

EXTENSIONS OF DISCRETE VALUATIONS & THEIR RAMIFICATION THEORY

by

ŞÜKRÜ UĞUR EFEM

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University

Spring 2011

EXTENSIONS OF DISCRETE VALUATIONS & THEIR
RAMIFICATION THEORY

APPROVED BY:


Prof. Dr. Henning Stichtenoth
(Thesis Supervisor)

.....


Prof. Dr. Oleg Belegradek

.....

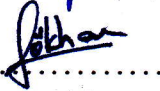
Prof. Dr. Alev Topuzođlu

.....

Assoc. Prof. Dr. Cem Gñneri

.....

Asst. Prof. Gñkhan Gñgñş

.....

DATE OF APPROVAL: 07/06/2011

©Şükrü Uğur Efem 2011
All Rights Reserved

EXTENSIONS OF DISCRETE VALUATIONS & THEIR RAMIFICATION THEORY

Şükrü Uğur Efem

Mathematics, Master Thesis, 2011

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Extensions of discrete valuations, inseparable residue class field extension, ramification theory, residue class field, valued fields.

Abstract

We study how a discrete valuation v on a field K can be extended to a valuation of a finite separable extension L of K . The ramification theory of extensions of discrete valuations to a finite separable extension is very well established whenever the residue class field extension is separable. This is the so called classical ramification theory. We investigate the classical ramification theory and also the ramification theory of extensions of discrete valuations with an inseparable residue class field extension. We show that some results from classical ramification theory, such as Hilbert's different formula can be modified to be true for extensions of valuations with inseparable residue class field extensions, whereas many other classical results fail to hold.

AYRIK DEĞERLERİN GENİŞLEMELERİ ve ONLARIN DALLANMA TEORİSİ

Şükrü Uğur Efem

Matematik, Yüksek Lisans Tezi, 2011

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: Ayrık değerlerin genişlemeleri, ayrışabilir olmayan kalan sınıfı cismi genişlemeleri, dallanma teorisi, değerli cisimler, kalan sınıfı cismi.

Özet

Bu tezde bir K cismi üzerindeki ayrık değer, K 'nın sonlu ve ayrılabilir bir cisim genişlemesi olan L 'ye nasıl genişletilebileceği üzerine çalışılmıştır. Ayrık değerlerin genişletilmesinin dallanma teorisi, kalan sınıfı cismi genişlemesinin ayrışabilir olduğu durumlarda çok iyi bilinmektedir. Bu duruma klasik dallanma teorisi denir. Bu tezde klasik dallanma teorisi ve kalan sınıf cisim genişlemesi ayrışabilir olmayan ayrık değer genişlemelerin dallanma teorisi incelenmiştir. Klasik dallanma teorisinin, Hilbert formülü gibi, bazı sonuçlarının cisim genişlemesi ayrışabilir olmayan ayrık değer genişlemelerin dallanma teorisinde de doğru olacak şekilde modifiye edilebileceği, ama bazı sonuçların ise bu durumda doğru olamayacakları gösterilmiştir.

*To my grandfathers;
Ahmet Őükrü Efem
and
Rauf Nasuhođlu*

Aknowledgements

Above all, I present my deepest and sincerest thanks to my advisor Prof. Dr. Henning Sticthenoth. Without his supervision, and invaluable advice this thesis would not be possible.

I am grateful to my parents Gül and Mehmet for their endless support during my studies, especially during the hard times that I overcame while writing this thesis. My good friend Haydar Göral deserves gratitude for his excellent friendship; both mathematically and personally.

Last but not least, a very special thanks goes to my former teachers Prof. Dr. Ali Nesin, and Prof. Dr. Oleg Belegadek. To their valuable education I owe deeply.

Contents

| | |
|--|----|
| Abstract | i |
| Özet | ii |
| Aknowledgements | iv |
| 1 Introduction | 1 |
| 2 Preliminaries | 2 |
| 3 Hensel's Lemma & Henselian Fields | 6 |
| 4 Extension of Valuations, Complete Case | 7 |
| 5 Extension of Valuations, Non-Complete Case | 10 |
| 6 Classical Ramification Theory | 14 |
| 7 Ramification Theory of Valuations With Inseparable Residue Class Field Extensions | 29 |

1 Introduction

For a field K a *valuation* is a map $v : K \rightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties:

- (i) v is onto
- (ii) $v(a) = \infty$ if and only if $a = 0$
- (iii) For all $a, b \in K$, $v(ab) = v(a) + v(b)$
- (iv) For all $a, b \in K$, $v(a + b) \geq \min\{v(a), v(b)\}$

More precisely, v is called a discrete valuation of rank one. We will be only interested in such valuations in this thesis. So whenever we say valuation, we mean discrete valuation of rank one. We say that (K, v) is a *valued field*; more precisely (K, v) is called a *discrete valuation field*. If the valuation v is clear from the context we will say K is a valued field for the sake of simplicity.

If L is a finite separable extension of a valued field (K, v) then it is possible to extend the valuation v to L . Our aim is to investigate the so called classical ramification theory of valuations (i.e. where the residue class field extension is separable), and to investigate what may happen if one tries to generalize the classical results to the case where residue class field extension is inseparable. We will show that some results of the classical ramification theory can be generalized, with some modifications, to the inseparable residue class field extension case. A modified version of *Hilbert's different formula* and theorems about *ramification jumps* are most probably the most important of such results. On the other hand the classical version of *Hilbert's different formula*, and *Herbrand's property* fails to hold in the general case. A natural limit for extending the results of classical ramification theory is the so called *monogenic extensions*.

First we will present basic results about valued fields, construction of the extension of a valuation to a separable extension of K . In the last two sections we will give the classical ramification theory, and in the last section we will abandon the assumption that the residue class field extension is separable in order to investigate what may happen to the results of classical ramification theory in this general case.

2 Preliminaries

In this section we will give basic results and terminology about valued fields.

Let (K, v) be a valued field, then we define the following sets:

$$\begin{aligned}\mathcal{O}_v &:= \{a \in K : v(a) \geq 0\} \\ \mathcal{M}_v &:= \{a \in K : v(a) > 0\}\end{aligned}$$

Lemma 2.1. (i) \mathcal{O}_v is a subring of K , \mathcal{M}_v is an ideal of \mathcal{O}_v and K is the field of fractions of \mathcal{O}_v .

(ii) \mathcal{O}_v is a local ring.

(iii) Let $A \triangleleft \mathcal{O}_v$ and $a \in A$ such that $v(a) \leq v(b)$ for all $b \in A$. Then $A = a\mathcal{O}_v$.

(iv) \mathcal{O}_v is a PID and \mathcal{M}_v is the unique prime ideal of \mathcal{O}_v .

(v) The generators of \mathcal{M}_v are exactly the elements $\pi \in K$ with $v(\pi) = 1$. Such elements are called prime elements of v . Given a prime element π , every $a \in K^\times$ has a representation $a = \pi^m u$ for some $m = v(a) \in \mathbb{Z}$, and $u \in \mathcal{O}_v^\times$.

(vi) \mathcal{O}_v is a maximal subring of K .

Since \mathcal{O}_v is a ring \mathcal{M}_v is its maximal ideal by lemma 2.1, \mathcal{O}_v is called *the valuation ring* of v and \mathcal{M}_v is called *the maximal ideal* of \mathcal{O}_v . Also \mathcal{M}_v is called *the valuation ideal* of v . Moreover, since \mathcal{M}_v is maximal, $k_v = \mathcal{O}_v/\mathcal{M}_v$ is a field. It is called *the residue class field*. The so called ramification theory of valuations strongly depends on the residue class field.

Corollary 2.2. Let v, w be valuations of K . Then the following are equivalent:

(i) $v = w$.

(ii) $\mathcal{O}_v = \mathcal{O}_w$.

(iii) $\mathcal{O}_v \subseteq \mathcal{O}_w$

Proof. $(i \Rightarrow ii \Rightarrow iii)$ is trivial. Moreover since \mathcal{O}_v is maximal we also have $(iii \Rightarrow ii)$. So the only thing that remains to be shown is $(ii \Rightarrow i)$. Indeed, since \mathcal{O}_v , and \mathcal{O}_w are local, $\mathcal{O}_v = \mathcal{O}_w$ implies $\mathcal{M}_v = \mathcal{M}_w$. Hence $v(\pi) = 1$ if and only if $w(\pi) = 1$. For $a \in K^\times$, $a = \pi^m u$, for some $u \in \mathcal{O}_v^\times = \mathcal{O}_w^\times$. So, $v(a) = m$ and $w(a) = m$. \square

Consider valued fields (K, v) and (L, w) where $K \subseteq L$. Then w is called an *extension* of v if $\mathcal{O}_v \subseteq \mathcal{O}_w$ and $\mathcal{M}_v \subseteq \mathcal{M}_w$. In this situation we also say, w *lies over* v , and write $w|v$. In this case we will also say that (L, w) is an extension of (K, v) . Beware that this does not mean $w|_K = v$!

Theorem 2.3. *Let (K, v) and (L, w) be valued fields, $K \subseteq L$ and $w|v$. Then*

- (i) $\mathcal{O}_v = \mathcal{O}_w \cap K$ and $\mathcal{M}_v = \mathcal{M}_w \cap K$.
- (ii) *The inclusion $\mathcal{O}_v \subseteq \mathcal{O}_w$ induces an embedding of the residue class fields as follows*

$$\begin{aligned} k_v = \mathcal{O}_v/\mathcal{M}_v &\rightarrow l_w = \mathcal{O}_w/\mathcal{M}_w \\ a + \mathcal{M}_v &\mapsto a + \mathcal{M}_w \end{aligned}$$

So, we will always consider k_v as a subfield of l_w . We write $f(w|v) = [l_w : k_v]$.

- (iii) *If $[L : K]$ is finite, then $[l_w : k_v] \leq [L : K]$ is also finite.*
- (iv) *$w(K^\times)$ is a subgroup of \mathbb{Z} of finite index. We write $e(w|v) = (\mathbb{Z} : w(K^\times))$.*
- (v) *For all $a \in K$, $w(a) = e(w|v)v(a)$. In particular if $\pi \in K$ is a prime element of v , then $w(\pi) = e(w|v)$.*
- (vi) $e(w|v)f(w|v) \leq [L : K]$.

The numbers $f(w|v)$ and $e(w|v)$ play an important role in extending valuations, and also in the ramification theory of valuations. Therefore they are given special names. $f(w|v)$ is called the *degree of $w|v$* or the *residue class degree*, $e(w|v)$ is called the *ramification index* of $w|v$. $w|v$ is said to be *unramified* if $e(w|v) = 1$, and *ramified* if $e(w|v) > 1$.

Lemma 2.4. *Let (K, v) , (L, w) , and (M, u) be valued fields such that $K \subseteq L \subseteq M$, and $w|v$ and $u|w$. Then $u|v$ and*

$$\begin{aligned} e(u|v) &= e(w|v)e(u|w) \\ f(u|v) &= f(w|v)f(u|w) \end{aligned}$$

A valuation v on a field K naturally gives rise to a metric on K as follows

Lemma 2.5. *Let (K, v) be a valued field, $\rho \in \mathbb{R}$ with $0 < \rho < 1$. Then, for $a, b \in K$*

$$d(a, b) = \begin{cases} 0 & \text{if } a = b \\ \rho^{v(a-b)} & \text{if } a \neq b \end{cases}$$

defines a metric on K .

Now, since K became a metric space, we can introduce some notions from analysis; such as convergence, Cauchy sequence, completion, etc. One of the most important aspects of valuations is that they allow us to use techniques from analysis in algebraic setting. Most importantly in number fields, and function fields, which are naturally valued fields via their prime ideals.

The following results translate some basic results about convergence into the language of valuations.

Lemma 2.6. *Let (K, v) be a valued field, $(a_n)_{a \geq 0}$ a sequence in K , and $a \in K$. Then*

(i) $(a_n)_{a \geq 0}$ converges to a if and only if $v(a - a_n) \rightarrow \infty$ as $n \rightarrow \infty$.

(ii) $(a_n)_{a \geq 0}$ is a Cauchy sequence if and only if $v(a_n - a_m) \rightarrow \infty$ for $n, m \rightarrow \infty$.

(iii) $(a_n)_{a \geq 0}$ is a Cauchy sequence if and only if $v(a_n - a_{n+1}) \rightarrow \infty$ for $n \rightarrow \infty$.

Proof. *i, ii* are clear. We only need show *iii*. We will show that $v(a_n - a_{n+1}) \rightarrow \infty$ if and only if $v(a_n - a_m) \rightarrow \infty$ for $n, m \rightarrow \infty$.

Given $c \in \mathbb{R}^{>0}$ there is an $N \in \mathbb{N}$ such that for all $n > N$

$$v(a_n - a_{n+1}) \geq c$$

Let $m, n > n$, without loss of generality say $m \geq n$. Then

$$\begin{aligned} v(a_n - a_m) &= v((a_n - a_{n+1}) + (a_{n+1} - a_{n+2}) + \dots + (a_{m-1} - a_m)) \\ &\geq \min\{v(a_n - a_{n+1}), \dots, v(a_{m-1} - a_m)\} \geq c \end{aligned}$$

The converse is obvious. Take $m = n + 1$. □

Lemma 2.7. *Assume that $a_n \rightarrow a$ in a valued field (K, v) . Then $v(a_n) \rightarrow v(a)$ in $\mathbb{Z} \cup \{\infty\}$.*

Proof. If $a = 0$ it follows immediately from Lemma 2.6.

So, assume that $a \neq 0$. Choose $N \in \mathbb{N}$ such that for all $n \geq N$

$$v(a_n - a) > v(a)$$

Then for all $n > N$,

$$v(a_n) = v((a_n - a) + a) = \min\{v(a_n - a), v(a)\} = v(a)$$

So the sequence $(v(a_n))_{n \geq 0}$ is eventually constant. Hence it converges to $v(a)$. \square

Corollary 2.8. \mathcal{O}_v and \mathcal{M}_v^r are closed subsets of K for all $r \in \mathbb{Z}$.

Proof. Recall that $\mathcal{O}_v = \{a \in K : v(a) \geq 0\}$. Let $a_n \rightarrow a$ with all $a_n \in \mathcal{O}_v$. Hence, by Lemma 2.7, $v(a) = \lim(a_n) \geq 0$. \square

Since there is a metric space structure on a valued field K we can talk about completeness, and completion of a field. Completion of a discrete valuation field plays a central role for extending a valuation to a separable finite extension.

A discrete valuation field (K, v) is called *complete*, if every Cauchy sequence in K is convergent. Also let $(\widehat{K}, \widehat{v})$ be a discrete valuation field and $\varepsilon : K \rightarrow \widehat{K}$ be an embedding. We say that $(\widehat{K}, \widehat{v}, \varepsilon)$ (or $(\widehat{K}, \widehat{v})$ whenever ε is clear from the context) is a completion of (K, v) if

- (i) $(\widehat{K}, \widehat{v})$ is complete.
- (ii) $\widehat{v} \circ \varepsilon = v$.
- (iii) $\varepsilon(K)$ is dense in \widehat{K} .

Theorem 2.9. *Let (K, v) be a discrete valuation field. There exists a completion $(\widehat{K}, \widehat{v}, \varepsilon)$. The completion is unique in the sense that: Given two completions $(\widehat{K}, \widehat{v}, \varepsilon)$ and $(\widetilde{K}, \widetilde{v}, \delta)$ there exists a unique continuous isomorphism $\sigma : \widehat{K} \rightarrow \widetilde{K}$ such that $\sigma \circ \varepsilon = \delta$. Moreover, $\widehat{v} = \widetilde{v} \circ \sigma$.*

The construction of the completion \widehat{K} and embedding K into it is similar to the construction of \mathbb{R} as the completion of $(\mathbb{Q}, |\cdot|)$ and embedding \mathbb{Q} into \mathbb{R} . For details see [1].

For a completion $(\widehat{K}, \widehat{v}, \varepsilon)$ of (K, v) we can identify K with $\varepsilon(K)$. Then $K \subseteq \widehat{K}$, and $v = \widehat{v}|_K$. Then we often write (\widehat{K}, v) is a completion of (K, v) . Moreover, because of the uniqueness, we call (\widehat{K}, v) the completion.

Theorem 2.10. *Assume $(\overline{K}, \overline{v})$ is a valued field and $K \subseteq \overline{K}$ a dense subfield. We define*

$$v = \overline{v}|_K \rightarrow \mathbb{Z} \cup \{\infty\}$$

Then,

- (i) v is valuation of K , and $\overline{v}|_v$. If $(\overline{K}, \overline{v})$ is complete then it is the completion of (K, v) .

(ii) Let $\pi \in K$ be a prime element for v . Then for all $r \in \mathbb{Z}$, $\mathcal{M}_v^r = \mathcal{M}_{\bar{v}}^r \cap K = \pi^r \mathcal{O}_v$, and $\mathcal{M}_{\bar{v}}^r = \mathcal{M}_v^r \mathcal{O}_{\bar{v}} = \pi^r \mathcal{O}_{\bar{v}}$. Moreover, for all $r \geq 1$ we get an isomorphism

$$\begin{aligned} \mathcal{O}_v / \mathcal{M}_v^r &\rightarrow \mathcal{O}_{\bar{v}} / \mathcal{M}_{\bar{v}}^r \\ a + \mathcal{M}_v^r &\mapsto a + \mathcal{M}_{\bar{v}}^r \end{aligned}$$

(iii) $e(\bar{v}|v) = f(\bar{v}|v) = 1$.

3 Hensel's Lemma & Henselian Fields

As we will later see Hensel's Lemma is an essential tool for extending valuations. In this section we will show that completion of a rank 1 valuation satisfies Hensel's Lemma. Although in this thesis we restrict our attention to discrete rank 1 valuations it should be remarked that Hensel's Lemma needs not to be true for completions of fields with respect to a valuation of higher rank. This leads to the notion of Henselian fields, which can be characterized as fields which satisfy Hensel's Lemma. Note that we will not give proofs of the results that we will mention in this section. The results themselves will be useful in the next sections, but their proofs are of not as useful for valuation theoretic purposes of this thesis.

The motivation for the Hensel's Lemma is as follows: Let (K, v) be valued field and $\mathcal{O}_v, \mathcal{M}_v$, and k_v be the valuation ring, valuation ideal, and residue class field respectively. For $f(X) \in \mathcal{O}_v[X]$ we define the residue class field polynomial $\bar{f}(X) \in k_v$ in the natural way.

Now, suppose that $\bar{f}(X) = \Phi(X)\Psi(X)$ where $\Phi(X), \Psi(X) \in k_v[X]$ are relatively prime. Can we lift this factorization to \mathcal{O}_v ? Before we answer this question we will give a special case of the Gauss Lemma.

Lemma 3.1. *Let (K, v) be a valued field, and let $f(x) \in \mathcal{O}_v[X]$ be monic. Suppose $f(X) = f_1(X)f_2(X) \in K[X]$, where $f_1(X)$, and $f_2(X)$ are monic. Then $f_1(X), f_2(X) \in \mathcal{O}_v[X]$.*

The proof is very similar to the proof of Gauss Lemma. One should also remark that whenever a polynomial $f(X) \in \mathcal{O}_v[X]$ can be factorized in $K[X]$ as in Lemma 3.1 then the residue class polynomial $\bar{f}(X)$ can be factorized in $k_v[X]$.

Theorem 3.2. *(Hensel's Lemma) Let (K, v) be a complete discrete valuation field with a rank 1 valuation, $f(X) \in \mathcal{O}_v[X]$, and $\bar{f}(X) \neq 0$ (in $k_v[X]$). Assume that $\bar{f}(X) = \Phi(X)\Psi(X)$ where $\Phi(X), \Psi(X) \in k_v[X]$ are relatively prime. Then there exists $g(X), h(X) \in \mathcal{O}_v[X]$ such that $\bar{g}(X) = \Phi(X)$, $\bar{h}(X) = \Psi(X)$ and $\deg g(X) = \deg \Phi(X)$ and $f(X) = g(X)h(X)$.*

Hensel's Lemma vaguely states that for a polynomial $f(X)$ over a complete discrete valuation field, if $\bar{f}(X)$ has a factorization over k_v then this factorization can be lifted to $\mathcal{O}_v[X]$ in a nice way. Hence the motivating question is answered positively. A proof of a more general version of Hensel's Lemma can be found in [1, Chap. 2].

Corollary 3.3. *Let (K, v) be a complete field, $f(X) \in \mathcal{O}_v[X]$ monic. Assume that $\bar{f}(X) \in k_v$ has a simple root $u \in k_v$. Then there exists an element $a \in \mathcal{O}_v$ such that $f(a) = 0$ and $\bar{a} = u$.*

A valued field (K, v) which satisfies the assertion in theorem 3.2 is said to be *Henselian*. Hensel's Lemma states that every complete discrete valuation field is Henselian.

4 Extension of Valuations, Complete Case

For the rest of this section (K, v) will always be a complete discrete valuation field. Let $L \supseteq K$ be a finite separable extension of K . Our aim in this section is to show that extending the valuation v to a valuation of L is possible. Moreover there is only one such extension. Also this section will form a basis for extension of valuations in the general case, where the assumption of completeness of (K, v) is dropped.

Before constructing the extension of v to L and giving the properties of such an extension, we will give a technical lemma by assuming such an extension is possible.

Lemma 4.1. *Let (K, v) be a complete discrete valuation field. Suppose w extends v to L , and let (u_1, \dots, u_n) be a basis of L over K . Given $m \leq n$ there exists a real number c such that for all $\alpha \in K^\times$ with a representation $\alpha = \sum_{j=1}^m a_j u_j$ where $a_j \in K$, we have*

$$w(a_j) \geq w(\alpha) - c$$

A proof of Lemma 4.1 can be found in [2, Chap. 4, Sect. 4.5, Lemma 4.5.2].

Theorem 4.2. *Let (K, v) be a complete discrete valuation field, L/K a finite separable extension with $[L : K] = n$. Set*

$$f = \min\{v(N_{L/K}(\alpha)) : N_{L/K}(\alpha) \in \mathcal{M}_v\}$$

Define

$$\begin{aligned} w : L &\rightarrow \mathbb{Z} \cup \{\infty\} \\ \alpha &\mapsto \frac{1}{f}v(N_{L/K}(\alpha)) \end{aligned}$$

and $w(0) = \infty$. Then

- (i) w is a valuation of L , and $w|_v$.
- (ii) \mathcal{O}_w is the integral closure of \mathcal{O}_v in L .
- (iii) \mathcal{O}_w is a free \mathcal{O}_v - module of rank n .
- (iv) w is the unique extension of v to L .
- (v) (L, w) is a complete discrete valuation field.
- (vi) $f(w|_v) = f$ and $e(w|_v) = \frac{n}{f}$.

Proof. (i) Consider the map $v \circ N_{L/K} : L^\times \rightarrow \mathbb{Z}$. It is a non-zero group homomorphism. Let $\pi \in K$ be a prime element of v , then $v \circ N_{L/K}(\pi) = v(\pi^n) = n > 0$. So, $v \circ N_{L/K}(L^\times) = f\mathbb{Z}$. Hence it follows $w : L^\times \rightarrow \mathbb{Z}$ is onto.

Now, it only remains to show the triangular inequality. To do so, we need the following supplementary claims:

(a) Let $\alpha \in L$ with $w(\alpha) \geq 0$. Let $u(X) \in K[X]$ be the minimal polynomial of α over K . Then $u(X) \in \mathcal{O}_v[X]$.

(b) Let $\alpha \in K$. If $w(\alpha) \geq 0$, then $w(\alpha + 1) \geq 0$.

By assuming (b), one can show the triangular inequality as follows: Let $\alpha, \beta \in L$. We can assume that $w(\alpha) \leq w(\beta) < \infty$. Then $w(\alpha + \beta) = w(\alpha(1 + \alpha^{-1}\beta)) = w(\alpha) + w(1 + \alpha^{-1}\beta)$. By (b) $w(1 + \alpha^{-1}\beta) \geq 0$. Hence $w(\alpha + \beta) \geq w(\alpha)$.

Also by assuming (a) one can show (b) as follows: Let

$$u(X) = X^r + a_{r-1}X^{r-1} + \dots + a_1X + a_0 \in K[X]$$

be the minimal polynomial of α over K . Let $q(X) = u(X - 1)$. By (a) $q(X) \in \mathcal{O}_v[X]$. Moreover

$$q(1 + \alpha) = u(\alpha + 1 - 1) = u(\alpha) = 0$$

Then $q(X)$ is the minimal polynomial of $\alpha + 1$. So, $N_{L/K}(\alpha + 1) \in \mathcal{O}_v$. Hence $w(\alpha) = v(N_{L/K}(\alpha)) \geq 0$.

We will finish the first part of the proof by proving (a): For the minimal polynomial $u(X) = X^r + a_{r-1}X^{r-1} + \dots + a_1X + a_0$ of α over K clearly $a_0 \in \mathcal{O}_v$ (since $a_0 = N_{L/K}(\alpha) \in \mathcal{O}_v$). Assume that $u(X) \notin \mathcal{O}_v[X]$. Choose $c \in K^\times$ such that for

$$f(X) = cu(X) = cX^r + (ca_{r-1})X^{r-1} + \dots + (ca_i)X^i + \dots + ca_0$$

i is the least index with $v(ca_i) = 0$. Then $\bar{f}(X) \neq 0$, and $0 < \deg \bar{f}(X) = i < r$. Set $\Phi(X) = \bar{f}(X)$, $\Psi(X) = 1$. By Hensel's Lemma there are $g(X), h(X) \in \mathcal{O}_v[X]$ such that $f(X) = g(X)h(X)$ and $\deg g(X) = i > 0$ and $\deg h(X) = r - i > 0$. This contradicts with the fact that $f(X) = cu(X)$ is irreducible in $K[X]$.

(ii) (\subseteq) Let $\alpha \in \mathcal{O}_w$. Then by (a) in the previous part α is integral over \mathcal{O}_v .

(\supseteq) Let $\alpha \in L$ be integral over \mathcal{O}_w . So, $N_{L/K}(\alpha) \in \mathcal{O}_v$. Then $\frac{1}{f}v(N_{L/K}(\alpha)) \geq 0$. Hence, $w(\alpha) \geq 0$. Which means $\alpha \in \mathcal{O}_w$. So \mathcal{O}_w is integrally closed, and by the previous part it is also in the integral closure of \mathcal{O}_v . So, \mathcal{O}_w is the integral closure of \mathcal{O}_v in L .

(iii) Recall that \mathcal{O}_v is a PID, and L is separable over K . Then integral closure of \mathcal{O}_v in L is a free \mathcal{O}_v - module of rank n .

(iv) Assume that \tilde{w} is another extension of v to L . Then $\mathcal{O}_v \subseteq \mathcal{O}_{\tilde{w}}$. But $\mathcal{O}_{\tilde{w}}$ is a PID, hence integrally closed in L . So, since \mathcal{O}_w is the integral closure of \mathcal{O}_v in L we have

$$\mathcal{O}_w \subseteq \mathcal{O}_{\tilde{w}} \subseteq L$$

On the other hand \mathcal{O}_w is a maximal subring of L . Hence $\mathcal{O}_w = \mathcal{O}_{\tilde{w}}$. Implying $w = \tilde{w}$.

(v) Choose a basis (u_1, \dots, u_n) of L over K . Let $(\alpha)_{i \geq 0}$ be a Cauchy sequence in L . Write $\alpha_i = \sum_{j=1}^n a_{ij}u_j$. where $a_{ij} \in K$.

By using lemma 4.1 one can show that for any fixed $s \in \{1, \dots, n\}$, $(a_{is})_{i \geq 0}$ is also a Cauchy sequence. So, we have n Cauchy sequences in K . But we know that K is complete, so $(a_{is})_{i \geq 0}$ is convergent for all s . Say $a_{is} \rightarrow a_s$ as $i \rightarrow \infty$. Define $\alpha = \sum_{j=1}^n a_j u_j$. Then again by lemma 4.1, $\alpha_i \rightarrow \alpha$. Hence (L, w) is complete.

(vi) Choose an element $c \in K$ with $v(c) = 1$. Then

$$e(w|v) = e(w|v)v(c) = w(c) = \frac{1}{f}v(N_{L/K}(c)) = \frac{1}{n}v(c^n)$$

Also, choose $\pi \in L$ with $w(\pi) = 1$. Then $\pi^{e(w|v)\mathcal{O}_w} = c\mathcal{O}_w$ and $k_v = \mathcal{O}_v/\mathcal{M}_v = \mathcal{O}_v/c\mathcal{O}_v$. Consider the following chain

$$\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w \supseteq \pi\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w \supseteq \dots \supseteq \pi^{e(w|v)}\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w$$

Clearly all factor groups in this chain are k_v - vector spaces. We will look at

$$(\pi^j\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w)/(\pi^{j+1}\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w) \simeq \pi^j\mathcal{O}_w/\pi^{j+1}\mathcal{O}_w \simeq \mathcal{O}_w/\pi\mathcal{O}_w$$

Where the isomorphism are vector space isomorphisms. Hence

$$\dim_{k_v}(\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w) = e(w|v) \dim_{k_v}(\mathcal{O}_w/\pi\mathcal{O}_w) = e(w|v) \dim_{k_v}(l_w) = e(w|v)f(w|v)$$

On the other hand since $\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w = \mathcal{O}_w/c\mathcal{O}_w$, $\dim_{k_v}(\mathcal{O}_w/\pi^{e(w|v)}\mathcal{O}_w) = n$.

□

Observe that the key point we used in the proof of the above theorem is Hensel's Lemma while proving that w is a valuation. Therefore we can change the assumption (K, v) is complete by (K, v) is Henselian and prove the same theorem with a minor modification on part (v). It should be modified as " (L, w) is Henselian". But we know that algebraic extensions of Henselian fields are Henselian.

5 Extension of Valuations, Non-Complete Case

In this section we drop the assumption that (K, v) is complete. As in the previous section $L \supseteq K$ is a finite separable extension, and $[L : K] = n$. We are interested in the question how one can extend v to L in this general case.

In the previous section we said that the complete case will form a basis in this case. The following lemma is about the topological nature of (K, v) in (L, w) where L/K is separable and $w|v$.

Lemma 5.1. *Let (K, v) be a discrete valuation field, (L, w) a separable extension. Consider the completion $(\widehat{L}, \widehat{w})$ of (L, w) with $L \subseteq \widehat{L}$. Let \overline{K} be the topological closure of K in \widehat{L} . Then*

(i) \overline{K} is a subfield of \widehat{L} .

(ii) $\bar{v} = \frac{1}{e(w|v)}\widehat{w} : \overline{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ is a valuation of \overline{K} , and (\overline{K}, \bar{v}) is a completion of (K, v) .

(iii) Let $\alpha \in L$ be algebraic over K . Then $K(\alpha)$ is dense in $\overline{K}(\alpha)$. Moreover, if $L = K(\alpha)$, then $\widehat{L} = \overline{K}(\alpha)$.

Proof. (i) Trivial.

(ii) Clearly, K is dense in \overline{K} . So, $e(\widehat{w}|v)\mathbb{Z} = \widehat{w}(K^\times) = \widehat{w}(\overline{K}^\times)$. Then it follows that $\bar{v} = \frac{1}{e(\widehat{w}|v)}\widehat{w} : \overline{K}^\times \rightarrow \mathbb{Z}$ is onto. Hence, \bar{v} is a valuation of \overline{K} and $\bar{v}|v$ and $\widehat{w}|\widehat{v}$.

Next, we will show that \overline{K} is complete. Let $(a_n)_n$ be a Cauchy sequence in \overline{K} . In particular $(a_n)_n$ is a Cauchy sequence in \widehat{L} . But \widehat{L} is complete. Then there is an $a \in \widehat{L}$ such that $a_n \rightarrow a$. Also, \overline{K} is closed. So, $a \in \overline{K}$. Hence \overline{K} is complete.

(iii) Let $x \in \overline{K}(\alpha)$. Then write $x = \sum_{j=0}^{m-1} a_j \alpha^j$, where $a_j \in \overline{K}$. Since K is dense

in \overline{K} there is a sequence $(a_{ji})_i$ in K that converges to a_j for each j . So

$$x = \lim_{i \rightarrow \infty} \sum_{j=0}^{m-1} a_{ji} \alpha^j.$$

□

Now, since L is a finite separable extension, by primitive element theorem we can assume that $L = K(\alpha)$. Let $(\widehat{K}, \widehat{v})$ be a completion of (K, v) . Let $g(X) \in K[X]$ be

the minimal polynomial of α over K . So, $\deg(g(X)) = n$. In $\widehat{K}[X]$, $g(X)$ splits into distinct irreducible factors, say

$$g(X) = g_1(X) \cdots g_r(X)$$

where $g_1(X), \dots, g_r(X) \in \widehat{K}[X]$. Now, choose an $\alpha_i \in \widehat{K}^a$, where \widehat{K}^a is the algebraic closure of \widehat{K} , such that $g_i(\alpha_i) = 0$; and set $M_i = \widehat{K}(\alpha_i)$ where $\deg g_i(X) = [\widehat{K}(\alpha_i) : \widehat{K}] = n_i$. So, $n = \sum_{i=1}^r n_i$.

Let w_i be the unique extension of \widehat{v} to M_i . Furthermore, clearly (M_i, w_i) is complete. Let $\sigma_i : L \rightarrow \widehat{K}(\alpha_i) = M_i$ be the unique embedding over K with $\sigma_i(\alpha) = \alpha_i$.

Theorem 5.2. (i) $\sigma_i(L)$ is dense in M_i with respect to w_i . Let $v_i = w_i \circ \sigma_i$, then v_i is a valuation of L extending v . Moreover (M_i, w_i, σ_i) is a completion of (L, v_i) . Also $e(v_i|v) = e(w_i|\widehat{v})$ and $f(v_i|v) = f(w_i|\widehat{v})$.

(ii) v_1, \dots, v_r are distinct.

(iii) v_1, \dots, v_r are all extensions of v to L .

(iv) $\sum_{i=1}^r e(v_i|v)f(v_i|v) = n$ (This equality is known as the fundamental equality).

(v) For $\gamma \in L$, $N_{L/K}(\gamma) = \prod_{i=1}^r N_{M_i/\widehat{K}}(\sigma_i\gamma)$, and $Tr_{L/K}(\gamma) = \sum_{i=1}^r N_{M_i/\widehat{K}}(\sigma_i\gamma)$.

Proof. (i) Consider the topological closure $\overline{\sigma_i(L)} = \overline{K(\alpha_i)}$ of $\sigma_i(L)$ in M_i . By the lemma 5.1 $K(\alpha_i)$ is dense in $\overline{K}(\alpha_i)$. Therefore $\overline{K(\alpha_i)} = \overline{K}(\alpha_i) \supseteq \widehat{K}(\alpha_i) = M_i$. Hence $\sigma_i(L)$ is dense in M_i .

The assertions v_i is a valuation of L and (M_i, w_i, σ_i) is a completion of (L, v_i) are clear.

By definition $e(w_i|\widehat{v}) = e(w_{|\sigma_i L}|v)$. We claim that $e(w_{|\sigma_i L}|v) = e(v_i|v)$. Indeed, let $\pi \in K$ be a prime element for v . Then observe that $v_i(\pi) = w_i \circ \sigma_i(\pi) = w_i(\pi)$. Hence $v_i(\pi) = e(w_i|v)$. On the other hand $e(w_{|\sigma_i L}|v) = w_{|\sigma_i L}(\pi) = w_i(\pi)$. Hence $e(w_{|\sigma_i L}|v) = e(v_i|v)$.

(ii) Assume that $v_i = v_j$. Since (M_i, w_i, σ_i) and (M_j, w_j, σ_j) are completions of (L, v_i) there is a unique continuous isomorphism $\varphi : M_i \rightarrow M_j$ such that $\sigma_j = \varphi \circ \sigma_i$.

Recall that on K φ is identity. Also, since φ is continuous, $\varphi|_{\widehat{K}} = id|_{\widehat{K}}$. Observe that

$$\alpha_j = \sigma_j(\alpha) = (\varphi \circ \sigma_i)(\alpha) = \varphi(\alpha_i)$$

Since minimal polynomials of α_i and α_j over \widehat{K} are $g_i(X)$ and $g_j(X)$ respectively, it follows that $i = j$.

- (iii) Let v_0 be a valuation of L with $v_0|v$. Choose a completion $(\widehat{L}_0, \widehat{v}_0)$ of (L, v_0) with $L \subseteq \widehat{L}_0$. Let \overline{K} be the topological closure of K in \widehat{L}_0 . On \overline{K} the valuation is given by

$$\overline{v} = \frac{1}{e(v_0|v)} \widehat{v}|_{\overline{K}}$$

From Lemma 5.1 we know that $(\overline{K}, \overline{v})$ is a completion of (K, v) . Then, as before, there is a unique continuous isomorphism $\varphi_0 : \overline{K} \rightarrow \widehat{K}$ with $\varphi_0|_K = id|_K$.

We also know that $\widehat{L}_0 = \overline{K}(\alpha)$. Extend φ_0 to an embedding of \widehat{L}_0 to \widehat{K}^a , call it φ . We know that $g(\alpha) = 0$. Since $\varphi_0|_K = id|_K$, $\varphi(g(\alpha)) = g(\varphi(\alpha))$. But $g(X) = g_1(X) \cdots g_r(X)$. Then there is an $i \in \{1, \dots, r\}$ such that $\varphi(\alpha)$ is a root of $g_i(X)$.

Let $\psi_i : \widehat{K}(\varphi(\alpha_i)) \rightarrow M_i$ be the unique \widehat{K} isomorphism with $\psi_i(\varphi(\alpha)) = \alpha_i$. Set $\varphi_i : \psi_i \circ \varphi : \widehat{L}_0 \rightarrow M_i$. Also observe that $\varphi_i|_{\overline{K}} = \varphi_0$. Consider the valuation $w_i \circ \varphi_i$ of \widehat{L}_0 . Clearly, $w_i \circ \varphi_i|_{\overline{v}}$. Now, we have two valuations of \widehat{L}_0 extending \overline{v} . Namely, \widehat{v}_0 and $w_i \circ \varphi_i$.

Since in a finite separable extension of a complete field there is only one extension of the valuation below, it follows that $\widehat{v}_0 = w_i \circ \varphi_i$. For $\gamma \in L$, $v_0(\gamma) = \widehat{v}_0(\gamma) = w_i(\varphi_i(\gamma)) = v_i(\gamma)$.

- (iv) Since (M_i, w_i) is the completion of (L, v_i) we have,

$$\sum_{i=1}^r e(v_i|v) f(v_i|v) = \sum_{i=1}^r e(w_i|\widehat{v}) f(w_i|\widehat{v}) = \sum_{i=1}^r n_i = n$$

- (v) Look at the embeddings of M_i into \widehat{K}^a over \widehat{K} . For any $i = 1, \dots, r$ there are n_i many embeddings of M_i into \widehat{K}^a . Call them τ_{ij} where $j \in \{1, \dots, n_i\}$. Then $\tau_{ij} \circ \sigma_i : L \rightarrow \widehat{K}^a$ is an embedding of L which maps α to one of n_j many roots of $g_i(X)$. So, $\{\tau_{ij} \circ \sigma_i : i = 1, \dots, r \text{ and } j = 1, \dots, n_i\}$ is the set of all embeddings of L over K .

Hence, for $\gamma \in L$

$$N_{L/K}(\gamma) = \prod_{i=1}^r \prod_{j=1}^{n_i} (\tau_{ij} \circ \sigma_i)(\gamma) = \prod_{i=1}^r \prod_{j=1}^{n_i} \tau_{ij}(\sigma_i \gamma) = \prod_{i=1}^r N_{M_i/\widehat{K}}(\sigma_i \gamma)$$

□

Let (K, v) be a valued field. A polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in K[X]$ is said to be *Eisenstein* (with respect to v), if $v(a_i) \geq 1$ for $i = 1, \dots, n-1$ and $v(a_0) = 1$. When K is a number field where any valuation comes from a prime ideal the reason of calling such polynomials Eisenstein becomes clear. In the context of number fields these are generalizations of Eisenstein polynomials in \mathbb{Q} . So in the context of general valued fields they should be thought as further generalizations.

Theorem 5.3. *Let (K, v) be a discrete valuation field. Assume that $L = K(\alpha)$ is separable over K , and α is a root of an Eisenstein polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ over K . Let w be an extension of v to L . Then f is irreducible in $K[X]$, and therefore $[L : K] = n$. w is the only extension of v to L with $e(w|v) = n$ and $f(w|v) = 1$. Moreover $w(\alpha) = 1$.*

Conversely, assume that L/K is a separable extension of degree n , and w is an extension of v to L such that $e(w|v) = n$. Then $L = K(\pi)$ and the minimal polynomial of π over K is an Eisenstein polynomial with respect to v .

Theorem 5.4. *Let (K, v) be discrete valuation field, L a separable extension of K with $[L : K] = n$. Suppose that $L = K(\alpha)$, and the minimal polynomial of α , say $g(X)$, is in $\mathcal{O}_v[X]$. Suppose that $\bar{g}(X)$ is irreducible over $\mathcal{O}_v/\mathcal{M}_v$. Then there is a unique extension w of v to L , and $e(w|v) = 1$ and $f(w|v) = n$.*

Conversely, assume there is an extension w of v to L with $f(w|v) = n$. Then there is some $\alpha \in \mathcal{O}_w$ whose minimal polynomial $g(X)$ is in \mathcal{O}_v such that $\bar{g}(X)$ is irreducible over $\mathcal{O}_v/\mathcal{M}_v$.

When $e(w|v) = n$ we say that v is *totally ramified* in L/K , or (L, w) is an *totally ramified extension* of (K, v) . When $e(w|v) = 1$ we say that v is *unramified* in L or (L, w) is an *unramified extension* of (K, v) .

Remark that in this situation one can also show that $\mathcal{O}_w = \mathcal{O}_v[\alpha]$. Such an extension \mathcal{O}_w is called *monogenic*. Let (K, v) be a discrete valuation field and (L, w) an extension. We will say that (L, w) is a *monogenic extension* of (K, v) if \mathcal{O}_w is monogenic (over \mathcal{O}_v). We will show that monogenic extensions have an important place in the ramification theory of valuations.

6 Classical Ramification Theory

Let (K, v) be discrete valuation field L/K a finite separable extension. In this section we will always assume that for an extension w to L , l_w is a separable extension of k_v . Number fields, and function fields in one variable over a perfect constant field, which are classical examples of valued fields, have this property.

Theorem 6.1. *Assume that (K, v) is complete and L a finite separable extension of K of degree $[L : K] = n$. Let w be the extension of v to L , then $e(w|v)f(w|v) = n$. Assume that l_w is separable over k_v . Then there exists an intermediate field $K \subseteq T \subseteq L$ such that $[T : K] = f(w|v)$ and for the unique valuation \tilde{v} of T extending v , one has $e(\tilde{v}|v) = 1$, $f(\tilde{v}|v) = f(w|v)$, $e(w|\tilde{v}) = e(w|v)$ and $f(w|\tilde{v}) = 1$*

Proof. Since l_w is a separable extension of k_v of degree $f(w|v)$, there is a $z \in l_w$ such that its minimal polynomial $g(X)$ over k_v is irreducible and of degree $f(w|v)$. Then we can write $g(X) = (X - z)g_1(X) \in l_w[X]$ where $(X - z)$, and $g_1(X)$ are relatively prime. By Hensel's Lemma there are monic $h_1(X), h_2(X), h_3(X) \in \mathcal{O}_w[X]$ with degrees $f(w|v), 1$, and $f(w|v) - 1$ respectively such that $\overline{h_1}(X) = g(X)$, $\overline{h_2}(X) = (X - z)$, and $h_1(X) = h_2(X)h_3(X)$.

So, $h_2(X) = X - \alpha$ for some $\alpha \in \mathcal{O}_w$, and $h_1(\alpha) = 0$. Set $T = K(\alpha)$, and \tilde{v} to be the valuation of T that extends v . Now, $[T : K] \leq f(w|v)$, but $\overline{h_1}(X) = g(X)$. So, in fact $[T : K] = f(w|v)$ and $f(\tilde{v}|v) = f(w|v)$ by theorem 5.4. Therefore $e(\tilde{v}|v) = 1$. The rest of the proof follows by multiplicativity. \square

Suppose that L is a Galois extension of K with $[L : K] = n$ and $G = \text{Gal}(L/K)$. Set

$$W = \{w : w \text{ is a valuation of } L \text{ with } w|v\}$$

We have already shown that W is finite, say $W = \{w_1, \dots, w_r\}$. The group G acts on W by

$$\sigma w = w \circ \sigma^{-1}$$

Note that $\sigma w|v$, since for $a \in K$, $(\sigma w)(a) = w(\sigma^{-1}a) = w(a)$. Moreover, $\mathcal{O}_{\sigma w} = \sigma(\mathcal{O}_w)$ and $\mathcal{M}_{\sigma w} = \sigma(\mathcal{M}_w)$.

Theorem 6.2. *Let (K, v) be discrete valuation field, L a Galois extension of K , with $G = \text{Gal}(L/K)$. Then all extensions of v to L are conjugate. In group theoretic terms, the action of G on W is transitive.*

Proof. Write $L = K(\alpha)$, and $g(X) \in K[X]$ be the minimal polynomial of α over K . Choose an extension w of v to L and a completion $(\widehat{L}, \widehat{w})$ of (L, w) with $L \subseteq \widehat{L}$. Let

\overline{K} be the topological closure K in $(\widehat{L}, \widehat{w})$

$$\overline{v} = \frac{1}{e(w|v)} \widehat{w}|_{\overline{K}}$$

We know that $(\overline{K}, \overline{v})$ is a completion of (K, v) and $\widehat{L} = \overline{K}(\alpha)$.

Take α_i with $g(\alpha_i) = 0$, $M_i = \overline{K}(\alpha_i) = \overline{K}(\alpha) = \widehat{L}$. Then we obtain all extensions of v to L as $\widehat{w} \circ \sigma_i = w \circ \sigma_i$. \square

Corollary 6.3. *Let (K, v) be discrete valuation field, L a Galois extension of K , with $G = \text{Gal}(L/K)$. Then for all extensions w, w' of v to L , $e(w|v) = e(w'|v)$, $f(w|v) = f(w'|v)$ and $n = [L : K] = e(w|v)f(w|v)r$ where r is the number of extensions of v to L .*

Let (K, v) be a discrete valuation field, and L be a Galois extension of K with $[L : K] = n$ and $\text{Gal}(L/K) = G$. For an extension w of v to L .

$$G_Z(w|v) = \{\sigma \in G : \sigma w = w\}$$

is called the *decomposition group of w over v* . Also in group theoretic terms this is the stabilizer of w under the group action.

$$G_T(w|v) = \{\sigma \in G : w(\sigma z - z) > 0 \text{ for all } z \in \mathcal{O}_w\}$$

is called the *inertia group of $w|v$* . Clearly, $G_T(w|v) \leq G_Z(w|v) \leq G$. Moreover for a $\rho \in G$, $G_Z(\rho w|v) = \rho G_Z(w|v) \rho^{-1}$ and $G_T(\rho w|v) = \rho G_T(w|v) \rho^{-1}$.

Choose a completion $(\widehat{L}, \widehat{w})$ of (L, w) with $L \subseteq \widehat{L}$. If $L = K(\alpha)$ then $\widehat{L} = \widehat{K}(\alpha)$, so $\widehat{L} = \widehat{K}L$. By the translation theorem of Galois theory, \widehat{L} is a Galois extension of \widehat{K} with $\text{Gal}(\widehat{L}/\widehat{K}) = \widehat{G}$. For $\sigma \in \widehat{G}$, $\sigma|_L \in G$. This gives an embedding of \widehat{G} into G . Therefore we can consider \widehat{G} as a subgroup of G .

Lemma 6.4. *In this situation*

$$(i) |G_Z(w|v)| = e(w|v)f(w|v).$$

$$(ii) \text{Gal}(\widehat{L}/\widehat{K}) = \widehat{G} = G_Z(w|v).$$

$$(iii) G_Z(\widehat{w}|\widehat{v}) = G_Z(w|v) \text{ and } G_T(\widehat{w}|\widehat{v}) = G_T(w|v).$$

Theorem 6.5. *Let (L, w) be a Galois extension of (K, v) , and $\text{Gal}(L/K) = G$.*

Then there is a homomorphism

$$\begin{aligned}\Phi : G_Z(w|v) &\rightarrow \text{Aut}(l_w/k_v) \\ \sigma &\mapsto \bar{\sigma}\end{aligned}$$

where $\bar{\sigma}(u + \mathcal{M}_w) = \sigma(u) + \mathcal{M}_w$. Its kernel is $\text{Ker } \Phi = G_T(w|v)$. Moreover, if k_v is perfect, then l_w is a Galois extension of k_v and $\Phi : G_Z(w|v) \rightarrow \text{Gal}(l_w/k_v)$ is surjective. Hence $G_T(w|v) \triangleleft G_Z(w|v)$, $(G_Z(w|v) : G_T(w|v)) = f(w|v)$, and $|G_T(w|v)| = e(w|v)$.

Proof. First we will show that $\bar{\sigma}$ is well defined. Let $u \in \mathcal{O}_w$. Then $\sigma u \in \mathcal{O}_{\sigma w} = \mathcal{O}_w$ and $\sigma(\mathcal{M}_w) \subseteq \mathcal{M}_w$ and Φ is a group homomorphism.

Secondly, let $\sigma \in \text{Ker } \Phi$. Then $\bar{\sigma}(u + \mathcal{M}_w) = \sigma u + \mathcal{M}_w = u + \mathcal{M}_w$ for all $u \in \mathcal{O}_w$ if and only if $\sigma u - u \in \mathcal{M}_w$ for all $u \in \mathcal{O}_w$ if and only if $\sigma \in G_T(w|v)$. Hence $\text{Ker } \Phi = G_T(w|v)$.

Let $f(X) \in \widehat{k}_{\widehat{v}}[X]$ be the minimal polynomial of α over $\widehat{k}_{\widehat{v}}$, and $\deg(f(X)) = f(w|v)$. Choose $g(X) \in \mathcal{O}_{\widehat{v}}[X]$ such that $\bar{g}(X) = f(X)$, and $g(X)$ is monic of degree $f(w|v)$, moreover $g(X) \in \widehat{K}[X]$ is irreducible. Consider $g(X) \bmod \mathcal{M}_w$. Then $\bar{g}(X) = f(X) = (X - \alpha)l(X)$ where $l(X) \in \widehat{l}_{\widehat{w}}$

Now, by Hensel's Lemma

$$g(X) = (X - u)h(X)$$

in $\widehat{L}[X]$ where $\bar{u} = \alpha$. Since \widehat{L} is Galois over \widehat{K} with Galois group \widehat{G} ,

$$g(X) = \prod_{i=1}^{f(w|v)} (X - u_i)$$

where $u_i \in \widehat{L}$, $u = u_1$, $\bar{u}_1 = \alpha$.

Since $g(X) \in \mathcal{O}_{\widehat{v}}[X]$, $u_i \in \mathcal{O}_{\widehat{w}}$. Then $f(X) = \bar{g}(X) = \prod_{i=1}^{f(w|v)} (X - u_i)$, with $u_i \in \widehat{l}_{\widehat{w}}$ pairwise distinct.

Let $\rho \in \text{Gal}(\widehat{l}_{\widehat{w}}/\widehat{k}_{\widehat{v}})$, then $\rho(\alpha) = g(\bar{u}_1 = \bar{u}_j)$ for some $j \geq 1$. Define $\sigma \in \text{Gal}(\widehat{L}/\widehat{K}) = G_Z(w|v)$ by $\sigma(u_1) = u_j$. Then $\bar{\sigma} = \rho$. Hence Φ is onto.

Further,

$$(G_Z(w|v) : G_T(w|v)) = |G_Z(w|v)/G_T(w|v)| = |\text{Gal}(l_w/k_v)| = f(w|v)$$

Then $G_T(w|v) = e(w|v)$. □

We are also interested in the fixed fields of the groups $G_Z(w|v)$ and $G_T(w|v)$. The

fixed field $L^{G_Z(w|v)}$ of $G_Z(w|v)$ will be called the *decomposition field* of $w|v$ and denoted by $Z_{w|v}$ (or simply by Z when the extension w is clear), and the fixed field $L^{G_T(w|v)}$ will be called the *inertia field* of $w|v$ and denoted by $T_{w|v}$ (or simply by T if the extension w is clear from the context).

Lemma 6.6. *Let (K, v) be a discrete valuation field and (L, w) a Galois extension, and Z and T be the decomposition and inertia fields with the normalized valuations w_Z and w_T on them respectively. Then $[Z : K] = r, [T : Z] = f(w|v), [L : T] = e(w|v)$ and $e(w_Z|v) = 1, f(w_Z|v) = 1, e(w_T|w_Z) = 1, f(w_T|w_Z) = f(w|v), f(w|w_T) = 1, e(w|w_T) = e(w|v)$.*

Corollary 6.7. *Let (L, w) be a Galois extension of the discrete valuation field (K, v) with $w|v$. Assume that k_v is perfect. Let M be an intermediate field, and w_M the restriction of w to M . Then*

- (i) $M \subseteq Z$ if and only if $e(w_M|v) = f(w_M|v) = 1$.
- (ii) $M \supseteq Z$ if and only if w is the only extension of w_M to L .
- (iii) $M \subseteq T$ if and only if $e(w_M|v) = 1$.
- (iv) $M \supseteq T$ if and only if w is totally ramified over w_M .

We define the higher ramification groups as follows. For any integer $i \geq -1$ the i^{th} ramification group of $w|v$ is

$$G_i(w|v) = \{\sigma \in G : w(\sigma z - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_w\}$$

One can immediately see that $G_{-1}(w|v) = G_Z(w|v)$, and $G_0(w|v) = G_T(w|v)$. Moreover $G_{i+1} \leq G_i(w|v)$ for all i . Therefore for a fixed w extending v we have a descending chain

$$G_Z(w|v) = G_{-1}(w|v) \geq G_T(w|v) = G_0(w|v) \geq G_1(w|v) \geq \dots \geq 1$$

This chain has the descending chain condition. I.e there is an index j such that for all $i \geq j$ $G_i(w|v) = 1$.

Lemma 6.8. *Let $\sigma \in \text{Gal}(L/K)$, and $i \geq -1$. Then the following are equivalent*

- (i) σ is trivial on the ring $\mathcal{O}_w/\mathcal{M}_w^{i+1}$.
- (ii) $w(\sigma x - x) \geq i + 1$ for all $x \in \mathcal{O}_w$.

Lemma 6.9. *Let $\sigma \in G_0(w|v)$, let $i \geq 0$. Then $\sigma \in G_i(w|v)$ if and only if $\sigma t/t \equiv 1 \pmod{\mathcal{M}_w^i}$, where $\mathcal{M}_w = t\mathcal{O}_w$ (i.e. t is a uniformizer).*

Lemma 6.10. *There is a homomorphism*

$$\chi : G_0(w|v) \rightarrow l_w^\times$$

with $\text{Ker } \chi = G_1(w|v)$.

Proof. Let t be a w -prime element (i.e. t is a uniformizer of \mathcal{M}_w). For $\sigma \in G_0(w|v)$ define

$$\chi(\sigma) = \frac{\sigma t}{t} + \mathcal{M}_w \in l_w^\times$$

Note that since $\sigma \in G_0(w|v)$, $w(\sigma t) = (\sigma^{*1}w)(t) = w(t) = 1$. Also remark that the definition of χ is independent of the choice of the uniformizer t .

Now, we will show that χ is a homomorphism. Let $\sigma, \tau \in G_0(w|v)$.

$$\chi(\sigma\tau) = \frac{\sigma\tau t}{t} + \mathcal{M}_w = \frac{\sigma(\tau t)}{\tau t} \frac{\tau t}{t} + \mathcal{M}_w$$

τt is also a prime element as $w(\tau t) = \tau^{-1}w(t) = w(t) = 1$. Hence $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$.

Next, observe that

$$\begin{aligned} \sigma \in \text{Ker } \chi &\Leftrightarrow \frac{\sigma t}{t} - 1 \in \mathcal{M}_w \Leftrightarrow w\left(\frac{\sigma t}{t} - 1\right) > 0 \\ &\Leftrightarrow w(\sigma t - t) - w(t) \geq 1 \Leftrightarrow w(\sigma t - t) \geq 2 \Leftrightarrow \sigma \in G_1(w|v). \end{aligned}$$

□

Corollary 6.11. *If $\text{Char}(l_w) = p > 0$, then G_0 is the semi-direct product of a cyclic group of order prime to p and a normal subgroup of order p^k for some k .*

Lemma 6.12. *For all $i \geq 1$, there is a homomorphism*

$$\Psi_i : G_i(w|v) \rightarrow (l_w, +)$$

with $\text{Ker } \Psi_i = G_{i+1}(w|v)$.

Proof. Let t be a w -prime element. For $\sigma \in G_i(w|v)$, $w(\sigma t - t) \geq i + 1$. Then $\sigma t = t + u_\sigma t^{i+1}$ for some $u_\sigma \in \mathcal{O}_w$. Then we define $\Psi_i(\sigma) = u_\sigma + \mathcal{M}_w \in l_w$. Note that Ψ_i depends on the choice of t .

Next, we will show that Ψ_i is a homomorphism. Let $\tau \in G_i(w|v)$, and write $\tau t = t + u_\tau t^{i+1}$ for some $u_\tau \in \mathcal{O}_w$. Then

$$\begin{aligned}
\sigma\tau t &= \sigma(t + u_\tau t^{i+1}) = \sigma t + (\sigma t)^{i+1} \sigma(u_\tau) = \sigma t + (t + u_\sigma t^{i+1})^{i+1} (u_\tau + tx) \\
&= \sigma t + t^{i+1} (1 + u_\sigma t^i)^{i+1} (u_\tau + tx) = \sigma t + t^{i+1} (1 + t^i z) (u_\tau + tx) \\
&= t + t^{i+1} u_\sigma + t^{i+1} u_\tau + t^{i+2} r = t + (u_\sigma + u_\tau) t^{i+1} + t^{i+2} r \\
&= t + (u_\sigma + u_\tau + tr) t^{i+1}
\end{aligned}$$

Then $\Psi_i(\sigma\tau) = (u_\sigma + u_\tau + tr) + \mathcal{M}_w = u_\sigma + \mathcal{M}_w + u_\tau + \mathcal{M}_w = \Psi_i(\sigma) + \Psi_i(\tau)$.

Next, observe that

$$\sigma \in \text{Ker } \Psi_i \Leftrightarrow \sigma t = t + ut^{i+2} \Leftrightarrow w(\sigma t - t) \geq i + 2 \Leftrightarrow \sigma \in G_{i+1}(w|v)$$

□

Main properties of the higher ramification groups are given in the following theorem

Theorem 6.13. (i) $|G_{-1}(w|v)| = e(w|v)f(w|v)$.

(ii) $|G_0(w|v)| = e(w|v)$.

(iii) Let $i \geq 0$, $\sigma \in G_0(w|v)$ and $t \in L$ with $w(t) = 1$. Then, $\sigma \in G_i(w|v)$ if and only if $w(\sigma t - t) \geq i + 1$.

(iv) If $\text{Char}(k_v) = 0$ then $G_1(w|v) = \{1\}$ and $G_0(w|v)$ is cyclic.

(v) If $\text{Char}(k_v) = p > 0$ then $G_{i+1}(w|v) \triangleleft G_i(w|v)$ for all $i \geq 1$ and $G_i(w|v)/G_{i+1}(w|v)$ is isomorphic to a subgroup of $(l_w, +)$, hence an elementary p -group.

(vi) If $\text{Char}(k_v) = p > 0$ then $G_1(w|v) \triangleleft G_0(w|v)$ and $G_0(w|v)/G_1(w|v)$ is cyclic of order prime to p .

Proof. (i) Previously we have shown that $[L : K] = n = re(w|v)f(w|v)$ where r is the number of extensions of v to L . Observe that $G_{-1}(w|v)$ is the stabilizer of w under the action of G . Moreover, since the action of G on the set of extensions of v to L is transitive, the orbit length of w is r . Hence, from orbit stabilizer theorem it follows that $|G_{-1}(w|v)| = e(w|v)f(w|v)$.

(ii) Trivial.

(iii) By corollary 6.7 w is totally ramified over v . Then we know that $\mathcal{O}_w = \mathcal{O}_{w_T}[t]$ with $w(t) = 1$.

(\Rightarrow) Clear.

(\Leftarrow) Let $\sigma \in G$ and $w(\sigma t - t) \geq i + 1$, take $z \in \mathcal{O}_w$. We will show that $w(\sigma z - z) \geq i + 1$. Write

$$z = \sum_{j=0}^{e(w|v)-1} x_j t^j$$

where $e(w|v) = [L : T]$, and $x_j \in \mathcal{O}_{w_T}$. Then

$$\sigma z - z = \sum_{j=0}^{e(w|v)-1} x_j ((\sigma t)^j - t^j) = \sum_{j=1}^{e(w|v)-1} x_j ((\sigma t)^j - t^j) = (\sigma t - t)y$$

where $y \in \mathcal{O}_w$. So, $w(\sigma z - z) \geq i + 1$.

(iv) By lemma 6.12 $G_1(w|v)$ is homomorphic to a subgroup of $(l_w, +)$. But in characteristic 0 no non trivial subgroup of additive subgroups is finite. Hence $G_1(w|v) = \{1\}$. Therefore by lemma 6.10 $G_0(w|v)$ is a finite subgroup of l_w^\times . Hence it is cyclic.

(v) Follows from lemma 6.12, since additive subgroup of a positive characteristic is elementary abelian.

(vi) Follows from lemma 6.10.

□

Consider the filtration with ramification groups

$$G_{-1}(w|v) \geq G_0(w|v) \geq G_1(w|v) \geq \dots \geq G_i(w|v) \geq G_{i+1} \geq \dots \geq 1$$

Next we will answer the natural question for which indices i we have the situation $G_i(w|v) \neq G_{i+1}(w|v)$. Such indices are called the *ramification jumps*. So, in other words we will answer the question where the ramification jumps can be in this filtration.

Lemma 6.14. *Let $\sigma \in G_i(w|v)$ and $\tau \in G_j(w|v)$ where $i, j \geq 1$. Then $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j}(w|v)$ and $\Psi_{i+j}([\sigma, \tau]) = (j - i)\Psi_i(\sigma)\Psi_j(\tau)$, where Ψ_i is the homomorphism given in lemma 6.12.*

Proof. Let t be a uniformizer of \mathcal{M}_w . Then we can write $\sigma t = t(1 + a)$, and $\tau t = t(1 + b)$ for some $a \in \mathcal{M}_w^i$, and $b \in \mathcal{M}_w^j$. Therefore $\sigma\tau t = t(1 + a + \sigma b + a\sigma b)$, and $\tau\sigma t = t(1 + b + \tau a + b\tau a)$.

Now, write $a = t^i\alpha$, and $b = t^j\beta$ for some $\alpha, \beta \in \mathcal{O}_w$. Then

$$\sigma b = \sigma t^j + \sigma\beta = t^j(1+a)^j\sigma\beta$$

Since $\sigma \in G_i(w|v)$, $\sigma\beta \equiv \beta \pmod{\mathcal{M}_w^{i+1}}$; and since $a \in \mathcal{M}_w^i$ we have $(1+a)^j \equiv 1+ja \pmod{\mathcal{M}_w^{i+1}}$. So,

$$\begin{aligned}\sigma b &\equiv \beta t^j(1+ja) \pmod{\mathcal{M}_w^{i+j+1}} \\ &\equiv b + jab \pmod{\mathcal{M}_w^{i+j+1}}\end{aligned}$$

Hence

$$a + \sigma b + a\sigma b \equiv a + b + (j+1)ab \pmod{\mathcal{M}_w^{i+j+1}}$$

and similarly

$$a + \tau a + b\tau a \equiv a + b + (i+1)ab \pmod{\mathcal{M}_w^{i+j+1}}$$

Now let $\tau\sigma t = t'$. Then

$$\begin{aligned}\sigma\tau\sigma^{-1}\tau^{-1}t' &= \sigma\tau t = t(1+a+\sigma b+a\sigma b) = t'(1+a+\sigma b+a\sigma b)(1+b+\tau a+b\tau a)^{-1} \\ &= t'(1+c)\end{aligned}$$

where $c = (a+\sigma b+a\sigma b-b-\tau a-b\tau a)(1+b+\tau a+b\tau a)^{-1} \equiv (j-i)ab \pmod{\mathcal{M}_w^{i+j+1}}$. Hence $[\sigma, \tau] \in G_{i+j}(w|v)$. Write $c = \gamma t^{i+j}$.

Next, observe that $\Psi_i(\sigma) = \alpha + \mathcal{M}_w$, $\Psi_j(\tau) = \beta + \mathcal{M}_w$, and $\Psi_{i+j}([\sigma, \tau]) = \gamma + \mathcal{M}_w$. Therefore,

$$\Psi_{i+j}([\sigma, \tau]) = (j-i)\Psi_i(\sigma)\Psi_j(\tau)$$

□

Theorem 6.15. *Let $i, j \geq 1$. Suppose that $G_i(w|v) \neq G_{i+1}(w|v)$, and $G_j(w|v) \neq G_{j+1}$. Then $i \equiv j \pmod{p}$, where p is the characteristic of l_w .*

Proof. If $G_1(w|v) = \{1\}$ then there is nothing to prove. Observe that this is also the case when $\text{Char}(l_w) = 0$. So we can suppose that $\text{Char}(l_w) = p > 0$. Now, let j be the largest index for which $G_j(w|v) \neq \{1\}$, and let $i > 1$ be such that $G_i(w|v) \neq G_{i+1}(w|v)$. We will show that $i \equiv j \pmod{p}$. Let $\sigma \in G_i(w|v) \setminus G_{i+1}(w|v)$ and $\tau \in G_j(w|v) \setminus G_{j+1}(w|v)$. By lemma 6.14 $[\sigma, \tau] \in G_{i+j}$. Hence $[\sigma, \tau] = 1$. Then $\Psi_{i+j}([\sigma, \tau]) = 0$, but $\Psi_i(\sigma), \Psi_j(\tau) \neq 0$. Therefore $i \equiv j \pmod{p}$.

□

Theorem 6.16. *Consider a separable field extension L of K of degree $[L : K] = n$. Let R, S be subrings of K and L respectively such that $R \subseteq S$. Define the*

complementary module of S/R as

$$\mathcal{C}_{S/R} = \{z \in L : \text{Tr}_{L/K}(zS) \subseteq R\}$$

Then

(i) $\mathcal{C}_{S/R}$ is an S - module. Also for a basis u_1, \dots, u_n of $\mathcal{C}_{S/R}$ let u_1^*, \dots, u_n^* be the dual basis.

(ii) If $\bigoplus_{i=1}^n Ru_i \subseteq S$ then $\mathcal{C}_{S/R} \subseteq \bigoplus_{i=1}^n Ru_i^*$.

(iii) If $\bigoplus_{i=1}^n Ru_i = S$ then $\mathcal{C}_{S/R} = \bigoplus_{i=1}^n Ru_i^*$.

(iv) Suppose $\alpha \in L$ satisfies $L = K(\alpha)$ and $S = R[\alpha]$, and moreover the minimal polynomial $f(X)$ of α over K is in $R[X]$. Then

$$\mathcal{C}_{S/R} = \frac{1}{f'(\alpha)}S$$

Proof. (i) Trivial.

(ii) Let $z \in \mathcal{C}_{S/R} \subseteq L$. Write $\sum_{i=1}^n x_i u_i^*$ where $x_i \in K$. Since $\text{Tr}_{L/K}(zS) \subseteq R$ and $u_j \in S$, $\text{Tr}_{L/K}(z u_j) \in R$ for all j . Then it follows that

$$\text{Tr}_{L/K}(z u_j) = \text{Tr}_{L/K}(u_j \sum_{i=1}^n x_i u_i^*) = \sum_{i=1}^n x_i \text{Tr}_{L/K}(u_j u_i^*) = x_j$$

So, $x_j \in R$.

(iii) Trivial.

(iv) Write $f(x) = (X - \alpha)(\beta_{n-1}X^{n-1} + \beta_{n-2}X^{n-2} + \dots + \beta_1X + \beta_0)$ where $\beta_i \in L$ and $\beta_{n-1} = 1$. The coefficient of X^j in $f(X)$ is in R , hence $\beta_{j-1} - \alpha\beta_j \in R$, for $j = 1, \dots, n-1$. Also note that $\alpha\beta_0 \in R$. Then $\beta_{n-1}, \dots, \beta_0 \in S$.

Now, we claim that the dual basis of $(1, \alpha, \dots, \alpha^{n-1})$ is $(\frac{\beta_0}{f'(\alpha)}, \dots, \frac{\beta_{n-1}}{f'(\alpha)})$. Indeed, consider an algebraically closed field \tilde{K} which contains K and the n distinct embeddings $\sigma_1, \dots, \sigma_n$ of L into \tilde{K} over K .

Set $\alpha_i = \sigma_i(\alpha)$. Then $\alpha_1, \dots, \alpha_n$ are distinct and $f(X) = \prod_{j=1}^n (X - \alpha_j)$. For $0 \leq l \leq n - 1$ define

$$g_l(X) = \left(\sum_{j=1}^n \frac{f(X)\alpha_j^l}{(X - \alpha_j)f'(\alpha_j)} \right) - X^l \in \tilde{K}[X]$$

Moreover $\deg g_l(X) \leq n - 1$. Observe that $g_l(\alpha_k) = 0$ for all $k = 1, \dots, n$, Then $g_l(X)$ is identically zero.

Extend σ_j to an embedding $\sigma_j : L[X] \rightarrow \tilde{K}[X]$. So,

$$\begin{aligned} X^l &= \sum_{j=1}^n \frac{f(X)\alpha_j^l}{(X - \alpha_j)f'(\alpha_j)} = \sum_{j=1}^n \frac{f(X)\sigma_j(\alpha^l)}{(X - \sigma_j(\alpha))\sigma_j(f'(\alpha))} \\ &= \sum_{j=1}^n \sigma_j \left(\frac{f(X)\alpha^l}{(X - \alpha)f'(\alpha)} \right) = \sum_{j=1}^n \sum_{i=1}^{n-1} \sigma_j \left(\beta_i \frac{\alpha^l}{f'(\alpha)} \right) X^i \\ &= \sum_{j=1}^n \left(\sum_{i=1}^{n-1} \sigma_j \left(\beta_i \frac{\alpha^l}{f'(\alpha)} \right) \right) X^i \end{aligned}$$

□

Let L be a separable extension of K of degree n , and $\sigma_1, \dots, \sigma_n : L \rightarrow \tilde{K}$ be the n distinct embeddings of L into an algebraically closed field $\tilde{K} \supseteq K$ over K . Let (u_1, \dots, u_n) be a basis of L over K . Then recall that the discriminant $d(u_1, \dots, u_n)$ is defined as

$$d(u_1, \dots, u_n) = \det(\text{Tr}_{L/K}(u_i u_j))_{i,j=1,\dots,n}$$

or equivalently as

$$d(u_1, \dots, u_n) = (\det(\sigma_i u_j)_{i,j=1,\dots,n})^2$$

Remark that for the dual basis (u_1^*, \dots, u_n^*) of (u_1, \dots, u_n) and the base change matrix Y which maps (u_1^*, \dots, u_n^*) to (u_1, \dots, u_n) we have

$$d(u_1, \dots, u_n) = \det Y$$

For the rest of this chapter we will assume in addition that (K, v) is complete. So v has a unique extension to L , as it is customary, say w . Note that due to the first part of theorem 5.2 and lemma 6.4 working with the completion of (\hat{K}, \hat{v}) does not change any thing in terms of ramification theory. So, by assuming that (K, v) is complete we do not sacrifice anything we did up to this point!

Remark that \mathcal{O}_w and \mathcal{O}_v are Dedekind rings, so any (fractional) ideal $0 \neq A \triangleleft \mathcal{O}_w$ is of the form $A = \mathcal{M}_w^a$ for some $a \in \mathbb{Z}$. For $A = \mathcal{M}_w^a$ we define $\mathcal{N}_{L/K}(\mathcal{M}_w^a) = \mathcal{M}_w^{rf(w|v)}$. This is called the *ideal norm*.

Recall that \mathcal{O}_w is a free \mathcal{O}_v - module of rank n . Then the complementary module $\mathcal{C}_{\mathcal{O}_w/\mathcal{O}_v}$ is a free \mathcal{O}_v - module, and it is also a module over \mathcal{O}_w . For the sake of simplicity we put, $\mathcal{C}_{L/K} = \mathcal{C}_{\mathcal{O}_w/\mathcal{O}_v}$. So, $\mathcal{C}_{L/K}$ is fractional ideal of \mathcal{O}_w . But we know that $\mathcal{O}_w \subseteq \mathcal{C}_{L/K}$. The ideal

$$\text{Diff}(L/K) = \mathcal{C}_{L/K}^{-1}$$

is called the *different of L/K*. Thus, $\text{Diff}(L/K) \triangleleft \mathcal{O}_w$. Hence, $\text{Diff}(L/K) = M_w^{d(w|v)}$ for some $d(w|v) \geq 0$. This $d(w|v)$ is called the *different exponent* of $w|v$.

The *discriminant of L/K* is defined as $\text{Discr}(L/K) = \mathcal{N}_{L/K}(\text{Diff}(L/K))$, which is an ideal of \mathcal{O}_v .

Theorem 6.17. (i) For $0 \neq \alpha \in L$, $\mathcal{N}_{L/K}(\alpha\mathcal{O}_w) = N_{L/K}(\alpha)\mathcal{O}_v$.

(ii) Let A, B be fractional ideals of \mathcal{O}_w . Let (u_1, \dots, u_n) and (z_1, \dots, z_n) be bases of A, B over \mathcal{O}_v respectively. Write

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = X \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

for some $X \in \text{GL}_n(K)$. Then $\mathcal{N}_{L/K}(A^{-1}B) = \det X \cdot \mathcal{O}_v$

(iii) Assume that $\mathcal{O}_w = \sum_{i=1}^n \mathcal{O}_v u_i$. Then $\mathcal{C}_{L/K} = \sum_{i=1}^n \mathcal{O}_v u_i^*$, and $\text{Discr}(L/K) = d(u_1, \dots, u_n)\mathcal{O}_v$.

(iv) Assume that $\mathcal{O}_w = \mathcal{O}_v[\alpha]$, and let $g(X) \in \mathcal{O}_v[X]$ be the minimal polynomial of α over K . Then

$$\text{Diff}(L/K) = g'(\alpha)\mathcal{O}_w$$

Proof. (i) We know that $\alpha\mathcal{O}_w = \mathcal{M}_w^{w(\alpha)}$. So, $\mathcal{N}_{L/K}(\alpha\mathcal{O}_w) = \mathcal{M}_w^{w(\alpha)f(w|v)}$. On the other hand $w(\alpha) = \frac{1}{f(w|v)}v(N_{L/K}(\alpha))$. Then $N_{L/K}(\alpha)\mathcal{O}_v = \mathcal{M}_v^{f(w|v)w(\alpha)}$.

(ii) Choose $\pi \in L$ with $w(\pi) = 1$. Write $A = \pi^r \mathcal{O}_w, B = \pi^s \mathcal{O}_w$ where $r, s \in \mathbb{Z}$. Then $B = \pi^{s-r} A$. So,

$$\sum_{i=1}^n \mathcal{O}_v z_i = B = \pi^{s-r} \sum_{i=1}^n \mathcal{O}_v u_i = \sum_{i=1}^n \mathcal{O}_w \pi^{s-r} u_i$$

Then

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = Y \begin{pmatrix} \pi^{s-r} u_1 \\ \vdots \\ \pi^{s-r} u_n \end{pmatrix} = YZ \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

Where $Y \in \mathrm{GL}_n(\mathcal{O}_v)$, and $Z \in \mathrm{GL}_n(K)$ describes multiplication by π^{s-r} .

So, $X = YZ$. Then

$$\begin{aligned} \det X \cdot \mathcal{O}_v &= (\det Y \cdot \mathcal{O}_v)(\det Z \cdot \mathcal{O}_v) = \det Z \cdot \mathcal{O}_v \\ &= \mathcal{N}_{L/K}(\pi^{s-r})\mathcal{O}_v = \mathcal{N}_{L/K}(\pi^{s-r}\mathcal{O}_w) = \mathcal{N}_{L/K}(A^{-1}B) \end{aligned}$$

(iii) Take $A = \mathcal{C}_{L/K} = \mathrm{Diff}(L/K)^{-1} = \sum_{i=1}^n \mathcal{O}_v u_i^*$, and $B = \mathcal{O}_w = \sum_{i=1}^n \mathcal{O}_v u_i$ in the previous part. Write

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = X \begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix}$$

Then $d(u_1, \dots, u_n) = \det X$. So,

$$d(u_1, \dots, u_n)\mathcal{O}_v = \det X \cdot \mathcal{O}_v = \mathcal{N}_{L/K}(A^{-1}B) = \mathcal{N}_{L/K}(\mathrm{Diff}(L/K)) = \mathrm{Discr}(L/K)$$

(iv) By theorem 6.16 $\mathrm{Diff}(L/K) = \mathcal{C}_{L/K}^{-1} = g'(\alpha)\mathcal{O}_w$. □

Theorem 6.18. *Let $K \subseteq M \subseteq L$ be finite separable extensions of complete discrete valuation fields with valuations v, v', w respectively. Then*

(i) *For any fractional ideal A of \mathcal{O}_w , $\mathcal{N}_{L/K}(A) = \mathcal{N}_{M/K}(\mathcal{N}_{L/M}(A))$.*

(ii) *$\mathrm{Diff}(L/K) = \mathrm{Diff}(M/K)\mathrm{Diff}(L/M)$.*

(iii) *$d(w|v) = e(w|v')d(v'|v) + d(w|v')$.*

(iv) *$\mathrm{Discr}(L/K) = \mathcal{N}_{M/K}(\mathrm{Discr}(L/M))\mathrm{Discr}(M/K)^{[L:M]}$.*

Proof. (i) Trivial.

(ii) Equivalently we will show that $\mathcal{C}_{L/K} = \mathcal{C}_{M/K}\mathcal{C}_{L/M}$.

(\subseteq) Let $x \in \mathcal{C}_{L/K}$. Clearly $\mathrm{Tr}_{L/M}(xy) \in \mathcal{C}_{M/K}$. Now, write $\mathcal{C}_{M/K} = u\mathcal{O}_{v'}$ where $u \in M$. Then $\mathrm{Tr}_{L/M}(xy) = ut$ for some $t \in \mathcal{O}_v$. So, $\mathrm{Tr}_{L/M}(u^{-1}xy) = t \in \mathcal{O}_{v'}$.

So, for all $y \in \mathcal{O}_w$, $Tr_{L/M}((u^{-1}x)y) \in \mathcal{O}_{v'}$. Then $x \in u\mathcal{C}_{L/M}$. Hence $x \in \mathcal{C}_{L/M}\mathcal{C}_{M/K}$.

(\supseteq) Let $x_1 \in \mathcal{C}_{M/K}$, $x_2 \in \mathcal{C}_{L/M}$, $y \in \mathcal{O}_w$. Then

$$Tr_{L/K}(x_1x_2y) = Tr_{M/K}(Tr_{L/M}(x_1x_2y)) = Tr_{M/K}(x_1Tr_{L/M}(x_2y)) \in \mathcal{O}_v$$

(iii) Follows from the previous part.

(iv)

$$\begin{aligned} \text{Discr}(L/K) &= \mathcal{N}_{L/K}(\text{Diff}(L/K)) = \mathcal{N}_{L/K}(\text{Diff}(M/K)\mathcal{O}_w)\mathcal{N}_{L/K}(\text{Diff}(L/M)) \\ &= \mathcal{N}_{M/K}(\mathcal{N}_{L/M}(\text{Diff}(M/K)\mathcal{O}_w))\mathcal{N}_{M/K}(\mathcal{N}_{L/M}(\text{Diff}(L/M))) \\ &= \mathcal{N}_{M/K}(\text{Diff}(M/K))^{[L:M]} \text{Discr}(L/M) \\ &= \text{Discr}(M/K)^{[L:M]} \text{Discr}(L/M) \end{aligned}$$

□

Theorem 6.19. (*Dedekind's different theorem*) Let (K, v) be a complete discrete valuation field, L a finite Galois extension of K , and w be the unique extension of v to L . Assume that l_w is a separable extension of k_v . Say $\text{Diff}(L/K) = \mathcal{M}_w^{d(w|v)}$. Then

(i) $d(w|v) \geq e(w|v) - 1$.

(ii) $d(w|v) = e(w|v) - 1$ if and only if $\text{Char}(k_v) \nmid e(w|v)$.

The case $d(w|v) > e(w|v) - 1$ is said to be the *wild ramification* and the case $d(w|v) = e(w|v) - 1$ is *tame ramification*.

Proof. (i) Choose an intermediate field $K \subseteq T \subseteq L$, and let v' be the canonical valuation on T extending v , with $e(w|v') = e(w|v) = [L : T]$, $f(w|v') = 1$, and $e(v'|v) = 1$, $f(v'|v) = f(w|v) = [T : K]$.

By, theorem 5.4 there exists an $\alpha \in T$ such that $\mathcal{O}_{v'} = \mathcal{O}_v[\alpha]$, and let $g(X)$ be the minimal polynomial of α over K . Then $g(X) \in \mathcal{O}_v[X]$, and $\bar{g}(X) \in k_v$ is irreducible over, and hence separable. So, it follows that

$$\bar{g}'(\bar{\alpha}) = \overline{g'(\alpha)} \neq 0$$

Hence $g'(\alpha)\mathcal{O}_{v'} = \mathcal{O}_{v'}$. So it follows $\text{Diff}(T/K) = \mathcal{O}_{v'}$ by theorem 6.17. Then

$$\text{Diff}(L/K) = \text{Diff}(T/K)\text{Diff}(L/T) = \text{Diff}(L/T)$$

Since different is transitive it follows that $\mathcal{M}_w^d = \text{Diff}(L/K) = \text{Diff}(L/T)$. Recall that $w|v'$ is totally ramified. So, $\mathcal{O}_w = \mathcal{O}_v'[\pi]$ where π is a prime element of (L, w) .

Moreover, the minimal polynomial of π over T is of the form

$$h(X) = X^{e(w|v)} + a_{e(w|v)-1}X^{e(w|v)-1} + \dots + a_0$$

with $v'(a_i) \geq 1$ for all $i = 1, \dots, e(w|v) - 1$, and $v'(a_0) = 1$. By theorem 6.17, $\text{Diff}(L/T) = h'(\pi)\mathcal{O}_w$. So, $d(w|v) = w(h'(\pi))$.

$$h'(\pi) = e(w|v)\pi^{e(w|v)} + (e(w|v) - 1)a_{e(w|v)-1}\pi^{e(w|v)-2} + \dots + a_1$$

Observe that $w(e(w|v)\pi^{e(w|v)}) \geq e(w|v) - 1$ and $w((e(w|v) - i)a_{e(w|v)-i}\pi^{e(w|v)-i-1}) \geq e(w|v)$ for all $i = 1, \dots, e(w|v) - 2$ and $w(a_1) \geq e(w|v)$. So, $w(h'(\pi)) \geq e(w|v) - 1$.

(ii) Assume that $\text{Char}(k_v) \mid e(w|v)$. So, $e(w|v) \bmod \mathcal{M}_v \equiv 0$. Which means $e(w|v) \in \mathcal{M}_v$. Therefore $v(e(w|v)) \geq 1$. So, $w(e(w|v)) \geq e(w|v)$. By triangular inequality, $w(h'(\pi)) \geq e(w|v)$.

Conversely, assume that $\text{Char}(k_v) \nmid e(w|v)$. Then $e(w|v) \bmod \mathcal{M}_v \not\equiv 0$. So, $v(e(w|v)) = 0$. So, $w(e(w|v)) = 0$. Then $w(e(w|v)\pi^{e(w|v)-1}) = e(w|v) - 1$. Hence $w(h'(\pi)) = e(w|v) - 1$.

□

Clearly, the assumption that " l_w is separable over k_v " is not used in the proof of the first part of Dedekind's different theorem. Therefore we can revise this theorem as follows:

Theorem 6.20. *(Dedekind's different theorem) Let (K, v) be a complete discrete valuation field, L a finite Galois extension of K , and w be the unique extension of v to L . Say $\text{Diff}(L/K) = \mathcal{M}_w^{d(w|v)}$. Then*

(i) $d(w|v) \geq e(w|v) - 1$.

(ii) $d(w|v) = e(w|v) - 1$ if and only if $\text{Char}(k_v) \nmid e(w|v)$ and l_w is separable over k_v .

Corollary 6.21. *The following are equivalent:*

(i) $e(w|v) = 1$.

(ii) $\text{Diff}(L/K) = \mathcal{O}_w$.

(iii) $\text{Discr}(L/K) = \mathcal{O}_v$.

Under the assumption that l_w is separable over k_v the connection between the different and the ramification groups is due to Hilbert.

Theorem 6.22. (Hilbert's different formula) *Let (L, w) be a Galois extension of (K, v) . Then*

$$d(w|v) = \sum_{i=0}^{\infty} (|G_i(w|v)| - 1) = w(g'(\alpha))$$

where d is the different exponent of $w|v$, $g(X) \in K[X]$ is the minimal polynomial of α , and $\mathcal{O}_w = \mathcal{O}_v[\alpha]$.

Proof. First assume that $w|v$ is totally ramified, i.e. $e(w|v) = |G|$ where $G = \text{Gal}(L/K)$. Set $e_i = |G_i(w|v)|$, and $e = e_0 = |G_0(w|v)| = |G|$. Write $G_i = G_i(w|v)$ for the sake of simplicity. Choose a $t \in L$ such that $w(t) = 1$. Then $1, t, \dots, t^{e-1}$ is an integral basis of \mathcal{O}_w . So, $d = w(\varphi'(t))$ where $\varphi(X) \in \mathcal{O}_v[X]$ is the minimal polynomial of t over K .

We can write

$$\varphi(X) = \prod_{\sigma \in G} (X - \sigma t)$$

therefore

$$\varphi'(X) = \sum_{\sigma \in G} \prod_{\tau \neq \sigma} (X - \tau t)$$

So, $\varphi'(t - \sigma t)$. Then

$$d = w\left(\pm \prod_{\sigma \neq 1} (\sigma t - t)\right) = \sum_{\sigma \neq 1} w(\sigma t - t) = \sum_{i=0}^{\infty} \sum_{\sigma \in G_i/G_{i+1}} w(\sigma t - t) \quad (6.1)$$

$$= \sum_{i=0}^{\infty} (e_i - e_{i+1})(i+1) = \sum_{i=0}^{\infty} (e_i - 1) \quad (6.2)$$

$$= (e_0 - 1) + (e_1 - 1) + \dots + (e_j - 1) \quad (6.3)$$

where j is the minimal index with $e_j \neq 1$.

For the general case, let T_0 denote the inertia field of $w|v$ and $\mathcal{M}_{w_0} = \mathcal{M}_w \cap T$. Then $w_0|v$ is unramified and $w|w_0$ is totally ramified. We know that $G_i(w|v) = G_i(w|w_0)$. Then

$$d(w|v) = e(w|w_0)d(w_0|v) + d(w|w_0) = d(w|w_0) \quad (6.4)$$

by part (iii) of theorem 6.18. Now it follows from (6.3) and (6.4). \square

Corollary 6.23. *Let (L, w) be a Galois extension of (K, v) , and let (K', v') be an intermediate field with the corresponding normal subgroup $H \triangleleft \text{Gal}(L/K)$. Then*

$$d(v'|v) = \frac{1}{e(v'|v)} \sum_{\sigma \notin H} v'(\sigma\alpha' - \alpha')$$

where $\mathcal{O}_{v'} = \mathcal{O}_v[\alpha']$.

7 Ramification Theory of Valuations With Inseparable Residue Class Field Extensions

In this section we drop the crucial assumption that we made in the classical ramification theory, namely the residue class field extension being separable. We will show that without this assumption some results from the classical ramification theory can be saved or modified such as Dedekind's different formula whereas some other results are not available any longer. We will also consider the monogenic extensions (i.e. where the valuation ring extension is generated by a single element). Monogenic extensions should be considered as an intermediate case between the classical ramification theory and the ramification theory of valuations with inseparable residue class field extension, as we have already shown that separability of residue class field extension implies monogeneity, and we will also show the monogeneity assumption is actually weaker than the separability of the residue class field extension. Also remark that in the classical theory we used the fact that the extension is monogenic to prove most of the results. So the results from the classical case are also true for the monogenic case. Furthermore monogenic extensions in the case of Galois p -extensions will be characterized in this section.

As before, throughout the rest of this section (K, v) will be a complete discrete valuation field, (L, w) will be an extension. Since we are working with complete fields, we write $e_{L/K} = e(w|v)$, and $f_{L/K} = f(w|v)$. Furthermore, we will write $e_{L/K} = e_{L/K}^{\text{tame}} e_{L/K}^{\text{wild}}$ where $e_{L/K}^{\text{tame}}$, the tame ramification index of L/K , is the part of $e_{L/K}$ that is coprime to p . From this point on we drop the assumption " l_w is separable over k_v ". Therefore $\text{Char}(k_v) = p > 0$. Since there may be inseparability in the extension l_w/k_v we need to revise some definitions about ramification. Let $f_{L/K}^s = [l_w : k_v]_s$, and $f_{L/K}^i = [l_w : k_v]_i$, i.e. $f_{L/K}^s$ and $f_{L/K}^i$ denotes the separable and inseparable degree of l_w/k_v respectively. Whenever the extension L/K is clear from the context, we will drop it from the indices and write $e, f, f^i, f^s, e^{\text{tame}}, e^{\text{wild}}$ for simplicity.

| L/K | $f_{L/K}^s$ | $f_{L/K}^i$ | e |
|-------------------------|-------------|-------------|------------------|
| unramified | arbitrary | 1 | 1 |
| tamely ramified | arbitrary | 1 | $p \nmid e(w v)$ |
| totally ramified | 1 | 1 | arbitrary |
| totally wildly ramified | 1 | 1 | p^k |
| weakly unramified | arbitrary | arbitrary | 1 |
| ferociously ramified | 1 | arbitrary | 1 |
| completely ramified | 1 | arbitrary | p^k |

At this point one should remark that we have a monogenic extension whenever $[L : K] = p$ without the separability condition. Simply, we can take $\mathcal{O}_w = \mathcal{O}_v[\alpha]$ where α is w - prime element or a representative of a generator of the residue class field extension.

Suppose now that L is a Galois extension of K , and let $G = \text{Gal}(L/K)$. We can generalize the notion of ramification groups defined in the previous section. Let $i \geq -1$, and $n \geq 0$ be two integers, then the $(i, n)^{\text{th}}$ ramification group of L/K is defined as

$$G_{i,n} = \{\sigma \in G : w(\sigma x - x) \geq i + n, \text{ for all } x \in \mathcal{M}_w^n\}$$

Now observe that that for $i \geq -1$ the classical i^{th} ramification group $G_i = G_{i+1,0}$. Also put $H_i = G_{i,1}$. Clearly we have a descending chain

$$G \supseteq H_{-1} = G_{-1} \supseteq H_0 \supseteq G_0 \supseteq H_1 \supseteq G_1 \supseteq H_2 \dots \supseteq \{1\}$$

Lemma 7.1. *For all $i \geq 1$, there is a group homomorphism*

$$\Psi_{i,n} : G \rightarrow \text{Aut}(\mathcal{M}_w^n / \mathcal{M}_w^{i+n})$$

where $\mathcal{M}_w^n / \mathcal{M}_w^{i+n}$ is considered as a ring, with $\text{Ker } \Psi_{i,n} = G_{i,n}$. Where

$$\begin{aligned} \Psi_{i,n}(\sigma) & : \mathcal{M}_w^n / \mathcal{M}_w^{i+n} \rightarrow \mathcal{M}_w^n / \mathcal{M}_w^{i+n} \\ a + \mathcal{M}_w^{i+n} & \mapsto \sigma a + \mathcal{M}_w^{i+n} \end{aligned}$$

Hence $G_{i,n}$ are normal subgroups of G . In particular, for $n = 0$ and $n = 1$, G_i and H_i are normal subgroups of G .

Observe that in the case of separable residue class field extension (i.e. when l_w is separable over k_v , so $f^i = 1$) we have $G_i = H_i$ for all $i \geq -1$. Indeed, let $T = L^{G_0}$ with the corresponding valuation w' . Then we have $\mathcal{O}_w = \mathcal{O}_T + \mathcal{M}_w$ since $t'_{w'} = l_w$. For $i \geq 1$, $\sigma \in H_i$ operates trivially on $\mathcal{M}_w / \mathcal{M}_w^{i+1}$ by lemma 7.1. Similarly, since $H_i \leq G_0$, σ operates trivially on \mathcal{O}_w . Therefore it operates trivially on $\mathcal{O}_w / \mathcal{M}_w^{i+1}$. Hence $\sigma \in G_i$.

Lemma 7.2. *For all $i \geq 1$ there is an homomorphism*

$$\Phi : G_i \rightarrow (l_w, +)$$

with $\text{Ker } \Phi = H_{i+1}$.

Lemma 7.3. For all $i \geq 1$ there is an homomorphism

$$\Phi : G_0 \rightarrow l_w^*$$

with $\text{Ker } \Phi = H_1$.

Theorem 7.4. (i) $G_{-1} = H_{-1} = H_0 = G$, and $|G| = ef$.

(ii) $|G_0| = ef^i$.

(iii) Recall that $\text{Char}(k_v) = p > 0$, then $G_{i+1} \triangleleft G_i$, and $H_{i+1} \triangleleft H_i$. Moreover $H_i \triangleleft G_{i-1}$. Also G_i/H_{i+1} is isomorphic to a subgroup of $(l_w, +)$, hence it is an elementary abelian group of exponent p for all $i \geq 1$.

(iv) G_0/H_1 is cyclic of order e^{tame} .

(v) H_1 is a p -group and $|H_1| = e^{\text{wild}} f^i$.

Proof. (i) Since (K, v) is complete, w is the unique extension of v to L . Hence $|G| = |G_{-1}| = ef$.

(ii) We will show that l_w/k_v is normal. Let $\bar{a} \in l_w$, and

$$P(X) = \prod_{\sigma \in G} (X - \sigma a)$$

Observe that $P(X)$ is a monic polynomial with coefficients in k_v . Consider the reduced polynomial $\bar{P}(X) \in k_v[X]$. Clearly $\bar{P}(X)$ has $\sigma a + \mathcal{M}_w$ as all of its roots. Hence l_w/k_w is normal. Moreover, $G/G_0 \simeq \text{Aut}(l_w/k_v) = \text{Gal}(l_w^{\text{sep}}/k_v)$ where l_w^{sep} is the separable closure of l_w in k_v [3, Chap. I, Sect. 7].

By the previous part we know that $|G| = ef$, and we just showed that $|G/G_0| = f^s$. Hence $|G_0| = ef^i$.

(iii) Follows from Lemma 7.1 and Lemma 7.2.

(iv) By Lemma 7.3 G_0/H_1 is cyclic and its order is relatively prime to p . As we will show in the next part H_1 is a p -group. Then it follows that $|G_0/H_1| = e^{\text{tame}}$.

(v) Let $\sigma \in H_1$. Then $\sigma y - y \in \mathcal{M}_w^2$ for all $y \in \mathcal{M}_w$. Now let $x \in \mathcal{O}_w$ and observe that

$$\sigma^p x - x = \sigma^{p-1}(\sigma x - x) + \sigma^{p-2}(\sigma x - x) + \dots + \sigma(\sigma x - x) + \sigma x - x$$

But since $\sigma \in G_0$ as well, $\sigma x - x \in \mathcal{M}_w$. Say $\sigma x - x = z \in \mathcal{M}_w$. But then $\sigma z - z \in \mathcal{M}_w^2$. Similarly $\sigma^2 z - z, \dots, \sigma^{p-1} z - z \in \mathcal{M}_w^2$. Hence $\sigma x - x \equiv pz \pmod{\mathcal{M}_w^2}$. On the other hand since $\text{Char}(l_w) = p$, $p \in \mathcal{M}_w$. So, $\sigma x - x \equiv pz \pmod{\mathcal{M}_w^2} \equiv 0 \pmod{\mathcal{M}_w^2}$. Which means $\sigma x - x \in \mathcal{M}_w^2$. Hence $\sigma \in G_1$. But we know that G_1/H_2 has exponent p . Therefore $(\sigma^p)^p \in H_2$. If $(\sigma^p)^p \neq 1$, by the same argument it is in G_2 .

We also know that for sufficiently large k , $G_k = \{1\}$. And it is clear from the above argument that $\sigma^{p^k} \in G_k$. Therefore the order of any element of H_1 is a power of p . Hence H_1 is a p -group.

Moreover, since $|G_0| = e f^i$, and $|G_0/H_1| = e^{\text{tame}}$, it follows $|H_1| = e^{\text{wild}} f^i$. □

By the theorem above $T = T_0 = L^{G_0}$ is the maximal unramified extension of K in L , $E_1 = L^{H_1}$ is the maximal tamely ramified extension of K in L . So the associated tower is as follows:

$$\begin{array}{c} L \\ \left. \begin{array}{c} f_{L/K}^i e_{L/K}^{\text{wild}} \\ E_1 \\ e_{L/K}^{\text{tame}} \\ T = T_0 \\ f_{L/K}^s \\ K \end{array} \right| \end{array}$$

If l_w/k_v is inseparable we can say more about G_0 . It is a semi-direct product of a cyclic group of order prime to p and a normal subgroup of order p^k for some k by Corollary 6.11.

Also, de Smit gave some generalizations of Theorem 6.15, which is about the ramification jumps in the classical case, to the double filtration we defined as follows [4].

Theorem 7.5. *If $\text{Gal}(L/K)$ is abelian then all $i > 0$ for which $G_i \neq H_{i+1}$ are congruent modulo p where $p = \text{Char}(l_w)$. Furthermore if there is such an index i for which $G_i \neq H_{i+1}$, then all j for which $G_j \neq H_j$ are divisible by p .*

Actually the first part of the theorem above remains true if $\text{Gal}(L/K)$ is not abelian.

Theorem 7.6. *Let $T = \{i > 0 : G_i \neq H_{i+1}\}$ and $S = \{j > 0 : H_j \neq G_j\}$. Then for any $i_1, i_2 \in T$, $i_1 \equiv i_2 \pmod{p}$ and for any $j \in S$ with $p \nmid j$, we have $j + i \in T$ for all $i \in T$. Further, $S \subseteq p\mathbb{Z}$ whenever $T \cap p\mathbb{Z} \neq \emptyset$.*

To prove Theorem 7.5 and Theorem 7.6 one needs to work with the \mathcal{O}_v derivations of the graded algebra $\bigoplus_{i \geq 0} (\mathcal{M}_w / \mathcal{M}_w^{i+1})$ as it is done by de Smit in [4].

In the previous section we showed that in the classical case there is connection between the different and the ramification groups. Namely, the Hilbert's different formula. Remark that Hilbert's different formula also holds under the weaker assumption that \mathcal{O}_w is monogenic over \mathcal{O}_v . A formula generalizing theorem 6.22 is due de Smit [5]. We will give de Smit's formula.

Let L/K be a Galois extension with Galois group G . We define the function $i_G : G \rightarrow \mathbb{Z} \cup \{\infty\}$ as $i_G(1) = \infty$, and

$$i_G(\sigma) = \inf_{x \in \mathcal{O}_w} w(\sigma x - x)$$

for $\sigma \neq 1$. Also remark that if $\mathcal{O}_w = \mathcal{O}_v[\alpha]$, then $i_G(\sigma) = w(\sigma\alpha - \alpha)$.

For any $\sigma \in G$ define $\mathfrak{a}_L(\sigma)$ to be the ideal generated by $\{\sigma x - x : x \in \mathcal{O}_w\}$. Since L/K is normal we have $\mathfrak{a}_L(\sigma) = \mathcal{M}_w^{i_G(\sigma)}$. The *monogeneity conductor* $\mathfrak{r}_{L/K}$ is defined to be the ideal \mathcal{M}_w^n where n is the smallest integer such that there is an $\alpha \in \mathcal{O}_w$ with $\mathcal{M}_w^n \subseteq \mathcal{O}_v[\alpha]$. Remark that, $\mathfrak{r}_{L/K} = \mathcal{O}_w$ if and only if \mathcal{O}_w is monogenic over \mathcal{O}_v .

Since L/K is separable, $L = K(\alpha)$ for some α , then we define the conductor of $\mathcal{O}_v[\alpha]$ as $\mathfrak{r}_\alpha = \mathcal{M}_w^n$ where n is the smallest positive integer with $\mathcal{M}_w^n \subseteq \mathcal{O}_v[\alpha]$.

Lemma 7.7. *There is an element $\alpha \in \mathcal{O}_w$ such that for any $\sigma \in G$, $\mathfrak{a}_L(\sigma) = (\sigma\alpha - \alpha)\mathcal{O}_w$.*

Proof. If \mathcal{O}_w is monogenic, say if $\mathcal{O}_w = \mathcal{O}_v[\alpha]$, then for a prime element $t \in \mathcal{O}_w$

$$\mathfrak{a}_L(\sigma) = \mathcal{M}_w^{i_G(\sigma)} = \mathcal{M}_w^{w(\sigma\alpha - \alpha)} = t^{w(\sigma\alpha - \alpha)}\mathcal{O}_w = t^{w(\sigma\alpha - \alpha)}u\mathcal{O}_w$$

where $u \in \mathcal{O}_w^*$ such that $t^{w(\sigma\alpha - \alpha)}u = \sigma\alpha - \alpha$. Hence $\mathfrak{a}_w(\sigma) = (\sigma\alpha - \alpha)\mathcal{O}_w$.

So, now suppose that \mathcal{O}_w is not monogenic. Then k_v cannot be perfect. Hence k_v is also infinite. Now, for any $\sigma \in G \setminus \{1\}$ consider

$$\begin{aligned} \overline{\sigma - 1} & : \mathcal{O}_w / \mathcal{M}_v \mathcal{O}_w \rightarrow \mathfrak{a}_w(\sigma) / \mathcal{M}_w \mathfrak{a}_w(\sigma) \\ a + \mathcal{M}_v \mathcal{O}_w & \mapsto (\sigma - 1)(a) + \mathcal{M}_w \mathfrak{a}_w(\sigma) \end{aligned}$$

Clearly $\overline{\sigma - 1}$ is a non - zero k_v - linear map. Moreover

$$\text{Ker } \overline{\sigma - 1} = \{a + \mathcal{M}_v \mathcal{O}_w : (\sigma - 1)(\mathcal{O}_w) \not\subseteq (\sigma a - a)\mathcal{O}_w\}$$

Since any vector space over an infinite field cannot be written as a finite union of proper subspaces, there is an $\alpha + \mathcal{M}_v \mathcal{O}_w \in \mathcal{O}_w / \mathcal{M}_v \mathcal{O}_w$ which is not in $\text{Ker } \overline{\sigma - 1}$ for any $\sigma \in G \setminus \{1\}$. Therefore $\mathfrak{a}_w(\sigma) = (\sigma\alpha - \alpha)\mathcal{O}_w$. \square

Theorem 7.8.

$$\text{Diff}(L/K)\mathfrak{r}_{L/K} = \prod_{\sigma \neq 1} \mathfrak{a}_L(\sigma)$$

Proof. $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_w$. Consider the conductor \mathfrak{r}_α of $\mathcal{O}_v[\alpha]$ in \mathcal{O}_w . More precisely $\mathfrak{r}_\alpha = \{x \in \mathcal{O}_w : x\mathcal{O}_w \subseteq \mathcal{O}_v[\alpha]\}$. Then $\mathfrak{r}_\alpha \text{Diff}(L/K) = f'(\alpha)\mathcal{O}_w$ where $f(X) \in K[X]$ is the minimal polynomial of α . [3]

Now, since

$$f'(\alpha) = \prod_{\sigma \neq 1} (\alpha - \sigma\alpha) \in \prod_{\sigma \neq 1} \mathfrak{a}_w(\sigma)$$

we have

$$\text{Diff}(L/K)\mathfrak{r}_\alpha \subseteq \prod_{\sigma \neq 1} \mathfrak{a}_w(\sigma)$$

Clearly, $\mathfrak{r}_{L/K} = \mathfrak{r}_\alpha$. So, we have the inclusion \subseteq .

On the other hand observe that $\alpha + \mathcal{M}_v \mathcal{O}_w \notin \text{Ker } \overline{\sigma - 1}$ for all $\sigma \in G \setminus \{1\}$ where $\overline{\sigma - 1}$ is as in lemma 7.7. Then by the same lemma $\mathfrak{a}_L(\sigma) = (\sigma\alpha - \alpha)\mathcal{O}_w$. Therefore

$$\prod_{\sigma \neq 1} \mathfrak{a}_L(\sigma) = f'(\alpha)\mathcal{O}_w$$

\square

Now by the above theorem we can give a generalization of the Hilbert's different formula to non monogenic case, which is due to Bart de Smit [5] as follows:

$$d(w|v) + n = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i=0}^{\infty} (|G_i| - 1) \quad (7.1)$$

where n is the smallest positive integer for which there is an $\alpha \in \mathcal{O}_w$ with $\mathcal{M}_w^n \subseteq \mathcal{O}_v[\alpha]$, i.e. $\mathfrak{r}_\alpha = \mathcal{M}_w^n$.

In the next several results we will consider the ramification groups of the intermediate fields of the Galois extension L/K .

Lemma 7.9. *Let K' be an intermediate field of L/K (i.e. $K \subseteq K' \subseteq L$). Then for any K - embedding $\tau : K' \rightarrow L$*

$$\mathfrak{a}_{K'}(\tau) \mid \prod_{\sigma|_{K'}=\tau} \mathfrak{a}_L(\sigma)$$

where the product ranges over all $\sigma \in G$ such that $\sigma|_{K'} = \tau$.

Proof. By lemma 7.7 there is an $\alpha \in \mathcal{O}_w$ with $K = L(\alpha)$ such that $\mathfrak{a}_L(\sigma) = (\sigma\alpha - \alpha)\mathcal{O}_w$ for all $\sigma \in G$. Let $f \in \mathcal{O}_{v'}[X]$ be the minimal polynomial of α over K' and v' is the corresponding valuation on K' . Then

$$f(X) = \prod_{\sigma \in G'} (X - \sigma\alpha)$$

where $G' = \text{Gal}(L/K')$. Therefore

$$\tau(f)(X) = \prod_{\sigma|_{K'}=\tau} (X - \sigma\alpha)$$

Also observe that $\tau(f)(X) - f(X) \in \mathfrak{a}_{K'}(\tau)[X]$. Therefore

$$\prod_{\sigma|_{K'}=\tau} \mathfrak{a}_L(\sigma) = \left(\prod_{\sigma|_{K'}=\tau} (\sigma\alpha - \alpha) \right) \mathcal{O}_w = \tau(f)(\alpha)\mathcal{O}_w = (\tau(f) - f)(\alpha)\mathcal{O}_w \subseteq \mathfrak{a}_{K'}(\tau)$$

□

Let (K', v') be an intermediate field extension of the Galois extension (L, w) of (K, v) . By the previous theorem, for any $\tau \in \text{Gal}(K'/K)$ there is an ideal $\mathfrak{d}(\tau)$ of \mathcal{O}_w such that $\mathfrak{d}(\tau)\mathfrak{a}_{K'}(\tau) = \prod_{\sigma|_{K'}=\tau} \mathfrak{a}_L(\sigma)$.

The lemma above also provides us with some immediate information about ramification groups of intermediate fields. Namely for a normal subgroup $H \triangleleft G = \text{Gal}(L/K)$ we will find upper and lower bounds for $i_{G/H}(\tau)$. Recall that for any $a \in K'$, we have $w(a) = e(w|v')v'(a)$. Consider the inclusion

$$\prod_{\sigma|_{K'}=\tau} \mathfrak{a}_L(\sigma) \subseteq \mathfrak{a}_{K'}(\tau)$$

as it is shown to be true in the lemma above. Now take w - valuation of both sides to get

$$\sum_{\sigma|_{K'}=\tau} i_G(\sigma) \geq e(w|v')i_{G/H}(\tau)$$

On the other hand, for $\tau \in G/H$ let $\sigma \in G$ such that $\sigma|_{K'} = \tau$. Then clearly $\mathfrak{a}_L(\sigma) \mid \mathfrak{a}_{K'}(\tau)$, i.e. $\mathfrak{a}_{K'}(\tau) \subseteq \mathfrak{a}_L(\sigma)$. Again, take w - valuation of both sides to get

$$e(w|v')i_{G/H}(\tau) = i_G(\sigma)$$

Therefore we can write

$$\frac{1}{e(w|v')} \sup_{\sigma|_{K'}=\tau} i_G(\sigma) \leq i_{G/H}(\tau) \leq \frac{1}{e(w|v')} \sum_{\sigma|_{K'}=\tau} i_G(\sigma) \quad (7.2)$$

Latter, by an example, we will show that these are the best possible bounds which can be found by just considering the ideals $\mathfrak{a}_L(\sigma)$ and $\mathfrak{a}_{K'}(\tau)$.

Lemma 7.10. *Let (L, w) be a Galois extension of (K, v) and (K', v') be an intermediate field. Then*

$$\mathfrak{r}_{L/K'} \mathfrak{r}_{K'/K} \prod_{\tau \neq 1} \mathfrak{d}(\tau) = \mathfrak{r}_{L/K}$$

where $\tau = \text{Gal}(K'/K) \setminus \{1\}$.

Proof. First of all write

$$\text{Diff}(L/K) \mathfrak{r}_{L/K} = \prod_{\sigma \neq 1} \mathfrak{a}_L(\sigma) = \prod_{\sigma|_{K'} \neq 1} \mathfrak{a}_L(\sigma) \cdot \prod_{\sigma|_{K'} = 1} \mathfrak{a}_L(\sigma)$$

Next observe that the Galois automorphism $\sigma \in \text{Gal}(L/K)$ with $\sigma|_{K'} = 1$ are exactly the Galois automorphisms of L over K' . Hence, by theorem 7.8

$$\prod_{\sigma|_{K'} = 1} \mathfrak{a}_L(\sigma) = \mathfrak{r}_{L/K'} \text{Diff}(L/K')$$

Now, recall that the Galois group $\text{Gal}(K'/K)$ is finite. Say, $\tau_1, \dots, \tau_{n-1}$ are its non-identity elements. Then we can write

$$\prod_{\sigma|_{K'} \neq 1} \mathfrak{a}_L(\sigma) = \prod_{\sigma|_{K'} = \tau_1} \mathfrak{a}_L(\sigma) \cdots \prod_{\sigma|_{K'} = \tau_{n-1}} \mathfrak{a}_L(\sigma)$$

Observe that $\prod_{\sigma|_{K'} = \tau_i} \mathfrak{a}_L(\sigma) = \mathfrak{d}(\tau_i) \mathfrak{a}_{K'}(\tau_i)$ for all $i = 1, \dots, n-1$ by definition of $\mathfrak{d}(\tau)$.

Therefore,

$$\prod_{\sigma|_{K'} \neq 1} \mathfrak{a}_L(\sigma) = \prod_{i=1}^{n-1} \mathfrak{a}_{K'}(\tau_i) \cdot \prod_{i=1}^{n-1} \mathfrak{d}(\tau_i) = \text{Diff}(K') \mathfrak{r}_{K'/K} \prod_{i=1}^{n-1} \mathfrak{d}(\tau_i)$$

Hence

$$\text{Diff}(L/K) \mathfrak{r}_{L/K} = \mathfrak{r}_{L/K'} \text{Diff}(L/K') \text{Diff}(K') \mathfrak{r}_{K'/K} \prod_{i=1}^{n-1} \mathfrak{d}(\tau_i)$$

By cancellation of differentials we get the desired result. \square

Corollary 7.11. *Let (L, w) be a Galois extension of (K, v) and (K', v') be an intermediate field. Then $\mathfrak{r}_{L/K'} \mathfrak{r}_{K'/K} \mid \mathfrak{r}_{L/K}$. Moreover, if \mathcal{O}_w is monogenic over \mathcal{O}_v , then $\mathcal{O}_{w'}$ is also monogenic over \mathcal{O}_v ; furthermore in this situation we have equality in theorem 7.8, and $\mathfrak{d}(\tau) = 1$ where $\tau \in \text{Gal}(K'/K) \setminus \{1\}$.*

By the above corollary, on the the right side of the inequality (7.2) becomes an equality in the monogenic case.

For a proof see [5].

Theorem 7.12. *(Herbrand's property) Let (L, w) be a monogenic extension of (K, v) , and $H \triangleleft G = \text{Gal}(L/K)$. Then for all $\tau \in G/H$*

$$i_{G/H}(\tau) = \frac{1}{e(w|v')} \sum_{\sigma|_{K'}=\tau} i_G(\sigma)$$

where v' is the corresponding valuation on $K' = L^H$.

Proof. If $\tau = 1$ both sides are equal to ∞ . Let α, β be the generators of \mathcal{O}_w and \mathcal{O}_{w_H} over \mathcal{O}_v respectively. Now $e(w|v')i_{G/H}(\tau) = w(\tau\beta - \beta)$, and $i_G(\sigma) = w(\sigma\alpha - \alpha)$. Choose a $\sigma \in G$ such that $\bar{\sigma} = \tau$. Then the other representatives are of the form $\sigma\rho$ for $\rho \in H$.

Now we will show that $a = \sigma\beta - \beta$ and $b = \prod_{\rho \in H} (\sigma\rho\alpha - \alpha)$ generate the same ideal of \mathcal{O}_w . So, let $f(X) \in \mathcal{O}_{w_H}[X]$ be the minimal polynomial of α over T . Then

$$f(X) = \prod_{\rho \in H} (X - \rho\alpha)$$

Then clearly

$$\sigma(f)(X) \prod_{\rho \in H} (X - \sigma\rho\alpha)$$

Now observe that all coefficients of $\sigma(f) - f$ are divisible by $\sigma\beta - \beta$. Therefore $a = \sigma\beta - \beta$ divides $\sigma(f)(\alpha) - f(\alpha) = \sigma(f)(\alpha) = \pm b$.

Next, we will show that b divides a . Observe that $\beta = g(\alpha)$ for some $g \in \mathcal{O}_v[X]$. Then α is a root of the polynomial $g(X) - \beta$. Moreover all of its coefficients are in \mathcal{O}_{w_H} . Hence, it is divisible by f . Say

$$g(X) - \beta = f(X)h(X)$$

for some $h(X) \in \mathcal{O}_{w_H}[X]$. By applying σ to this equality and evaluating at α we get

$$\beta - \sigma\beta = \sigma(f)(\alpha)\sigma(h)(\alpha)$$

Hence $b = \pm\sigma(f)(\alpha)$ divides a . □

In the classical case Herbrand's property already tells what are the ramification groups of the intermediate fields of the Galois extension L/K in terms of the ramification groups of L/K . Although we will show that the ramification groups of an intermediate field cannot be determined by the ramification groups of L/K .

Corollary 7.13. *Let (L, w) be a Galois extension of (K, v) with Galois group $G = \text{Gal}(L/K)$. Assume that l_w is separable over k_v . Consider the quotient G/G_j . It is the Galois group of $K' = L^{G_j}$. Then $(G/G_j)_i = G_i/G_j$ for $i \leq j$, and $(G/G_j)_i = \{1\}$ for $i \geq j$.*

Proof. Clearly, we have

$$G_0/G_j \subseteq G_1/G_j \subseteq \dots \subseteq G_i/G_j \subseteq \dots \subseteq G_{j-1}/G_j \subseteq G_j/G_j = \{1\}$$

where $i \leq j$. In other words, the quotients G_i/G_j forms a decreasing filtration of the Galois group G/G_j of K' . Let $\tau \in G/H \setminus \{1\}$. Then there is a unique $i < j$ for which $\tau \in G_i/G_j$ but $\tau \notin G_{i+1}/G_j$.

Let $\sigma \in G$ be a representative of τ . Then $\sigma \in G_i$ but $\sigma \notin G_{i+1}$. So $i_G(\sigma) = i + 1$. Also, since $G_j \leq G_0$ the extension L/K' is totally ramified by corollary 6.7. Moreover $|G_j| = e(w|v')$ where w and v' are the valuations on L and K' respectively. By Herbrand's property

$$i_{G/G_j}(\tau) = \frac{1}{e(w|v')} \sum_{\sigma|_{K'}=\tau} i_G(\sigma) = i + 1$$

Therefore the filtration given by G_i/G_j as above is the same as the filtration $(G/G_j)_i$ for $i \leq j$. A fortiori we have $(G/G_j)_i = G_i/G_j$ for $i \leq j$. □

Remark that one can generalize corollary 7.13 for an arbitrary normal subgroup of $\text{Gal}(L/K)$. But for this one needs to modify the numbering of the ramification groups, more precisely one needs the so called *upper numbering of ramification groups* to generalize corollary 7.13 for arbitrary normal subgroups [3]. We will not define the upper numbering in this thesis, but one should also remark that there is no satisfactory definition of the upper numbering of ramification groups in the case of inseparable residue class field extensions [4].

Now we will show that the previous lemma about ramification groups of intermediate fields of L/K in the classical case cannot be generalized.

Example 7.14. Let k be an imperfect field of characteristic p . Consider the field of formal Laurent series over k , say $K = k((t))$ with the natural valuation on it; denoted by v . Fix $s \in \{1, \dots, p\}$, and let $K' = K(\pi)$ where π is a root of the polynomial $f(X) = X^p - t^{s(p-1)}X - t \in \mathcal{O}_v[X]$. Observe that $f(X)$ is an Eisenstein polynomial with respect to v . Therefore $[K' : K] = p$, $e(v'|v) = p$ and $v'(\pi) = 1$. Also, K'/K is Galois with the Galois group $G = \langle \tau | \tau : \pi \mapsto \pi + t^s \rangle$. Moreover, as $\text{Char}(k_v) \mid e(v'|v)$, K' is a wildly ramified extension of K . More precisely K' is totally wildly ramified! Since π is a v' -prime element, $\mathcal{O}_{v'} = \mathcal{O}_v[\pi]$.

Now, let $a \in k \setminus k^p$, and $L = K'(\alpha)$ where α is a root of $g(X) = X^p - t^{2(p-1)} - a - t^{p-s}(1 - t^{p-1})\pi \in K'[X]$, denote the extension of v' to L by w . Then L/K' is Galois with the Galois group $H = \langle \sigma | \sigma : \alpha \mapsto \alpha + t^2 \rangle$. Observe that $l_w = l'_v(\bar{\alpha})$, moreover it is purely inseparable. Hence we also have $\mathcal{O}_w = \mathcal{O}_{v'}[\alpha]$.

We can extend σ to L by $\sigma : \alpha \mapsto \alpha + t$. Moreover $\text{Gal}(L/K) = \langle \tau, \sigma \rangle$ is elementary abelian of order p^2 . The filtration of $\text{Gal}(L/K)$ with ramification groups of the extension L/K can be computed as follows:

$$G = G_0 = \dots = G_{p-1} \neq G_p = \langle \sigma \rangle = \dots = G_{2p-1} \neq G_{2p} = \{1\}$$

On the other hand observe that the first trivial ramification group of K'/K is $(\text{Gal}(L/K)/H)_{sp}$. If one considers $s > 1$, the lemma above, if it was true, would yield that $G_p/H = (\text{Gal}(L/K)/H)_p = \{1\}$. Which is not the case as we have shown. Therefore, the previous lemma even cannot be generalized.

Next, we will verify the bounds given by (7.2). Consider the subgroup $\text{Gal}(L/K)/H = G$. One can easily compute that the given inequality becomes

$$p \leq sp \leq p^2$$

Observe that when $s = p$ we have equality on the right hand side, and we have equality on the left hand side when $s = 1$. Therefore, the bound given by (7.2) can be reached.

Theorem 7.15. Let (L, w) be a finite Galois p -extension of (K, v) . Then the following are equivalent

- (i) $\mathcal{O}_w = \mathcal{O}_v[\alpha]$ for some $\alpha \in L$.
- (ii) For any normal subgroup $H \triangleleft G$ the Herbrand property holds.
- (iii) the Hilbert formula holds.

Proof. ($i \Rightarrow ii$) Proved in theorem 7.12.

($i \Rightarrow iii$) Proved in the previous section as Hilbert's different formula (see theorem 6.22).

($iii \Rightarrow i$) Follows from the formula (7.1). Since Hilbert's formula holds, $n = 0$ in the formula (7.1). Hence \mathcal{O}_w is monogenic over \mathcal{O}_v .

($ii \Rightarrow i$) Since L/K is a Galois p -extension, $[L : K] = p^n$. We will proceed by induction on n . If $n = 1$, as there is no non trivial intermediate extension, there is nothing to be shown.

Next, assume this implication holds for $n - 1$. Let $H \triangleleft G$ with $|H| = p^{n-1}$, and put $L^H = K'$ with v' as the corresponding valuation. By definition

$$\mathfrak{d}(\tau)\mathfrak{a}_{K'}(\tau) = \prod_{\sigma|_{K'}=\tau} \mathfrak{a}_L(\sigma)$$

for all $\tau \in \text{Gal}(K'/K) \simeq G/H$. Now by taking valuation (with respect to w) of both sides we get

$$w(\mathfrak{d}(\tau)) + i_{G/H}(\tau) = \sum_{\sigma|_{K'}} i_G(\sigma)$$

Since Herbrand property holds $w(\mathfrak{d}(\tau)) = 0$. Implying that $\mathfrak{d}(\tau) = \mathcal{O}_w$. Therefore by lemma 7.10 we have

$$\mathfrak{r}_{L/K'}\mathfrak{r}_{K'/K} = \mathfrak{r}_{L/K}$$

Since $[K' : K] = p$, it is monogenic and $\mathfrak{r}_{K'/K} = \mathcal{O}_{v'}$.

Next, $A \triangleleft H$ be a normal subgroup, $s \in H$, and $L^A = \tilde{K}$ with the corresponding valuation \tilde{v} . Now, we will show that

$$i_{H/A}(\rho) = \frac{1}{e(w|\tilde{v})} \sum_{s|_{\tilde{K}}=\rho} i_H(s)$$

for all $\rho \in H/A$, where $s \in H$. Then, by inductive hypothesis it will follow that \mathcal{O}_w is monogenic over \mathcal{O}'_v .

Indeed suppose that $\rho \in H/A$ and $s \in H$ with $s|_{\tilde{K}} = \rho$. Then

$$i_{H/A}(\rho) = \inf_{x \in \mathcal{O}'_v} \tilde{v}(\rho x - x) = i_{G/T}(\rho)$$

Observe that

$$\begin{aligned}
i_{H/A}(\rho) &= i_{G/A}(\rho) = \frac{1}{e(w|\tilde{v})} \sum_{s|_{\tilde{K}}=\rho, s \in G} i_G(s) = \\
&= \frac{1}{e(w|\tilde{v})} \sum_{s|_{\tilde{K}}=\rho, s \in H} i_G(s) + \frac{1}{e(w|\tilde{v})} \sum_{s|_{\tilde{K}}=\rho, s \in G \setminus H} i_G(s) = \\
&= \frac{1}{e(w|\tilde{v})} \sum_{s|_{\tilde{K}}=\rho, s \in G} i_H(s)
\end{aligned}$$

since the second sum $\sum_{s|_{\tilde{K}}=\rho, s \in G \setminus H} i_G(s)$ is empty. Then by inductive hypothesis \mathcal{O}_w is monogenic over $\mathcal{O}_{v'}$. Hence $\mathfrak{r}_{L/K'} = \mathcal{O}_w$. Then $\mathfrak{r}_{L/K} = \mathcal{O}_{v'} \mathcal{O}_w = \mathcal{O}_w$, since $\mathfrak{r}_{L/K'} \mathfrak{r}_{K'/K} = \mathfrak{r}_{L/K}$. \square

Remark that the assumption that L/K is a p -extension is only used at proving the implication $(ii \Rightarrow i)$. The theorem can still be proved if we interchange this assumption with L/K is completely ramified [7]. We can say that theorem 7.15 characterizes the monogenic extensions.

Now we will give an example of a monogenic extension with inseparable residue class field extension to verify that being monogenic is indeed more general than having a separable residue class field extension.

Example 7.16. Let (K, v) be a discrete valuation field of characteristic 0. Let $\zeta_{p^2} \in K$ be primitive $p^{2\text{th}}$ root of unity. Let $L = K(\alpha)$ where α is a root of the polynomial $f(X) = X^{p^2} - (1 + u\pi)a^p$ where $a, u \in \mathcal{O}_v^*, \bar{a} \notin k_v^p$, and π is a prime element of (K, v) . Observe that $\frac{\alpha^{p^2}}{a^p} = 1 + u\pi$. Hence $\frac{\bar{\alpha}^p}{\bar{a}} = 1$ in k_v . Therefore, $\bar{\alpha}^p = \bar{a} \in k_v \setminus k_v^p$. Hence $\bar{\alpha} \notin k_v$. So, $\bar{\alpha}$ is purely inseparable over k_v ; implying $f^i \geq p$.

Next, we will show that $e(w|v) \geq p$. Write

$$\begin{aligned}
\left(\frac{\alpha^p}{a} - 1\right)^p &= \left(\frac{\alpha^p}{a}\right)^p - 1 + \binom{p}{1} \left(\frac{\alpha^p}{a}\right)^{p-1} + \dots + \binom{p}{p-1} \\
&= u\pi + \binom{p}{1} \left(\frac{\alpha^p}{a}\right)^{p-1} + \dots + \binom{p}{p-1}
\end{aligned}$$

Now by taking valuation under w of the above equation we get $p \mid e_{L/K}$. Implying, $e(w|v) \geq p$.

The facts $e_{L/K} \geq p$ and $f_i \geq p$ together with the fundamental equality yields that $e_{L/K} = p = f^i$. So l_w is not separable over k_v . Also by checking Herbrand property

one can show $\mathcal{O}_w = \mathcal{O}_v[\alpha]$.

We have shown that although monogeneity assumption is an actual weakening of the separability assumption of residue class field, many of the nice properties from the classical theory such as Hilbert different formula and Herbrand property can be saved. We will show by an example, given by Spriano [6], in the general case nice properties of the classical (and monogenic) case cannot be saved further.

Lemma 7.17. *Let L/K be an extension of complete fields with the corresponding valuations v and w . Let $\pi \in L$ be an w -prime element. Assume $\theta_1, \dots, \theta_{f(w|v)} \in \mathcal{O}_w$ such that $\overline{\theta_1}, \dots, \overline{\theta_{f(w|v)}}$ is a basis of l_w over k_v . Then $\{\theta_i \pi^j : 1 \leq i \leq f(w|v), 0 \leq j \leq e(w|v) - 1\}$ forms a basis of \mathcal{O}_w over \mathcal{O}_v , and a basis of L over K .*

Example 7.18. *Let (K, v) be a complete field of characteristic 0. Let $k_v = \mathbb{F}_2(u_1, u_2)$, and $a, b \in \mathcal{O}_v$ such that $\bar{a} = u_1$ and $\bar{b} = u_2$. Also assume $v(2) = 4$. Consider $f(X) = X^4 - a\pi X^2 + b \in \mathcal{O}_v[X]$. Clearly $f(X)$ is irreducible.*

Define L to be the splitting field of $f(X)$. Let α, β be roots of $f(X)$ such that $\beta \neq \pm\alpha$. Then $K(\alpha)$ is ferociously ramified over K and moreover $[K(\alpha) : K] = 4$. Also the Eisenstein polynomial $g(X) = X^2 - 2\alpha X - \pi(a - 2\alpha^2/\pi)$ is the minimal polynomial of $\alpha + \beta$. Therefore $L = K(\alpha + \beta)$ is totally ramified over $K(\alpha)$, and $e(L/K) = 2$. Hence $[L : K] = 8$. Observe that by lemma 7.17 $\mathcal{O}_w = \mathcal{O}_v[\alpha, \alpha + \beta]$. Then by theorem 7.15, Herbrand property and Hilbert's different formula also fails to hold for L/K .

References

- [1] I. B. Fesenko and S. V. Vostokov, “Local Fields and Their Extensions”, AMS, Translations of Mathematical Monographs, Providence, Rhode Island, 2000.
- [2] H. Koch “Number Theory” AMS, Graduate Studies in Mathematics Vol. 24, Providence, Rhode Island, 2000.
- [3] J. P. Serre, “Corps Locaux” Hermann, Paris, 1962, English Translation: “Local Fields” Graduate Texts in Math. 67, Springer, New York 1979 .
- [4] B. de Smit, “Ramification groups of local fields with imperfect residue class field ”, *J. Number Theory*, 44 No.3 (1993), 229-236.
- [5] B. de Smit, “The different and differentials of local fields with imperfect residue class field”, *Proceedings of Edinburgh Math. Soc.* 40 (1997), 353-365.
- [6] L. Spriano, “On ramification theory of monogenic extensions ”, *Geometry & Topology Monographs Vol. 3: Invitation to higher local fields*, Part I section 18, (2000) 151-164.
- [7] L. Spriano, “Well ramified extensions of complete discrete valuation fields with applications to Kato conductor ”, *Canadian J. Math.* Vol. 52 (6), (2000) 1296-1309.
- [8] O. Zariski and P. Samuel, “Commutative Algebra Vol. I” Graduate Texts in Math. 28, Springer - Verlag, New York, 1975.