigma \in G} b_\sigma \chi_i(\sigma) \in R$ in this case, put $c_i = \sum_{\sigma \in G} b_\sigma \chi_i(\sigma)$ for $c_i \in R$. The situation remain to solve the linear system associated to the matrix $M = (\chi_i(\sigma))_{1 \leq i \leq n}^{\sigma \in G}$. The matrix M is invertible and has inverse $M^{-1} = \frac{1}{n} (\chi_i(\sigma^{-1}))_{1 \leq i \leq n}^{\sigma \in G}$, then $b_\sigma = \sum_{j=1}^{n} c_j \chi_j(\sigma^{-1})$. Therefore $u = \sum_{\sigma \in G} b_\sigma \sigma = \sum_{\sigma \in G} \left(\sum_{j=1}^{n} c_j \chi_j(\sigma)\right) \sigma$. Rewriting u one gets

$$u = c_1 \frac{1}{n} \sum_{\sigma \in G} \chi_1(\sigma^{-1})\sigma + c_2 \frac{1}{n} \sum_{\sigma \in G} \chi_2(\sigma^{-1})\sigma + \cdots + c_n \frac{1}{n} \sum_{\sigma \in G} \chi_n(\sigma)\sigma.$$

Which implies that $\mathfrak{A}_{L/K} = \oplus_{\chi \in \widehat{G}} R[G] \cdot e_\chi$, and by Proposition 1.5.2 we obtain $\mathfrak{A}_{L/K} = \mathcal{S}_{K[G]}$. ∎

Remark 2.2.4. *We note that Theorem 2.2.4 can be established in another way if we assume that the extension L/K ($L = K(\alpha)$ such that $\alpha^n = a \in K$) is kummer of degree n, $\mu_n \subseteq K$. Indeed, The associated order of L/K can be expressed as $E = \{P \in K_n[\sigma] \mid P(\zeta^i) \in R, \forall i \in [\![1, n-1]\!]\}$. For that we set $P_i(X) = \sum_{j=0}^{n-1} X^j \zeta_n^{i(n-1-j)}$ hence we observe that $E = \oplus_{0 \leqslant i \leqslant n} R P_i(\sigma)$, where $P_i(\sigma) = e_{\chi^i}$, then:*

$$\mathfrak{A}_{L/K} = \oplus_{i=0}^{n-1} R[G] \cdot e_{\chi^i} = \mathcal{S}_{K[G]}.$$

2.2.8 Cyclic extension ever a fields of prime characteristic

Theorem 2.2.5. *Let L be a field, G be the finite group of automorphisms of L and $|G| = n$, let E be the fixed field of G. Then $[L : E] = n$ and L is a galois extension of E of galois group G.*

Proof. See Theorem 3 of [8] *V.* 64.

Corollary 2.2.6. *Let K be a field of $char(K) = p$, $p \neq 0$. Let $L = K(T)$ and $\sigma \in Aut_K(L)$ such that $\sigma(T) = T + 1$. Let $G =< \sigma >$ and $E = L^G$ then L/E is Galois and $G = Gal(L/E)$ of degree p. In this case $E = K(U)$ such that $U = T^p - T$.*

Proof. It is clear that $\sigma^p = id_L$ therefore G is cyclic of degree p, hence the extension is of degree p. Let $U = T^p - T$, $Irred(T, E)$ divides $X^p - X - U$ as $L = E'(T)$ then $[L : E'] \leq p$ where $E' = K(U)$, but $\sigma(U) = U$ and hence $U \in E$ therefore $E' = K(U) \subseteq E$ and hence $[L : E'] \geq [L : E] = p$ since $\mid G \mid = p$, and $E = L^G$ we conclude that $E = K(U)$. ∎

Corollary 2.2.7. *Let K be a field of $char(K) = p$ and $p \neq 0$. Let $L = K(T)$. Then the ring of integers of L is $\mathcal{O}_L = K[T]$.*

Proof. This follows from the fact that $K[T]$ is a principal ideal domain.

Proposition 2.2.14. *Let K be a field of $char(K) = p$, $p \neq 0$. Let $L = K(T)$ and $\sigma \in Aut_K(L)$ such that $\sigma(T) = T + 1$. Let $G =< \sigma >$ and $E = L^G$, then $\alpha = T^{p-1}$ is a normal basis generator of L over E.*

Proof. It is already known that $\mathcal{B}_0 = \{T^{p-1}, (T+1)^{p-1}, \cdots, (T+p-1)^{p-1}\}$ is a basis of L/E.

Proposition 2.2.15. *Let K be a field of $char(K) = p$, $p \neq 0$. Let $L = K(T)$ and $\sigma \in Aut_K(L)$ such that $\sigma(T) = T + 1$. Let $G =< \sigma >$ and $E = L^G$. Let $\alpha = T^{p-1}$, then:*

$$I_G(\alpha) = [\mathcal{O}_L : \mathcal{O}_E[G].\alpha] = (p-1)! \prod_{i=1}^{p} \binom{i-1}{p-1} Det(V').$$

With $(V')_{ij} = j^{p-i-1}$, for $1 \leq i, j \leq p-1$, and α generate a normal integral basis.

Proof. Let $A = \mathcal{M}(\mathcal{B}_0, \mathcal{B})$, thus:

$$(A)_{i,j} = \begin{cases} 0 & if\ j = 1 \text{ and } i \neq p \\ 1 & if\ j = 1 \text{ and } i = p \\ (j-1)^{p-i}\binom{i-1}{p-1} & if\ j \geq 2. \end{cases}$$

therefore $Det(A) = Det(A')$ where:

$$(A')_{i,j} = j^{p-i}\binom{i-1}{p-1}.$$

Hence $Det(A) = Det(A') = \prod_{i=1}^{p} \binom{i-1}{p-1} Det(A'')$, where:

$$(A'')_{i,j} = j^{p-i}.$$

Finally we get: $Det(A) = Det(A') = (p-1)! \prod_{i=1}^{p} \binom{i-1}{p-1} Det(V')$, such that:

$$(V')_{i,j} = j^{p-i-1}.$$

We note that $I_G(\alpha)$ is invertible, hence α generate a normal integral basis generator. ∎

Chapter 3

Discriminant and Steinitz class

3.1 Tower formula of discriminant

3.1.1 Introduction

The discriminant is an extreme tool in number theory, this notion has been generalized for a free R-algebra of a finite rank, and also for a sub-lattice of a separable R-algebra of a finite dimension see ([47],[15],[52],[64]...). In this section we study the discriminant of bilinear module over commutative ring with unit, also we establish the tower formula which is an effective tools to compute discriminants in much easier way, so we see the possible towers and we compute the discriminant of the main structure using intermediate discriminants, a concreted example is given, we mention that the result here can be recovered in many context (Number field, K-algebra, orders), we mention also that this formula is for an arbitrary bilinear form, specially the trace form (classical discriminants).

3.1.2 Discriminant of bilinear modules

Definition 3.1.1. *An R-module M is called an R-bilinear module (or bilinear module for short) if there exists an R-bilinear form ϕ on M. If we need to specify the bilinear form ϕ attached to M, we may use the notation (M, ϕ) instead of M. If ϕ is symmetric, we say that (M, ϕ) is a symmetric R-module.*

Let M be a finitely generated R-module and let n be the minimal number of a system of generators of M. We denote this number by $\mu_R(M)$.

Let A be a free R-algebra, for an element x in A let $\widetilde{x} : A \to A$ with $\widetilde{x}(a) = ax$, define $N_{A/R}(x) = det(\widetilde{x})$. For a principal ideal $I = aA$ of A with $a \in A$, we define it's norm as $N_{A/R}(I) = N_{A/R}(a)R$.

Let R be a commutative ring, (M,ϕ) a free bilinear R-module, let $S=\{x_1,x_2,....,x_n\}$ be a free system of n elements of M, we define the discriminant of S by $disc_\phi(x_1,x_2,....,x_n)=det(\phi(x_i,x_j))_{1\leq i,j\leq n}$, another step allow as to define the discriminant of M, hence in many references we found that this invariant is defined as the class of $disc_\phi(x_1,x_2,...,x_n)$ in R^*/R^{*2} this is well defined because of Lemma 3.1.1, here we define the discriminant of M.

Definition 3.1.2. *Let (M,ϕ) be a finitely generated symmetric bilinear R-module and $n=\mu_R(M)$. Define the ϕ-discriminant over R of a system $\{x_1,x_2,....,x_n\}$ of n elements of M as $D_\phi(x_1,x_2,....,x_n)=det(\phi(x_i,x_j))$, and the ϕ-discriminant of M over R to be the ideal $D_\phi(M)$ of R generated by $D_\phi(x_1,x_2,....,x_n)$ for all $x_1,x_2,....,x_n\in M$.*

Proposition 3.1.1. *Let (M,φ) be a free symmetric bilinear R-module of rank n. Then the ideal discriminant $D_\phi(M)$ is principal.*

Proof. It follows immediately from the next Lemma. ∎

Lemma 3.1.1. *Let (M,ϕ) a finitely generated bilinear R-module. If $y_j=\sum a_{ij}x_i$ then $D_\phi(y_1,...,y_n)=det(a_{ij})^2D_\phi(x_1,...,x_n)$.*

Proof. Since $y_j=\sum a_{ij}x_i$ then $\phi(y_i,y_j)=\sum\limits_{k,l}a_{i,k}a_{j,l}\phi(x_k,x_l)$ then one get $(\phi(y_i,y_j))_{i,j}=X(\phi(x_i,x_j))_{i,j}X^t$ with $X=(a_{i,j})$, hence $D_\phi(y_1,...,y_n)=det(a_{ij})^2D_\phi(x_1,...,x_n)$. ∎

Let R be a commutative ring and A a free R-algebra of rank m. Let (M,φ) be a free symmetric bilinear A-module of rank n. Consider $D_\varphi(M)$ the φ-discriminant over A generated by discriminants of systems of n elements of M. The fact that M is free imply that $D_\varphi(M)$ is generated by $D_\varphi(x_1,x_2,....,x_n)$, where $x_1,x_2,....,x_n$ is a basis of M. In other word $D_\varphi(M)=D_\varphi(x_1,x_2,....,x_n)A=det(\varphi(x_i,x_j))A$. The set M can be seen as a free R-module of rank mn, we will denote it M_R to avoid confusions. Define the bilinear form ψ of M_R over R by $\psi=Tr_{A/B}\circ\varphi$.

The ψ-discriminant of M_R over R is a principal ideal of R generated by the discriminant of a basis of M_R over R. We will exhibit the relation between $D_\psi(M_R)$ and $D_\varphi(M)$.

The set $Bil_A(M)$ equipped with structure of A-module is identified with the A-module $Hom_A(M,\,M^*)$ via the map

$$\begin{array}{rccc}\Gamma & : & Bil_A(M) & \to & Hom_A(M,\,M^*)\\ & & \phi & \mapsto & \Gamma(\phi)=\phi_r.\end{array}$$

where

$$\begin{array}{rccc}\phi_r(x) & : & M & \to & A\\ & & y & \mapsto & \phi(y,x).\end{array}$$

with $x \in M$.

Proposition 3.1.2. *Let (M, ϕ) be a free bilinear R-module. Let $\mathcal{B} = \{e_1, ..., e_n\}$ be a basis of M over R. Let U be the matrix of ϕ_r over the basis $\mathcal{B}$ and $\mathcal{B}^*$, $U = \mathcal{M}(\phi_r, \mathcal{B}, \mathcal{B}^*)$. Then $D_\phi(e_1, ..., e_n) = detU$.*

Proof. Let $\mathcal{B} = \{e_1, ..., e_n\}$ be a basis of M over R and $\mathcal{B}^* = \{e_1^*, ..., e_n^*\}$ it's dual basis, since $\phi_r(e_i) = \sum_j b_{ij} e_j^*$ then by Parseval formula we get $U = (\phi(e_i, e_j))_{i,j}$, finally $D_{\phi_r}(e_1, ..., e_n) = detU$. ∎

3.1.3 Tower formula of discriminants

Let M be an A-module. Let $M^* = Hom_A(M, A)$ be its dual A-module. Recall that if M is finitely generated A-module (resp. free of rank n) then M^* is also a finitely generated A-module (resp. free of rank n).

Theorem 3.1.1. *Let R be a commutative ring and A a free R-algebra of rank m. Let (M, φ) be a free symmetric bilinear A-module of rank n. Let M_R the A-module seen as R-module, and $\psi = Tr_{A/B} \circ \varphi$. Then*

$$D_\psi(M_R) = D_{Tr}^n(A) N_{A/R}(D_\varphi(M)).$$

Proof. Define the maps ϕ_r and ψ_r corresponding to ϕ and ψ respectively, and let

$$\begin{array}{rccc} \tilde{T}_{A/R} & : & M^* & \to & (M_R)^* \\ & & f & \mapsto & Tr_{A/R} \circ f. \end{array}$$

Let $x \in M$, for $y \in M$ we have $\psi_r(x)(y) = \psi(y, x) = T_{A/R} \circ \varphi(y, x) = Tr_{A/R}(\varphi_r(x)(y))$ then $\psi_r(x) = T_{A/R} \circ \varphi_r(x)$, this is true for all $x \in M$ then $\psi_r = \tilde{T}_{A/R} \circ \varphi_r$(composition of application). The maps φ_r and $\tilde{T}_{A/R}$ can be regarded as homomorphisms of R-module, denote those maps in this case by $(\varphi_r)_R$ and $(\tilde{T}_{A/R})_R$ respectively, thus, the equality

$$\psi_r = (\tilde{T}_{A/R})_B \circ (\varphi_r)_R \quad (1)$$

is more convenient (instead of $\psi_r = \tilde{T}_{A/R} \circ \varphi_r$) and clarify that the relation of composition is between R-homomorphisms. By the previous proposition we have $D_\varphi(M) = det(\varphi_r)$ and $D_\psi(M_R) = det(\psi_r)$ hence it is suffice to show that

$$det(\psi_r) = D_{Tr}^n(A) N_{A/R}(det(\varphi_r)).$$

using (1) then $det(\psi)_r = det((\tilde{T}_{A/R})_B \circ (\varphi_r)_R)$, as determinant of composite is product of determinants, it follows $det(\psi) = det((\tilde{T}_{A/R})_R)det((\varphi_r)_R)$ via [7] proposition 6 page III.112. we get $det((\varphi_r)_R) = N_{A/R}(det(\varphi_r))$.
Now we show that $det((\tilde{T}_{A/R})_R) = D^n_{Tr}(A)$, for this let $\{x_1, x_2, ..., x_n\}$ be a basis of M over A, $\{x_1^*, x_2^*, ..., x_n^*\}$ it's dual basis, and $\{y_1, y_2, ..., y_m\}$ a basis of A over R hence

$$\{x_1^* y_1, x_1^* y_2, ..., x_1^* y_m, x_2^* y_1, ..., x_2^* y_m, x_n^* y_1, ..., x_n^* y_m\}$$

is a basis of $Hom_A(M, A)$ over R and

$$\{x_1 y_1, ..., x_1 y_m, x_2 y_1, ..., x_2 y_m, x_n y_1, ..., x_n y_m\}$$

is a basis of M over R (this order of elements of bases is necessary), hence some calculations shows $det((\tilde{T}_{A/R})_R) = det((\tilde{T}_{A/R})_R(x_i^* y_j)(x_t y_k)) = det(Tr(y_j y_k)\delta_{i,t})$ thus we get a block matrix, its contain n submatrices and the discriminant of every submatrix is a exactly $D_{Tr}(A)$ hence $det((\tilde{T}_{A/R})_R) = D_{Tr}(A)^n$

$$\begin{pmatrix} Tr(y_1y_1)\delta_{1,1} & \cdots & Tr(y_my_1)\delta_{1,1} & 0 & \cdots & 0 \\ Tr(y_1y_2)\delta_{1,1} & \cdots & Tr(y_my_2)\delta_{1,1} & & & \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ Tr(y_1y_m)\delta_{1,1} & \cdots & Tr(y_my_m)\delta_{1,1} & & & \\ & & \ddots & 0 & \cdots & 0 \\ 0 & \cdots & 0 & Tr(y_1y_1)\delta_{n,n} & \cdots & Tr(y_my_1)\delta_{n,n} \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & Tr(y_1y_m)\delta_{n,n} & \cdots & Tr(y_my_m)\delta_{n,n} \end{pmatrix}.$$

∎

3.1.4 Applications

In the case of number theory if we take a tower of fields such that $K \subseteq L \subseteq F$ and consider the bilinear form $Tr_{F/L} : F \to L$, then 2.10 Corollary of [59] on page 202 is a special case of our main result.

Let $K \subset L$ be a finite extension of fields such that $[L : K] = m$, and $L = K(\alpha)$, let $A = L[X, X^{-1}]$, $B = K[X, X^{-1}]$, $C = K[X^n, X^{-n}]$, hence $C \subset B \subset A$ is a tower of graded algebra then:

$$D_C(A) = D_C(B)^n N_{B/C}(D_B(A))$$

Since $\{1, X, X^2, ..., X^{n-1}\}$ is a basis of B over C, then $D_C(B) = n^n X^{n-1}$ and $D_B(A)$ is the discriminant of the minimal polynomial of α, which we denote P, then $D_B(A) = D(P)$ hence

$$D_C(A) = (n^n X^{n-1})^m (D(P))^n.$$

Let R be a ring and $A = R[X,Y]/ < X^m + aX + b, Y^n - X >$, where $x = \overline{X}, y = \overline{Y}$ and $a, b \in R$, to compute the discriminant of A we need to compute the determinant of matrix with $m \times n$ entries, but the tower formula reduce considerably the computation, using isomorphism theorem, one can see that $R[x,y] \simeq B[Y]/ < Y^n - X >$ where $B = R[X]/ < X^m + aX + b >$, then we are under the hypothesis of the main theorem hence $D_R(A) = (D_R(B))^n N_{B/R}(D_B(A))$. It's known that $D_B(A) = disc(Y^n - X)$ and $D_R(B) = disc(X^m + aX + b)$, we have $disc(Y^n - X) = n^n X^{n-1}$ and $dics(X^m + aX + b) = (-1)^{\frac{(m-1)(m-2)}{2}}(m-1)^{(m-1)}a^m + (-1)^{\frac{m(m-1)}{2}} m^m b^{m-1}$, so we get

$$D_R(A) = ((-1)^{\frac{(m-1)(m-2)}{2}}(m-1)^{(m-1)}a^m + (-1)^{\frac{m(m-1)}{2}} m^m b^{m-1})^n N_{B/R}((n^n(X)^{n-1}))$$

computing $N_{B/R}(X)$, we found $N_{B/R}(X) = -b$ finally:

$$D_R(A) = (-1)^{\frac{n(m-1)(m-2)}{2}}((m-1)^{(m-1)}a^m + (-1)^{(m-1)} m^m b^{m-1})^n (n^{nm}(-b)^{n-1}).$$

3.2 Tower formula of Steinitz class

3.2.1 Steinitz class

Let R be a Dedekind ring. In the next Lemma we recall some properties of ideals of a Dedekind ring.

Lemma 3.2.1. *Let R be a Dedekind ring, Let I, J two fractional ideals of R, then :*

1. *If $I, J \subseteq R$. Then $I \simeq J$ if and only if $\exists a \in K$ such that $I = aJ$.*
2. *If $J \subseteq R$, Then there exists $a \in I$ such that $I^{-1}a + J = R$.*
3. *$I \oplus J \simeq R \oplus IJ$.*
4. *If $R^{n-1} \oplus I \simeq R^{n-1} \oplus J$, then $I \simeq J$, for all $n \in \mathbb{N}$ and $n \geq 2$.*

Theorem 3.2.1 ([30]). *1. Every fractional ideal is projective in R.*

2. *Let M be a nonzero projective R-module projective of finite type n and torsion free. Then $M \simeq R^{n-1} \oplus \mathfrak{a}$, where $\mathfrak{a}$ is a fractional ideal .*

Definition 3.2.1. *Let M be a nonzero projective R-module projective of finite type n and torsion free. Set $S_R(M) = \mathfrak{a}\mathcal{P}_R$, with $\mathcal{P}_R$ is the set of principal ideals. Then $S_R(M)$ is uniquely determinate and is called "Steinitz class".*

Proposition 3.2.1 ([30])**.** *Let M be a nonzero projective R-module projective of finite type n and torsion free.*

1. *$S_R(M_1 \oplus M_2) = S_R(M_1)S_R(M_2)$.*

2. *$M \simeq L$ if and only if $rang_R(M) = rang_R(L)$ and $S_R(M) = S_R(L)$.*

Let denote by $Proj_f(R)$ the category of projective modules of finite rank over R, then we define the following application:

$$\begin{array}{rccc} S_R & : & Proj_f(R) & \to & Cl(R) \\ & & M & \to & S_R(M) \end{array}$$

with kernel the set of free modules of finite type in the case where $M = \mathcal{O}_L$, let denote $S_R(\mathcal{O}_L)$ by $S_{L/K}$.

Theorem 3.2.2. *[Invariant Factor Theorem, [61], page 49.] Let M, N, two R-modules of finite type with torsion-free such that: $N \subseteq KM$, then there exists $x_1, ..., x_r$ in M, and fractional ideals $\mathfrak{b}_1, ..., \mathfrak{b}_r$, and $\mathfrak{a}_1, ..., \mathfrak{a}_s$ in R such that :*

$$M = \mathfrak{b}_1 x_1 \oplus \mathfrak{b}_2 x_2 \oplus .... \oplus \mathfrak{b}_r x_r$$

$$N = \mathfrak{b}_1\mathfrak{a}_1 x_1 \oplus \mathfrak{b}_2\mathfrak{a}_2 x_2 \oplus .... \oplus \mathfrak{b}_s\mathfrak{a}_s x_s$$

where $r = rang_R M, s = rang_R N$ and $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq ..... \supseteq \mathfrak{a}_s$, if $N \subseteq M$ then $\mathfrak{a}_i$ are an integer ideals of R.

It was shown that the notion of order ideal Ord_R (R a Dedekind ring) coincide with that of the norm of this ideal we use this result to prove the following lemma. In what follow L/K is a finite extension of $K = Fr(R)$ where R is a Dedekind ring, if $\mathfrak{a}$ is an ideal of $\mathcal{O}_L$ we denote $S_{L/K}(\mathfrak{a})$ by $S_R(\mathfrak{a})$.

Proposition 3.2.2. *Let K a number field with ring of integer R and L is a finite extension of K. Let $\mathfrak{a}$ an ideal of $\mathcal{O}_L$ then,*

$$S_R(\mathfrak{a}) = [N_{L/K}(\mathfrak{a})]S_{L/K}.$$

Proof. We use Lemma 3.2.2 ∎

Lemma 3.2.2. *Let K be a number field with ring of integer R and L a finite extension of K. Let $\mathfrak{a}$ be a ideal of $\mathcal{O}_L$ then,*

$$\mathfrak{a} \simeq R^{n-1} \oplus N_{L/K}(\mathfrak{a}).J,$$

where $[J] = S_{L/K}$.

Proof. By the Invariant Factor Theorem we have :

$$\mathcal{O}_L \simeq R^{n-1} \oplus \prod_{i=1}^{n} \mathfrak{b}_i$$

$$\mathfrak{a} \simeq R^{n-1} \oplus \prod_{i=1}^{n} \mathfrak{a}_i \prod_{i=1}^{n} \mathfrak{b}_i,$$

as $N_{L/K}(\mathfrak{a}) = Ord_R(\mathcal{O}_L/\mathfrak{a})$, and $\mathcal{O}_L/\mathfrak{a} \simeq R/\prod \mathfrak{a}_i$, hence $N_{L/K}(\mathfrak{a}) = \prod \mathfrak{a}_i$, we deduce that

$$\mathfrak{a} \simeq R^{n-1} \oplus N_{L/K}(\mathfrak{a}).J.$$

∎

Proposition 3.2.3 (Tower Formula)**.** *Let K, L and F three number fields such that , $K \subseteq L \subseteq F$, then :*

$$S_{F/K} = S_{L/K}^{[F:L]} N_{L/K}(S_{F/L}).$$

Proof. By Theorem 3.2.1 one can write :

$$\mathcal{O}_F \simeq \mathcal{O}_L^{[F:L]-1} \oplus \mathfrak{a}_1,$$

$$\mathcal{O}_L \simeq R^{[L:K]-1} \oplus \mathfrak{a}_2,$$

$$\mathcal{O}_F \simeq R^{[F:K]-1} \oplus \mathfrak{a}_3,$$

and

$$\mathfrak{a}_1 = R^{[L:K]-1} \oplus N_{L/K}(\mathfrak{a}_1)\mathfrak{a}_2.$$

Then we have :

$$\mathcal{O}_F \simeq (R^{[L:K]-1} \oplus \mathfrak{a}_2)^{[F:L]-1} \oplus R^{[L:K]-1} \oplus N_{L/K}(\mathfrak{a}_1)\mathfrak{a}_2.$$

hence :

$$\mathcal{O}_F \simeq R^{[F:K]-1} \oplus N_{L/K}(\mathfrak{a}_1)\mathfrak{a}_2^{[F:L]}.$$

in view of Theorem 3.2.1 we see that :

$$\mathfrak{a}_3 \simeq \mathfrak{a}_2^{[F:L]} N_{L/K}(\mathfrak{a}_1),$$

which complete the proof. ∎

Proposition 3.2.4. *Let K be a number field and L, F two finite extensions of K. Assume that L and F are arithmetically disjoint over K, then :*

$$S_{LF/K} = S_{L/K}^{[F:K]} S_{F/K}^{[L:K]}.$$

Proof. Observe first that $\mathcal{O}_{LF} = \mathcal{O}_L \mathcal{O}_F$, and by Theorem 3.2.1 we have :

$$\mathcal{O}_L \simeq R^{[L:K]-1} \oplus I_1$$

$$\mathcal{O}_F \simeq R^{[F:K]-1} \oplus I_2$$

and L and F are arithmetically disjoint then $\mathcal{O}_{LF} = \mathcal{O}_L \mathcal{O}_F \simeq \mathcal{O}_L \otimes \mathcal{O}_F$ and since $R^n \otimes_R R^m \simeq R^{nm}$, we have :

$$\begin{aligned}
\mathcal{O}_{LF} &\simeq (R^{[L:K]-1} \oplus I_1) \otimes_R (R^{[F:K]-1} \oplus I_2) \\
&\simeq R^{([L:K]-1)([F:K]-1)} \oplus \underbrace{I_1 \oplus \ldots \oplus I_1}_{[F:K]-1\, times} \oplus \underbrace{I_2 \oplus \ldots \oplus I_2}_{[L:K]-1\, times} \oplus I_1 I_2 \\
&\simeq R^{[L:K][F:K]-1} \oplus I_1^{[F:K]} I_2^{[L:K]} \\
&\simeq R^{[LF:K]-1} \oplus I_1^{[F:K]} I_2^{[L:K]}
\end{aligned}$$

hence $S_{LF/K} = S_{L/K}^{[F:K]} S_{F/K}^{[L:K]}$. ∎

Applying an inductive argument to former Proposition we obtain the following general case.

Proposition 3.2.5. *Let L_i be a finite extension of degree n_i of K for $i = 1, 2, \cdots, r$ and $L = L_1 L_2 \cdots L_r$, if for $i \neq j$ the extensions L_i and L_j are arithmetically disjoint, then :*

$$S_{L/K} = \prod_{i=1}^{r} S_{L_i/K}^{\frac{N}{n_i}}$$

such that $N = n_1 n_2 \cdots n_r$.

Lemma 3.2.3. *Let K be a number field and L a finite extension of K. Then the square of steinitz*

class of L over K coincides with the discriminant of L over K in the class group of K.

$$S_{L/K}^2 = [D_{L/K}].$$

Before tackling the proof, we need the following lemma.

Lemma 3.2.4. *Let R be a Dedekind ring and $\mathfrak{a}$ a fractional ideal of R then :*

$$Hom_R(\mathfrak{a}, R) \simeq \mathfrak{a}^{-1}.$$

Proof. We have the following isomorphism

$$\begin{array}{rccc} g & : & \mathfrak{a}^{-1} & \to & Hom_R(\mathfrak{a}, R) \\ & & a & \to & \widetilde{a} \end{array}$$

where $\widetilde{a}$ defined by :

$$\begin{array}{rccc} \widetilde{a} & : & \mathfrak{a} & \to & R \\ & & x & \to & ax \end{array}$$

g is a group isomorphism. We have also the following isomorphism :

$$\begin{array}{rccc} h & : & Hom_R(\mathfrak{a}, R) & \to & \mathfrak{a}^{-1} \\ & & \varphi & \to & \varphi(1) \end{array}$$

Hence $goh = Id_{Hom_R(\mathfrak{a},R)}$, therefore $hog = Id_{\mathfrak{a}^{-1}}$. ∎

Proof. (Lemma 3.2.5.) Let $\mathfrak{C}_{L/K}$ be the inverse different ideal and we claim that:

$$Hom_R(\mathcal{O}_L, R) \simeq \mathfrak{C}_{L/K}.$$

Let $d \in \mathfrak{C}_{L/K}$, we have $\phi_d(x) = Tr(dx) \in Hom_R(\mathcal{O}_L, R)$, for all x in $\mathcal{O}_L$. The following application :

$$\begin{array}{ccc} \mathfrak{C}_{L/K} & \to & Hom_R(\mathcal{O}_L, R) \\ d & \mapsto & \phi_d, \end{array}$$

is surjective, as for any element of $Hom_R(\mathcal{O}_L, R)$ is the restriction of element of $Hom_K(L, K)$ and the trace is non-degenerated hence it has the form ϕ_d, where d in L, and hence the restriction of $\mathcal{O}_L$ give an element of $Hom_R(\mathcal{O}_L, R)$, $d \in \mathfrak{C}$. as, $\mathcal{O}_L \simeq R^{n-1} \oplus \mathfrak{c}(\mathcal{O}_L)$, et $\mathfrak{C}_{L/K} = R^{n-1} \oplus N_{L/K}(\mathfrak{C}_{L/K})\mathfrak{c}(\mathcal{O}_L)$, we have also $Hom_R(\mathcal{O}_L, R) \simeq R^{n-1} \oplus \mathfrak{c}(\mathcal{O}_L)^{-1}$, as, $Hom_R(\mathfrak{c}(\mathcal{O}_L), R) \simeq \mathfrak{c}(\mathcal{O}_L)^{-1}$,

then, $\mathfrak{c}(\mathcal{O}_L)^{-1} \simeq N_{L/K}(\mathfrak{C}_{L/K})\mathfrak{c}(\mathcal{O}_L)$. This prove that, $\mathfrak{c}(\mathcal{O}_L)^2 \simeq D_{L/K}$, and hence

$$S^2_{L/K} = [D_{L/K}].$$

∎

3.2.2 Steinitz module and index

Let α in L integer over R such that $L = K(\alpha)$, where $P(X)$ its minimal polynomial , as R is integrally closed we have $P(X) \in R[X]$. Let $Disc_R(P)$ the principal ideal generated by the resultant of P and P' ,$(disc_R(P) = (Res(P, P'))R,$ P' its derivative $P)$, to α we associate the ideal $[\mathcal{O}_L : R[\alpha]]$ called the index of α and denoted by $Ind_R(\alpha)$.

The following results proved in [18], and is based on a property of the discriminant established in [27] (or [30]) which asserts that for two projective R-algebra A and B of constant rank such that $A \subseteq B$ we have $D_{A/R} = [B : A]^2_R D_{B/R}$.)

Theorem 3.2.3. *With the above notations we prove*

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

Before tackling the proof, we need the following Lemma.

Lemma 3.2.5. *Let $P(X)$ be a monic polynomial of degree n in $R[X]$, let $M \in \mathscr{M}_n(R)$ be the companion matrix of P, and set $N = (Tr(M^{i+j-2}))$, $i, j = 1...n$, then :*

$$Disc_R(P) = (det(N))R.$$

Proof. let $\alpha_1, \alpha_2, ..., \alpha_n$, be the roots of P in an algebraic closure of K, for $l \geq 0$, we have $Tr(M^l) = \sum_{k=1}^{n} \alpha_k^l$, as $\alpha_1^l, ..., \alpha_n^l$, are the eigenvalues of M^l, Let $V = V(\alpha_1, \alpha_2, ..., \alpha_n)$ be the Vandermonde matrix attached to $(\alpha_1, \alpha_2, ..., \alpha_n)$, then we have :

$$det(V) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Furthermore, the (i, j) entry of V est α_i^{j-1}, and for ${}^tV$ is α_j^{i-1}, then we see that the (i, j) entry of the product ${}^tVV$, is :

$$\sum_{k=1}^{n} \alpha_k^{i-1} \alpha_k^{j-1} = \sum_{k=1}^{n} \alpha_k^{i+j-2} = Tr(M^{i+j-2})$$

then ${}^tVV = N$, and hence $det(N) = det(V)^2 = \prod_{1\leq i,j\leq n}(\alpha_i - \alpha_j)^2$, as desired. ∎

Proof. (Theorem 3.2.3)
We have

$$D_{R[\alpha]/R} = (Ind_R(\alpha))^2 D_{\mathcal{O}_L/R}.$$

as $R[\alpha] \subseteq \mathcal{O}_L$, are finitely generated projective R-modules.
Let

$$\begin{array}{rccc} \phi_\alpha & : & R[X] & \to & L \\ & & f(X) & \mapsto & f(\alpha) \end{array}$$

the ring homomorphism. Observe that $Ker(\phi_\alpha)$ is a prime ideal of $R[X]$ (L is a field), since R is integrally closed , $Ker(\phi_\alpha)$ is principal and is generated by P, hence :

$$R[\alpha] \simeq R[X]/PR[X].$$

Let $\mathcal{B} = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ be an R-basis of $R[\alpha]$, It follows then that ,

$$D_{R[\alpha]/R} = d_R(1, \alpha, \alpha^2, ..., \alpha^{n-1})R$$

for any $x \in R[\alpha]$ we can define an homomorphism $\widetilde{x}$ of $R[\alpha]$ by:

$$\begin{array}{rccc} \widetilde{x} & : & R[\alpha] & \to & R[\alpha] \\ & & y & \mapsto & xy \end{array}$$

Since $R[\alpha]$ is a commutative free R-algebra, each endomorphism is represented by a matrix in $\mathscr{M}_n(R)$. And hence $\widetilde{x^k} = \widetilde{x}^k$ $k \geq 1$ as :

$$\begin{array}{ccc} R[\alpha] & \to & End_R(R[\alpha]) \\ x & \mapsto & \widetilde{x} \end{array}$$

is a ring homomorphism. Let A be the matrix representing $\widetilde{\alpha}$, then A^k is the matrix representing $\widetilde{\alpha}^k$ and $Tr_{R[\alpha]/R}(\alpha^k) = Tr(A^k)$, $d_R(1, \alpha, \alpha^2, ..., \alpha^{n-1}) = det(Tr_{R[\alpha]/R}(\alpha^{i+j})) = det(Tr(A^{i+j}))$, where $0 \leq i, j \leq n-1$ It follows that $d_R(1, \alpha, \alpha^2, ..., \alpha^{n-1}) = \prod_{1\leq i,j\leq n}(\alpha_i - \alpha_j)^2$ as P is the characteristic polynomial of A,then $D_{R[\alpha]/R} = disc_R(P)$, this complete the proof. ∎

Corollary 3.2.1. *If h_K is odd, we have the inverse of the steinitz module coincides with the class of $Ind_R(\alpha)$ in the field of class of K.*

Proof. By Theorem 3.2.3 we have :

$$[Disc_R(P)] = [Ind_R(\alpha)]^2[D_{\mathcal{O}_L/R}].$$

$Disc_R(P)$ is a principal ideal of R, then $[(Ind_R(\alpha))]^{-2} = [D_{\mathcal{O}_L/R}]$, hence $S^2_{L/K} = [(Ind_R(\alpha))]^{-2}$, this complete the proof. ∎

Proposition 3.2.6. *Let L be a Galois extension of K with Galois group $G = Gal(L/K)$ where K is a number field, and $\alpha \in \mathcal{O}_L$ is a generator of a normal basis of L/K. We have $R[G].\alpha \subseteq \mathcal{O}_L$. If h_K is odd then $S_{L/K} = [I_G(\alpha)]^{-1}$.*

Proof. It is already known that $D_R(R[G].\alpha) = [\mathcal{O}_L : R[G].\alpha]^2 D_{L/K}$, and

$$D_R(R[G].\alpha) = d_R(\alpha, \sigma_1(\alpha), ..., \sigma_{[L:K]-1}(\alpha))$$

then $d_R(\alpha, \sigma_1(\alpha), ..., \sigma_{[L:K]-1}(\alpha))R = I_G(\alpha)^2 D_{L/K}$ by Lemma 3.2.3 we see that $S^2_{L/K} = [I_G]^{-2}$ as h_K is odd, then $S_{L/K} = [I_G(\alpha)]^{-1}$. ∎

3.2.3 Steinitz class of Kummer extension

Theorem 3.2.4. *Let L be a finite cyclic extension of K. Suppose that L/K is tamely ramified. Let $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$ and $\alpha^n = a \in K$ and let $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_n$ be the associated ideals to aR. Then the steinitz class $S_{L/K}$ of L/K is $[\prod_{i=1}^n \mathfrak{b}_i]^{-1}$.*

Proof. Let $P(X) = X^n - a$ be the irreducible polynomial of α and $a\mathcal{O}_L = \prod_{i=1}^n \mathfrak{a}_i^i$ the ascending power decomposition, We have that

$$Disc(P)\mathcal{O}_L = n^n a^{n-1}\mathcal{O}_L = n^n \prod_{i=1}^n \mathfrak{a}_i^{in}$$

and since L/K is tamely ramified

$$D_{L/K} = \prod_{i=1}^n \mathfrak{a}_i^{n-(m\wedge i)}.$$

The by discriminant-index formula,

$$S^2_{L/K} = [Ind_R(\alpha)]^{-2} = \left[n^n \prod_{i=1}^n \mathfrak{a}_\mathfrak{i}^{i(n-1)-n+(n\wedge i)} \right]^{-2}$$

using 2.2.4, it follows that

$$S_{L/K}^2 = \left[n^n \prod_{i=0}^{n-1} \mathfrak{b}_i^2 \right]^{-2}$$

. Then we have two cases:

- If n is even then we get

$$S_{L/K} = \left[n^{\frac{n}{2}} \prod_{i=0}^{n-1} \mathfrak{b}_i \right]^{-1} = \left[\prod_{i=0}^{n-1} \mathfrak{b}_i \right]^{-1}.$$

- If n is odd then we have that

$$m\mathcal{O}_L = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \mathcal{O}_L = (1-\zeta_{p_1})^{(p_1-1)a_1} (1-\zeta_{p_2})^{(p_2-1)a_2} \cdots (1-\zeta_{p_r})^{(p_r-1)a_r} \mathcal{O}_F$$

  hence

$$S_{L/K} = \left[(1-\zeta_{p_1})^{(p_1-1)a_1} (1-\zeta_{p_2})^{(p_2-1)a_2} \cdots (1-\zeta_{p_r})^{(p_r-1)a_r} \prod_{i=1}^{n-1} \mathfrak{b}_i \right]^{-1} = \left[\prod_{i=1}^{n-1} \mathfrak{b}_i \right]^{-1}.$$

∎

3.3 Discriminant of compositum of number fields

Let $L = E.F$ be an extension such that E and F are linearly disjoint extensions then $L \simeq E \otimes_K F$, hence

$$\mathcal{O}_E.\mathcal{O}_F \simeq \mathcal{O}_E \otimes_R \mathcal{O}_F \tag{3.1}$$

as $\mathcal{O}_E.\mathcal{O}_F \subseteq \mathcal{O}_L$, then by the discriminant-index formula we obtain

$$[\mathcal{O}_L : \mathcal{O}_E.\mathcal{O}_F]_R^2 D_R(\mathcal{O}_L) = D_R(\mathcal{O}_E.\mathcal{O}_F) \tag{3.2}$$

and according to 3.1, and using the next Proposition 3.3.1, we get

$$D_R(\mathcal{O}_E.\mathcal{O}_F) = D_R(\mathcal{O}_E)^{[L:F]} \times D_R(\mathcal{O}_F)^{[L:E]} \tag{3.3}$$

Proposition 3.3.1. *Let S and T be two projective R-algebra of ranks n, m respectively. Then*

$$D_R(S \otimes_R T) = D_R(S)^m D_R(T)^n$$

Proof. See Proposition 3 [27]. ∎

Combining the forgoing results, we deduce the following Theorem.

Theorem 3.3.1. *Let R be a Dedekind ring, K its quotient field. Let $L = E.F$ be an extension such that E and F are linearly disjoint. Then*

$$D_R(\mathcal{O}_L)[\mathcal{O}_L : \mathcal{O}_E.\mathcal{O}_F]_R^2 = D_R(\mathcal{O}_E)^{[L:E]} \times D_R(\mathcal{O}_F)^{[L:E]}. \tag{3.4}$$

In particular, the equality $\mathcal{O}_L = \mathcal{O}_E\mathcal{O}_F$ is equivalent to $D_R(\mathcal{O}_L) = D_R(\mathcal{O}_E)^{[L:E]} \times D_R(\mathcal{O}_F)^{[L:E]}$.

Proof. It follows from 3.2 and 3.3. ∎

Chapter 4

Monogenity of relative extension

4.1 Dedekind criterion

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 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 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 ;

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

We denote by $\mathrm{Spec}(R)$, 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:

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

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 $\mathfrak{F}ib_R(\mathfrak{p})$.

Let K be a nonzero commutative field and v be a valuation on K. Let $P = a_0 + a_1X + \ldots + a_nX^n \in K[X]$. 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. Let first present a new simple version of Dedekind Criterium in global case:

Theorem 4.1.1 (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 $P = \mathrm{Irrd}(\alpha, R) \in R[X]$ be the monic irreducible polynomial of α. Let 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 $\bar{P} = \prod_{i=1}^{r} \bar{P_i^{l_i}}$ 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 $v_\mathfrak{p}$ be the $\mathfrak{p}-$adic discrete valuation associated to p. Let v_G be the Gauss valuation on $K[X]$ associated to $v_\mathfrak{p}$. Then $\mathfrak{p}$ doesn't divide the index ideal $Ind_R(\alpha)$ if and only if $v_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$*

Proof. See [21].

4.2 Monogenicity of relative cubic-power pure extensions

4.2.1 Monogeneity of relative cubic-power pure extension - local case

Since we are going to apply the Dedekind criterium recalled in introduction, we begin by formulate our first main result in case of discrete valuation ring as part of simplifying the general case.

Theorem 4.2.1. *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 $P(X) = X^{3^n} - \beta$ 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. Then*

1. *If $v_\mathfrak{p}(\beta) \geq 1$ then α is PBG of $L = K$ if and only if $v_\pi(\beta) = 1$.*
2. *If $v_\pi(\beta) = 0$, then the following properties hold:*
   (a) *If $c_k = 3$, then α is PBG of L/K if and only if*

$$v_\pi(\beta^{m-1} - 1) = 1 \; if \; f \geq n \tag{4.1}$$

$$v_\pi(\beta^{m^{r+1}-1} - 1) = 1 \; if \; f < n \; and \; n - rf \leq f \tag{4.2}$$

Where r is the smallest positif integer such that $n - rf \leq f$.

(b) If $c_k \neq 3$, then α is PBG of L/K.

Proof.

1. First we note that $\overline{P} = \overline{X}^{3^n}$ *modulo* $\mathfrak{p}$, then the remainder of the Euclidean division of P by X is $r(X) = \beta$. So, α is a PBG if and only if $v_\pi(\beta) = 1$.

2. We assume that $v_\mathfrak{p}(\beta) = 0$.

   (a) Since $c_k = 3$, we have $m = 3^f$ for some integer f. Now by reducing P modulo the unique prime ideal πR which lies above $3R$, yields:

$$\begin{aligned} \overline{P(X)} &= \overline{X}^{3^n} - \overline{\beta} \ mod(\pi R) \\ &= \overline{X}^{3^n} - \overline{\beta}^{3^f} mod(\pi R) \ (Since\, \beta^m \equiv \beta \ modulo\, \pi\,.) \end{aligned} \tag{4.3}$$

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

   - If $f \geq n$, the formula 4.3 can be written as:

$$\begin{aligned} \overline{P(X)} &\equiv \overline{X}^{3^n} - \overline{\beta}^{3^f} mod(\pi R) \\ &\equiv \left(\overline{X} - \overline{\beta}^{3^{f-n}}\right)^{3^n} mod(\pi R). \end{aligned}$$

     Let us denote by R_1, the remainder of the Euclidean division of P by $X - \beta^{3^{f-n}}$. Then, $R_1 = P(\beta^{3^{f-n}}) = \left(\beta^{3^{f-n}}\right)^{3^n} - \beta = \beta^{3^f} - \beta$. It follows immediately that α is PBG if and only if $v_\pi(\beta^{m-1} - 1) = 1$.

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

$$\begin{aligned} \overline{P(X)} &\equiv \overline{X}^{3^n} - \overline{\beta} \ mod\, \pi R \\ &\equiv \left(\overline{X}^{3^{n-rf}} - \overline{\beta}\right)^{3^{rf}} \ mod\, \pi R \\ &\equiv \left(\overline{X}^{3^{n-rf}} - \overline{\beta}^{3^f}\right)^{3^{rf}} \ mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{\beta}^{3^{f-n+rf}}\right)^{3^{rf}.3^{n-rf}} \ mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{\beta}^{3^{(r+1)f-n}}\right)^{3^n} \ mod\, \pi R. \end{aligned}$$

     Then $R_2 = \beta^{m^{r+1}} - \beta$, is the remainder of the Euclidean division of P by $X -$

$\beta^{3^{(r+1)f-n}}$. So, α is a PBG if and only if $v_\pi(\beta^{m^{r+1}} - \beta) = 1$, which completes the proof, since $v_\pi(\beta) = 0$.

(b) For the second case: 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 $P'(X) = 3^n X^{3^n-1}$ we get $\alpha = 0$ which means that $\beta \in \mathfrak{p}$ and complete the proof in this case.

∎

We are going in table 1 to schematizes our results: We denote

Table 4.1: 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>$c_k \neq 3$</td><td colspan="2">$c_k = 3$</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>

Remark 4.2.1. *1. We can replace the two properties 4.1 and 4.2 with the following:*

$$v_\pi(\beta^{m^{r+1}-1} - 1) = 1 \tag{4.4}$$

Where r is the smallest positif integer such that $n - rf \leq f$.

2. In the case of the characteristic of k equal to 3, we can checks that the condition $v_\pi(\beta^{m-1} - 1) = 1$, is equivalent to: β is not a 3-power modulo π^2

4.2.2 Monogeneity of relative cubic-power pure extension - Dedekind case

Theorem 4.2.2. *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 $P = X^{3^n} - \beta \in R[X]$ 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 $\mathfrak{q} \in \mathfrak{Fib}_R(3)$, then α is a PBG of L over K if and only if β is square free.

2. *Let $\mathfrak{F}ib_R(3) - V(\beta R) = \{\mathfrak{p}_1; ...; \mathfrak{p}_h\}$. 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 $R/\mathfrak{p}_i$. Then α is a PBG of L over K if and only if " β is square free" and for all $i \in \{1; ....; h\}$*

$$v_i(\beta^{m_i-1} - 1) = 1 \ if \ f_i \geq n \tag{4.5}$$

$$v_i(\beta^{m_i^{r_i+1}-1} - 1) = 1 \ if \ f_i < n \ and \ n - r_i f_i \leq f_i \tag{4.6}$$

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 $f_i < n$.

Proof. Our proof starts with the observation that the discriminant of $P(X)$ is $Disc_R(P) = 27^{p^2}\beta^{3^p-1}$, then the set $S_P = V(\beta\, R) \cup (\mathfrak{F}ib_R(3) - V(\beta\, R))$ 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. We may then use Theorem 4.2.1.

1. Our condition in the first case implies that $S_P = V(\beta\, R)$. Let $\mathfrak{p} \in V(\beta R)$, then by Theorem 4.2.1, 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 $charR/\mathfrak{p}_i = 3$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to 3 since $3R \subset \mathfrak{p}_i$). According to the second case in Theorem 4.2.1, we can conclude that $\mathfrak{p}_i$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $v_i(\beta^{m_i^{r_i+1}-1} - 1) = 1$ 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.

∎

Remark 4.2.2. *Theorem 4.2.2 is a generalization in relative case of p-power extension for $p = 3$, studied in [19] Theorem 4.2.*

4.2.3 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 $\mathcal{O}_K$ of K is $\mathcal{O}_K = \mathbb{Z}[t]$ such that:

$$t = \begin{cases} \sqrt{d} & if \ d \equiv 2, 3 \ \text{modulo} \ 4 \\ \frac{1+\sqrt{d}}{2}, & if \ d \equiv 1 \ \text{modulo} \ 4. \end{cases} \tag{4.7}$$

And the discriminant is given by:

$$D_{K/\mathbb{Q}} = \begin{cases} 4d, & if\ d \equiv 2,\ 3\ \text{ modulo }\ 4 \\ d, & if\ d \equiv 1\ \text{ modulo }\ 4. \end{cases} \tag{4.8}$$

Theorem 4.2.3. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free $d \equiv 0$ modulo 3. Let $L = K(\alpha)$ such that $\alpha^{3^n} = b = \sqrt{d} + 1$ ($n \in \mathbb{N}^*$), furthermore we assume that the ideal $(\sqrt{d}+1)$ is square free in $\mathcal{O}_K$, then L/K is monogenic. In this case we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}.$$

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

Proof. First of all we note that $v_{\mathfrak{p}}(b) = 0$ where $3O_K = \mathfrak{p}^2$, it is known that the cardinality of $\mathcal{O}_K/\mathfrak{p}$ is 3 since the residual degree of $\mathfrak{p}$ is $f = 1$ then two cases arises:

1. If $n = 1$, then by Theorem 4.2.2, L/K is monogenic if and only if $v_{\mathfrak{p}}(b^2 - 1) = 1$, we have $b^2 - 1 = d + 2\sqrt{d} = \sqrt{d}(\sqrt{d} + 2)$. Since $v_3(d) = 1$ (d square free and $d \equiv 0$ modulo 3) then, $v_{\mathfrak{p}}(\sqrt{d}) = \frac{1}{2}v_{\mathfrak{p}}(d) = \frac{1}{2}e_{K/\mathbb{Q}}v_3(d) = 1$. Since otherwise by property of dominance principle $v_{\mathfrak{p}}(\sqrt{d}+2) = 0$. So, we can deduce that $v_{\mathfrak{p}}(b^2 - 1) = 1$.

2. If $n \geq 2$, it follows by Theorem 4.2.2, that α is a power basis generator if and only if $v_{\mathfrak{p}}(b^{3^{n-1}} - 1) = 1$ we have that

$$b^{3^{n-1}} - 1 = \sum_{k=1}^{3^n-1} \binom{k}{3^n - 1} (\sqrt{d})^k = \sqrt{d} \left(\sum_{k=1}^{3^n-1} \binom{k}{3^n - 1} (\sqrt{d})^{k-1} \right),$$

   By property of dominance principle, it is easy to check that

$$v_{\mathfrak{p}}(\sum_{k=1}^{3^n-1} \binom{k}{3^n - 1} (\sqrt{d})^{k-1}) = 0$$

   and so,

$$v_{\mathfrak{p}}(b^{3^{n-1}} - 1) = v_{\mathfrak{p}}(\sqrt{d}) + v_{\mathfrak{p}}(\sum_{k=1}^{3^n-1} \binom{k}{3^n - 1} (\sqrt{d})^{k-1}) = 1.$$

Satisfying the conditions of Theorem 4.2.2, so that L is monogenic, let denote $\{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}\}$ such RMIB. Using [20, Lemma 3.1] it's obvious that

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2 \cdot 3^n$. ∎

Theorem 4.2.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free, $3 \nmid d$ and $d \equiv 2$ modulo 9. Let $L = K(\alpha)$ such that $\alpha^{3^n} = b = \sqrt{d} + 1$ ($n = 1, 2$), furthermore we assume that the ideal $(\sqrt{d} + 1)$ is square free in $\mathcal{O}_K$ and $3\mathbb{Z}$ is inert in $\mathcal{O}_K$, then L/K is monogenic. In this case we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}.$$

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

Proof. The ideal $3\mathcal{O}_K = \mathfrak{p}$ is prime in $\mathcal{O}_K$. We claim that $v_\mathfrak{p}(b+1) = 0$, we have $v_\mathfrak{p}(b^2 - 2b - 1) = v_\mathfrak{p}(d-2) \geq 1$ then $v_\mathfrak{p}(b^2 - 2b) = 0$ and $v_\mathfrak{p}(b-2) = 0$ (since $v_\mathfrak{p}(b) = 0$), therefore $v_\mathfrak{p}(b+1) = v_\mathfrak{p}(b-2+3) = inf(v_\mathfrak{p}(b-2), v_\mathfrak{p}(3)) = 0$.
By Theorem 4.2.2 it is known that L/K is monogenic if and only if $v_\mathfrak{p}(b^8 - 1) = 1$. we already have that $b^8 - 1 = \sqrt{d}(b^7 + b^6 + b^5 + \ldots + 1)$, put $h = b^7 + b^6 + b^5 + \ldots + 1$, expressing h as a polynomial in $\alpha = d - 2$, we get

$$h = \underbrace{(b+7)\alpha^3}_{A} + \underbrace{(34b+70)\alpha^2}_{B} + \underbrace{(194b+182)\alpha}_{C} + \underbrace{(288b+120)}_{D}.$$

we calculate the valuation of every term of h,

- $v_\mathfrak{p}(D) = 1$ since $v_\mathfrak{p}(120) = 1$ and $v_\mathfrak{p}(288b) = 2$.
- $v_\mathfrak{p}(C) = v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(194(b+1) - 9) = v_\mathfrak{p}(\alpha)$ since $v_\mathfrak{p}(9) = 2$ and $v_\mathfrak{p}(194(b+1)) = 0$.
- $v_\mathfrak{p}(B) = 2v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(34(b+1) + 36) = 2v_\mathfrak{p}(\alpha) + 0$ since $v_\mathfrak{p}(36) = 2$ and $v_\mathfrak{p}(34(b+1)) = 0$.
- $v_\mathfrak{p}(A) = 3v_\mathfrak{p}(\alpha) + v_\mathfrak{p}((b+1) + 6) = 3v_\mathfrak{p}(\alpha) + 0$ since $v_\mathfrak{p}(b+1) = 0$ and $v_\mathfrak{p}(6) = 1$.

As we assumed that $d \equiv 2$ modulo 9, $v_\mathfrak{p}(\alpha) \geq 2$ which means that $3v_\mathfrak{p}(\alpha) > 2v_\mathfrak{p}(\alpha) > v_\mathfrak{p}(\alpha) > v_\mathfrak{p}(D)$ then $v_\mathfrak{p}(A) > v_\mathfrak{p}(B) > v_\mathfrak{p}(C) > v_\mathfrak{p}(D) = 1$, as a result we get $v_\mathfrak{p}(b^8 - 1) = 1$, thus L/K is monogenic. Let denote $\{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}\}$ such RMIB. Using [20, Lemma 3.1] it's obvious that

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2 \cdot 3^n$. ∎

Corollary 4.2.1. *With previous conditions in Theorem 4.2.3 and Theorem 4.2.4, the discriminant $D_{L/\mathbb{Q}}$ is given by:*

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

Proof. Since L/K is monogenic we obtain $D_{L/K} = (3^n)^{3^n}\beta^{3^n-1}$, then $N_{K/\mathbb{Q}}(D_{L/K}) = 3^{2n.3^n}N_{L/K}(\beta)$ and the norm of $\sqrt{d}+1$ is $N_{K/\mathbb{Q}}(\beta) = 1-d$, by discriminant tower formula ($D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K})(D_{K/\mathbb{Q}})^{[L:K]}$), it follows that:

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

∎

Remark 4.2.3. *The number field $L/\mathbb{Q}$ is not seen as composite fields which split algebraically or arithmetically.*

4.3 Monogenicity of some relative cubic-power non-pure extensions

4.3.1 Monogeneity of relative cubic-power extension - local case

We start by studying local case, which deal the monogeneity of $L = K(\alpha)$ over its subfield K where α is a root of a monic irreducible polynomial of the form

$$P(X) = X^{3^n} + a\,X^{3^s} - b \in O_K[X]\ with\ n\ >\ s\ and\ n,\ s \in \mathbb{N}.$$

Theorem 4.3.1. *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 $v_\pi = v_\mathfrak{p}$ be the $\mathfrak{p}-$adic discrete valuation associated to $\mathfrak{p}$. Let $\alpha \in L$ be a primitive element of L which is integral over R and $P(X) = X^{3^n} + aX^{3^s} - b$ its monic irreducible polynomial in $R[X]$ such that $n > s$ and $v_\mathfrak{p}(a) \geq 1$. We denote by c_k (resp. $m = c_k^f$) the characteristic (resp. the cardinality) of the finite residual field k. Then*

1. *If $v_\mathfrak{p}(b) \geq 1$ then α is PBG of L/K if and only if $v_\pi(b) = 1$.*
2. *If $v_\mathfrak{p}(b) = 0$, then the following properties hold:*

(a) *If* $c_k = 3$, *then* α *is* PBG *of* L/K *if and only if* $v_\pi(b^{m-1} + ab^{3^{f-n+s}-1} - 1) = 1$, *or* $v_\pi(b^{m^{r+1}-1} + ab^{3^{(r+1)f-n+s}-1} - 1) = 1$ *according to the values of* n *and* f.

(b) *If* $c_k \neq 3$, *then* α *is* PBG *of* L/K.

Proof. 1. First we note that $\overline{P} = \overline{X}^{3^n}$ *modulo* $\mathfrak{p}$, then 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. From now we make the assumption $v_\mathfrak{p}(b) = 0$.

(a) Assume that we start with $c_k = 3$, then by reducing P modulo the prime ideal πR of R which contains $3R$, we get:

$$\begin{aligned}\overline{P(X)} &= \overline{X}^{3^n} + a\overline{X}^{3^s} - \overline{b} \bmod \pi R \\ &= \overline{X}^{3^n} - \overline{b}^{3^f} \bmod \pi R \ (\textit{Since } b^m \equiv b \textit{ modulo } \pi \textit{ and } m = 3^f.)\end{aligned}$$

For the rest we must be careful to distinguish two cases

- If $f \geq n$ then:

$$\begin{aligned}\overline{P(X)} &\equiv \overline{X}^{3^n} - \overline{b}^{3^f} \bmod \pi R \\ &\equiv \left(\overline{X} - \overline{b}^{3^{f-n}}\right)^{3^n} \bmod \pi R.\end{aligned}$$

Hence, we can consider the Euclidean division of P by $X - b^{3^{f-n}}$ then the remainder $R_1(X)$ is given as follows $R_1(X) = P(b^{3^{f-n}}) = \left(b^{3^{f-n}}\right)^{3^n} + a\left(b^{f-n}\right)^{3^s} - b = b^{3^f} + ab^{3^{f-n+s}} - b$. Hence α is PGB if and only if $v_\pi(b^m + ab^{3^{f-n+s}} - b) = 1$ and by $v_\mathfrak{p}(b) = 0$, the last condition becomes $v_\pi(b^{m-1} + ab^{3^{f-n+s}-1} - 1) = 1$.

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

$$\begin{aligned}\overline{P(X)} &\equiv \overline{X}^{3^n} - \overline{b} \bmod \pi R \\ &\equiv \left(\overline{X}^{3^{n-rf}} - \overline{b}\right)^{3^{rf}} \bmod \pi R \\ &\equiv \left(\overline{X}^{3^{n-rf}} - \overline{b}^{3^f}\right)^{3^{rf}} \bmod \pi R \\ &\equiv \left(\overline{X} - \overline{b}^{3^{f-n+rf}}\right)^{3^{rf}.3^{n-rf}} \bmod \pi R \\ &\equiv \left(\overline{X} - \overline{b}^{3^{(r+1)f-n}}\right)^{3^n} \bmod \pi R.\end{aligned}$$

Hence, we can consider the Euclidean division of P by $X - b^{3^{(r+1)f-n}}$ then the remainder $R_2(X)$ is given as follows $R_2(X) = P(b^{3^{(r+1)f-n}}) = \left(b^{3^{(r+1)f-n}}\right)^{3^n} + a\left(b^{3^{(r+1)f-n}}\right)^{3^s} - b = b^{3^{(r+1)f}} + ab^{3^{(r+1)f-n+s}} - b$. Hence α is PGB if and only if $v_\pi(b^{m^{r+1}} + ab^{3^{(r+1)f-n+s}} - b) = 1$ and by $v_\mathfrak{p}(b) = 0$, the last condition becomes $v_\pi(b^{m^{r+1}-1} + ab^{3^{(r+1)f-n+s-1}} - 1) = 1$.

(b) Since $b \in R\backslash\mathfrak{p}$, it follows that P is a separable polynomial in residual field k. Otherwise, if P has α as a double root, then from $P'(X) = 3^n\alpha^{3^n-1} = 0$ we get $\alpha \equiv 0 \ mod\, \mathfrak{p}$ which means that $b \in \mathfrak{p}$ and complete the proof in this case.

∎

We are going in table 1 to schematizes our results: We denote $T_1 = b^{m-1} + ab^{3^s-1} - 1$ and $T_2 = v_\pi(b^{m^{r+1}-1} + ab^{3^{(r+1)f-n+s-1}} - 1) = 1$.

Table 4.2: monogeneity in local case

$v_\mathfrak{p}(b) \geq 1$	α is PBG iff $v_\pi(b) = 1$		
$v_\mathfrak{p}(b) = 0$	$c_k \neq 3$	$c_k = 3$	
	α is PBG	$f \geq n$	$f < n$
		α is a PBG iff $v_\pi(T_1) = 1$	α is a PGB iff $v_\pi(T_2) = 1$

4.3.2 Monogeneity of relative cubic-power extension - Dedekind case

Another class of fields which we can studying the monogeneity is the class of non-pure cubic fields, defined by the monic polynomial $P(X) = X^n - aX^k + b$ satisfying some conditions given in consequence 4.3.1 or Theorem 4.3.2.

First, we show the following lemma which generalizes the one given in [71]:

Lemma 4.3.1. *Let R be a commutative integral domain containing $\mathbb{Z}$, K its field of fractions of characteristic 0. Let consider the polynomial $P(x) = x^n + ax^k + b$ of degree n in $R[X]$, where $n > k > 0$. If $d = (n,\ k)$, then:*

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

Proof. For simplicity of notation, we let $\mathfrak{R}$ stand for the resultant, then for any polynomial P of degree n:

$$\begin{aligned} disc_R(P) &= (-1)^{n(n-1)/2}\mathfrak{R}(f', f) = (-1)^{n(n-1)/2}\mathfrak{R}(nx^{n-1} + kax^{k-1},\ x^n + ax^k + b) \\ &= (-1)^{n(n-1)/2}(-1)^{n(n-1)}\mathfrak{R}(\ x^n + ax^k + b, nx^{n-1} + kax^{k-1}) \text{ by } \mathfrak{R}(f,\ g) = (-1)^{\deg f.\deg g}\mathfrak{R}(g, f) \\ &= (-1)^{n(n-1)/2}\mathfrak{R}(\ x^n + ax^k + b, nx^{n-1} + kax^{k-1}). \end{aligned} \tag{4.9}$$

Therefore,

$$\begin{aligned} disc_R(P) &= (-1)^{n(n-1)/2}\mathfrak{R}(x^n + ax^k + b, x^{k-1})R(x^n + ax^k + b, nx^{n-k} + ka), \\ &\quad by\ \mathfrak{R}(f_1f_2,\ g) = \mathfrak{R}(f_1,\ g)\mathfrak{R}(f_2,\ g) \\ &= (-1)^{n(n-1)/2}b^{k-1}\mathfrak{R}(x^n + ax^k + b, nx^{n-k} + ka) \text{ by } \mathfrak{R}(f, x^m) = f(0)^m \\ &= (-1)^{n(n-1)/2}n^nb^{k-1}T \text{ by } \mathfrak{R}(f,\ a) = a^{\deg f}.\ Where\ T = \mathfrak{R}(x^n + ax^k + b, x^{n-k} + kn^{-1}a) \end{aligned} \tag{4.10}$$

Now, It is easily seen that $x^n + ax^k + b = x^k(x^{n-k} + n^{-1}ka) + a(1 - n^{-1}k)x^k + b$. So by using $\mathfrak{R}(f,\ g)\ = b^{\deg f - \deg r}\mathfrak{R}(r,\ g)$ where b is the leading coefficient of g and $\ f = gq + r$. we get

$$\begin{aligned} T &= \mathfrak{R}(a(1 - n^{-1}k)x^k + b\,x^{n-k} + kn^{-1}a) \\ &= \mathfrak{R}(a(1 - n^{-1}k)(x^k + \frac{b}{a(1 - n^{-1}k)}), x^{n-k} + n^{-1}ka\ ) \\ &= \mathfrak{R}(x^{n-k} + kn^{-1}a, a(1 - n^{-1}k)\ )\mathfrak{R}(x^k + \frac{b}{a(1 - n^{-1}k)}, x^{n-k} + kn^{-1}a) \\ &= (a(1 - n^{-1}k))^{n-k}\mathfrak{R}(x^k + \frac{b}{a(1 - n^{-1}k)}, x^{n-k} + kn^{-1}a\ ) \\ &= a^{n-k}(\frac{n-k}{n})^{n-k}(-1)^{n-k}[(\frac{-b}{a(1 - n^{-1}k)})^{\frac{n-k}{d}} - (-\frac{ka}{n})^{\frac{k}{d}}]^d \text{ by } \mathfrak{R}(x^r - \alpha,\ x^s - b) = (-1)^s[\alpha^{s_1} - b^{r_1}]^d \\ &= [a^{\frac{n-k}{d}}(\frac{n-k}{n})^{\frac{n-k}{d}}(-1)^{\frac{n-k}{d}}(\frac{-b.n}{a(n-k)})^{\frac{n-k}{d}} - a^{\frac{n-k}{d}}(\frac{n-k}{n})^{\frac{n-k}{d}}(-1)^{\frac{n-k}{d}}(-\frac{ka}{n})^{\frac{k}{d}}]^d \\ &= [b^{\frac{n-k}{d}} - (-1)^{\frac{n}{d}}(k)^{\frac{k}{d}}a^{\frac{n}{d}}(n-k)^{\frac{n-k}{d}}n^{-\frac{n}{d}}]^d \end{aligned} \tag{4.11}$$

Finally,

$$\begin{aligned} disc_R(P) &= (-1)^{n(n-1)/2}n^nb^{k-1}[b^{\frac{n-k}{d}} - (-1)^{\frac{n}{d}}(k)^{\frac{k}{d}}a^{\frac{n}{d}}(n-k)^{\frac{n-k}{d}}n^{-\frac{n}{d}}]^d \\ &= (-1)^{n(n-1)/2}b^{k-1}[n^{\frac{n}{d}}b^{\frac{n-k}{d}} - n^{\frac{n}{d}}(-1)^{\frac{n}{d}}(k)^{\frac{k}{d}}a^{\frac{n}{d}}(n-k)^{\frac{n-k}{d}}n^{-\frac{n}{d}}]^d \\ &= (-1)^{n(n-1)/2}b^{k-1}[n^{\frac{n}{d}}b^{\frac{n-k}{d}} - (-1)^{\frac{n}{d}}(k)^{\frac{k}{d}}a^{\frac{n}{d}}(n-k)^{\frac{n-k}{d}}]^d. \end{aligned} \tag{4.12}$$

∎

Corollary 4.3.1. *Let consider the particular polynomial $P = x^n + ax^k - b \in R[X]$ of degree*

$n = 3^t k$ with $k = 3^s$ and $d = (n,\ k)$. Then,

$$disc_R(P) = (-1)^{\frac{3^{s+t}(3^{s+t}-1)}{2}} 3^{s.3^{s+t}} b^{3^s-1}[\Delta]^{3^s},$$

with $\Delta = 3^{t.3^t}.b^{3^t-1} + (3^t-1)^{3^t-1}a^{3^t}$. In particular, If $t = 1$,

$$disc_R(P) = (-1)^{\frac{3^{s+1}(3^{s+1}-1)}{2}} (-b)^{3^s-1}[27^s\,\Delta]^{3^s},$$

with $\Delta = 27\,b^2 + 4\,a^3$,

Proof. The statement follows immediately from Lemma 4.3.1. ∎

This being said, We can now formulate our main results in Dedekind case.

Theorem 4.3.2. *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 $P(X) = X^n + aX^k - b \in R[X]$ be the monic minimal polynomial of α of degree $n = 3^t k$ where $k = 3^s$. Assume that $v_{\mathfrak{p}}(a) \geq 1$ for all primes ideals $\mathfrak{p}$ in $V(disc_R(P).R)$, where $v_{\mathfrak{p}}$ be 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 primes ideals $\mathfrak{q} \in \mathfrak{Fib}_R(3)$, then α is a PBG of L over K if and only if b is square free.*

2. *Let $\mathfrak{Fib}_R(3) - V(bR) = \{\mathfrak{p}_1; ...; \mathfrak{p}_h\}$. 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:*

$$\begin{array}{ll} v_{\mathfrak{p}_i}(b^{m_i-1} + ab^{3^{f_i-t}} - 1) & = 1 \quad if\ f_i \geq s + t. \\ v_{\mathfrak{p}_i}(b^{m_i^{r_i+1}-1} + ab^{3^{(r_i+1)f_i-t}-1} - 1) & = 1 \quad if\ f_i < s + t. \end{array}.$$

Where the optimal value of r_i is the smallest integer satisfying the inequality $s+t \leq (r_i+1)f_i$.

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

$$disc_R(P) = (-1)^{\frac{3^{s+t}(3^{s+t}-1)}{2}} 3^{s.3^{s+t}} b^{3^s-1}[\Delta]^{3^s}$$

by consequence 4.3.1, then the set $S_P = V(b\,R) \cup (\mathfrak{Fib}_R(3) - V(b.R))$ is a disjoint union, since for each Prime ideal $\mathfrak{q}$ containing Δ, this implies that we must have $\mathfrak{q} \in \mathfrak{Fib}_R(3)$ 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 Theorem 4.3.1.

1. Our condition in the first case implies that $S_P = V(b\,R)$. Let $\mathfrak{p} \in V(b\,R)$, then by Theorem 4.3.1, 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 complete 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 $charR/\mathfrak{p}_i = 3$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to 3 since $3R \subset \mathfrak{p}_i$). According to the second case in Theorem 4.3.1, we can conclude that $\mathfrak{p}_i$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if

$$\begin{array}{ll} v_{\mathfrak{p}_i}(b^{m_i-1} + ab^{3^{f_i-t}} - 1) & = 1 \quad if\ f_i \geq s + t. \\ v_{\mathfrak{p}_i}(b^{m_i^{r_i+1}-1} + ab^{3^{(r_i+1)f_i-t}-1} - 1) & = 1 \quad if\ f_i < s + t. \end{array}.$$

   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.

∎

Corollary 4.3.2. *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 $P(X) = X^n - 3aX^k + b \in R[X]$ be the monic minimal polynomial of α of degree $n = 3k$ where $k = 3^s$ and a is a root of polynomial $H(X) = X^3 - b^2$ and square in R. Then, α is not monogenic.*

Proof. The discriminant of $P(X)$ is

$$disc_R(P) = (-1)^{(3^{s+1}+1)/2} 3^{3^s(3s+4)}\, b^{3^{s+1}-1}.$$

Ended, By substitution in Lemma 4.3.1 we get:

$$\begin{aligned} disc_R(P) &= (-1)^{3^{s+1}(3^{s+1}-1)/2}\, b^{3^s-1}[(3^{s+1})^3 b^2 - (-1)^3(3^{s+1} - 3^s)^2(3^s)(-3a)^3]^{3^s}. \\ &= (-1)^{3^{s+1}(3^{s+1}-1)/2}\, b^{3^s-1}[(3^{s+1})^3 b^2 - (-1)^3(3^{s+1} - 3^s)^2(3^s)\,(-3)^3\, b^2)]^{3^s}. \\ &= (-1)^{3^{s+1}(3^{s+1}-1)/2}\, b^{3^s-1} b^{2.3^s}[(3^{s+1})^3 - 4.3^{2s}(3^s)3^3]^{3^s}. \\ &= (-1)^{3^{s+1}(3^{s+1}-1)/2}\, b^{3^{s+1}-1}\, 3^{(3s+3)3^s}[1-4]^{3^s}. \\ &= (-1)^{(3^{s+2}-1)/2} b^{3^{s+1}-1}\, 3^{(3s+3)3^s}\, 3^{3^s}. \\ &= (-1)^{(3^{s+2}-1)/2} 3^{3^s(3s+4)}\, b^{3^{s+1}-1}. \end{aligned}$$

and hence the result.

We starts with the observation that $S_P = V(b\,R)$ or $S_P = V(b\,R) \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_h\}$, where $\mathfrak{p}_i \in \mathfrak{F}ib_R(3) - V(b\,R)$ for $i = 1, ..., h$ according to $\mathfrak{F}ib_R(3) \subseteq v_{\mathfrak{q}}(b\,R)$ or not.

Let $\mathfrak{p} \in V(b\,R)$, then by Theorem 4.3.2, 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. This is a contradiction with $a^3 = b^2$. ∎

4.3.3 Illustrations

1. Let $K = \mathbb{Q}(\alpha)$ such that $P = Irred(\alpha) = X^9 - 3b^2X^3 - b^3$ we have $disc_{\mathbb{Z}}(P) = -3^{21}b^{24}$ by Theorem 4.3.2 α is not monogenic.

2. 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 $\mathcal{O}_K$ of K is $\mathcal{O}_K = \mathbb{Z}[t]$ such that:

$$t = \sqrt{d}\ if\ d \equiv 2, 3 \ \text{modulo}\ 4.$$

And the discriminant is given by:

$$D_{K/\mathbb{Q}} = 4d. \tag{4.13}$$

By the previous application if p is a prime number such that $4p + 1$ be a $3-$power and $L = K(\alpha)$ where α is a root of the monic minimal polynomial $P(x) = X^{3^{s+1}} + 3pX^{3^s} - p$ ($s \in \mathbb{N}$), then L/K is monogenic. So, we denote such basis $\{1; \alpha; \alpha^2; ...; \alpha^{3^s}\}$. It is obvious that:

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^p-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^p-1}\}$$

is an integral basis of L.

Corollary 4.3.3. *With previous conditions the discriminant $D_{L/\mathbb{Q}}$ is given by:*

$$D_{L/\mathbb{Q}} = 3^{2s.3^{s+1}} p^{2(3^s-1)} [\Delta]^{2.3^s} .(4\,d)^{3^{s+1}}.$$

Proof. Since L/K is monogenic we obtain $D_{L/K} = (-1)^{\frac{3^{s+1}(3^{s+1}-1)}{2}} 3^{s.3^{s+1}} p^{3^s-1} [\Delta]^{3^s}$ with $\Delta = 27.p^2(4p + 1)$, then $N_{K/\mathbb{Q}}(D_{L/K}) = (3^{s.3^{s+1}} p^{3^s-1} [\Delta]^{3^s})^2$, by discriminant tower formula ($D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K})(D_{K/\mathbb{Q}})^{[L:K]}$) and 4.13, it follows that: $D_{L/\mathbb{Q}} = 3^{2s.3^{s+1}} p^{2(3^s-1)} [\Delta]^{2.3^s} .(4\,d)^{3^{s+1}}$.

∎

3. The following computations were performed by using Maple. Let $K = \mathbb{Q}(\sqrt{22})$, $L = K(\alpha)$ where $P(X) = X^3 + 3aX - a$ and $a = -5 - \sqrt{22}$ the irreducible polynomial of α, then L/K is monogenic.

   First, the prime ideal (3) has the factorisation $(3) = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ where $\overline{\mathfrak{p}}_3$ is the conjugate of $\mathfrak{p}_3$, and we have $(a) = \mathfrak{p}_3$ is square free, one can check also that the factorization of the discriminant of $P(X)$ is $(disc_{O_K}(P)) = \mathfrak{p}_3^5\overline{\mathfrak{p}}_3^5$, it's obvious that this facts satisfies conditions in Theorem 4.3.2, and since $v_{\overline{\mathfrak{p}}_3}(4a^2 - 1) = 1$ then L/K is monogenic. If so, since $22 \equiv 2 \ \text{modulo}\ 4$ we have that $\{1; \sqrt{22}; \alpha; \alpha\sqrt{22}; \alpha^2; \alpha^2\sqrt{22}\}$ is an integral basis of $L/\mathbb{Q}$, by [**?**, Lemma 3.1].

4. Let p be a prime integer, $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$ a finite extension of the field of rational integer with irreducible polynomial $P(x) = X^{3^{s+1}} - 3pX^{3^s} + p$ $(t = 1)$. We have

$$disc_{\mathbb{Z}}(P) = (-1)^{\frac{3^{s+1}(3^{s+1}-1)}{2}} 3^{s.3^{s+1}} p^{3^s-1} [\Delta]^{3^s}$$

with $\Delta = 27.p^2(-4p+1)$, by the assumptions of theorem 4.3.2, the number $-4p+1$ must be a 3-power. By calculation using Maple, we get 16 numbers satisfying this condition ≤ 10000. The first teen of them are given in Table 2:

Table 4.3: Table 2.

power of 3	The prime p
3	7
5	61
7	547
13	398581
23	23535794707
43	82064241848634269407
281	29445069578863612104789418133159256661148453875684032393263578374823854 75520093891958138154374710535513487956849686948341665893255620 1
359	48358236294175535529774510575156768874056312486184316998563366306744736576 71795828921188691385754149614471385782311327948265274217043081424865223 1 582390480258542967168326 7
487	57015253176222661346517090764455068260985046671850094115725037888465198381 35668789228799349783480007393134845093247079756243862052578597019391997 5 62062710282047892937605435575182278439902989107284501065905427033720270043 3458906977347
577	49762705254736861825730168682118223754517254694359539862318946038397061197 94544548921693103492698906252466527404743863604790906794817319188168538 2 11222110819372784958729644518289008804493034244131350300610264564694637 11 68360442782710862336005262315091673654492534620449045441

With the above assumptions, we have $h = 1$ and $f_1 = f = 1$. We consider the following three cases. $p = 3$, "$p \geq 5$ *and* $s = 0$" or "$p \geq 5$ *and* $s \geq 1$"

(a) Let $p = 3$. As p is square free, then the extension $L/\mathbb{Q}$ is monogenic for all $s \in \mathbb{N}$.

(b) Suppose that $p \geq 5$ *and* $s = 0$, the first point in second property of Theorem 4.3.2 is equivalent to $v_3(4p^2 - 1) = 1$ which is verified for all prime p as illustrated in Table 4.3.

Moreover, p is square free, hence $K/\mathbb{Q}$ is monogenic.

(c) If $p \geq 5$ *and* $s \geq 1$, we are under the second condition in second property of Theorem 4.3.2, that we can translate into $v_3(-(p^{3^{s+1}} - 3p\,p^{3^s} - p)) = 1$. With the above considerations, we have $r = s$. Contrary to (2) we prove that $p^{3^{s+1}} - 3p\,p^{3^s} - p \equiv 0 \; mod\, 9$ however, we prove that $v_3(-(p^{3^s} - 3p\,p^{3^s} - p)) \geq 2$. Which gives in this case the non-monogeneity of α.

Let p be one of the primes integers given in table 2. Then there exist $i \geq 3$ such tat $-4p + 1 = 3^i$.

$$\begin{aligned} p^{3^{s+1}} - 3p\,p^{3^s} - p &= p^{3^{s+1}} - (-3^i - p + 1)p^{3^s} - p \\ &= p^{3^{s+1}} + 3^i p^{3^s} + pp^{3^s} - p^{3^s} - p \\ &= p^{3^{s+1}} + 3^i p^{3^s} - p^{3^s} - p(1 - p^{3^s}) \\ &= [(p^{3^s})^3 - 1] - [p^{3^s} - 1] + p[p^{3^s} - 1] + 3^i p^{3^s} \\ &= [p^{3^s} - 1].[(p^{3^s})^2 + (p^{3^s}) + p] + 3^i p^{3^s} \end{aligned} \tag{4.14}$$

on the other hand

$$\begin{aligned} (p^{3^s})^2 + (p^{3^s}) + p &\equiv p^2 + p + p \; mod\, 3 \\ &\equiv p^2 + 2p \; mod\, 3 \\ &\equiv p(p-1) \; mod\, 3 \\ &\equiv p(-3p - 3^j) \; mod\, 3 \\ &\equiv 0 \; mod\, 3 \end{aligned} \tag{4.15}$$

and

$$\begin{aligned} p^{3^s} - 1 &= (-3^i - 3p + 1)^{3^s} - 1 \\ &= \sum_{k=0}^{k=3^s} C_{3^s}^k (1 - 3p)^{3^s - k}(-3^i)^k - 1 \\ &\equiv C_{3^s}^0 (1 - 3p)^{3^s - 0}(-3^i)^0 - 1 \; mod\, 3 \\ &\equiv (1 - 3p)^{3^s} - 1 \; mod\, 3 \\ &\equiv (1 - 3p) - 1 \; mod\, 3 \\ &\equiv 0 \; mod\, 3 \end{aligned} \tag{4.16}$$

Which proves our assertion.

Conclusion and perspectives

The study of the galois module structure have been studied largely by many authors in this direction we had established some remarkable results, and we proved some results about some algebraic invariant such as the discriminant and the steinitz class and their interpretation in the abelian extensions, moreover we study the monogeneity of some relative extensions, this work take our intension to:

1. Study the structure of the ring of integers as a module over the associated order of an abelian extension with diagonal integral basis, and give a generator if it's free.
2. Give conditions for abelian extensions to admit an normal integral basis.
3. Give conditions for extensions to be monogenic for relative pure and non pure extensions of arbitrary degree.
4. Study the relation between the existence of power integral basis and normal integral basis for abelian extensions.

Bibliography

[1] A. Aiba, *Carlitz modules and Galois module structure*, J. Number Theory, (**62**), (1997), 213-219. (Cited on page 8.)

[2] A. Aiba, *Artin-Schreier extensions and Galois module structure*, Journal of Number Theory (**102**), (1), (2003), 118-124. (Cited on page 8.)

[3] E.J. Gómez Ayala, *Bases normales d'entiers dans les extensions de Kummer de degré premier* , Journal de Théorie des Nombres de Bordeaux, (**6**), (1), (1994), 95-116. (Cited on page 8.)

[4] A-M. Bergé, *À propos de l'ordre associé à l'anneau des entiers d'une extension, d'après H. Jacobinski*, Séminaire de Théorie des Nombres de Bordeaux, Exposé no 8, (1971-1972), 1-12. (Cited on page 8.)

[5] W. Bley, *A Leopoldt-type result for rings of integers of cyclotomic extensions*, Canad. Math. Bull. (**38**), (1995), 141–148. (Cited on page 7.)

[6] D. Blessenohl, *On the normal basis theorem*, Note Mat. (**27**), (1), (2007), 5-10. (Cited on page 7.)

[7] N. Bourbaki, *Algèbre*, Chapitres 1 à 3, Springer ,1981. (Cited on pages 17 and 55.)

[8] N. Bourbaki, *Algèbre*, Chapitres 4 à 7, Masson,1981. (Cited on page 49.)

[9] N. P. Byott and G. Lettl, *Relative Galois module structure of integers of Abelian fields*, J. Th. Nombres, Bordeaux (**8**), (1996), 125-141. (Cited on pages 7, 23, 31, and 35.)

[10] N. Byott, J. Carter, C. Greither and H. Johnston. *On the restricted hilbert–speiser and leopoldt properties*, Illinois Journal of Mathematics, (**55**), (2), (2011), 623–639. (Not cited.)

[11] P. H. Cassou-Nogués and M. J. Taylor, *A Note on elliptic curves and the monogeneity of rings of integers*, J. London Math. Soc. (**37**), (2), (1988), 63-72. (Cited on page 10.)

[12] P. H. Cassou-Noguès and M. J. Taylor, *Uniés Modulaires et monogénéité d'anneaux d'entiers* , Séminaire de Théorie des nombres, Paris, no. 3, 347-353. 1986-1987, Vol. 75, pp, 35-64. Progr.Math, Bikharuset, Boston (1988). (Cited on page 10.)

[13] S. Chan, *Galois module structure of non-Kummer extensions*, Arch. Math. (**70**), (1998), 286–292. (Cited on page 8.)

[14] S. P. Chan and C.H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. reine angew. Math. (**434**), (1993), 205–220. (Cited on pages 7 and 35.)

[15] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London and New york, 1967. (Cited on page 52.)

[16] M. Charkani, *Pontryagin duality.* (Cited on page 20.)

[17] M. Charkani, *Cours de la theorie de corps de classe*, *Faculté des Sciences Dhar-Mahraz. BP 1796 Fés.* (Master Géométrie et Arithmétique.) (Not cited.)

[18] M. Charkani, A. Deajim, *Relative index in extension of dedekind ring*, JP journal of algebra, number theory and application. (**27**), (1), (2012), 73-84. (Cited on page 61.)

[19] M. E. Charkani and O. Lahlou, *On Dedekind's criterion and monogenicity over Dedekind rings*, Int. J. of Math. and Math. Sci. (**2003**), (2003), 4455-4464. (Cited on page 70.)

[20] M. E. Charkani and M. Sahmoudi, *Sextic Extension with cubic subfield*, JP Journal of Algebra, Number Theory et Applications, (**34**), (2), (2014), 139-150. (Cited on pages 10, 71, and 72.)

[21] M. E. Charkani and M. Sahmoudi, *On relative pure cyclic fields with power integral basis*, to appear. (Cited on pages 42 and 67.)

[22] M. E. Charkani and A. Soullami, *Tower Formula For Discriminant*, JP Journal of Algebra, Number Theory et Applications, (**43**), (1), (2019), 13-21. (Not cited.)

[23] R. Dedekind, *Uber den zussamenhang zwischen der theorie der ideals und der theorie der hoheren cyclotimy index*, Abh. Akad. Wiss. Gottingen, Math.-Phys. KL, (**23**), (1878), 1–23. (Cited on page 10.)

[24] I. Del Corso and L. P. Rossi, *Normal integral bases for cyclic Kummer extensions*, Journal of Pure and Applied Algebra, (**214**), (2010), 385-391. (Cited on pages 8, 9, 46, and 47.)

[25] M. Deuring, *Galoissche Theorie und Darstellungstheorie*, Math. Ann., (**107**), (1932), 140-144. (Cited on page 9.)

[26] G. Eisenstein, *Lehrzstze*, J.reine angew. 2007. (Cited on page 9.)

[27] L. El Fadil, M. Charkani, *Generalisation of the discriminat and applications*. The Arabian Journal for Science and Engineering, (**29**), (1A), (2004), 93-98. (Cited on pages 61 and 65.)

[28] W. Feit, *The representation theory of finite groups*, North–Holland, Amsterdam–New York, 1982. (Cited on pages 16 and 20.)

[29] A. Fröhlich, *Local Fields* Algebraic Number Theory (London), (J.W.S. Cassels and A. Fr¨ohlich, eds.), Academic Press (1967), 1–47. (Cited on page 33.)

[30] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Combridge Studies in Advenced Mathematics, (**27**), 1993. (Cited on pages 56, 57, and 61.)

[31] A. Fröhlich, *The discriminats of ralative extensions and the existence of integral bases*, Mathematika, (**7**), (1960),15-22. (Cited on page 9.)

[32] G. Fujisaki, *Some examples of number fields without relative integral bases*, J. Fac. Sei. Univ. Tokyo Sect. (**21**), (1974), 93-95. (Cited on page 10.)

[33] R. Gilmer, *Commutative semi-groupe rings*, Chicago Lecture in math. Univ. Chicago Press, 1984. (Cited on pages 11 and 12.)

[34] M. N. Gras, *Lien entre le groupe des unités et la monogénéité des corps cubiques cycliques*, Publ. Math. Fac. Sci. Besançon Théorie des nombres, (1975/1976), 19. (Cited on page 10.)

[35] M. N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$*, J. Number Theory, (**23**), (3), (1986), 347-353. (Cited on page 10.)

[36] M. N. Gras, *Conditions nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de Q*, Séminaire de Théorie des nombres, Paris 1984-85, (**63**), (1986), 97-107. (Cited on page 10.)

[37] C. Greither, D. Replogle, A. Srivastav *Swan modules and Hilbert–Speiser number fields*, Journal of Number Theory, (**79**), (1), (1999), 164-173. (Cited on pages 8 and 34.)

[38] M. Haghighi, *Relative integral basis for algebraic number fields*, Int. J. Math. Math. Sci. (**9**), (1), (1986), 97-104. (Cited on page 10.)

[39] R. R. Hall and M.N. Huxley, *Dedekind sums and continued fractions*, Acta Arith. (**63**), (1993), 79-90. (Cited on page 46.)

[40] K. Hensel, *Ueber die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*, J. reine angew. Math. (**103**), (1888), 230-273. (Cited on page 9.)

[41] B. Huppert, *Endliche Gruppen. I,* Die Grundlehren der Mathematischen Wissenschaften, Band (**143**), Springer-Verlag, Berlin, 1967. (Cited on page 22.)

[42] H. Ichimura, *Note on the ring of integers of a kummer extension of prime degree: V*, Proc. Japan Acad. Ser. A Math. Sci. Volume (**78**), (6), (2002), 76-79. (Cited on page 8.)

[43] H. Ichimura and A. Sumida, *A note on integral bases of unramified cyclic extensions of prime degree. II*, H. manuscripta math. (**104**), (2001), 201–210. (Cited on page 8.)

[44] H. Ichimura, *On the ring of integers of a tame Kummer extension over a number field*, Journal of Pure and Applied Algebra, (**187**), (2004), 169–182. (Cited on page 8.)

[45] H. Ichimura, *Note on Galois descent of a normal integral basis of a cyclic extension of degree p*, Proc. Japan Acad. (**85**), (A), (2009), 160-162. (Cited on page 8.)

[46] H. Johnston, *Relative Galois module structure of rings of integers of absolutely abelian number fiel*, J. reine angew. Math. (**620**), (2008), 85-103. (Cited on pages 8 and 35.)

[47] G.J. Janusz, *Algebraic number Fields* , Academic Press, New York, Second Edition, 1996. (Cited on page 52.)

[48] C. Khar, D. Prasad, *On steinitz module and capitulation of ideals*, Nagoya Math.J, (**160**), (2000), 1-15. (Cited on page 9.)

[49] G. Karpilovsky, *The Jacobson radical of group algebras*, Notas de mathematica, (**135**), Elsevier science, 1987. (Cited on page 12.)

[50] G. Karpilovsky, *Clifford Theory for Group Representations*, Mathematics Studies, North-Holland, (**156**), 1989. (Cited on page 12.)

[51] L.A. Kurdachenko, J. Otal, and I.Y. Subbotin, *Artinian Modules over Group Rings*, Mathematics Studies, Birkhäuser, Basel, 2007. (Cited on page 15.)

[52] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics (**110**), Springer-Verlag New York, 1986. (Cited on page 52.)

[53] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. (**201**), (1959), 119–149. (Cited on page 35.)

[54] G. Lettl, *The ring of integers of an abelian number field,* J. reine angew. Math. (**404**), (1990), 162–170. (Cited on page 35.)

[55] R. MacKenzie and J. Scheuneman, *A Number Field Without a Relative Integral Basis*, Amer. Math. Monthly, (**78**), (1971), 882-883. (Cited on page 10.)

[56] Melisa J. Lavallee, Blair K. Spearman and K. S. Williams, *Lifting Monogenic Cubic Fields to Monogenic Sextic Fields*, KODAI MATH. J. (**34**), (2011), 410-425. (Cited on page 10.)

[57] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Second Edition, 1990. (Cited on page 10.)

[58] W. Narkiewicz , *Elementary and analytic number theory of algebraic numbers* , Springer-Verlag Berlin Heidelberg GmbH, 2004. (Not cited.)

[59] J. Neukirch *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, (**322**), Springer-Verlag Berlin Heidelberg, 1999. (Cited on page 55.)

[60] C. Polcino Milies, S.K. Sehgal, *An introduction to group rings, Algebras and Applications*, Dordrecht: Kluwer Academic Publishers, 2002. (Cited on pages 13 and 22.)

[61] I. Reiner, *Maximal orders*, Academic, Press, London, 1975. (Cited on pages 26, 27, and 57.)

[62] M. Sahmoudi and A. Soullami, *On Sextic Integral Bases Using Relative Quadratic Extension*, Bol. Soc. Paran. Mat., (**38**), (4), (2020), 175-180. (Cited on page 10.)

[63] M. Sahmoudi and A. Soullami, *On Monogenicity Of Relative Cubic-Power Pure Extensions*, Adv. Math., Sci. J., (**9**), (9), (2020), 6817–6827. (Not cited.)

[64] P. Samuel, *Théorie algèbrique des nombres*, Hermann Paris, 2^{eme} edition revue et corrigée, 1971. (Cited on page 52.)

[65] J. P. Serre, *Corps locaux*, Hermann Paris, 1968. (Not cited.)

[66] A. N. Sengupta, *Representing Finite Groups: A Semisimple Introduction*, Springer New York Dordrecht Heidelberg London, 2011. (Cited on pages 12, 13, and 16.)

[67] T. Schönemann, *Über einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze*, J. reine angew. Math. (**40**) (1850), 185-187. (Cited on page 9.)

[68] B. K. Spearman and K. S. Williams, *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., (**70**), (1996), 185-192. (Cited on page 10.)

[69] A. Soullami, M. Sahmoudi, and O. Boughaleb, *On relative power integral basis of a family of numbers fields*, to appear in Rocky Mountain Journal Of Mathematics (Not cited.)

[70] A. Srivastav and S. Venkataraman, *Relative Galois module structure of quadratic extensions*, Indian J. Pure Appl. Math. (**25**), (5), (1994), 473-488. (Cited on page 7.)

[71] R. Swan, *Factorization of polynomials over finite fields*. Pacific J. Math. (**12**), (1962), 1099-1106. (Cited on page 75.)

[72] L. C. Washington, *Inroduction to cyclotomic fields*, Graduate Texts in Mathematics, (**83**), Second edition Springer-Verlag, Berlin, New York , 1997. (Cited on pages 19 and 40.)

[73] L. C. Washington, *Relative integral bases*, Proceedings of the American Mathemtical Society, (**56**), (1976), 93-94. (Cited on page 10.)