A Study of Valued Fields

NEERAJ

A thesis submitted for the partial fulfillment
of the degree of
Doctor of Philosophy

Department of Mathematical Sciences
Indian Institute of Science Education and Research Mohali
Mohali-140306

November 2017

Dedicated

to

my beloved family members

Abstract

Let R be an integrally closed domain with quotient field K and θ be an element of an integral domain containing R with θ integral over R. Let $F(x)$ be the minimal polynomial of θ over K and $\mathfrak{p}$ be a maximal ideal of R. Kummer proved that if $R[\theta]$ is an integrally closed domain, then the maximal ideals of $R[\theta]$ which lie over $\mathfrak{p}$ can be explicitly determined from the irreducible factors of $F(x)$ modulo $\mathfrak{p}$. In 1878, Dedekind gave a criterion to be satisfied by $F(x)$ for $R[\theta]$ to be integrally closed in case R is the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the nonzero prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$. In 2006, Ershov extended Dedekind Criterion replacing $\mathbb{Z}_{(p)}$ by the valuation ring of any Krull valuation. Using Generalized Dedekind Criterion in this thesis, we have given explicit necessary and sufficient conditions involving only a, b, m, n for $R[\theta]$ to be integrally closed when θ is a root of an irreducible trinomial $F(x) = x^n + ax^m + b$ belonging to $R[x]$, R being a valuation ring. As an application, we have deduced that if K_1, K_2 are algebraic number fields which are linearly disjoint over the field of rational numbers and one of them is a quadratic field with the compositum $A_{K_1}A_{K_2}$ integrally closed, A_{K_i} being the ring of algebraic integers of K_i, then the discriminants of K_1, K_2 are coprime. In an attempt to extend the above result to any pair of algebraic number fields linearly disjoint over $K_1 \cap K_2$, we have proved a more general result which deals with the compositum of integral closures of a given valuation ring R in a pair of finite separable extensions of the quotient field K of R which are linearly disjoint over K. In the course of its proof, we have established an analogue for finite extensions of valued fields of the classical result that the discriminant of an extension of algebraic number fields can be expressed as a product of local discriminants as well as a generalization of the weak Approximation Theorem. We have also generalized an extended version of the classical theorem of factorization of Ore for polynomials with coefficients in henselian valued fields of arbitrary rank.

Declaration

The work presented in this thesis has been carried out by me under the supervision of Professor Sudesh Kaur Khanduja at Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Date:

Place: Neeraj

In my capacity as the supervisor of the candidate's thesis work, I certify that the above statements by the candidate are true to the best of my knowledge.

Professor Sudesh Kaur Khanduja

(Supervisor)

Acknowledgements

First and foremost I wish to thank my supervisor, Professor Sudesh Kaur Khanduja. I am very grateful to her for her most valuable guidance, immense support and her constant encouragement. Her enthusiasm and love for teaching is contagious. Her hardworking nature has been a continuous source of inspiration for me. I definitely consider it an honor to have worked with her.

I am thankful to the Director IISER Mohali, Head of the Department of Mathematics, and the Mathematics faculty of Indian Institute of Science Education and Research for providing facilities of the Institute. I also thank Professor I. B. S. Passi for his guidance. I am thankful to IISER Mohali for providing me financial support in the form of research fellowship. A special thanks goes to Dr. P. Visakhi, the librarian IISER Mohali for providing the necessary facilities during the course of my research work. My sincere thanks to Professor Peter Roquette, Emeritus Professor Universität Heidelberg for his keen interest and valuable suggestions.

A special acknowledgement goes to Anuj Jakhar who helped me academically and emotionally through the rough road to finish this thesis. I am also thankful to Dr. Bablesh Jhorar for her timely help. I especially thank my mom, dad, sister and other family members for their unconditional love and care. I would not have made it this far without them.

I thank all my friends Deep Raj, Nishant, Pankaj (too many to list here but you know who you are!) for providing support and friendship I needed.

Date:

Place: Neeraj

Contents

Chapter 1

Introduction

Valuations have been around in mathematics since ancient times. When Euclid proved the fundamental theorem of arithmetic, then this result permitted to code the natural numbers by the exponents with which various primes p divide these numbers; those exponents in fact represent the p-adic valuations used in number theory. The theory of valuations was started in 1912 by the Hungarian mathematician Josef K*ü*rch*á*k [Kur]. K*ü*rch*á*k formally introduced the concept of a valuation of a field K as being a real valued function ϕ defined on K satisfying the following axioms for all $a, b \in K$:
(i) $\phi(a) > 0$ for $a \neq 0, \phi(0) = 0$,
(ii) $\phi(ab) = \phi(a)\phi(b)$,
(iii) $\phi(a + b) \leq \phi(a) + \phi(b)$.
Such functions are now a days called absolute values. Although the formal definition of a valuation was given by K*ü*rch*á*k, the ideas which governed valuation theory in its first phase came from Hensel's theory of p-adic numbers. As pointed out by Peter Roquette in his article "A history of valuation theory" (cf. [K-K-M]), Hensel may be called the grandfather of valuation theory. The development of valuation theory was motivated by the discovery that it is an important tool to study algebraic number fields. Later it was Alexander Ostrowski who played a significant role in developing the theory further to a considerable degree (cf. [Ost1], [Ost2], [Ost3], [Ost4]). Ostrowski introduced the terminology of archimedean and

non-archimedean for absolute values. An absolute value ϕ of a field K is called non-archimedean if $\phi(a+b) \leq \max\{\phi(a), \phi(b)\}$ for all $a, b \in K$. Valuations in additive form were first used by Ostrowski in his 1918 paper [Ost2]. An additive valuation v of a field K is a mapping from K into $\mathbb{R} \cup \{\infty\}$ satisfying the following axioms for all $a, b \in K$:
(i) $v(a) = \infty$ if and only if $a = 0$;
(ii) $v(ab) = v(a) + v(b)$;
(iii) $v(a+b) \geq \min\{v(a), v(b)\}$.
It is clear that the additive valuations of K are in one-to-one correspondence with its non-archimedean absolute values (via the correspondence $v \longrightarrow \phi = exp(-v)$). In 1932, Krull extended the notion of valuation of a field. In this thesis, by a valuation v of a field K, we mean a Krull valuation, i.e., v is a mapping from K onto $G \cup \{\infty\}$, where G is a totally ordered additive abelian group, such that for all $a,\ b$ in K, the following properties are satisfied:
(i) $v(a) = \infty$ if and only if $a = 0$;
(ii) $v(ab) = v(a) + v(b)$;
(iii) $v(a+b) \geq \min\{v(a), v(b)\}$.
The pair (K, v) is called a valued field and G the value group of v. The subring $R_v = \{a \in K \mid v(a) \geq 0\}$ of K with unique maximal ideal $M_v = \{a \in K \mid v(a) > 0\}$ is called the valuation ring of v and R_v/M_v its residue field. As in [En-Pr, §2.1,§3.1], it can be easily seen that the valuation ring R_v of v is integrally closed and the collection of all convex subgroups of G is linearly ordered by inclusion. The order type of the chain of all convex subgroups of the value group G of v distinct from G is called the rank of v. It is well known that v has rank one if and only if G is order isomorphic to a non-zero subgroup of the group of all real numbers under addition (see [En-Pr, Proposition 2.1.1]); that is why rank one valuations are also called real valuations. A valuation whose value group is isomorphic to the group $\mathbb{Z}$ of integers is called discrete. Indeed the oldest known example of a discrete valuation is the p-adic valuation (to be denoted by v_p) of the field $\mathbb{Q}$ of rational numbers which is defined for any non-zero rational number $a = \frac{m}{n}p^r, m, n, r \in \mathbb{Z}, p \nmid mn$ as $v_p(a) = r$. The valuation ring of v_p which is the localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$ will

be denoted by $\mathbb{Z}_{(p)}$.

If K'/K is an extension of fields and v is a valuation of K, then a valuation v' of K' is said to be an extension or a prolongation of v to K' if v' coincides with v on K. In this situation, the valued field (K', v') is said to be an extension of (K, v). For a valued field extension $(K', v')/(K, v)$, if $G \subseteq G'$ and R_v/M_v embedded in $R_{v'}/M_{v'}$ denote respectively the value groups and the residue fields of v, v', then the index $[G' : G]$ and the degree of the field extension $R_{v'}/M_{v'}$ over R_v/M_v are respectively called the index of ramification and the residual degree of v'/v. Two valued fields (K, v) and (K_1, v_1) are said to be isomorphic if there exists an isomorphism λ from K onto K_1 such that $v_1 \circ \lambda = v$. A valued field (K, v) or a valuation v of K is said to be henselian if v has a unique prolongation to the algebraic closure of K. It is known that henselian valued fields are those valued fields for which one of the several equivalent versions of Hensel's Lemma holds (cf. [En-Pr, Theorem 4.1.3]). It was K*ü*rsh*á*k [Kur] who proved in 1913 that every complete rank one valued field is henselian.

Background of work. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ an algebraic integer and A_K denote the ring of algebraic integers of K. It is immediate from Lagrange's theorem [Her, Theorem 2.4.1] for finite groups that if a prime p does not divide the index $[A_K : \mathbb{Z}[\theta]]$, then $A_K \subseteq \mathbb{Z}_{(p)}[\theta]$, $\mathbb{Z}_{(p)}$ being the localization of $\mathbb{Z}$ at $p\mathbb{Z}$. The converse assertion also holds because if p divides $[A_K : \mathbb{Z}[\theta]]$, then by Cauchy's theorem [Her, §2.7], the group $A_K/\mathbb{Z}[\theta]$ has an element $\xi + \mathbb{Z}[\theta]$ of order p, in which case the element ξ of A_K does not belong to $\mathbb{Z}_{(p)}[\theta]$. Thus p does not divide $[A_K : \mathbb{Z}[\theta]]$ if and only if $A_K \subseteq \mathbb{Z}_{(p)}[\theta]$, which is the same as requiring that the integral closure of $\mathbb{Z}_{(p)}$ in K is $\mathbb{Z}_{(p)}[\theta]$. In 1878, Dedekind gave a necessary and sufficient criterion to be satisfied by the minimal polynomial $F(x)$ of θ over $\mathbb{Q}$ so that $p \nmid [A_K : \mathbb{Z}[\theta]]$. He proved that if $\overline{F}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_t(x)^{e_t}$ is the factorization of the polynomial $\overline{F}(x)$ obtained by replacing coefficients of $F(x)$ modulo p as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $g_i(x) \in \mathbb{Z}[x]$ monic, then $\mathbb{Z}_{(p)}[\theta]$ is integrally closed if and only if for each i, either $e_i = 1$ or $\bar{g}_i(x) \nmid \overline{M}(x)$, where $M(x) = \frac{1}{p}(F(x) - \prod\limits_{i=1}^{t} g_i(x)^{e_i})$ (see [Coh, Theorem 6.1.4], [Ded]). As $\mathbb{Z}_{(p)}$ is the valuation ring of the p-adic valuation of rationals, the above criterion gives a motivation to investigate when is a simple ring extension of a valuation ring integrally closed. In 2006, Ershov generalized the above criterion replacing $\mathbb{Z}_{(p)}$ by the valuation ring of a Krull valuation (cf. [Ers],[Kh-Ku1]) and proved the following:

Theorem 1.1.A(Generalized Dedekind Criterion). *Let v be a Krull valuation of arbitrary rank of a field with valuation ring R_v having maximal ideal M_v. For $g(x) \in R_v[x]$, let $\bar{g}(x)$ denote the polynomial obtained on replacing each coefficient of $g(x)$ by its image under the canonical homomorphism from R_v onto R_v/M_v. Let $F(x) \in R_v[x]$ be a monic irreducible polynomial having a root θ in its splitting field and $\overline{F}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_t(x)^{e_t}$ be the factorization of $\overline{F}(x)$ into a product of powers of distinct irreducible polynomials over R_v/M_v with $g_i(x) \in R_v[x]$ monic. Then $R_v[\theta]$ is integrally closed if and only if either $e_i = 1$ for each i or some $e_j > 1$, in which case M_v is a principal ideal say generated by π and $\bar{g}_j(x)$ does not divide $\overline{M}(x)$ for such an index j, where $M(x) = \frac{1}{\pi}(F(x) - g_1(x)^{e_1} \cdots g_t(x)^{e_t})$.*

Using the above criterion in Chapter 2, we have given necessary and sufficient conditions involving a, b, m, n for $R_v[\theta]$ to be integrally closed when θ is a root of an irreducible trinomial $F(x) = x^n + ax^m + b$ belonging to $R_v[x]$. For an element α belonging to R_v, $\bar{\alpha}$ will denote its image under the canonical homomorphism from R_v onto R_v/M_v. We shall denote by D the discriminant of the trinomial $F(x) = x^n + ax^m + b$. It is known (cf. [Swa]) that

$$D = (-1)^{\binom{n}{2}} b^{m-1} [b^{n_1 - m_1} n^{n_1} - (-1)^{n_1} a^{n_1} m^{m_1} (n-m)^{n_1 - m_1}]^{d_0}$$

where $d_0 = \gcd(m, n)$, $n_1 = \frac{n}{d_0}$, $m_1 = \frac{m}{d_0}$. In Chapter 2, we prove

Theorem 1.1.1. *Let v be a Krull valuation of arbitrary rank of a field having valuation ring R_v, maximal ideal M_v and perfect residue field. Let p denote the characteristic of the residue field R_v/M_v in case it is positive. Let θ be a root of a monic irreducible trinomial $F(x) = x^n + ax^m + b$ belonging to $R_v[x]$ and d_0, m_1, n_1, D be as above. Assume*[1] *that $v(D) > 0$. Then $R_v[\theta]$ is integrally closed if and only if M_v is a principal ideal say generated by π and one of the following conditions is*

[1] If $v(D) = 0$, then $\overline{F}(x)$ has no repeated factor and hence $R_v[\theta]$ is integrally closed by Theorem 1.1.A.

satisfied:

(i) when $a, b \in M_v$*, then* $v(b) = v(\pi)$*;*

(ii) when $a \in M_v$ *and* $b \notin M_v$ *with* $j \geq 1$ *as the highest power of* p *dividing* n*, then either* $v(a_2) \geq v(\pi)$ *and* $v(b_1) = 0$ *or* $v(a_2) = 0 = v((-b)^{m_1}a_2^{n_1} - (-b_1)^{n_1})$*, where* $a_2 = \frac{a}{\pi}$*,* b' *is an element of* R_v *satisfying* $(\bar{b'})^{p^j} = \bar{b}$ *and* $b_1 = \frac{1}{\pi}(b + (-b')^{p^j})$*;*

(iii) when $a \notin M_v$*,* $b \in M_v$ *and* $v(n-m) = 0$*, then* $v(b) = v(\pi)$*;*

(iv) when $a \notin M_v$*,* $b \in M_v$ *and* $v(n-m) > 0$ *with* $l \geq 1$ *as the highest power of* p *dividing* $n - m$*, then either* $v(a_1) \geq v(\pi)$ *and* $v(b_2) = 0$ *or* $v(a_1) = 0 = v(b_2^{m-1}[(-a)^{m_1}(a_1)^{n_1-m_1} - (-b_2)^{n_1-m_1}])$*, where* $a_1 = \frac{1}{\pi}(a + (-a')^{p^l})$*,* $b_2 = \frac{b}{\pi}$*,* $a' \in R_v$ *satisfies* $(\bar{a'})^{p^l} = \bar{a}$*;*

(v) when $ab \notin M_v$ *and* $m \in M_v$ *with* $n = s'p^k$*,* $m = sp^k$*,* p *does not divide* $\gcd(s', s)$*, then the polynomials* $x^{s'} + ax^s + b$ *and* $\frac{1}{\pi}[ax^{sp^k} + b + (-a'x^s - b')^{p^k}]$ *are coprime modulo* M_v*, where* a', b' *are in* R_v *satisfying* $(\bar{a'})^{p^k} = \bar{a}$*,* $(\bar{b'})^{p^k} = \bar{b}$*;*

(vi) when abm *does not belong to* M_v*, then* $v(C - E) = v(\pi)$*, where* $C = b^{n_1-m_1}n_1^{n_1}$ *and* $E = (-1)^{n_1}a^{n_1}m_1^{m_1}(n_1 - m_1)^{n_1-m_1}$*.*

In the special case when the characteristic of the residue field of v is zero, we obtain the following simple result.

Corollary 1.1.2. *Let* $v, R_v, M_v, F(x)$ *and* D *be as in the above theorem with* $v(D) > 0$*. Assume that the characteristic of* R_v/M_v *is zero. Then* $R_v[\theta]$ *is integrally closed if and only if* M_v *is a principal ideal say generated by* π *and either I)* $v(b) = v(\pi)$ *or II)* $v(ab) = 0$*,* $v(C - E) = v(\pi)$ *holds, where* C*,* E *are as in Theorem* 1.1.1*(vi).*

It is well known that if K_1, K_2 are algebraic number fields with coprime discriminants, then K_1, K_2 are linearly disjoint over the field $\mathbb{Q}$ of rational numbers and $A_{K_1K_2} = A_{K_1}A_{K_2}$, here and elsewhere A_L stands for the ring of algebraic integers of an algebraic number field L (cf. [Nar, Theorem 4.26], [Es-Mu, Exercise 4.5.12]). The converse of this classical result is already known when both K_1, K_2 are distinct quadratic fields (cf. [Mar, Chapter 2, Exercise 42]). As an application of Theorem 1.1.1, we have proved the following theorem which proves the converse when one of K_1 or K_2 is a quadratic field not contained in the other.

Theorem 1.1.3. *Let K_1 be an algebraic number field and K_2 be a quadratic field not contained in K_1. If $A_{K_1K_2}$ equals the composite ring $A_{K_1}A_{K_2}$, then the discriminants of K_1 and K_2 are coprime.*

Theorems 1.1.1,1.1.3 and some related results of independent interest are proved in the paper [J-K-S3] which has appeared in *Journal of Pure and Applied Algebra* Vol. 222 (2018), 889-899.

The following problem naturally arises from Theorem 1.1.3.

Let K_1, K_2 be algebraic number fields linearly disjoint over $K = K_1 \cap K_2$. If $A_{K_1}A_{K_2} = A_{K_1K_2}$, then is it true that the relative discriminants[2] *of K_1/K and K_2/K are coprime?*

We deal with the above problem in a more general situation in the fourth chapter and deduce that the answer to the foregoing question is in the affirmative. In the course of its proof, we establish an analogue for finite extensions of valued fields of the classical result that the discriminant of an extension of algebraic number fields can be expressed as product of local discriminants (cf. [Ca-Fr, Proposition 5, Chapter I]); the latter result is proved in the third chapter. It will be precisely stated after introducing some notations.

Definition 1.1.B. Let R be a integral domain and A be a commutative ring with identity which is a free R-module of finite rank n. Let $\{\beta_1, \cdots, \beta_n\}$ be an R-basis of A. For an arbitrary element α of A, we can write $\alpha\beta_i = \sum_{j=1}^{n} c_{ij}\beta_j,\ c_{ij} \in R$. The trace $\sum_i c_{ii}$ of the matrix $(c_{ij})_{ij}$ does not depend upon the choice of R-basis of A; it is called the trace of α with respect to A/R and will be denoted by $Tr_{A/R}(\alpha)$. The discriminant $D_{A/R}(\beta_1, \cdots, \beta_n)$ of the basis $\{\beta_1, \cdots, \beta_n\}$ is defined to be the determinant of the $n \times n$ matrix $(Tr_{A/R}(\beta_i\beta_j))_{ij}$. If $\{\beta'_1, \cdots, \beta'_n\}$ is another R-basis of A and T is the transition matrix from $\{\beta_1, \cdots, \beta_n\}$ to $\{\beta'_1, \cdots, \beta'_n\}$, then $D_{A/R}(\beta'_1, \cdots, \beta'_n) = (det\ T)^2 D_{A/R}(\beta_1, \cdots, \beta_n)$. So $D_{A/R}(\beta_1, \cdots, \beta_n)$ is uniquely determined up to the square of a unit of R. The ideal generated by $D_{A/R}(\beta_1, \cdots, \beta_n)$

[2]As in [Nar], the relative discriminant of an extension L/K of algebraic number fields is the norm relative to L/K of the inverse of the fractional ideal $\{\lambda \in L \mid Tr_{L/K}(\lambda A_L) \subseteq A_K\}$ of the ring A_L of algebraic integers of L.

in R will be called the discriminant of A/R and will be denoted by $d(A/R)$.

Notation 1.1.C. A henselian valued field (K^h, v^h) which is an extension of a valued field (K, v) and is smallest in the sense that every henselian valued field extension of (K, v) contains a (K, v)-isomorphic image of (K^h, v^h) is called henselization of (K, v). It is known that every valued field admits a henselization (see [En-Pr, Proposition 5.2.2.]). The valuation ring of the henselization (K^h, v^h) will be denoted by R_v^h.

With the above notation, the main result of Chapter 3 can be stated as follows.

Theorem 1.1.4. *Let (K, v) be a valued field of arbitrary rank with valuation ring R_v and (K^h, v^h) be its henselization having valuation ring R_v^h. Let L be a finite separable extension of K and S be the integral closure of R_v in L. Let $w_1, \cdots, w_s$ be all the prolongations of v to L. Assume that S is a free R_v-module. Then the valuation ring $R_{w_i}^h$ of the henselization of (L, w_i) is a free R_v^h-module and $d(S/R_v)R_v^h = \prod_{i=1}^{s} d(R_{w_i}^h/R_v^h)$.*

For proving the above theorem, we have proved the result stated below which extends the weak Approximation Theorem which states that if $\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_k$ are non-comparable valuation rings of a field K with maximal ideals $\mathcal{M}_1, \mathcal{M}_2, \cdots, \mathcal{M}_k$, then for any tuple $(a_1, a_2, \cdots, a_k) \in \mathcal{B}_1 \times \mathcal{B}_2 \times \cdots \times \mathcal{B}_k$, there exists an $c \in \cap_{i=1}^k \mathcal{B}_i$ with $c - a_i \in \mathcal{M}_i$ for all $i \in \{1, 2, \cdots, k\}$ (cf. [En-Pr, Theorem 3.2.7]).

Theorem 1.1.5. *Let $\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_k$ be non-comparable valuation rings of a field K with maximal ideals $\mathcal{M}_1, \mathcal{M}_2, \cdots, \mathcal{M}_k$ and $R = \cap_{i=1}^k \mathcal{B}_i$. Then for each tuple $(a_1, \cdots, a_k)$ belonging to $\mathcal{B}_1 \times \cdots \times \mathcal{B}_k$ such that a_k is a unit of $\mathcal{B}_i\mathcal{B}_k$ for $1 \leq i \leq k-1$, there exists an element $c \in R$ such that $c - a_i \in \mathcal{M}_i$ for $1 \leq i \leq k-1$ and $c - a_k \in a_k\mathcal{M}_k$.*

In Chapter 3, we have also proved the following theorem which has been used in the proof of Theorem 1.1.4.

Theorem 1.1.6. *Let $(K, v), R_v^h, L, S, w_1, \cdots, w_s$ and $R_{w_i}^h$ be as in Theorem 1.1.4. Assume that S is a free R_v-module. Then one can choose a suitable R_v^h-basis $\mathcal{B}_i \subseteq S$ of $R_{w_i}^h$ such that (i) $\cup_{i=1}^s \mathcal{B}_i$ is an R_v-basis of S; (ii) for every $B_{ij} \in \mathcal{B}_i$ and for each $k \neq i$, $w_k(B_{ij}) \geq v(a) > 0$ for some a in K.*

The paper [J-J-K-S] containing the proofs of Theorems 1.1.4-1.1.6 has been published in *Journal of Algebra and its Applications*, Vol. 16 (2017) 1750198 (7 pages).

Using results of the third chapter, we have proved the following theorem in the fourth chapter.

Theorem 1.1.7. *Let (K, v) be a henselian valued field of arbitrary rank with perfect residue field and K_1, K_2 be finite separable extensions of K which are linearly disjoint over K. Let S_1, S_2 denote the integral closures of the valuation ring R_v of v in K_1, K_2 respectively. If S_1, S_2 are free R_v-modules and S_1S_2 is integrally closed, then either $d(S_1/R_v)$ or $d(S_2/R_v)$ is the unit ideal.*

The corollary stated below has been deduced from the above theorem. It proves the converse of the well known theorem which says that if discriminants of algebraic number fields K_1, K_2 are coprime, then they are linearly disjoint over $\mathbb{Q}$ and $A_{K_1K_2} = A_{K_1}A_{K_2}$ (see [Nar, Theorem 4.26]).

Corollary 1.1.8. *Let K_1, K_2 be algebraic number fields which are linearly disjoint over $K = K_1 \cap K_2$ such that $A_{K_1K_2} = A_{K_1}A_{K_2}$. Then the relative discriminants of the extensions K_1/K and K_2/K are coprime.*

For proving Theorem 1.1.7, we have proved the following theorem as a preliminary result in Chapter 4. It happens to be of independent interest.

Theorem 1.1.9. *Let $(K, v), K_1, K_2, S_1, S_2$ be as in Theorem 1.1.7 without the assumption that the residue field of v is perfect. Assume that S_1, S_2 are free R_v-modules and S_1S_2 is integrally closed. If r, s, t denote respectively the number of prolongations of v to K_1, K_2 and K_1K_2, then $t = rs$.*

Theorems 1.1.7,1.1.9 and their applications are proved in the paper entitled "*On the compositum of integral closures of valuation rings*" which has been accepted for publication in Journal of Pure and Applied Algebra.

Factorization of polynomials having integral coefficients into irreducible factors over the ring $\mathbb{Z}_p$ of p-adic integers is an important problem in algebraic number theory. In 1894, Hensel developed a powerful approach by showing that the prime ideals of the ring A_K of algebraic integers of an algebraic number field $K = \mathbb{Q}(\theta)$ with θ an algebraic integer having minimal polynomial $F(x)$ over $\mathbb{Q}$, occurring in the factorization of pA_K for any prime p are in one-to-one correspondence with the monic irreducible factors of $F(x)$ over $\mathbb{Z}_p$ and that the ramification index together with the residual degree of a prime ideal of A_K lying over p are same as those of a simple extension of the field $\mathbb{Q}_p$ of p-adic numbers obtained by adjoining a root of the corresponding irreducible factor of $F(x)$ belonging to $\mathbb{Z}_p[x]$ (see [Hen], [Nar, Proposition 6.1]). If the factorization of $F(x)$ modulo p is given by

$$\overline{F}(x) = \overline{\phi_1}(x)^{e_1} \cdots \overline{\phi_r}(x)^{e_r} \tag{1.1.1}$$

as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $\phi_i(x)$ monic polynomials belonging to $\mathbb{Z}[x]$, then by Hensel's Lemma [End, Theorem 16.7] $F(x) = F_1(x) \cdots F_r(x)$, where $F_i(x)$ is a polynomial over $\mathbb{Z}_p$ with $F_i(x) \equiv \phi_i(x)^{e_i}$ mod p. If p divides $[A_K : \mathbb{Z}[\theta]]$, then these factors $F_i(x)$ need not be irreducible over $\mathbb{Q}_p$. In 1928, Ore in a series of papers [Ore1], [Ore2], [Ore3] described a method to further split $F_i(x)$ into a product of irreducible factors over $\mathbb{Z}_p$. For this purpose, he considered the ϕ_i-Newton polygon of $F_i(x)$ (as defined in the paragraph preceding Definition 1.1.K) for each i , having k_i sides with positive slope which leads to a factorization of $F_i(x)$ into k_i factors, say $F_i(x) = F_{i1}(x) \cdots F_{ik_i}(x)$ in $\mathbb{Z}_p[x]$. Moreover to each side S of the ϕ_i-Newton polygon of $F_i(x)$, he associated a polynomial $(F_i)_S(y)$ over the finite field $\mathbb{F}_{q_i}, q_i = p^{\deg \phi_i(x)}$ in an indeterminate y. The factorization of the associated polynomial $(F_i)_S(y)$ over $\mathbb{F}_{q_i}$ provides a further factorization of the factor of $F_i(x)$ corresponding to the side S. Finally, Ore showed that if for some i, all these polynomials $(F_i)_{S_j}(y)$ corresponding to various sides $S_j, 1 \leq j \leq k_i$, of the ϕ_i-Newton polygon of $F_i(x)$ have no multiple factor, say $(F_i)_{S_j}(y)$ splits into n_{ij} distinct irreducible factors over $\mathbb{F}_{q_i}$, then all the $\sum_{j=1}^{k_i} n_{ij}$ factors of $F_i(x)$ obtained in this way are irreducible over $\mathbb{Q}_p$. Further, the slopes of the sides of the ϕ_i-Newton polygon of $F_i(x)$ and the degrees of the irreducible factors of $(F_i)_S(y)$ over $\mathbb{F}_{q_i}$ for S ranging over all the sides of such a polygon lead to the explicit determination of the residual degrees and the ramification indices of all those prime ideals of A_K lying over p which correspond to the irreducible factors of $F_i(x)$ (see [G-M-N, Theorem 1.19, Corollary 1.20], [Kh-Ku3]).

In 1934, Ostrowski established a deep connection between valuations of an algebraic number field K and the prime ideals of A_K. He proved that the prime ideals of A_K dividing pA_K are in one-to-one correspondence with the valuations of K extending the p-adic valuation of $\mathbb{Q}$ (see [Ost4], [Nar, Theorem 3.3]). Keeping this in mind, the following well known theorem [End, Theorem 17.17] extends Hensel's approach (stated in the opening lines of the previous paragraph) to general valued fields.

Theorem 1.1.D. *Let v be a valuation of arbitrary rank of a field K and $K(\theta)$ be a finite separable extension of K. Let $F(x)$ be the minimal polynomial of θ over K and $\prod_{i=1}^{s} f_i(x)$ be the factorization of $F(x)$ into a product of distinct monic irreducible polynomials over the henselization (K^h, v^h) of (K, v). Let $\tilde{v}_h$ denote the unique prolongation of v^h to the algebraic closure of K^h. Then there are exactly s prolongations of v to $K(\theta)$. Let θ_i be a root of $f_i(x)$. The valuations $w_1, \cdots, w_s$ of $K(\theta)$ defined by*

$$w_i(\sum_j a_j\theta^j) = \tilde{v}^h(\sum_j a_j\theta_i^j), a_j \in K \tag{1.1.2}$$

are all the distinct prolongations of v to $K(\theta)$.

The above theorem gives rise to the following problem :

Given an irreducible polynomial $F(x)$ with coefficients in a valued field (K, v) of arbitrary rank, how to extend the method of Ore to obtain information about the irreducible factors of $F(x)$ over (K^h, v^h).

It may be pointed out that Ore's technique was extended by Cohen et al. in 2000 for polynomials over complete discrete valued fields and was further extended to more general henselian valued fields by Jhorar, Khanduja and Kumar (see [C-M-S], [Kh-Ku3], [Jh-Kh1]). All these generalizations of Ore's results for factorization are proved using ϕ-Newton polygons which later came to be known as Newton polygons of order one (see Definition 1.1.K). In 2012, Guàrdia, Montes and Nart [G-M-N] introduced the notion of Newton polygons of higher order to extend the method of factorization of Ore in a different direction for polynomials with coefficients in $\mathbb{Z}_p$

when the polynomial $(F_i)_{S_j}(y)$ mentioned above has repeated irreducible factors over $\mathbb{F}_q$. In the fifth chapter, we extend the notion of Newton polygons of higher order to polynomials with coefficients in henselian valued fields of arbitrary rank (see Definition 1.1.K) and use higher order Newton polygons to give a factorization for such polynomials. Our approach involves prolongations of a valuation V_0 of a field K to a simple transcendental extension $K(x)$ of K whose residue fields are transcendental over the residue field of V_0; such prolongations of V_0 to $K(x)$ are called residually transcendental. In 1988, Alexandru, Popescu and Zaharescu [A-P-Z1] proved that residually transcendental prolongations are given by means of minimal pairs which are defined after introducing some notations.

Notation 1.1.E. In what follows, V_0 is a henselian valuation of arbitrary rank of a field K with value group G_0 whose valuation ring will be denoted by R_0 having unique maximal ideal M_0. We shall denote by $\widetilde{K}$ an algebraic closure of K and by $\widetilde{V}_0$ a fixed prolongation of the valuation V_0 of K to $\widetilde{K}$; $\widetilde{G}_0$ will stand for the value group of $\widetilde{V}_0$. For an element α belonging to the valuation ring of $\widetilde{V}_0, \overline{\alpha}$ will denote its $\widetilde{V}_0$-residue, i.e., the image of α under the canonical homomorphism from the valuation ring of $\widetilde{V}_0$ onto its residue field. When $f(x) \in R_0[x]$, $\bar{f}(x)$ will stand for the polynomial over R_0/M_0 obtained by replacing each coefficient of $f(x)$ by its V_0-residue. For any subfield L of $\widetilde{K}, \overline{L}, G(L)$ will denote respectively the residue field and the value group of the valuation of L which is the restriction of $\widetilde{V}_0$.

Definition 1.1.F. A pair $(\alpha, \delta) \in \widetilde{K} \times \widetilde{G}_0$ is said to be a minimal pair (more precisely a (K, V_0)-minimal pair) if whenever β belongs to $\widetilde{K}$ with $[K(\beta) : K] < [K(\alpha) : K]$, then $\widetilde{V}_0(\alpha - \beta) < \delta$, i.e., α has least degree over K in the closed ball $B(\alpha, \delta) = \{\beta \in \widetilde{K} \mid \widetilde{V}_0(\alpha - \beta) \geq \delta\}$.

Example. If $\phi(x)$ belonging to $R_0[x]$ is a monic polynomial of degree $m \geq 1$ with $\overline{\phi}(x)$ irreducible over the residue field of V_0 and α is a root of $\phi(x)$ in the algebraic closure $\widetilde{K}$ of K, then (α, δ) is a (K, V_0)-minimal pair for each positive δ in G_0, because whenever β belongs to $\widetilde{K}$ with degree $[K(\beta) : K] < m$, then $\widetilde{V}_0(\alpha - \beta) \leq 0$, for otherwise $\overline{\alpha} = \overline{\beta}$, which in view of the Fundamental Inequality ([En-Pr, Theorem 3.3.4]) would imply that $[K(\beta) : K] \geq [\overline{K}(\overline{\beta}) : \overline{K}] = m$ leading to a contradiction.

Note that to the minimal pair $(0,0)$ belonging to $\widetilde{K} \times \widetilde{G}_0$, one can associate in a natural way, the Gaussian prolongation V_0^x of V_0 to a simple transcendental extension $K(x)$ of K defined on $K[x]$ by

$$V_0^x\big(\sum_i a_i x^i\big) = \min_i\{V_0(a_i)\}, a_i \in K. \tag{1.1.3}$$

In the same manner, for a (K, V_0)-minimal pair (α, δ), we can define a valuation $\widetilde{w}_{\alpha,\delta}$ of $\widetilde{K}(x)$ by

$$\widetilde{w}_{\alpha,\delta}\big(\sum_i c_i(x-\alpha)^i\big) = \min_i\{\tilde{V}_0(c_i) + i\delta\},\ c_i \in \widetilde{K}; \tag{1.1.4}$$

its restriction to $K(x)$ will be denoted by $w_{\alpha,\delta}$. It is known that a prolongation W of V_0 to $K(x)$ is residually transcendental if and only if $W = w_{\alpha,\delta}$ for some (K, V_0)-minimal pair (α, δ) (cf. [A-P-Z2, Theorem 2.2]). With Notation 1.1.E, the valuation $w_{\alpha,\delta}$ and its residue field are described by the following basic theorem proved in [A-P-Z1, Theorem 2.1].

Theorem 1.1.G. *Let (K, V_0), $(\widetilde{K}, \widetilde{V}_0)$ be as in Notation 1.1.E. Let (α, δ) be a (K, V_0)-minimal pair and $\widetilde{w}_{\alpha,\delta}$ be as defined by equation (1.1.4). Let $f(x)$ be the minimal polynomial of α over K of degree m with $w_{\alpha,\delta}(f(x)) = \mu$. Let $\overline{K(\alpha)}$, $G(K(\alpha))$ denote respectively the residue field and the value group of the valuation obtained by restricting $\widetilde{V}_0$ to $K(\alpha)$. Then the following hold:*

(i) For any polynomial $g(x)$ belonging to $K[x]$ with f-expansion[3] $\sum_i g_i(x)f(x)^i$, $\deg g_i(x) < m$, one has $w_{\alpha,\delta}(g(x)) = \min_i\{\widetilde{V}_0(g_i(\alpha)) + i\mu\}$.

(ii) If $c(x)$ belonging to $K[x]$ is a non-zero polynomial of degree less than m, then the $\widetilde{w}_{\alpha,\delta}$-residue of $c(x)/c(\alpha)$ equals 1.

(iii) Let e be the smallest positive integer such that $e\mu \in G(K(\alpha))$ and $h(x)$ belonging to $K[x]$ be a polynomial of degree less than m with $\widetilde{V}_0(h(\alpha)) = e\mu$. Then the $w_{\alpha,\delta}$-residue z of $f(x)^e/h(x)$ is transcendental over $\overline{K(\alpha)}$ and the residue field of $w_{\alpha,\delta}$ is $\overline{K(\alpha)}(z)$.

[3]On dividing by successive powers of $f(x)$, every polynomial $g(x) \in K[x]$ can be uniquely written as a finite sum $\sum_{i\geq 0} g_i(x)f(x)^i$ with $\deg(g_i(x)) < \deg(f(x))$, called the f-expansion of $g(x)$.

Using the canonical homomorphism from the valuation ring R_0 of V_0 onto its residue field R_0/M_0, as usual one can lift any monic polynomial $x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0}$ with coefficients in R_0/M_0 to yield a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over R_0. In 1995, Popescu and Zaharescu [Po-Za] extended this notion using (K, V_0)-minimal pairs as follows:

Definition 1.1.H. For a (K, V_0)-minimal pair (α, δ), let $f(x), m, \mu, e$ and $h(x)$ be as in Theorem 1.1.G. A monic polynomial $F(x)$ belonging to $K[x]$ is said to be a lifting of a monic polynomial $T(y)$ in an indeterminate y belonging to $\overline{K(\alpha)}[y]$ having degree $t \geq 1$ with respect to (α, δ) if the following three conditions are satisfied:

(i) $\deg F(x) = etm$,

(ii) $w_{\alpha,\delta}(F(x)) = w_{\alpha,\delta}(h(x)^t) = et\mu$,

(iii) the $w_{\alpha,\delta}$-residue of $F(x)/h(x)^t$ is $T(z)$, where z is the $w_{\alpha,\delta}$-residue of $f(x)^e/h(x)$.

To be more precise, this lifting will be referred to as the one with respect to (α, δ) and $h(x)$. Keeping in mind that the valuation $w_{\alpha,\delta}$ is uniquely determined by $f(x)$ and $\mu = w_{\alpha,\delta}(f(x))$ in view of Theorem 1.1.G(i), sometimes we avoid referring to the minimal pair (α, δ) and say that the above lifting is with respect to $f(x), \mu$ and $h(x)$ or more briefly with respect to $f(x), \mu$. It may be pointed out that this notion of lifting extends the usual one because a usual lifting of a polynomial belonging to $\overline{K}[x]$ is its lifting with respect to the minimal pair $(0, 0) \in K \times G_0$ with $h(x) = 1$.

In 1936, Maclane [Mac] introduced the notion of key polynomials (defined below) in order to construct residually transcendental prolongations.

Definition 1.1.I. Let W be a Krull valuation of $K(x)$. Two polynomials f and g belonging to $K[x]$ are said to be equivalent in W if $W(f - g) > W(f)$; f is said to be equivalence divisible by h belonging to $K[x]$ in W if there exists $q \in K[x]$ such that f is equivalent to qh in W. A monic polynomial $\phi = \phi(x) \in K[x]$ is said to be a key polynomial over W if it satisfies the following two conditions: (i) ϕ is equivalence irreducible in W, i.e., whenever a product of two polynomials is equivalence divisible by ϕ in W, then one of the factors is equivalence divisible by ϕ in W; (ii) any non-zero polynomial of $K[x]$ equivalence divisible by ϕ in W has degree in x not less than the degree of $\phi(x)$. A key polynomial $\phi(x)$ over a residually transcendental prolongation $(K(x), W)$ of a valued field (K, V_0) is called nontrivial if there exists a (K, V_0)-minimal pair (α_1, δ_1) such that $W = w_{\alpha_1,\delta_1}$ and the minimal polynomial of α_1 over K is not equivalent to $\phi(x)$ in W.

L. Popescu and N. Popescu in [Po-Po, Theorem 4.6] gave a connection between key polynomials over any residually transcendental prolongation w_{α_1,δ_1} of V_0 and liftings of polynomials. They proved that if a monic polynomial $\phi(x) \in K[x]$ has degree strictly greater than that of the the minimal polynomial of α_1 over K, then $\phi(x)$ is a key polynomial over w_{α_1,δ_1} if and only if $\phi(x)$ is a lifting of an irreducible polynomial different from y belonging to $\overline{K(\alpha_1)}[y]$ with respect to the minimal pair (α_1, δ_1) .

Example 1.1.J. Let $\phi(x) \in R_0[x]$ be a monic polynomial with $\bar{\phi}(x)$ irreducible over $\overline{K}$. We show that $\phi(x)$ is a key polynomial over the Gaussian valuation V_0^x defined by (1.1.3). If $V_0^x(gh - \phi q) > V_0^x(gh)$ for some polynomials $g, h, q \in K[x]$, then $V_0^x(\phi q) = V_0^x(gh) = -V_0(cd)$, where $c, d \in K$ are such that $V_0^x(g) = -V_0(c)$, $V_0^x(h) = -V_0(d)$; so $\left(\overline{cdq}\right)\bar{\phi} = (\overline{cg})\left(\overline{dh}\right)$. Since $\bar{\phi}$ is irreducible over $\overline{K}$, $\bar{\phi}$ divides either $\overline{cg}$ or $\overline{dh}$, say $\bar{\phi}$ divides $\overline{cg}$. So there exists $q_1(x) \in R_0[x]$ such that $\overline{cg} = \bar{\phi}\bar{q}_1$ and hence $V_0^x(g - c^{-1}\phi q_1) > -V_0(c) = V_0^x(g)$ which shows that g is equivalence divisible by ϕ in V_0^x. This proves that ϕ is equivalence irreducible in V_0^x. To verify the second property of key polynomials, let $g, q \in K[x]$ be such that $V_0^x(g - \phi q) > V_0^x(g)$. So there exists $c_1 \in K$ such that $\bar{0} \neq (\overline{c_1 q})\bar{\phi} = \overline{c_1 g}$. Consequently $\deg(g) = \deg(c_1 g) \geq \deg(\overline{c_1 g}) \geq \deg(\bar{\phi}) = \deg(\phi)$. This completes the verification that ϕ is a key polynomial over V_0^x. By definition, this key polynomial is nontrivial if $\bar{\phi}(x) \neq x$.

Newton polygon is a simple, yet powerful tool in Valuation Theory for studying irreducible factors of polynomials over valued fields (see [Dum]). The notion of a Newton polygon originally due to Dumas was extended to ϕ-Newton polygon by Ore in his 1923 thesis. Recall that if V_0 is a real valuation of K and $\phi(x)$ belonging to $R_0[x]$ is a monic polynomial with $\bar{\phi}(x)$ irreducible over $\overline{K}$, then as in [Kh-Ku3, Definition 1.C], the ϕ-Newton polygon (with underlying valuation V_0) of any polynomial $F(x) \in K[x]$ not divisible by $\phi(x)$ with ϕ-expansion $\sum\limits_{i=1}^{s} A_i(x)\phi(x)^i$, $A_s(x) \neq 0$ is the lower convex hull of the points $\{(j, V_0^x(A_{s-j}(x))) \mid 0 \leq j \leq s, A_{s-j}(x) \neq 0\}$, where V_0^x is the Gaussian prolongation of V_0 to $K(x)$ defined by (1.1.3). In the next definition, we extend the notion of ϕ-Newton polygon replacing V_0^x by a residually transcendental prolongation W of V_0 and $\phi(x)$ by a key polynomial over W.

Definition 1.1.K. Let W be a residually transcendental extension of V_0 to $K(x)$ and $\phi(x)$ be a key polynomial over W. Let $F(x)$ belonging to $K[x]$ be a polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$, $A_s(x) \neq 0$. Let P_i stand for the pair $(i, W(A_{s-i}(x)\phi(x)^{s-i})$ when $A_{s-i}(x) \neq 0, 0 \leq i \leq s$. For distinct pairs P_i, P_j, let μ_{ij} denote the element of the divisible closure of G_0 defined by

$$\mu_{ij} = \frac{W(A_{s-j}(x)\phi(x)^{s-j}) - W(A_{s-i}(x)\phi(x)^{s-i})}{j-i}.$$

Let i_1 denote the largest index $0 < i_1 \leq s$ such that

$$\mu_{0i_1} = \min\{\ \mu_{0j} \mid 0 < j \leq s,\ A_{s-j}(x) \neq 0\}.$$

If $i_1 < s$, let i_2 be the largest index such that $i_1 < i_2 \leq s$ and

$$\mu_{i_1 i_2} = \min\{\ \mu_{i_1 j} \mid i_1 < j \leq s,\ A_{s-j}(x) \neq 0\}.$$

Proceeding in this way if $i_r = s$, then the ϕ-Newton polygon of $F(x)$ with respect to W is said to have r sides whose slopes are defined to be $\lambda_1 = \mu_{0i_1}, \lambda_2 = \mu_{i_1 i_2}, \cdots, \lambda_r = \mu_{i_{r-1} i_r}$ which are in strictly increasing order. The interval $[i_{j-1}, i_j]$ will be referred to as the interval of horizontal projection of the j-th side, $1 \leq j \leq r$ with $i_0 = 0$.

Example. Let V_0 be a henselian discrete valuation of a field K of characteristic zero having value group $\mathbb{Z}$. Let a, b be elements of R_0 with $V_0(a) > 0$ and $V_0(b) = 1$. Take $V_1 = w_{0,\frac{1}{2}}$ corresponding to the minimal pair $(0, \frac{1}{2})$ defined by (1.1.4) and $\phi(x) = x^2 + ax + b$. In view of Theorem 4.6 of [Po-Po] (stated in the paragraph following Definition 1.1.I), $\phi(x)$ is a key polynomial over V_1. Let $F(x)$ be $(\phi(x))^2 + b_2\phi(x) + b^2(b_0 x + b_1)$ with $V_0(b_i) \geq i$ for $i = 1, 2$ and $V_0(b_0) = 0$. It follows that the ϕ-Newton polygon of $F(x)$ with respect to V_1 consists of a single side joining the point $(0, 2)$ to $(2, \frac{5}{2})$ having slope $\frac{1}{4}$.

With notations as in 1.1.E, the theorem stated below is the main result of the fifth chapter .

Theorem 1.1.10. *Let (K, V_0) be a henselian valued field of arbitrary rank with value group G_0 and residue field $\overline{K}$. Let $\widetilde{K}$ be a fixed algebraic closure of K and $\widetilde{V}_0$ be the unique prolongation of V_0 to $\widetilde{K}$. Let W be a residually transcendental extension of V_0 to $K(x)$ and $\phi(x)$ be a nontrivial key polynomial of degree m over W having a root $\alpha \in \widetilde{K}$. Let $F(x)$ belonging to $K[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$, $A_s(x) = 1$. Suppose that the ϕ-Newton polygon of $F(x)$ with respect to W consists of r sides $S_1, \ldots, S_r$ having positive slopes $\lambda_1, \ldots, \lambda_r$. Then the following hold:*

(i) $F(x) = F_1(x) \cdots F_r(x)$, where each $F_i(x)$ belonging to $K[x]$ is a monic polynomial of degree ml_i whose ϕ-Newton polygon with respect to W has a single side which is a translate of S_i and l_i is the length of the horizontal projection of S_i.

(ii) If θ_i is a root of $F_i(x)$, then $\widetilde{V}_0(\phi(\theta_i)) = W(\phi(x)) + \lambda_i = \mu_i'$ (say) and $G(K(\alpha)) \subseteq G(K(\theta_i))$. The index $[G(K(\theta_i)) : G(K(\alpha))]$ is divisible by e_i, where e_i is the smallest positive integer such that $e_i\mu_i' \in G(K(\alpha))$. The degree $[\overline{K(\theta_i)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}]$.

(iii) $F_i(x)$ is a lifting of a monic polynomial $T_i(y) \in \overline{K(\alpha)}[y]$ not divisible by y of degree l_i/e_i with respect to $\phi(x), \mu_i'$.

(iv) If $U_{i1}(y)^{a_{i1}} \cdots U_{in_i}(y)^{a_{in_i}}$ is the factorization of $T_i(y)$ into powers of distinct monic irreducible polynomials over $\overline{K(\alpha)}$, then $F_i(x)$ factors as $F_{i1}(x) \cdots F_{in_i}(x)$ over K, each $F_{ij}(x)$ is a lifting of $U_{ij}(y)^{a_{ij}}$ with respect to $\phi(x), \mu_i'$ with degree $me_i a_{ij} \deg U_{ij}$ and $\widetilde{V}_0(\phi(\theta_{ij})) = \mu_i'$. If some $a_{ij} = 1$, then $F_{ij}(x)$ is irreducible over K and for any root θ_{ij} of $F_{ij}(x)$, the index $[G(K(\theta_{ij})) : G(K(\alpha))] = e_i$ and the degree $[\overline{K(\theta_{ij})} : \overline{K}] = \deg U_{ij}(y)[\overline{K(\alpha)} : \overline{K}]$ in this case.

The following result which is already known in the particular case when W is the Gaussian prolongation V_0^x (cf. [Jh-Kh4, Theorem 1.5]), has been deduced from Theorem 1.1.10.

Corollary 1.1.11. *Let $(K, V_0), \phi(x), m, W$ and α be as in Theorem 1.1.10. Let $F(x)$ belonging to $K[x]$ be a polynomial having ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$ with*

$A_s(x) = 1$, $A_i(x) \neq 0$ *for some* $i < s$ *and assume that all the sides in the* ϕ*-Newton polygon of* $F(x)$ *with respect to* W *have positive slopes. If* l *is the smallest non-negative integer for which* $\min_{0 \leq i \leq s-1} \left\{ \frac{W(A_i(x)\phi(x)^i) - W(\phi(x)^s)}{s-i} \right\} = \frac{W(A_l(x)\phi(x)^l) - W(\phi(x)^s)}{s-l}$ *and* $\frac{W(A_l(x))}{d}$ *does not belong to* $G(K(\alpha))$ *for any number* $d > 1$ *dividing* $s - l$*, then for any factorization* $G(x)H(x)$ *of* $F(x)$ *over* K*,* $\min\{\deg G(x), \deg H(x)\} \leq lm$*.*

The above corollary immediately yields Generalized Schönemann Irreducibility Criterion (cf. [Bro], [Kh-Kh]) which can be stated as follows.

Theorem 1.1.L(Generalized Schönemann Irreducibility Criterion.) *Let* V_0 *be a Krull valuation of arbitrary rank of a field* K *with value group* G_0*, valuation ring* R_0 *having maximal ideal* M_0*. Let* $\phi(x) \in R_0[x]$ *be a monic polynomial of degree* m *with* $\overline{\phi}(x)$ *irreducible over* R_0/M_0*. Let* $F(x)$ *belonging to* $R_0[x]$ *be a polynomial having* $\phi(x)$*-expansion* $\sum_{i=0}^{s} A_i(x)\phi(x)^i$ *with* $A_s(x) = 1, A_0(x) \neq 0$*. Assume that (i)* $\frac{V_0^x(A_i(x))}{s-i} \geqslant \frac{V_0^x(A_0(x))}{s} > 0$ *for* $0 \leqslant i \leqslant s-1$ *and (ii)* $V_0^x(A_0(x)) \notin dG_0$ *for any number* $d > 1$ *dividing* s*. Then* $F(x)$ *is irreducible over* K*.*

Theorem 1.1.10 together with its applications and several preliminary results which are of independent interest as well are proved in the paper entitled "*On factorization of polynomials in henselian valued fields*" which has been accepted for publication in Communications in Algebra.

Chapter 2

Integrally closed simple extensions of valuation rings

2.1 Motivation of the problem and statements of the results.

Let R be an integrally closed domain and θ be an element of an integral domain containing R with θ integral over R. The question "when is $R[\theta]$ integrally closed" has inspired many mathematicians (cf. [Ch-De], [Jh-Kh2], [Kh-Ku1], [Uch]). It was answered by K. Uchida when R is a Dedekind domain. He proved that $R[\theta]$ is integrally closed if and only if the minimal polynomial $F(x)$ of θ over the quotient field of R does not belong to $\mathcal{M}^2$ for any maximal ideal $\mathcal{M}$ of the polynomial ring $R[x]$. This problem is closely related with the existence of a power basis of an algebraic number field. Recall that a power basis of an algebraic number field K is a $\mathbb{Z}$-basis of the ring of algebraic integers A_K of K consisting of powers of a single element; indeed θ would be such an element if and only if $\mathbb{Z}[\theta]$ is integrally closed in its quotient field K. As pointed out on page 3, a prime p does not divide $[A_K : \mathbb{Z}[\theta]]$ if and only if $\mathbb{Z}_{(p)}[\theta]$ is integrally closed where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. Dedekind gave a criterion to be satisfied by the minimal polynomial $F(x)$ of θ over $\mathbb{Q}$ so that $p \nmid [A_K : \mathbb{Z}[\theta]]$ which can be stated as follows :

Theorem 2.1.A. Let $F(x)$ be the minimal polynomial of θ over $\mathbb{Q}$ and p be a prime number. If $\overline{F}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_t(x)^{e_t}$ is the factorization of the polynomial $\overline{F}(x)$ obtained by replacing coefficients of $F(x)$ modulo p as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $g_i(x)$ monic, then $\mathbb{Z}_{(p)}[\theta]$ is integrally closed if and only if for each i, $1 \leq i \leq t$, either $e_i = 1$ or $\bar{g}_i(x) \nmid \overline{M}(x)$, where $M(x) = \frac{1}{p}(F(x) - \prod_{i=1}^{t} g_i(x)^{e_i})$.

As $\mathbb{Z}_{(p)}$ is the valuation ring of the p-adic valuation of rationals, the above criterion gives a motivation to investigate the question "When is a simple ring extension of a valuation ring R_v integrally closed ?". In this chapter, we use a generalized version of the Dedekind criterion (see Theorem 1.1.A) to give necessary and sufficient conditions involving a, b, m, n for $R_v[\theta]$ to be integrally closed when θ is a root of an irreducible trinomial $F(x) = x^n + ax^m + b$ belonging to $R_v[x]$. In what follows, v, R_v, M_v are as in Theorem 1.1.A. For an element α belonging to R_v, $\bar{\alpha}$ will denote its image under the canonical homomorphism from R_v onto R_v/M_v. When a polynomial $g(x)$ belongs to $R_v[x]$, $\bar{g}(x)$ will have the same meaning as in Theorem 1.1.A.

We shall denote by D the discriminant of the trinomial $F(x) = x^n + ax^m + b$. It is known (cf. [Swa]) that

$$D = (-1)^{\binom{n}{2}} b^{m-1}[b^{n_1-m_1}n^{n_1} - (-1)^{n_1}a^{n_1}m^{m_1}(n-m)^{n_1-m_1}]^{d_0}, \tag{2.1.1}$$

where $d_0 = \gcd(m, n)$, $n_1 = \frac{n}{d_0}$, $m_1 = \frac{m}{d_0}$. In this chapter, we prove

Theorem 2.1.1. *Let v be a Krull valuation of arbitrary rank of a field having valuation ring R_v, maximal ideal M_v and perfect residue field. Let p denote the characteristic of the residue field R_v/M_v in case it is positive. Let θ be a root of a monic irreducible trinomial $F(x) = x^n+ax^m+b$ belonging to $R_v[x]$ and d_0, m_1, n_1, D be as above. Assume*[1] *that $v(D) > 0$. Then $R_v[\theta]$ is integrally closed if and only if M_v is a principal ideal say generated by π and one of the following conditions is*

[1] If $v(D) = 0$, then $\overline{F}(x)$ has no repeated factor and hence $R_v[\theta]$ is integrally closed by Theorem 1.1.A.

satisfied:
(i) when a, b *belong to* M_v*, then* $v(b) = v(\pi)$*;*
(ii) when $a \in M_v$ *and* $b \notin M_v$ *with* $j \geq 1$ *as the highest power of* p *dividing* n*, then either* $v(a_2) \geq v(\pi)$ *and* $v(b_1) = 0$ *or* $v(a_2) = 0 = v((-b)^{m_1} a_2^{n_1} - (-b_1)^{n_1})$*, where* $a_2 = \frac{a}{\pi}$*,* b' *is an element of* R_v *satisfying* $(\bar{b'})^{p^j} = \bar{b}$ *and* $b_1 = \frac{1}{\pi}(b + (-b')^{p^j})$*;*
(iii) when $a \notin M_v$*,* $b \in M_v$ *and* $v(n-m) = 0$*, then* $v(b) = v(\pi)$*;*
(iv) when $a \notin M_v$*,* $b \in M_v$ *and* $v(n-m) > 0$ *with* $l \geq 1$ *as the highest power of* p *dividing* $n - m$*, then either* $v(a_1) \geq v(\pi)$ *and* $v(b_2) = 0$ *or* $v(a_1) = 0 = v(b_2^{m-1}[(-a)^{m_1}(a_1)^{n_1-m_1} - (-b_2)^{n_1-m_1}])$*, where* $a_1 = \frac{1}{\pi}(a + (-a')^{p^l})$*,* $b_2 = \frac{b}{\pi}$*,* a' *belonging to* R_v *satisfies* $(\bar{a'})^{p^l} = \bar{a}$*;*
(v) when $ab \notin M_v$ *and* $m \in M_v$ *with* $n = s'p^k$*,* $m = sp^k$*,* p *does not divide* $\gcd(s', s)$*, then the polynomials* $x^{s'} + ax^s + b$ *and* $\frac{1}{\pi}[ax^{sp^k} + b + (-a'x^s - b')^{p^k}]$ *are coprime modulo* M_v*, where* a', b' *are in* R_v *satisfying* $(\bar{a'})^{p^k} = \bar{a}$*,* $(\bar{b'})^{p^k} = \bar{b}$*;*
(vi) when abm *does not belong to* M_v*, then* $v(C - E) = v(\pi)$*, where* $C = b^{n_1-m_1} n_1^{n_1}$ *and* $E = (-1)^{n_1} a^{n_1} m_1^{m_1} (n_1 - m_1)^{n_1-m_1}$*.*

In the special case when the characteristic of the residue field of v is zero, we obtain the following simple result.

Corollary 2.1.2. *Let* $v, R_v, M_v, F(x)$ *and* D *be as in the above theorem with* $v(D) > 0$*. Assume that the characteristic of* R_v/M_v *is zero. Then* $R_v[\theta]$ *is integrally closed if and only if* M_v *is a principal ideal say generated by* π *and either I)* $v(b) = v(\pi)$ *or II)* $v(ab) = 0$*,* $v(C - E) = v(\pi)$ *holds, where* C*,* E *are as in Theorem* 2.1.1*(vi).*

Taking v to be the p-adic valuation of rationals, on applying Theorem 2.1.1 to the irreducible polynomial $F(x) = x^n + ax^m + b$ belonging to $\mathbb{Z}[x]$ having a root θ and keeping in mind Fermat's little theorem, we see that $\mathbb{Z}_{(p)}[\theta]$ is integrally closed in $K = \mathbb{Q}(\theta)$ if and only if one of the five conditions mentioned in the following Corollary 2.1.3 is satisfied. Using the fact (stated in the opening paragraph of the chapter) that $\mathbb{Z}_{(p)}[\theta]$ is integrally closed if and only if $p \nmid [A_K : \mathbb{Z}[\theta]]$, the corollary stated below follows at once. This corollary gives the main results of [J-K-S1] and [J-K-S2].

Corollary 2.1.3. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring A_K of algebraic integers of K having minimal polynomial $F(x) = x^n + ax^m + b$ over $\mathbb{Q}$, where $\gcd(m, n) = d_0$ with $m = m_1 d_0,\ n = n_1 d_0$. A prime factor p of the discriminant D of $F(x)$ does not divide $[A_K : \mathbb{Z}[\theta]]$ if and only if p satisfies one of the following conditions:*
(i) when $p \mid a$ and $p \mid b$, then $p^2 \nmid b$;
(ii) when $p \mid a$ and p does not divide b with $j \geq 1$ as the highest power of p dividing n, then either $p \mid a_2$ and $p \nmid b_1$ or p does not divide $a_2[(-b)^{m_1} a_2^{n_1} - (-b_1)^{n_1}]$, where $a_2 = \frac{a}{p}$, $b_1 = \frac{1}{p}[b + (-b)^{p^j}]$;
(iii) when p does not divide a and $p|b$, with $l \geq 0$ as the highest power of p dividing $n - m$, then either $p \mid a_1$ and $p \nmid b_2$ or p does not divide $a_1 b_2^{m-1}[(-a)^{m_1} a_1^{n_1 - m_1} - (-b_2)^{n_1 - m_1}]$, where $a_1 = \frac{1}{p}[a + (-a)^{p^l}]$ and $b_2 = \frac{b}{p}$;
(iv) when p does not divide ab and $p|m$ with $n = s'p^k,\ m = sp^k,\ p$ does not divide $\gcd(s', s)$, then the polynomials $x^{s'} + ax^s + b$ and $\frac{1}{p}[ax^{sp^k} + b + (-ax^s - b)^{p^k}]$ are coprime modulo p;
(v) when p does not divide abm, then p^2 does not divide $(C - E)$, where $C = b^{n_1 - m_1} n_1^{n_1}$ and $E = (-1)^{n_1} a^{n_1} m_1^{m_1} (n_1 - m_1)^{n_1 - m_1}$.

The following corollary is an immediate consequence of the above corollary. It extends the main result of [Jh-Kh3] which is proved for trinomials of the type $x^n + ax + b$.

Corollary 2.1.4. *Let $K = \mathbb{Q}(\theta)$, $F(x)$ and D be as in the above corollary. Then $A_K = \mathbb{Z}[\theta]$ if and only if each prime p dividing D satisfies one of the conditions $(i) - (v)$ of Corollary 2.1.3.*

As a quick application of assertions (i) and (ii) of Theorem 2.1.1, we obtain

Corollary 2.1.5. *Let $v, R_v, M_v, F(x), \theta$ and D be as in Theorem* 1.1 *with $a = 0$, R_v/M_v perfect and $v(D) > 0$. Let the prime p denote the characteristic of R_v/M_v in case it is positive. Then $R_v[\theta]$ is integrally closed if and only if M_v is a principal ideal generated by an element π and either $I)$ $v(b) = v(\pi)$ or $II)$ $v(b) = 0$, $v(b + (-b')^{p^j}) = v(\pi)$, where $j \geq 1$ is the highest power of p dividing n and b' is an element of R_v with $(\bar{b}')^{p^j} = \bar{b}$.*

It is well known that if K, L are algebraic number fields with coprime discriminants, then $A_{KL} = A_K A_L$ (cf. [Nar, Theorem 4.26, p. 159]), where A_{K_0} stands for the ring of algebraic integers of an algebraic number field K_0. The converse of this classical result is already known when both K, L are distinct quadratic fields (cf. [Mar, Chapter 2, Exercise 42]). As an application of Theorem 2.1.1, we have proved the following theorem which proves the converse when one of K or L is a quadratic field not contained in the other.

Theorem 2.1.6. *Let K be an algebraic number field and L be a quadratic field not contained in K. Then $A_K A_L = A_{KL}$ if and only if the discriminants of K and L are coprime.*

In the course of proving the above theorem, we prove the following propositions which are of independent interest as well. Proposition 2.1.7 quickly yields Theorem 5.1 of [Ch-De]; moreover it also proves the converse of the latter.

Proposition 2.1.7. *Let R be a Dedekind domain of characteristic different from 2 and b_0 be an element of R such that $\frac{b_0-1}{4} \in R$. Let $F(x) = x^2 - x + \frac{1-b_0}{4}$ be an irreducible polynomial over R with a root θ. Then $R[\theta]$ is integrally closed if and only if $b_0 R$ is not divisible by the square of any maximal ideal of R.*

Proposition 2.1.8. *Let R be a Dedekind domain and θ be a root of an irreducible polynomial $F(x) = x^2 + b \in R[x]$. Assume that for each maximal ideal $\wp$ of R containing 2, $R/\wp$ is a perfect field. Then $R[\theta]$ is integrally closed if and only if for every maximal ideal $\wp$ dividing $4bR$ either I) $b \in \wp \setminus \wp^2$ or II) $2 \in \wp$, $b \notin \wp$ and $b + (b')^2 \in \wp \setminus \wp^2$, where $b' \in R$ is such that $(b')^2 \equiv b (mod\ \wp)$.*

2.2 Preliminary results

Lemma 2.2.1. *Let $F(x) = x^n + ax^m + b$ and $h(x) = x^{s'} + a'x^s + b'$ belonging to $R_v[x]$ be monic polynomials of degree n and s' respectively with $n = p^k s'$, $m = p^k s$, $k \in \mathbb{N}$ where p is a prime number. Then*

$$F(x) = h(x)^{p^k} + ph(x)M_1(x) + (-a'x^s - b')^{p^k} + (ax^{sp^k} + b)$$

for some polynomial $M_1(x) \in R_v[x]$.

Proof. We first show that

$$(x^{s'} - h(x))^{p^k} = x^{s'p^k} - ph(x)M_1(x) - (h(x))^{p^k} \tag{2.2.1}$$

for some $M_1(x) \in R_v[x]$. When p is odd, on applying Binomial theorem, (2.2.1) can be easily seen. When $p = 2$, write

$$(x^{s'} - h(x))^{2^k} = x^{s'2^k} - (h(x))^{2^k} + N_1(x),$$

where $N_1(x) = \binom{2^k}{1}x^{s'(2^k-1)}(-h(x)) + \cdots + \binom{2^k}{2^k-1}x^{s'}(-h(x))^{2^k-1} + 2h(x)^{2^k} = -2h(x)N_2(x)$ with $N_2(x) \in R_v[x]$ and (2.2.1) follows.

Since $(x^{s'} - h(x)) = -a'x^s - b'$, on taking p^kth power and then using (2.2.1), we see that $x^{s'p^k} - ph(x)M_1(x) - (h(x))^{p^k} = (-a'x^s - b')^{p^k}$ which gives

$$(h(x))^{p^k} = x^{s'p^k} - ph(x)M_1(x) - (-a'x^s - b')^{p^k}.$$

On subtracting the above equation from $h(x^{p^k}) = x^{s'p^k} + a'x^{sp^k} + b'$, we have

$$h(x^{p^k}) - a'x^{sp^k} - b' = h(x)^{p^k} + ph(x)M_1(x) + (-a'x^s - b')^{p^k}. \tag{2.2.2}$$

On writing $F(x)$ as $(h(x^{p^k}) - a'x^{sp^k} - b') + ax^{sp^k} + b$ and using (2.2.2) we obtain the desired equality.

Corollary 2.2.2. *Let* $x^n + c$ *and* $x^{s'} + c'$ *be polynomials with* $c, c' \in R_v \setminus M_v$ *and* $n = p^k s'$, $k \in \mathbb{N}$ *where* p *is a prime number. If* $\bar{g}_1(x) \cdots \bar{g}_t(x)$ *is the factorization of* $x^{s'} + \bar{c'}$ *into a product of irreducible polynomials over* R_v/M_v *with* $g_i(x) \in R_v[x]$, *then*

$$x^n + c = \left(\prod_{i=1}^{t} g_i(x) + \beta H(x)\right)^{p^k} + pT(x)\prod_{i=1}^{t} g_i(x) + p\beta U(x) + (-c')^{p^k} + c$$

for some polynomials $H(x), T(x), U(x) \in R_v[x]$ *and* $\beta \in M_v$.

Proof. The corollary follows on applying Lemma 2.2.1 to the polynomials x^n+c, $x^{s'}+c'$ and then substituting $g_1(x)\cdots g_t(x)+\beta H(x)$ for $x^{s'}+c'$ with $\beta\in M_v$.

Lemma 2.2.3. *Let $v, R_v, M_v, F(x)$ and D be as in Theorem* 2.1.1 *without the hypothesis R_v/M_v perfect. Suppose that $v(D)>0$ and $v(abm)=0$. Then there exists $d\in R_v\backslash M_v$ satisfying $a(m-n)d\equiv bn \ (mod\ M_v^2)$. Moreover for any $d\in R_v\backslash M_v$ satisfying the last congruence, all the repeated roots of $\overline{F}(x)$ in the algebraic closure of R_v/M_v are roots of $x^m-\bar{d}$ and any common root of $\overline{F}(x)$, $x^m-\bar{d}$ is a repeated root of $\overline{F}(x)$.*

Proof. Since $v(D)>0$ and $v(abm)=0$, it follows from (2.1.1) that $v(n(n-m))=0$. Let ξ be a repeated root of $\overline{F}(x)$ in the algebraic closure of R_v/M_v. Then

$$\overline{F}(\xi)=\xi^n+\bar{a}\xi^m+\bar{b}=\bar{0};\quad \overline{F}'(\xi)=\bar{n}\xi^{n-1}+\bar{a}\bar{m}\xi^{m-1}=\bar{0}. \tag{2.2.3}$$

On substituting $\xi^{n-m}=\dfrac{-\bar{a}\bar{m}}{\bar{n}}$ in the first equation of (2.2.3) and keeping in mind that $v(a(n-m))=0$, we see that

$$\xi^m=\frac{\bar{b}\bar{n}}{\bar{a}(\bar{m}-\bar{n})}. \tag{2.2.4}$$

Since $a(m-n)bn$ is a unit of R_v, we can choose $d\in R_v\setminus M_v$ satisfying

$$a(m-n)d\equiv bn\ (mod\ M_v^2). \tag{2.2.5}$$

It follows from (2.2.4) and (2.2.5) that ξ is a root of $x^m-\bar{d}$. Conversely if ξ is a root of $x^m-\bar{d}$ and of $\overline{F}(x)$, then it follows from equations (2.2.3) – (2.2.5) that ξ is a root of $\overline{F}'(x)$ and hence the lemma is proved.

Lemma 2.2.4. *Let v, R_v, M_v be as in the above lemma and $\alpha_1,\ \alpha_2$ be elements of R_v. Suppose that m, n, m_1, n_1 are positive integers with* $\gcd(m,n)=d_0$, $n_1=\frac{n}{d_0}$ *and $m_1=\frac{m}{d_0}$. Then the polynomials $x^n-\bar{\alpha}_1$ and $x^m-\bar{\alpha}_2$ are coprime if and only if $\bar{\alpha}_1^{m_1}\neq\bar{\alpha}_2^{n_1}$, i.e., $v(\alpha_1^{m_1}-\alpha_2^{n_1})=0$.*

Proof. It is enough to prove that the polynomials $x^n - \bar{\alpha}_1$ and $x^m - \bar{\alpha}_2$ have a common root in the algebraic closure of R_v/M_v if and only if $\bar{\alpha}_1^{m_1} = \bar{\alpha}_2^{n_1}$. The lemma needs to be proved when both α_1, α_2 are units of R_v. Suppose first that $x^n - \bar{\alpha}_1$ and $x^m - \bar{\alpha}_2$ have a common root ξ. Then $\bar{\alpha}_1^{m_1} = (\xi^n)^{m_1} = (\xi^m)^{n_1} = \bar{\alpha}_2^{n_1}$ as desired. Conversely suppose that $\bar{\alpha}_1^{m_1} = \bar{\alpha}_2^{n_1}$. Choose positive integers r, s such that $sm_1 - rn_1 = 1$. Let ξ be a root of the polynomial $x^{d_0} - (\bar{\alpha}_1)^{-r}\bar{\alpha}_2^s$ in the algebraic closure of R_v/M_v. We show that ξ is a common root of $x^n - \bar{\alpha}_1$ and $x^m - \bar{\alpha}_2$. Keeping in mind $\bar{\alpha}_1^{m_1} = \bar{\alpha}_2^{n_1}$, we have $\xi^n = (\xi^{d_0})^{n_1} = (\bar{\alpha}_1)^{-n_1 r}\bar{\alpha}_2^{n_1 s} = (\bar{\alpha}_1)^{m_1 s - n_1 r} = \bar{\alpha}_1$ and $\xi^m = (\bar{\alpha}_1)^{-m_1 r}\bar{\alpha}_2^{m_1 s} = (\bar{\alpha}_2)^{m_1 s - n_1 r} = \bar{\alpha}_2$ as desired.

2.3 Proof of Theorem 2.1.1

Since $v(D) > 0$, the polynomial $\overline{F}(x)$ is divisible by the square of an irreducible polynomial belonging to $(R_v/M_v)[x]$. Hence in view of Theorem 1.1.A, the condition of M_v being a principal ideal is necessary for $R_v[\theta]$ to be integrally closed. Thus for proving Theorem 2.1.1, we may assume that M_v is a principal ideal generated by an element π.

Consider first the case when a, b belong to M_v. Then $F(x) \equiv x^n \ (mod\ M_v)$. Taking $g_1(x) = x$ and applying Theorem 1.1.A, we see that $R_v[\theta]$ is integrally closed if and only if x does not divide $\overline{M}(x)$, where $M(x) = \frac{a}{\pi}x^m + \frac{b}{\pi}$. Thus $R_v[\theta]$ is integrally closed in this case if and only if $\overline{(\frac{b}{\pi})} \neq \bar{0}$, i.e., $v(b) = v(\pi)$.

Consider now the case when $a \in M_v$ and $b \notin M_v$. As $v(D) > 0$, it is clear from (2.1.1) that $v(n) > 0$. So the characteristic p of R_v/M_v is positive and divides n. Write $n = p^j s', p \nmid s'$. Since R_v/M_v is a perfect field, there exists $b' \in R_v$ such that $(\bar{b}')^{p^j} = \bar{b}$. Therefore

$$F(x) \equiv x^n + b \equiv (x^{s'} + b')^{p^j} \ (mod\ M_v). \qquad (2.3.1)$$

Let $\bar{g}_1(x) \cdots \bar{g}_t(x)$ be the factorization of $x^{s'} + \bar{b}'$ over R_v/M_v, where $g_i(x) \in R_v[x]$ are monic polynomials which are distinct and irreducible modulo M_v. Applying

Corollary 2.2.2 to the polynomials $x^n + b$, $x^{s'} + b'$, we see that

$$F(x) = \left(\prod_{i=1}^{t} g_i(x) + \beta H(x)\right)^{p^j} + pT(x)\prod_{i=1}^{t} g_i(x) + p\beta U(x) + (-b')^{p^j} + b + ax^m \tag{2.3.2}$$

for some polynomials $H(x), T(x), U(x) \in R_v[x]$ and $\beta \in M_v$. Denote $\frac{a}{\pi}$, $\frac{b+(-b')^{p^j}}{\pi}$ by a_2, b_1 respectively. In view of (2.3.1), $\overline{F}(x) = \prod\limits_{i=1}^{t} \bar{g}_i(x)^{p^j}$. Write $F(x)$ as $\prod\limits_{i=1}^{t} g_i(x)^{p^j} + \pi M(x)$, $M(x) \in R_v[x]$. Keeping in mind that $j \geq 1$, it is immediate from (2.3.2) that

$$\overline{M}(x) = \overline{\left(\frac{p}{\pi}\right)}\overline{T}(x)\prod_{i=1}^{t} \bar{g}_i(x) + \bar{b}_1 + \bar{a}_2 x^m. \tag{2.3.3}$$

In view of Theorem 1.1.A, $R_v[\theta]$ is integrally closed if and only if $\overline{M}(x)$ is coprime to $\prod\limits_{i=1}^{t} \bar{g}_i(x)$, which by virtue of (2.3.3) holds if and only if $\bar{a}_2 x^m + \bar{b}_1$ is coprime to $\prod\limits_{i=1}^{t} \bar{g}_i(x)$. Recall that $\prod\limits_{i=1}^{t} \bar{g}_i(x)^{p^j} = x^n + \bar{b}$. Now $\bar{a}_2 x^m + \bar{b}_1$ and $x^n + \bar{b}$ are coprime if and only if either I) $\bar{a}_2 = \bar{0}$ and $\bar{b}_1 \neq \bar{0}$ or II) $\bar{a}_2 \neq \bar{0}$ and the polynomials $x^m + \dfrac{\bar{b}_1}{\bar{a}_2}$, $x^n + \bar{b}$ are coprime. In view of Lemma 2.2.4, II) holds if and only if $v(a_2) = 0$ and $v((-b)^{m_1} a_2^{n_1} - (-b_1)^{n_1}) = 0$. So $R_v[\theta]$ is integrally closed if and only if either I) $v(a_2) \geq v(\pi)$ and $v(b_1) = 0$ or II) $v(a_2) = 0$ and $v((-b)^{m_1} a_2^{n_1} - (-b_1)^{n_1}) = 0$.

We now deal with the case when $a \notin M_v$, $b \in M_v$ and $v(n-m) = 0$. In this case keeping in mind that $v(D) > 0$, it follows from (2.1.1) that $m \geq 2$. Since $v(n-m) = 0$, $x^{n-m} + \bar{a}$ does not have any repeated root and hence the only irreducible repeated factor of $\overline{F}(x) = x^m(x^{n-m} + \bar{a})$ is x. So we can write $F(x)$ as $x^m(\prod\limits_{i=1}^{t} g_i(x) + \pi T(x)) + b$, where $T(x) \in R_v[x]$ and $g_i(x) \in R_v[x]$ are monic polynomials which are distinct and irreducible modulo M_v. Consequently the polynomial

$$\frac{1}{\pi}(F(x) - x^m \prod_{i=1}^{t} g_i(x)) = x^m T(x) + \frac{b}{\pi}$$

is not divisible by x modulo M_v if and only if $v(b) = v(\pi)$. So the result is proved in this case by virtue of Theorem 1.1.A.

Now consider the case when $a \notin M_v$, $b \in M_v$ and $v(n-m) > 0$. Here the characteristic p of R_v/M_v is positive and divides $n - m$. Let $l \geq 1$ denote the highest power of p dividing $n-m$; write $n-m=p^l s'$. Since R_v/M_v is perfect, choose $a' \in R_v$ such that $(\bar{a'})^{p^l} = \bar{a}$. Let $\bar{g}_1(x)\cdots\bar{g}_t(x)$ be the factorization of $x^{s'}+\bar{a'}$ over R_v/M_v, where $g_i(x) \in R_v[x]$ are monic polynomials which are distinct and irreducible modulo M_v. Applying Corollary 2.2.2 to the polynomials $x^{n-m}+a$, $x^{s'}+a'$, we can write $F(x) = x^m(x^{n-m}+a)+b$ as

$$F(x) = x^m\left[(\prod_{i=1}^{t} g_i(x) + \beta H(x))^{p^l} + pT(x)\prod_{i=1}^{t} g_i(x) + p\beta U(x) + (-a')^{p^l} + a\right] + b, \tag{2.3.4}$$

where $\beta \in M_v$ and $H(x), T(x), U(x)$ belong to $R_v[x]$. Denote $\dfrac{a+(-a')^{p^l}}{\pi}, \dfrac{b}{\pi}$ by a_1, b_2 respectively. Since $\overline{F}(x) = x^m \prod_{i=1}^{t} \bar{g}_i(x)^{p^l}$ and $l \geq 1$, it follows on applying Theorem 1.1.A that $R_v[\theta]$ is integrally closed if and only if $x^{m-1}\prod_{i=1}^{t}\bar{g}_i(x)$ is coprime to $\overline{M}(x)$, where $M(x) = \frac{1}{\pi}(F(x) - x^m \prod_{i=1}^{t} g_i(x)^{p^l})$. It is clear from (2.3.4) that

$$\overline{M}(x) = \overline{\left(\frac{p}{\pi}\right)} x^m \overline{T}(x)\prod_{i=1}^{t}\bar{g}_i(x) + \bar{a}_1 x^m + \bar{b}_2.$$

Keeping in mind that $\prod_{i=1}^{t}\bar{g}_i(x)^{p^l} = x^{n-m}+\bar{a}$, the above equation shows that $\overline{M}(x)$ is coprime to $x^{m-1}\prod_{i=1}^{t}\bar{g}_i(x)$ if and only if $\bar{a}_1 x^m + \bar{b}_2$ is coprime to $x^{m-1}(x^{n-m}+\bar{a})$. The last statement is true if and only if either I) $\bar{a}_1 = \bar{0}$, $\bar{b}_2 \neq \bar{0}$ or II) $\bar{a}_1 \neq \bar{0}$ and the polynomials $x^m + \frac{\bar{b}_2}{\bar{a}_1}$, $x^{m-1}(x^{n-m}+\bar{a})$ are coprime. Applying Lemma 2.2.4 to the polynomials $x^m + \frac{\bar{b}_2}{\bar{a}_1}$, $x^{n-m}+\bar{a}$, it can be easily seen that II) holds if and only if $v(a_1) = 0, v(b_2^{m-1}) = 0$ and $v((-a)^{m_1}a_1^{n_1-m_1} - (-b_2)^{n_1-m_1}) = 0$.

We now deal with case (v) when $ab \notin M_v$ and $m \in M_v$. Keeping in mind that $v(D) > 0$, it follows from (2.1.1) that $v(n) > 0$. So the characteristic p of R_v/M_v divides both m, n. Write $n = s'p^k$, $m = sp^k$ and $p \nmid \gcd(s', s)$. Choose $a', b' \in R_v$ such that $(\bar{a'})^{p^k} = \bar{a}$ and $(\bar{b'})^{p^k} = \bar{b}$ and denote $x^{s'} + a'x^s + b'$ by $h(x)$. Let $\bar{h}(x) = \bar{g}_1(x)^{d_1}\cdots\bar{g}_t(x)^{d_t}$ be the factorization of $\bar{h}(x)$ into a product of powers of irreducible polynomials over R_v/M_v with $g_i(x) \in R_v[x]$ monic, $d_i > 0$. Applying

Lemma 2.2.1 to the polynomials $F(x), h(x)$, we see that

$$F(x) = h(x)^{p^k} + ph(x)M_1(x) + (ax^{sp^k} + b) + (-a'x^s - b')^{p^k}$$

for some $M_1(x) \in R_v[x]$. Substituting $h(x) = g_1(x)^{d_1} \cdots g_t(x)^{d_t} + \beta N(x)$ with $N(x) \in R_v[x]$ and $\beta \in M_v$ in the above equation, it follows that there exists $N_1(x) \in R_v[x]$ such that

$$F(x) = \prod_{i=1}^{t} g_i(x)^{d_i p^k} + \beta p N_1(x) + ph(x)M_1(x) + (ax^{sp^k} + b) + (-a'x^s - b')^{p^k}. \tag{2.3.5}$$

As $ax^{sp^k} + b + (-a'x^s - b')^{p^k}$ belongs to $M_v[x]$ in view of the choice of a', b', it is clear from (2.3.5) that $\overline{F}(x) = \prod_{i=1}^{t} \bar{g}_i(x)^{d_i p^k}$. Since $k > 0$, applying Theorem 1.1.A, we see that $R_v[\theta]$ is integrally closed if and only if $\prod_{i=1}^{t} \bar{g}_i(x)$ is coprime to $\overline{M}(x)$, where $M(x) = \frac{1}{\pi}(F(x) - g_1(x)^{d_1 p^k} \cdots g_t(x)^{d_t p^k})$. Keeping in mind the equality $\bar{h}(x) = \prod_{i=1}^{t} \bar{g}_i(x)^{d_i}$, it is immediate from (2.3.5) that $\overline{M}(x)$ is coprime to $\bar{h}(x) = \prod_{i=1}^{t} \bar{g}_i(x)^{d_i}$ if and only if $\frac{1}{\pi}[ax^{sp^k} + b + (-a'x^s - b')^{p^k}]$ is coprime to $h(x)$ modulo M_v. Hence the theorem is proved in the present case.

Finally consider case (vi) when $abm \notin M_v$. By Lemma 2.2.3, ξ is a repeated root of $\overline{F}(x)$ if and only if ξ is a common root of $\overline{F}(x)$ and $x^m - \bar{d}$ where $d \in R_v \setminus M_v$ satisfies (2.2.5). Choose positive integers r, s such that $m_1 s - n_1 r = 1$. Also $(ad + b) \notin M_v$ because $(m - n)(ad + b) \equiv bm \ (mod\ M_v^2)$ in view of (2.2.5) and $bm \notin M_v$. Therefore we can choose $c \in R_v$ satisfying the congruence

$$c \equiv d^s(-(ad + b))^{-r} \ (mod\ M_v^2). \tag{2.3.6}$$

Claim is that $x^{d_0} - \bar{c} = \gcd(\overline{F}(x), x^m - \bar{d})$. Since $mcd \notin M_v$, the polynomials $x^{d_0} - \bar{c}$, $x^m - \bar{d}$ have all their roots simple, to prove the claim it is enough to show that any root of $x^{d_0} - \bar{c}$ is a common root of $x^m - \bar{d}$, $\overline{F}(x)$ and vice versa. Let ξ be a root of $x^{d_0} - \bar{c}$. Keeping in mind (2.3.6), we see that

$$\xi^m = \xi^{m_1 d_0} = (\bar{c})^{m_1} = \bar{d}^{m_1 s}(-(\bar{a}\bar{d} + \bar{b}))^{-m_1 r};$$

consequently using equation (2.3.11) of the following lemma, we have

$$\xi^m = \bar{d}^{m_1 s}(\bar{d})^{-n_1 r} = \bar{d}. \tag{2.3.7}$$

So ξ is a root of $x^m - \bar{d}$. Further again using (2.3.6) and (2.3.11), we see that

$$\xi^n = \xi^{n_1 d_0} = (\bar{c})^{n_1} = \bar{d}^{n_1 s}(-(\bar{a}\bar{d}+\bar{b}))^{-n_1 r} = (-(\bar{a}\bar{d}+\bar{b}))^{m_1 s - n_1 r} = -(\bar{a}\bar{d}+\bar{b}).$$

Therefore keeping in mind (2.3.7), we have $\xi^n + \bar{a}\xi^m + \bar{b} = \bar{0}$ and hence ξ is a root of $\overline{F}(x)$. Conversely let ξ is a common root of $\overline{F}(x)$, $x^m - \bar{d}$. Then $\xi^m = \bar{d}$ and $\xi^n = -(\bar{a}\bar{d}+\bar{b})$; consequently using (2.3.6), we have $\xi^{d_0} = \xi^{ms-nr} = \bar{d}^s(-(\bar{a}\bar{d}+\bar{b}))^{-r} = \bar{c}$ as desired. Hence the claim is proved.

By division algorithm, write $F(x) = (x^{d_0})^{n_1} + a(x^{d_0})^{m_1} + b$ as

$$F(x) = (x^{d_0} - c)q(x) + c^{n_1} + ac^{m_1} + b \tag{2.3.8}$$

for some $q(x) \in R_v[x^{d_0}]$. In view of the claim proved above, $\overline{F}(x) = (x^{d_0} - \bar{c})\bar{q}(x)$. Let $\overline{F}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_t(x)^{e_t}$ be the factorization of $\overline{F}(x)$ into a product of powers of distinct irreducible polynomials over R_v/M_v with each $g_i(x) \in R_v[x]$ monic. If necessary, after renaming assume that $e_i > 1$ for $1 \le i \le t_1$ and $e_i = 1$ for $t_1 < i \le t$. Keeping in mind the claim, Lemma 2.2.3 and the fact that $x^{d_0} - \bar{c}$ has simple roots, it follows that the polynomial $x^{d_0} - \bar{c}$ is the product of all distinct monic repeated irreducible factors of $\overline{F}(x)$. Therefore we can write

$$x^{d_0} - c = \prod_{i=1}^{t_1} g_i(x) + \beta_1 h_1(x), \; q(x) = \prod_{i=1}^{t_1} g_i(x)^{e_i - 1} \prod_{i=t_1+1}^{t} g_i(x) + \beta_2 h_2(x)$$

for some $h_1(x), h_2(x) \in R_v[x]$ and $\beta_1, \beta_2 \in M_v$. Substituting for $x^{d_0} - c$ and $q(x)$ from the above equation in (2.3.8), we see that

$$\begin{aligned} F(x) = {} & \prod_{i=1}^{t} g_i(x)^{e_i} + \beta_1 h_1(x) \prod_{i=1}^{t_1} g_i(x)^{e_i-1} \prod_{i=t_1+1}^{t} g_i(x) + \beta_2 h_2(x) \prod_{i=1}^{t_1} g_i(x) \\ & + \beta_1\beta_2 h_1(x)h_2(x) + c^{n_1} + ac^{m_1} + b. \end{aligned}$$

Denote $c^{n_1} + ac^{m_1} + b$ by c_0. Write $F(x) = \prod_{i=1}^{t} g_i(x)^{e_i} + \pi M(x)$, $M(x) \in R_v[x]$. It is immediate from the above equation that

$$\overline{M}(x) = \overline{\left(\frac{\beta_1}{\pi}\right)}\bar{h}_1(x) \prod_{i=1}^{t_1} \bar{g}_i(x)^{e_i-1} \prod_{i=t_1+1}^{t} \bar{g}_i(x) + \overline{\left(\frac{\beta_2}{\pi}\right)}\bar{h}_2(x) \prod_{i=1}^{t_1} \bar{g}_i(x) + \overline{\left(\frac{c_0}{\pi}\right)}. \tag{2.3.9}$$

Applying Theorem 1.1.A, we see that $R_v[\theta]$ is integrally closed in this case if and only if $\overline{M}(x)$ is coprime to $\prod_{i=1}^{t_1} \bar{g}_i(x)$, which by virtue of (2.3.9) holds if and only if $\overline{\left(\frac{c_0}{\pi}\right)} \neq \bar{0}$. In view of the following Lemma 2.3.1, $\overline{\left(\frac{c_0}{\pi}\right)} \neq \bar{0}$ if and only if $C - E \notin M_v^2$. Hence in this case, $R_v[\theta]$ is integrally closed if and only if $C - E \notin M_v^2$.

Lemma 2.3.1. *Let $v, R_v, M_v, F(x), d_0, m_1, n_1$ and D be as in Theorem* 2.1.1 *without the hypothesis R_v/M_v perfect. Assume that $v(D) > 0$ and $v(abm) = 0$. Let c, d, r, s be as in the first paragraph of the proof of case (vi). Then $c^{n_1} + ac^{m_1} + b \equiv 0$ $(mod\ M_v^2)$ if and only if $C \equiv E$ $(mod\ M_v^2)$, where C, E are as in Theorem 2.1.1(vi).*

Proof. We first show that

$$(a(m-n))^{n_1}(d^{n_1} - (-ad-b)^{m_1}) \equiv b^{m_1} d_0^{n_1}(C - E)\ (mod\ M_v^2). \qquad (2.3.10)$$

Denote the expression on the left hand side of the above congruence by L, which we rewrite as $(a(m-n)d)^{n_1} - a^{n_1}(m-n)^{n_1 - m_1}(-a(m-n)d - b(m-n))^{m_1}$. Using (2.2.5), we obtain

$$L \equiv (bn)^{n_1} - a^{n_1}(m-n)^{n_1-m_1}(-bm)^{m_1}\ (mod\ M_v^2).$$

Substituting $n = n_1 d_0,\ m = m_1 d_0$ in the right hand side of the above congruence, (2.3.10) is proved.

Recall that by virtue of the hypothesis $ab(m-n) \notin M_v$ and $D = \pm b^{m-1} d_0^n (C - E)^{d_0}$ belongs to M_v. Therefore $C - E \in M_v$. It now follows from (2.3.10) that

$$\bar{d}^{n_1} = (-1)^{m_1}(\bar{a}\bar{d} + \bar{b})^{m_1}. \qquad (2.3.11)$$

Further keeping in mind (2.3.10), the lemma is proved as soon as we prove that

$$c^{n_1} + ac^{m_1} + b \equiv 0\ (mod\ M_v^2) \text{ if and only if } d^{n_1} \equiv (-ad-b)^{m_1}\ (mod\ M_v^2). \quad (2.3.12)$$

Since $(m-n)(ad+b) \equiv bm$ $(mod\ M_v^2)$ in view of (2.2.5), we have $ad + b \notin M_v$ and hence we can choose $Z \in R_v$ such that $Z \equiv d^{n_1}(-(ad+b))^{-m_1}$ $(mod\ M_v^2)$. By virtue of (2.3.11), we have

$$Z \equiv 1\ (mod\ M_v). \qquad (2.3.13)$$

Thus (2.3.12) and hence the lemma is proved once we show that

$$c^{n_1} + ac^{m_1} + b \equiv 0 \ (mod\ M_v^2) \text{ if and only if } Z \equiv 1 \ (mod\ M_v^2). \qquad (2.3.14)$$

Recall that by (2.3.6), we have $c \equiv d^s(-ad-b)^{-r}\ (mod\ M_v^2)$; consequently

$$c^{n_1} + ac^{m_1} + b \equiv d^{n_1 s}(-ad-b)^{-n_1 r} + ad^{m_1 s}(-ad-b)^{-m_1 r} + b\ (mod\ M_v^2). \quad (2.3.15)$$

Using $m_1 s - n_1 r = 1$, the right hand side of the above congruence equals

$$(d^{n_1}(-ad-b)^{-m_1})^s(-ad-b) + ad(d^{n_1}(-ad-b)^{-m_1})^r + b,$$

which in view of the choice of Z is congruent modulo M_v^2 to $(-ad-b)Z^s + adZ^r + b$. So (2.3.15) can be rewritten as

$$c^{n_1} + ac^{m_1} + b \equiv ad(Z^r - Z^s) + b(1 - Z^s)\ (mod\ M_v^2).$$

Note that $s > r$, for otherwise $1 = m_1 s - n_1 r \leq r(m_1 - n_1) < 0$. On arranging the terms on the right hand side, we rewrite the last congruence as

$$c^{n_1} + ac^{m_1} + b \equiv (1-Z)\left[adZ^r\left(\sum_{i=0}^{s-r-1} Z^i\right) + b\left(\sum_{i=0}^{s-1} Z^i\right)\right]\ (mod\ M_v^2).$$

Denote the right hand side of the above congruence by $(1-Z)A$. It is clear from this congruence that (2.3.14) is proved as soon as we show that A does not belong to M_v. By virtue of (2.3.13), we see that $A \equiv (ad(s-r) + bs)\ (mod\ M_v)$; so using (2.2.5), we have $(m-n)A \equiv bd_0\ (mod\ M_v)$. Since $bd_0 \notin M_v$, it follows that $A \notin M_v$ as desired.

Remark 2.3.2. *It may be pointed out that Theorem* 2.1.1 *is true in cases* $(i), (iii)$ *and* (vi) *without the hypothesis "R_v/M_v perfect" as this condition is not used in the proof of these cases.*

2.4 Proof of Theorem 2.1.6

Proof of Proposition 2.1.7. As is well known, $R[\theta]$ is integrally closed if and only if so is $R_\wp[\theta]$ for each maximal ideal $\wp$ of R, where $R_\wp$ stands for the localization of R at $\wp$. If the discriminant b_0 of $F(x)$ belongs to a maximal ideal $\wp$ of R, then $R_\wp[\theta]$ is integrally closed if and only if $b_0 \in \wp \setminus \wp^2$ in view of Theorem 2.1.1 (vi), because $\frac{1-b_0}{4} \notin \wp$. In case $b_0 \notin \wp$, $F(x)$ has no repeated factor modulo $\wp$ and hence $R_\wp[\theta]$ is integrally closed by Theorem 1.1.A in this case. So we conclude that $R[\theta]$ is integrally closed if and only if b_0R is not divisible by the square of any maximal ideal of R.

Proof of Proposition 2.1.8. As pointed out in the proof of the above proposition, $R[\theta]$ is integrally closed if and only if so is $R_\wp[\theta]$ for any maximal ideal $\wp$ of R containing the discriminant $-4b$ of $F(x)$. Using assertion (i) of Theorem 2.1.1 and Remark 2.3.2, it follows that for a maximal ideal $\wp$ of R containing b, $R_\wp[\theta]$ is integrally closed if and only if $b \in \wp \setminus \wp^2$. Further by assertion (ii) of Theorem 2.1.1, for a maximal ideal $\wp$ of R containing 2 and not containing b, $R_\wp[\theta]$ is integrally closed if and only if $b + (-b')^2 \in \wp \setminus \wp^2$, where $b' \in R$ is such that $(b')^2 \equiv b (mod\ \wp)$. Hence the proposition is proved.

Proof of Theorem 2.1.6. Let $L = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer and $\beta = \frac{1+\sqrt{d}}{2}$ or $\sqrt{d}$ according as $d \equiv 1\ (mod\ 4)$ or not. Denote the Dedekind domain A_K by R. Then $A_K A_L = R[\beta]$. To prove the theorem, it is enough to prove that $R[\beta]$ is integrally closed if and only if the discriminants of K and L are coprime. The proof is split into two cases. First consider the case when $d \equiv 1 (mod\ 4)$. Since $L \not\subseteq K$, the minimal polynomial of $\beta = \frac{1+\sqrt{d}}{2}$ over the quotient field K of R is $x^2 - x + \frac{1-d}{4}$. Applying Proposition 2.1.7, we see that $R[\beta]$ is integrally closed in this case if and only if $d \notin \wp^2$ for any maximal ideal $\wp$ of R, i.e., $R[\beta]$ is integrally closed if and only if each prime number dividing d (which is the discriminant of $\mathbb{Q}(\sqrt{d})$ in this case) is unramified in K; this is same as requiring that each prime dividing the discriminant of L is coprime to the discriminant of K in view of the well known Dedekind's theorem which states that a prime p is ramified in an algebraic number field K_0 if and only if it divides the discriminant of K_0 (cf. [Ded, Corollary 3, p. 158]). Hence the theorem is proved in this case.

Now consider the case when $d \equiv 2$ or $3\ (mod\ 4)$, the minimal polynomial of $\beta = \sqrt{d}$ over K is $x^2 - d$. Applying Proposition 2.1.8, $R[\beta]$ is integrally closed if and only if for each maximal ideal $\wp$ dividing $4dR$ either I) $d \in \wp \setminus \wp^2$ or II) $2 \in \wp$, $d \notin \wp$ and $-d + (d')^2 \in \wp \setminus \wp^2$ where d' can be chosen to be d. Note that condition II) is vacuous when $d \equiv 2 \ (mod\ 4)$. When $d \equiv \ 3 \ (mod\ 4)$, then II) holds if and only if $d(d-1) \in \wp \setminus \wp^2$ for every maximal ideal $\wp$ of R containing 2, which clearly is true if and only if the prime 2 is unramified in K. Hence $R[\beta]$ is integrally closed if and only if each prime dividing $4d$ is unramified in K and the desired result in the present case follows from Dedekind's theorem quoted above.

Chapter 3

Discriminant as a product of local discriminants

3.1 Origin of problem and statements of results.

Discriminant of an extension of algebraic number fields is an important tool for studying such extensions. One of the basic properties of discriminant is that it can be expressed as a product of local discriminants (cf. [Ca-Fr, Proposition 5, Chapter I]). There is a similar property for discrete valuation rings. Let R be a discrete valuation ring with maximal ideal $\mathfrak{p}$ and S be the integral closure of R in a finite separable extension L of K. For a maximal ideal $\mathfrak{P}$ of S, let $\hat{R}_{\mathfrak{p}}, \hat{S}_{\mathfrak{P}}$ denote respectively the valuation rings of the completions of K, L with respect to $\mathfrak{p}, \mathfrak{P}$. The discriminant satisfies $disc(S/R)\hat{R}_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} disc(\hat{S}_{\mathfrak{P}}/\hat{R}_{\mathfrak{p}})$. In this chapter, we extend the above equality on replacing R by the valuation ring of a Krull valuation of arbitrary rank and completion by henselization.

In what follows, for a valuation v of a field K, R_v will denote its valuation ring and M_v the maximal ideal of R_v. (K^h, v^h) will denote the henselization of (K, v) whose valuation ring will be denoted by R_v^h. As in Definition 1.1.B, $d(S/R_v)$ will stand for the discriminant of S/R_v with S a free R_v-module of finite rank. In this chapter, our main aim is to prove the following theorem.

Theorem 3.1.1. *Let (K, v) be a valued field of arbitrary rank with valuation ring R_v and (K^h, v^h) be its henselization having valuation ring R_v^h. Let L be a finite separable extension of K and S be the integral closure of R_v in L. Let $w_1, \cdots, w_s$ be all the prolongations of v to L. Assume that S is a free R_v-module. Then the valuation ring $R_{w_i}^h$ of the henselization of (L, w_i) is a free R_v^h-module and $d(S/R_v)R_v^h = \prod_{i=1}^{s} d(R_{w_i}^h/R_v^h)$.*

The above theorem plays a crucial role in extending the well known theorem of Index of Ore [Kh-Ku4] to polynomials with coefficients in arbitrary valued fields (see [Jh-Kh5, Lemma 3.2]). While proving Theorem 3.1.1, we prove a generalization of the weak Approximation Theorem ([En-Pr, Theorem 3.2.7]) which is of independent interest as well.

3.2 Preliminary Results

The following theorem will be needed in the sequel.

Theorem 3.2.1. *Let $\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_k$ be non-comparable valuation rings of a field K with maximal ideals $\mathcal{M}_1, \mathcal{M}_2, \cdots, \mathcal{M}_k$ and $R = \cap_{i=1}^{k} \mathcal{B}_i$. Then for each tuple $(a_1, \cdots, a_k)$ belonging to $\mathcal{B}_1 \times \cdots \times \mathcal{B}_k$ such that a_k is a unit of $\mathcal{B}_i\mathcal{B}_k$ for $1 \leq i \leq k-1$, there exists an element $c \in R$ such that $c - a_i \in \mathcal{M}_i$ for $1 \leq i \leq k-1$ and $c - a_k \in a_k\mathcal{M}_k$.*

Proof. Denote $R \cap \mathcal{M}_i$ by $\mathfrak{p}_i$. By Lemma 3.2.6 of [En-Pr], $\mathfrak{p}_i$ is a maximal ideal of R and $\mathcal{B}_i = R_{\mathfrak{p}_i}$. Since $\mathcal{B}_i/\mathcal{M}_i \cong R/\mathfrak{p}_i$, there exists $b_i \in R$ such that $a_i - b_i \in \mathcal{M}_i, 1 \leq i \leq k-1$. Write $a_k = \frac{r_k}{s_k}$ with $r_k \in R, s_k \in R \backslash \mathfrak{p}_k$. As $\mathfrak{p}_k$ is a maximal ideal of R, $\mathfrak{p}_k + s_kR = R$, so there exists $t_k \in R$ such that $s_kt_k + p_k = 1$ for some $p_k \in \mathfrak{p}_k$. Denote r_kt_k by b_k. Then $b_k = a_ks_kt_k$ and $a_k - b_k = a_k(1 - s_kt_k) = a_kp_k$ belongs to $a_k\mathcal{M}_k$. So it is enough to find $c \in R$ such that

$$c - b_i \in \mathcal{M}_i \text{ for } 1 \leq i \leq k-1 \text{ and } c - b_k \in b_k\mathcal{M}_k \subseteq a_k\mathcal{M}_k. \qquad (3.2.1)$$

Since $\mathcal{M}_i \cap R$ are distinct maximal ideals of R, the existence of an element $c \in R$ satisfying (3.2.1) is proved in view of Chinese Remainder Theorem once we show that

$$\mathcal{M}_i \cap R + (b_k\mathcal{M}_k) \cap R = R \text{ for } 1 \leq i \leq k-1. \tag{3.2.2}$$

For simplicity of notation, we verify (3.2.2) for $i = 1$. Suppose to the contrary it is false, then

$$\mathcal{M}_1 \cap R \supseteq (b_k\mathcal{M}_k) \cap R. \tag{3.2.3}$$

Define $\mathcal{B}' = \left\{\frac{a}{b} | a \in \mathcal{B}_k, b \in R \setminus \mathcal{M}_1\right\}$. Then $\mathcal{B}'$ is a ring containing $\mathcal{B}_1\mathcal{B}_k$. Let $\mathcal{M}_{1k}$ denote the maximal ideal of $\mathcal{B}_1\mathcal{B}_k$. As $\mathcal{B}_1, \mathcal{B}_k$ are not comparable, it follows that $\mathcal{B}_k \subsetneqq \mathcal{B}_1\mathcal{B}_k$. Fix $z \in \mathcal{M}_k \setminus \mathcal{M}_{1k}$. Claim is that $\frac{1}{zb_k} \notin \mathcal{B}'$. If $\frac{1}{zb_k} \in \mathcal{B}'$, then $\frac{1}{zb_k} = \frac{a}{b}$, where $a \in \mathcal{B}_k, b \in R \setminus \mathcal{M}_1$ which implies that $b = b_k z a \in b_k\mathcal{M}_k \cap R \subseteq \mathcal{M}_1 \cap R$ in view of (3.2.3). This is a contradiction as $b \notin \mathcal{M}_1$ and hence the claim is proved. Since a_k is a unit of $\mathcal{B}_1\mathcal{B}_k$ by hypothesis and $b_k = a_k s_k t_k$ with $s_k t_k$ a unit of $\mathcal{B}_k$, it follows that b_k is a unit of $\mathcal{B}_1\mathcal{B}_k$. So $b_k^{-1} \in \mathcal{B}_1\mathcal{B}_k$. By choice $z \in \mathcal{M}_k \setminus \mathcal{M}_{1k}$; consequently $z^{-1} \in \mathcal{B}_1\mathcal{B}_k$. Thus $\frac{1}{zb_k} \in \mathcal{B}_1\mathcal{B}_k \subseteq \mathcal{B}'$, which contradicts the claim and hence (3.2.2) is proved.

Remark 3.2.A. It may be pointed out that the above theorem yields the weak Approximation Theorem ([En-Pr, Theorem 3.2.7]) because if $(a_1, \cdots, a_k)$ is any tuple belonging to $\mathcal{B}_1 \times \cdots \times \mathcal{B}_k$, then applying Theorem 3.2.1 to the tuples $(a_1, \cdots, a_{k-1}, 1) \in \mathcal{B}_1 \times \cdots \times \mathcal{B}_k$ and $(a_k, 1, \cdots, 1) \in \mathcal{B}_k \times \mathcal{B}_1 \times \cdots \times \mathcal{B}_{k-1}$, we see that there exist $c, c' \in R$ such that $c - a_i \in \mathcal{M}_i$ for $1 \leq i \leq k-1, c - 1 \in \mathcal{M}_k$ and $c' - a_k \in \mathcal{M}_k, c' - 1 \in \mathcal{M}_i$ for $1 \leq i \leq k-1$; consequently $cc' - a_i \in \mathcal{M}_i$ for $1 \leq i \leq k$.

We now deduce the following corollary (to be used in the proof of Theorem 3.2.3) from Theorem 3.2.1.

Corollary 3.2.2. *Let $(K, v), L$ and S be as in Theorem 3.1.1 without the assumption that L/K is separable. If w_j is a prolongation of v to L with value group G_{w_j} which has a smallest positive element μ, then there exists an element $c \in S$ such that $w_j(c) = \mu$.*

Proof. Let $w_1, \cdots, w_s$ be all the prolongations of v to L. Let R_{w_i} denote the valuation ring of w_i for $1 \leq i \leq s$. Let π_j be an element of K such that $w_j(\pi_j)$ is the smallest positive element of G_{w_j}. Note that π_j is a unit of $R_{w_i}R_{w_j}, 1 \leq i \leq s, i \neq j$, because otherwise π_j belongs to the maximal ideal M_{ij} of $R_{w_i}R_{w_j}$ which implies that the maximal ideal of R_{w_j} generated by π_j is contained in M_{ij}; this in turn implies that $R_{w_i}R_{w_j}$ is contained in R_{w_j}, which is impossible as the rings R_{w_i} and R_{w_j} are not comparable for $i \neq j$. Applying Theorem 3.2.1 to the valuation rings $R_{w_1}, \cdots, R_{w_s}$, taking $a_i = 1$ for $1 \leq i \leq s, i \neq j$ and $a_j = \pi_j$, we see that there exists c belonging to $\cap_{i=1}^{s} R_{w_i} = S$ such that $w_j(c - \pi_j) > w_j(\pi_j)$ and hence $w_j(c) = w_j(\pi_j)$.

The following lemma is an immediate consequence of Theorems 18.2,18.6 of [End]. For the sake of completeness we prove it here using the notion of initial index defined below.

Definition 3.2.B. If H is a subgroup of finite index of a abelian group G, then the initial index of H in G which will be denoted by $\mathcal{E}(G : H)$ is defined to be the cardinality of the set

$$E_{G,H} = \{\epsilon \in G | 0 \leq \epsilon < \delta \text{ for all positive } \delta \in H\}.$$

Clearly distinct elements of $E_{G,H}$ lie in different cosets of H in G; consequently $\mathcal{E}(G : H) \leq [G : H]$.

Lemma 3.2.C. *Let $(K, v), R_v^h, L, S, w_1, \cdots, w_s$ and $R_{w_i}^h$ be as in Theorem 3.1.1. If S is a free R_v-module, then $R_{w_i}^h$ is a free R_v^h-module for $1 \leq i \leq s$.*

Proof. Write $L = K(\theta)$ where θ is an element of S and $F(x) \in R_v[x]$ is the minimal polynomial of θ over K. Let $\prod_{i=1}^{s} G_i(x)$ be the factorization of $F(x)$ into a product of distinct monic irreducible factors over the henselization (K^h, v^h) of (K, v). Let θ_i be a root of $G_i(x)$. Let w_i denote the prolongation of v to $K(\theta)$ defined by

$$w_i(\sum_j a_j \theta^j) = \tilde{v}^h(\sum_j a_j \theta_i^j), a_j \in K, \tag{3.2.4}$$

$\tilde{v}^h$ being unique prolongation of v^h to algebraic closure of K^h. Then in view of Theorem 1.1.D, $w_1, \cdots, w_s$ are all the distinct prolongations of v to $K(\theta)$. Let e_i, f_i denote the index of ramification and the residual degree respectively of w_i/v and G_v, G_{w_i} the value groups of v, w_i. Since S is a free R_v-module, in view of Theorems 18.2, 18.6 of [End], $e_i f_i = [K^h(\theta_i) : K^h]$ and the initial index $\mathcal{E}(G_{w_i} : G_v) = [G_{w_i} : G_v] = e_i$ for $1 \leq i \leq s$. Note that by virtue of (3.2.4), $K^h(\theta_i)$ is K^h-isomorphic (as a valued field) to the henselization of $K(\theta)$ with respect to w_i. Hence $R^h_{w_i}$ is a free R^h_v-module of rank $e_i f_i$ by [End, Theorem 18.6].

Using the above lemma and Corollary 3.2.2, we shall prove the following theorem which is needed for proving Theorem 3.1.1.

Theorem 3.2.3. *Let $(K, v), R^h_v, L, S, w_1, \cdots, w_s$ and $R^h_{w_i}$ be as in Theorem 3.1.1. Assume that S is a free R_v-module. Then one can choose a suitable R^h_v-basis $\mathcal{B}_i \subseteq S$ of $R^h_{w_i}$ such that (i) $\cup_{i=1}^s \mathcal{B}_i$ is an R_v-basis of S; (ii) for every $B_{ij} \in \mathcal{B}_i$ and for each $k \neq i$, $w_k(B_{ij}) \geq v(a) > 0$ for some a in K.*

Proof. Let e_i, f_i, G_v, G_{w_i} and the initial index $\mathcal{E}(G_{w_i} : G_v)$ be as in the proof of Lemma 3.2.C. Let $\mathcal{M}_{w_i}$ denote the maximal ideal of the valuation ring R_{w_i} of w_i. Set $\mathbf{m}_i = S \cap \mathcal{M}_{w_i}$. Then $\mathbf{m}_1, \cdots, \mathbf{m}_s$ are distinct maximal ideals of S. Let $\alpha_{i_1} + \mathcal{M}_{w_i}, \cdots, \alpha_{if_i} + \mathcal{M}_{w_i}$ be a basis of $R_{w_i}/\mathcal{M}_{w_i}$ over R_v/M_v. Fix one pair (i, j). By weak Approximation Theorem, there exists $\alpha'_{ij} \in L$ such that $w_i(\alpha_{ij} - \alpha'_{ij}) > 0$ and $w_k(\alpha'_{ij}) \geq 0$ for $k \neq i$. Then $\alpha'_{ij} \in S$. Since $\mathbf{m}_i + \prod\limits_{k=1, k\neq i}^{s} \mathbf{m}_k^{e_k} = S$, on applying Chinese Remainder Theorem we see that there exists $\beta_{ij} \in S$ satisfying $\alpha'_{ij} - \beta_{ij} \in \mathbf{m}_i$ and $\beta_{ij} \in \prod\limits_{k\neq i} \mathbf{m}_k^{e_k}$. Thus there exists $a \in K$ such that

$$w_k(\beta_{ij}) \geq v(a) > 0 \text{ for } k \neq i. \tag{3.2.5}$$

If G_{w_i} has a smallest positive element μ_i, then by Corollary 3.2.2, we can choose $\pi_i \in S$ such that $w_i(\pi_i) = \mu_i$. In case G_{w_i} does not have a smallest positive element, then by [End, Theorem 18.3] $\mathcal{E}(G_{w_i} : G_v) = 1$; consequently $G_{w_i} = G_v$ by virtue of the hypothesis that S is a free R_v-module and Theorem 18.6 of [End]. In this situation we take $\pi_i = 1$. It will be shown that $\mathcal{B}_i = \{\beta_{ij}\pi_i^k \mid 1 \leq j \leq f_i, 1 \leq k \leq e_i - 1\}$ is an R^h_v-basis of $R^h_{w_i}$ and $\cup_{i=1}^s \mathcal{B}_i$ is an R_v-basis of S.

Denote the R_v-submodule $\sum\limits_{k=0}^{e_i-1}\sum\limits_{j=1}^{f_i} R_v\beta_{ij}\pi_i^k$ of S by N_i. We first show that

$$S = \sum_{i=1}^{s} N_i + M_v S. \tag{3.2.6}$$

In view of Nakayama's Lemma and the hypothesis that S is a free R_v-module of finite rank, the above equation will imply that $S = \sum\limits_{i=1}^{s} N_i$ and hence $\cup_{i=1}^{s}\mathcal{B}_i$ would be an R_v-basis of S. Applying the above result with R_v, S replaced by $R_v^h, R_{w_i}^h$ respectively and keeping in mind that $R_{w_i}^h$ is a free R_v^h-module by Lemma 3.2.C, we shall conclude that $\mathcal{B}_i$ is an R_v^h-basis of $R_{w_i}^h$.

To verify (3.2.6), let ξ be any element of S. We show that for each i, $1 \leq i \leq s$, there exists $\xi_i \in N_i$ such that

$$w_i(\xi - \xi_i) \geq v(a_i) > 0 \tag{3.2.7}$$

for some $a_i \in K$. In view of (3.2.5) and the fact that $\pi_i \in S$, we have for every $\eta \in N_i$ and $l \neq i$, $w_l(\eta) \geq v(a) > 0$ for some $a \in K$. So (3.2.7) will imply that for each l, $1 \leq l \leq s$, $w_l(\xi - \sum\limits_{i=1}^{s}\xi_i) \geq v(b) > 0$ for some $b \in K$, which shows that $\frac{1}{b}(\xi - \sum\limits_{i=1}^{s}\xi_i) \in S$ and consequently ξ belongs to the right hand side of (3.2.6). Thus (3.2.6) will be proved and hence the theorem.

It only remains to verify (3.2.7). For simplicity of notation, we verify it for $i = 1$. Since $\beta_{11} + \mathcal{M}_{w_1}, \cdots, \beta_{1f_1} + \mathcal{M}_{w_1}$ form a basis of $R_{w_1}/\mathcal{M}_{w_1}$ over R_v/M_v, there exist $a_{1j} \in R_v$ such that

$$\xi \equiv \sum_{j=1}^{f_1} a_{1j}\beta_{1j}\ (mod\ \mathcal{M}_{w_1}). \tag{3.2.8}$$

We distinguish two cases. Consider first the case when $G_{w_1} = G_v$. In this case $M_{w_1} = M_v R_{w_1}$. On taking $\xi_1 = \sum\limits_{j=1}^{f_1} a_{1j}\beta_{1j}$, it now follows from (3.2.8) that $\xi - \xi_1 \in M_v R_{w_1}$ and hence (3.2.7) is verified in this case. Consider now the case when $[G_{w_1} : G_v] = e_1 > 1$. Then $\mathcal{E}(G_{w_1} : G_v) = [G_{w_1} : G_v] > 1$ and hence by Theorem 18.3 of [End], G_{w_1} has a smallest positive element which we denote by $w_1(\pi_1), \pi_1 \in S$. In this case, (3.2.8) implies that $\dfrac{1}{\pi_1}\left(\xi - \sum\limits_{j=1}^{f_1} a_{1j}\beta_{1j}\right)$ belongs to R_{w_1}. So there exist $b_{1j} \in R_v$ such that

$$\frac{\xi - \sum\limits_{j=1}^{f_1} a_{1j}\beta_{1j}}{\pi_1} \equiv \sum_{j=1}^{f_1} b_{1j}\beta_{1j}\ (mod\ \pi_1) \text{ in } R_{w_1}.$$

Thus we obtain

$$\xi \equiv \sum_{j=1}^{f_1} a_{1j}\beta_{1j} + \sum_{j=1}^{f_1} b_{1j}\beta_{1j}\pi_1\ (mod\ \pi_1^2).$$

Repeating the above process e_1-times, we see that

$$\xi \equiv \sum_{j=1}^{f_1} a_{1j}\beta_{1j} + \sum_{j=1}^{f_1} b_{1j}\beta_{1j}\pi_1 + \cdots + \sum_{j=1}^{f_1} u_{1j}\beta_{1j}\pi_1^{e_1-1}\ (mod\ \pi_1^{e_1})$$

in R_{w_1}. Denote the right hand side of the above congruence by ξ_1. Since $0 < w_1(\pi_1^{e_1}) \in G_v$, the above congruence implies that $\xi - \xi_1 \in M_v R_{w_1}$ and hence (3.2.7) is verified. This completes the proof of the theorem.

The following remarks will be used in the next section.

Remark 3.2.D. Let R be an integral domain and A be a commutative ring which is a free R-module of finite rank. If $\Lambda : A \longmapsto A'$ is an isomorphism of R-modules as well as of rings from A onto A', then clearly for any $\alpha \in A$, $Tr_{A/R}(\alpha) = Tr_{A'/R}(\Lambda(\alpha))$, where Tr stands for the trace map as introduced in Definition 1.1.B.

Remark 3.2.E. Let R be an integral domain and A_1, A_2 be commutative rings with identity which are free as R-modules with basis $\{B_{11}, \cdots, B_{1n_1}\}$, $\{B_{21}, \cdots, B_{2n_2}\}$ respectively. Consider the R-basis $\{(B_{11}, 0), \cdots, (B_{1n_1}, 0), (0, B_{21}), \cdots, (0, B_{2n_2})\}$ of $A_1 \times A_2$. With notation as in Definition 1.1.B, it can be easily verified that

$$D_{A_1 \times A_2/R}((B_{11}, 0), \cdots, (0, B_{2n_2})) = D_{A_1/R}(B_{11}, \cdots, B_{1n_1}) D_{A_2/R}(B_{21}, \cdots, B_{2n_2})$$

.

3.3 Proof of Theorem 3.1.1.

The proof of the theorem is divided into three steps.

Step I. Let $\mathcal{B}_i$ be as in Theorem 3.2.3. We take $S \subseteq R_{w_i} \subseteq R_{w_i}^h$. Denote the elements of $\mathcal{B}_i$ by $\{B_{ij} | 1 \leq j \leq n_i\}$. Let $\overline{B}_{ij}$ denote the element of $\prod\limits_{i=1}^{s} R_{w_i}^h$ whose i-th co-ordinate is B_{ij} and rest all co-ordinates are zero. By elementary ring theory, the family $\overline{\mathcal{B}} = \{\overline{B}_{ij} \mid 1 \le i \le s, 1 \le j \le n_i\}$ is an R_v^h-basis of $\prod_{i=1}^{s} R_{w_i}^h$. Let $\overline{C}_{ij}$ denote the element of $\prod_{i=1}^{s} R_{w_i}^h$ whose each co-ordinate is B_{ij}. Claim is that $\overline{\mathcal{C}} = \{\overline{C}_{ij} \mid 1 \le i \le s, 1 \le j \le n_i\}$ is an R_v^h-basis of $\prod_{i=1}^{s} R_{w_i}^h$. Keeping in mind that the elements B_{ij} satisfy property (ii) of Theorem 3.2.3, it can be easily seen that the transition matrix T from $\overline{\mathcal{B}}$ to $\overline{\mathcal{C}}$ (both sets arranged in lexicographic order with respect to the subscripts i, j) is congruent to the identity matrix modulo the maximal ideal of R_v^h. So T is unimodular and the claim is proved.

Step II. Consider the mapping

$$R_v^h \times S \longrightarrow \prod_{i=1}^{s} R_{w_i}^h$$

$$(r, \alpha) \longmapsto (r\alpha, \cdots, r\alpha), r \in R_v^h, \alpha \in S.$$

This R_v-bilinear map gives rise to a homomorphism

$$\Lambda : R_v^h \otimes_{R_v} S \longrightarrow \prod_{i=1}^{s} R_{w_i}^h$$

which is a homomorphism of rings as well as of R_v^h-modules. Clearly Λ maps $(1 \otimes B_{ij})$ to $\overline{C}_{ij}$ and hence maps the R_v^h-basis $\{1 \otimes B_{ij} \mid 1 \le i \le s, 1 \le j \le n_i\}$ of $R_v^h \otimes_{R_v} S = S^h$ (say) onto $\overline{\mathcal{C}}$. Since $\overline{\mathcal{C}}$ is R_v^h-basis of $\prod_{i=1}^{s} R_{w_i}^h$ in view of the claim proved in Step I, it follows that Λ is an isomorphism of S^h with $\prod_{i=1}^{s} R_{w_i}^h$.

Step III. Arrange the elements $\{B_{ij} \mid 1 \le i \le s, 1 \le j \le n_i\}$ in lexicographic order and label these as $\{\beta_1, \cdots, \beta_n\}$. By Definition 1.1.B, we have $d(S/R_v) = D_{S/R_v}(\beta_1, \cdots, \beta_n)R_v$. It can be easily seen that

$$D_{S/R_v}(\beta_1, \cdots, \beta_n) = D_{S^h/R_v^h}(1 \otimes \beta_1, \cdots, 1 \otimes \beta_n). \tag{3.3.1}$$

Since Λ maps the R_v^h-basis $\{1 \otimes \beta_i \mid 1 \le i \le n\}$ of S^h onto $\overline{\mathcal{C}}$, it follows from Remark 3.2.D that the right hand side of (3.3.1) equals $D_{\prod_{i=1}^{s} R_{w_i}^h / R_v^h}(\overline{C}_{11}, \cdots, \overline{C}_{1n_1}, \overline{C}_{21}, \cdots, \overline{C}_{sn_s})$.

Since both $\overline{\mathcal{C}}$ and $\overline{\mathcal{B}}$ are R_v^h-basis of $\prod_{i=1}^{s} R_{w_i}^h$, it is now immediate from (3.3.1) that

$$D_{S/R_v}(\beta_1, \cdots, \beta_n) = u^2 D_{\prod_{i=1}^{s} R_{w_i}^h / R_v^h}(\overline{B}_{11}, \cdots, \overline{B}_{1n_1}, \cdots, \overline{B}_{sn_s}), \tag{3.3.2}$$

where u is a unit of R^h_v. Keeping in mind Remark 3.2.E, we see that

$$D_{\prod_{i=1}^{s} R^h_{w_i}/R^h_v}(\overline{B}_{11}, \cdots, \overline{B}_{1n_1}, \overline{B}_{21}, \cdots, \overline{B}_{sn_s}) = \prod_{i=1}^{s} D_{R^h_{w_i}/R^h_v}(B_{i1}, \cdots, B_{in_i}).$$

The theorem now follows from (3.3.2).

Chapter 4

On the compositum of integral closures of valuation rings

4.1 Motivation of the problem and statements of the results.

As before, A_K will denote the ring of its algebraic integers of an algebraic number field K. It is well known that if K_1, K_2 are algebraic number fields with coprime discriminants, then the composite ring $A_{K_1}A_{K_2}$ is integrally closed and K_1, K_2 are linearly disjoint over the field $\mathbb{Q}$ of rational numbers (cf. [Nar, Theorem 4.26], [Es-Mu, Exercise 4.5.12]). This gives rise to the following natural question :

If K_1, K_2 are algebraic number fields linearly disjoint over $\mathbb{Q}$ for which $A_{K_1}A_{K_2}$ is integrally closed, then is it true that the discriminants of K_1 and K_2 are coprime?

We proved in Theorem 2.1.6 that the answer to the above question is in the affirmative when one of K_1 or K_2 is a quadratic field. In the present chapter, we prove that the answer to the above question is always "yes". Indeed we prove the following more general result.

Theorem 4.1.1. *Let (K, v) be a valued field of arbitrary rank with perfect residue field and K_1, K_2 be finite separable extensions of K which are linearly disjoint over*

K. Let S_1, S_2 denote the integral closures of the valuation ring R_v of v in K_1, K_2 respectively. If S_1, S_2 are free R_v-modules and S_1S_2 is integrally closed, then the discriminant of one of S_1/R_v or S_2/R_v is the unit ideal.

The following corollary will be quickly deduced from the above theorem.

Corollary 4.1.2. *Let K_1, K_2 be algebraic number fields which are linearly disjoint over $K = K_1 \cap K_2$ such that $A_{K_1K_2} = A_{K_1}A_{K_2}$. Then the relative discriminants of the extensions K_1/K and K_2/K are coprime.*

For proving Theorem 4.1.1, we shall prove the following theorem as a preliminary result. It is of independent interest as well.

Theorem 4.1.3. *Let $(K, v), K_1, K_2, S_1, S_2$ be as in Theorem 4.1.1 without the assumption that the residue field of v is perfect. Assume that S_1, S_2 are free R_v-modules and S_1S_2 is integrally closed. If r, s, t denote respectively the number of prolongations of v to K_1, K_2 and K_1K_2, then $t = rs$.*

4.2 Preliminary results

As in Chapter 3, for a valued field (K, v), (K^h, v^h) will denote its henselization whose valuation ring will be denoted by R_v^h and $d(S/R_v)$ will stand for the discriminant of S/R_v with S a free R_v-module of finite rank.

The proof of the following lemma is contained in the proof of Theorem 3.1.1. We omit its proof.

Lemma 4.2.A. *Let (K, v) be a valued field of arbitrary rank with valuation ring R_v and (K^h, v^h) be its henselization having valuation ring R_v^h. Let L be a finite separable extension of K and S be the integral closure of R_v in L. Let $w_1, \cdots, w_t$ be all the prolongations of v to L. Assume that S is a free R_v-module. Then the R_v-bilinear map from $R_v^h \times S$ into $\prod_{i=1}^t R_{w_i}^h$ mapping (a, α) to $(a\alpha, a\alpha, \cdots, a\alpha)$ for $a \in R_v^h, \alpha \in S$, gives rise to an R_v^h-module isomorphism Λ from $R_v^h \otimes_{R_v} S$ onto $\prod\limits_{i=1}^{t} R_{w_i}^h$.*

We prove a simple lemma needed for the proof of Theorem 4.1.3.

Lemma 4.2.B. *Let (K, v) be a valued field and K_1, K_2 be finite separable extensions of K which are linearly disjoint over K. Let v_1, v_2 be prolongations of v to K_1, K_2 respectively. Then there exists a prolongation v' of v to K_1K_2 such that v' coincides with v_i on K_i for $i = 1, 2$.*

Proof. Let w denote the unique prolongation of v^h to an algebraic closure Ω of K^h. By Theorem 1.1.D, there exists a K-isomorphism σ_i of K_i into Ω such that the valuation v_i is defined on K_i by $v_i(\alpha_i) = w(\sigma_i(\alpha_i)), \alpha_i \in K_i, i = 1, 2$. Since K_1, K_2 are linearly disjoint over K, there exists a K-isomorphism σ of K_1K_2 into Ω such that $\sigma\,|_{K_i} = \sigma_i$. So $v' = w \circ \sigma$ is a prolongation of v extending both v_1, v_2.

Using the above results, we now prove Theorem 4.1.3.

Proof of Theorem 4.1.3. Let $\{w_{1i} \mid 1 \le i \le r\}, \{w_{2j} \mid 1 \le j \le s\}, \{w_k \mid 1 \le k \le t\}$ denote all the prolongations of v to K_1, K_2, K_1K_2 respectively. It will be assumed that the henselizations under consideration are contained in a fixed algebraic closure of K^h. The degrees of the extensions $K^h_{w_{1i}}/K^h$, $K^h_{w_{2j}}/K^h$ will be denoted by n_{1i}, n_{2j} respectively and the degree of the henselization of K_1K_2 with respect to w_k over K^h will be denoted by m_k. Fix a pair (i, j), $1 \le i \le r, 1 \le j \le s$. Let w_k be a valuation of K_1K_2 extending the valuations w_{1i}, w_{2j} of K_1, K_2 respectively; such a prolongation exists in view of Lemma 4.2.B. Consider the R^h_v-bilinear map from $R^h_{w_{1i}} \times R^h_{w_{2j}}$ to $R^h_{w_k}$defined by $(\xi, \eta) \mapsto \xi\eta$ which gives rise to an R^h_v-module homomorphism $\Phi_{ij} : R^h_{w_{1i}} \otimes_{R^h_v} R^h_{w_{2j}} \longrightarrow R^h_{w_k}$. We first prove that Φ_{ij} is one-one. By Theorem 3.2.3, there exists an R^h_v-basis $\mathcal{B}_i = \{\xi_l \mid 1 \le l \le n_{1i}\}$ of $R^h_{w_{1i}}$ contained in an R_v-basis of S_1. Similarly choose an R^h_v-basis $\mathcal{C}_j = \{\eta_m \mid 1 \le m \le n_{2j}\}$ of $R^h_{w_{2j}}$ contained in an R_v-basis of S_2. Let $a_{lm} \in R^h_v$ be such that $\Phi_{ij}(\sum_{l,m} a_{lm}(\xi_l \otimes \eta_m)) = \sum_{l,m} a_{lm}\xi_l\eta_m = 0$. We have to prove that $a_{lm} = 0$ for each l, m. Let S denote the integral closure of R_v in K_1K_2. Since S_1S_2 is integrally closed, we have $S = S_1S_2$. If Λ denotes the R^h_v-module isomorphism as in Theorem 3.2.3 from $R^h_v \otimes_{R_v} S$ onto $\prod_{i=1}^t R^h_{w_i}$, then

$$\Lambda(\sum_{l,m} a_{lm} \otimes \xi_l\eta_m) = (\sum_{l,m} a_{lm}\xi_l\eta_m, \sum_{l,m} a_{lm}\xi_l\eta_m, \cdots, \sum_{l,m} a_{lm}\xi_l\eta_m) = (0, 0, \cdots, 0).$$

Since Λ is one-one, we see that

$$\sum_{l,m} a_{lm} \otimes \xi_l \eta_m = 0. \tag{4.2.1}$$

As K_1, K_2 are linearly disjoint over K, it follows from the choice of $\mathcal{B}_i, \mathcal{C}_j$ that $\{\xi_l \eta_m \mid 1 \leq l \leq n_{1i}, 1 \leq m \leq n_{2j}\}$ is contained in an R_v-basis of $S_1 S_2 = S$. Thus $\{1 \otimes \xi_l \eta_m \mid 1 \leq l \leq n_{1i}, 1 \leq m \leq n_{2j}\}$ is contained in an R_v^h-basis of $R_v^h \otimes_{R_v} S$. It now follows from (4.2.1) that $a_{lm} = 0$ for all l, m. So Φ_{ij} is one-one. Consequently taking into consideration the ranks of the domain and range of Φ_{ij}, it follows that

$$n_{1i} n_{2j} \leq m_k. \tag{4.2.2}$$

Since the composite field $K^h_{w_{1i}} K^h_{w_{2j}}$ being a finite extension of K^h is henselian, we see that

$$m_k \leq [K^h_{w_{1i}} K^h_{w_{2j}} : K^h] \leq n_{1i} n_{2j}. \tag{4.2.3}$$

Comparing (4.2.2) and (4.2.3), we have

$$m_k = [K^h_{w_{1i}} K^h_{w_{2j}} : K^h] = n_{1i} n_{2j}. \tag{4.2.4}$$

The above equation implies that $t = rs$ keeping in mind Theorem 1.1.D and the fact that

$$\sum_{k=1}^{t} m_k = [K_1 K_2 : K] = [K_1 : K][K_2 : K] = (\sum_{i=1}^{r} n_{1i})(\sum_{j=1}^{s} n_{2j}).$$

Remark 4.2.C. It may be pointed out that in view of equation (4.2.4), $K^h_{w_{1i}}$ and $K^h_{w_{2j}}$ are linearly disjoint over K^h for $1 \leq i \leq r, 1 \leq j \leq s$.

4.3 Proof of Theorem 4.1.1 and Corollary 4.1.2.

In the proof of the theorem, we shall use the following notation.

If $\lambda_i : M_i \longrightarrow N_i$ is a homomorphism of R-modules for $i = 1, 2$ with R a commutative ring with identity, then as usual $\lambda_1 \otimes \lambda_2 : M_1 \otimes M_2 \longrightarrow N_1 \otimes N_2$ will denote the R-module homomorphism satisfying $\lambda_1 \otimes \lambda_2 (m_1 \otimes m_2) = \lambda_1(m_1) \otimes \lambda_2(m_2)$

for all $m_1 \in M_1, m_2 \in M_2$.

If $\lambda_i : M_i \longrightarrow N_i$ is a mapping of sets for $1 \leq i \leq t$, then $\prod_{i=1}^{t} \lambda_i$ will stand for the map from $\prod_{i=1}^{t} M_i$ into $\prod_{i=1}^{t} N_i$ defined by $(\prod_{i=1}^{t} \lambda_i)(m_1, m_2, \cdots, m_t) = (\lambda_1(m_1), \lambda_2(m_2), \cdots, \lambda_t(m_t))$, $m_i \in M_i$.

The proof of the theorem is divided into three steps.

Step I. In this step, we prove the theorem assuming that (K, v) is henselian. Keeping in mind this assumption, the hypothesis R_v/M_v perfect and S_i a free R_v-module together with Theorem 18.6 of [End], it follows from Theorem 1.2 of [Kh-Ku1] that S_i is a simple ring extension of R_v for $i = 1, 2$, say $S_1 = R_v[\alpha_1], S_2 = R_v[\beta_2]$. Let $F_1(x), F_2(x)$ denote the minimal polynomials of α_1, β_2 respectively over K. For $g(x) \in R_v[x]$, $\bar{g}(x)$ has the same meaning as in Theorem 1.1.A. Suppose that $d(S_1/R_v)$ is not the unit ideal of R_v, i.e., the discriminant of $F_1(x)$ is not a unit of R_v. We have to prove that the discriminant of $F_2(x)$ is a unit of R_v. Since (K, v) is henselian, there exists a monic polynomial $g_1(x)$ belonging to $R_v[x]$ with $\bar{g}_1(x)$ irreducible over R_v/M_v such that $\overline{F}_1(x) = \bar{g}_1(x)^{e_1}$. Note that $e_1 > 1$, because otherwise the polynomial $\overline{F}_1(x)$ would be irreducible over the perfect field R_v/M_v and hence its discriminant would be nonzero contrary to our supposition. Therefore keeping in mind that $S_1 = R_v[\alpha_1]$ is integrally closed, it follows from Theorem 1.1.A that the value group G_v of v has a smallest positive element say $v(\pi), \pi \in K$ and

$$F_1(x) = g_1(x)^{e_1} + \pi M_1(x), \quad \bar{g}_1(x) \nmid \overline{M}_1(x). \tag{4.3.1}$$

Let w_1 with valuation ring S_1 denote the unique prolongation of the henselian valuation v to K_1. Claim is that the value group G_{w_1} of w_1 has a smallest positive element which is strictly less than $v(\pi)$. If G_{w_1} does not have a smallest positive element, then by [End, Theorem 18.3] the initial index[1] $\mathcal{E}(G_{w_1} : G_v)$ would be 1 and hence $G_{w_1} = G_v$ by virtue of the hypothesis that S_1 is a free R_v-module and Theorem 18.6 of [End]; this is not possible as G_v has a smallest positive element. So G_{w_1} has a smallest positive element say $w_1(\pi_1), \pi_1 \in K_1$. Recall that $F_1(\alpha_1) = 0$; therefore it follows from (4.3.1) that $w_1(g_1(\alpha_1)) = \frac{v(\pi)}{e_1} + \frac{w_1(M_1(\alpha_1))}{e_1}$. As $e_1 > 1$, the

[1]Recall that in Definition 3.2.B, the initial index $\mathcal{E}(G_{w_i} : G_v)$ is defined to be the cardinality of the set $\{\epsilon \in G_{w_i} \mid 0 \leq \epsilon < \delta$ for all positive $\delta \in G_v\}$.

claim follows from the last equation as soon as we show that $w_1(M_1(\alpha_1)) = 0$. If $w_1(M_1(\alpha_1)) > 0$, i.e., $\overline{M}_1(\bar{\alpha}_1) = \bar{0}$, then the minimal polynomial $\bar{g}_1(x)$ of $\bar{\alpha}_1$ over R_v/M_v would divide $\overline{M}_1(x)$ which contradicts (4.3.1). So $w_1(M_1(\alpha_1)) = 0$ and the claim is proved.

Arguing as for (4.3.1), we can write

$$F_2(x) = g_2(x)^{e_2} + \pi M_2(x), \tag{4.3.2}$$

where $g_2(x)$ belongs to $R_v[x]$ with $\bar{g}_2(x)$ irreducible over R_v/M_v, $e_2 \geq 1$ and $M_2(x)$ belongs to $R_v[x]$. Observe that $\bar{g}_2(x)$ is irreducible over the residue field of w_1, for otherwise in view of Hensel's Lemma, $F_2(x)$ would be reducible over the valuation ring S_1 of w_1 which is not so as the degree $[K(\beta_2) : K] = [K_1(\beta_2) : K_1]$ by virtue of K_1, K_2 being linearly disjoint over K. Therefore on rewriting (4.3.2) as $F_2(x) = g_2(x)^{e_2} + \pi_1 N_2(x)$ where $N_2(x) = \frac{\pi}{\pi_1} M_2(x)$ and keeping in mind the claim proved above together with the fact that $S_1[\beta_2] = S_1S_2$ is integrally closed, it follows from Theorem 1.1.A that $e_2 = 1$; consequently $discr(\overline{F}_2(x)) = discr(\bar{g}_2(x)) \neq \bar{0}$. Hence $d(S_2/R_v)$ (which is the ideal generated by discriminant of $F_2(x)$) is the unit ideal. This proves the theorem when (K, v) is henselian.

Step II. In this step, we prove that the composite ring $R^h_{w_{1i}} R^h_{w_{2j}}$ is integrally closed for $1 \leq i \leq r, 1 \leq j \leq s$. Let S denote the integral closure of R_v in K_1K_2. As S_1S_2 is integrally closed, we have $S = S_1S_2$. By Lemma 4.2.A, there exist R^h_v-module (onto) isomorphisms

$$\Lambda_1 : R^h_v \otimes_{R_v} S_1 \longrightarrow \prod_{i=1}^{r} R^h_{w_{1i}}; \quad \Lambda_2 : R^h_v \otimes_{R_v} S_2 \longrightarrow \prod_{j=1}^{s} R^h_{w_{2j}}; \quad \Lambda : R^h_v \otimes_{R_v} S \longrightarrow \prod_{k=1}^{t} R^h_{w_k}$$

such that for $a \in R^h_v, \alpha \in S_1, \beta \in S_2$ and $\gamma \in S$, we have

$$\Lambda_1(a \otimes \alpha) = (a\alpha, a\alpha, \cdots, a\alpha); \; \Lambda_2(a \otimes \beta) = (a\beta, a\beta, \cdots, a\beta); \; \Lambda(a \otimes \gamma) = (a\gamma, a\gamma, \cdots, a\gamma).$$

The R_v-bilinear map from $S_1 \times S_2$ into S defined by $(\alpha, \beta) \longmapsto \alpha\beta$ gives rise to a homomorphism $\Psi : S_1 \otimes_{R_v} S_2 \longrightarrow S$. Note that Ψ is one-one and onto because for an R_v-basis $\{\alpha_i \mid 1 \leq i \leq n_1\}$ of S_1 and an R_v-basis $\{\beta_j \mid 1 \leq j \leq n_2\}$ of S_2, the set $\{\Psi(\alpha_i \otimes \beta_j) \mid 1 \leq i \leq n_1, 1 \leq j \leq n_2\}$ is an R_v-basis of $S_1S_2 = S$ in view of the hypothesis K_1, K_2 linearly disjoint over K. Consequently we have an R_v^h-module isomorphism $\Lambda \circ (Id \otimes \Psi)$ of $R_v^h \otimes_{R_v} (S_1 \otimes_{R_v} S_2)$ onto $\prod_{k=1}^{t} R_{w_k}^h$. Also there is a natural isomorphism from $R_v^h \otimes_{R_v} S_1 \otimes_{R_v} S_2$ onto $(R_v^h \otimes_{R_v} S_1) \otimes_{R_v^h} (R_v^h \otimes_{R_v} S_2)$ mapping $a \otimes (\alpha \otimes \beta)$ to $(a \otimes \alpha) \otimes (1 \otimes \beta)$. Composing it with $\Lambda_1 \otimes \Lambda_2$ and identifying $\prod_{i=1}^{r} R_{w_{1i}}^h \otimes_{R_v^h} \prod_{j=1}^{s} R_{w_{2j}}^h$ with $\prod_{i=1}^{r}\prod_{j=1}^{s}(R_{w_{1i}}^h \otimes_{R_v^h} R_{w_{2j}}^h)$, we obtain an isomorphism Φ(say) from $R_v^h \otimes_{R_v} (S_1 \otimes_{R_v} S_2)$ with $\prod_{i=1}^{r}\prod_{j=1}^{s}(R_{w_{1i}}^h \otimes_{R_v^h} R_{w_{2j}}^h)$ which maps $a \otimes (\alpha \otimes \beta)$ to $(a\alpha \otimes \beta, a\alpha \otimes \beta, \cdots, a\alpha \otimes \beta)$. For a fixed pair $(i,j), 1 \leq i \leq r, 1 \leq j \leq s$, in view of Lemma 4.2.B and Theorem 4.1.3, there exists a unique valuation w_k of K_1K_2 which extends both w_{1i}, w_{2j}. Let $\Phi_{ij} : R_{w_{1i}}^h \otimes R_{w_{2j}}^h \longrightarrow R_{w_k}^h$ be the homomorphism as in the proof of Theorem 4.1.3. Now $(\prod_{i,j}\Phi_{ij}) \circ \Phi$ gives a homomorphism from $R_v^h \otimes_{R_v} (S_1 \otimes_{R_v} S_2)$ into $\prod\limits_{k=1}^{t} R_{w_k}^h$ which clearly agrees with the (onto) isomorphism $\Lambda \circ (Id \otimes \Psi)$. So $(\prod_{i,j}\Phi_{ij}) \circ \Phi$ is also an (onto) isomorphism. Since Φ is one-one and onto, we conclude that $\prod_{i,j}\Phi_{ij}$ is onto and hence so is each Φ_{ij}. Consequently $R_{w_{1i}}^h R_{w_{2j}}^h = \Phi_{ij}(R_{w_{1i}}^h \otimes R_{w_{2j}}^h)$ is the valuation ring $R_{w_k}^h$ and hence is integrally closed.

Step III. In this step, we show that at least one of $d(S_1/R_v)$, $d(S_2/R_v)$ is the unit ideal of R_v. Assume that $d(S_1/R_v)$ is not the unit ideal of R_v, then it is contained in the maximal ideal M_v of R_v. By Theorem 3.1.1, we have

$$d(S_1/R_v)R_v^h = \prod_{i=1}^{r} d(R_{w_{1i}}^h/R_v^h).$$

So $d(R_{w_{1i}}^h/R_v^h)$ is contained in the maximal ideal M_v^h of R_v^h for some i and hence $d(R_{w_{1i}}^h/R_v^h)$ is not the unit ideal of R_v^h. Keeping in mind that $K_{w_{1i}}^h$ and $K_{w_{2j}}^h$ are linearly disjoint over K^h in view of Remark 4.2.C and that the composite ring $R_{w_{1i}}^h R_{w_{2j}}^h$ is integrally closed by *Step II*, it now follows from *Step I* (applied to $K_{w_{1i}}^h$ and $K_{w_{2j}}^h$) that $d(R_{w_{2j}}^h/R_v^h)$ is unit ideal of R_v^h for each j, $1 \leq j \leq s$. As $d(S_2/R_v)R_v^h = \prod_{j=1}^{s} d(R_{w_{2j}}^h/R_v^h)$ by Theorem 3.1.1, we see that $d(S_2/R_v)$ is the unit ideal of R_v. This completes the proof of the theorem. □

Proof of Corollary 4.1.2. Fix a maximal ideal $\mathfrak{p}$ of A_K. We shall prove that if $\mathfrak{p}$ divides the relative discriminant $D(K_1/K)$ of K_1/K, then $\mathfrak{p}$ does not divide

$D(K_2/K)$. Let v denote the valuation of K corresponding to $\mathfrak{p}$ defined for any $\alpha \in A_K$ to be the highest power of $\mathfrak{p}$ dividing the ideal αA_K. Let S_1, S_2, S denote the integral closures of the valuation ring R_v of v in K_1, K_2, K_1K_2 respectively. Keeping in view the hypothesis $A_{K_1K_2} = A_{K_1}A_{K_2}$ and the fact that R_v is the localization of A_K at $\mathfrak{p}$, it can be easily seen that $S = S_1S_2$ and hence S_1S_2 is integrally closed. So in view of Theorem 4.1.1, $d(S_1/R_v)$ and $d(S_2/R_v)$ are coprime. Thus when the prime ideal $\mathfrak{p}$ of A_K divides the relative discriminant $D(K_1/K)$ which is the same as saying that the maximal ideal $\mathfrak{p}R_v$ of R_v divides $d(S_1/R_v)$, then $\mathfrak{p}R_v$ will not divide $d(S_2/R_v)$ and hence $\mathfrak{p}$ will not divide $D(K_2/K)$ as desired.

Chapter 5

On factorization of polynomials in henselian valued fields

5.1 History of the problem and statements of the results.

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring A_K of algebraic integers of K and $F(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. Hensel's lemma is a useful tool to give information about the factors of polynomials with integral coefficients over the ring $\mathbb{Z}_p$ of p-adic integers. With $F(x)$ as above, if $F(x) \equiv \phi_1(x)^{\nu_1} \cdots \phi_r(x)^{\nu_r}$ $(mod\ p)$ where $\phi_i(x)$ belonging to $\mathbb{Z}[x]$ are monic polynomials which are distinct as well as irreducible modulo p, then by Hensel's lemma, $F(x) = F_1(x) \cdots F_r(x)$ where $F_i(x)$ belonging to $\mathbb{Z}_p[x]$ is congruent to $\phi_i(x)^{\nu_i}$ modulo p. If p divides the index $[A_K : \mathbb{Z}[\theta]]$, then these polynomials $F_i(x)$ need not be irreducible over $\mathbb{Z}_p$. Ore described a method to determine a further factorization of $F_i(x)$ over $\mathbb{Z}_p$ using ϕ_i-Newton polygon of $F_i(x)$ (as defined in the paragraph preceding Definition 1.1.K). For simplicity of notation, fix one i; denote $\phi_i(x)$ by $\phi(x)$, its degree by m and $F_i(x)$ by $g(x)$. Ore proved that if the ϕ-Newton polygon of $g(x)$ has k sides $S_1, \cdots, S_k$, then $g(x) = g_1(x) \cdots g_k(x)$ where each $g_j(x) \in \mathbb{Z}_p[x]$ is a monic polynomial whose ϕ-Newton polygon consists of a single side which is a translate of S_j and $\deg(g_j(x)) = ml_j$, l_j being the length of horizontal projection of the side S_j. Corresponding to S_j, he associated a polynomial $G_{S_j}(y)$ in an indeterminate y over the finite field $\mathbb{F}_q, q = p^{\deg \phi}$ to the polynomial $g_j(x)$. The factorization of $G_{S_j}(y)$ in $\mathbb{F}_q[y]$ leads to a further factorization of $g_j(x)$ over $\mathbb{Z}_p$. Finally Ore showed that if each of these polynomials $G_{S_j}(y), 1 \leq j \leq k$, decomposes into n_j distinct monic irreducible factors over $\mathbb{F}_q$, then all the $\sum\limits_{j=1}^{k} n_j$ factors of $g(x)$ obtained in this way are irreducible over $\mathbb{Z}_p$ and their product equals $g(x)$.

In 2000, Cohen, Movahhedi and Salinier generalized Ore's method of factorization for polynomials with coefficients in complete discrete valued fields (see [C-M-S, Theorem 1.5]). In 2012, its scope was extended to complete valued fields of rank one (cf. [Kh-Ku3, Theorem 1.1]) and later in 2015, the analogues of Ore's results were proved for polynomials with coefficients in henselian valued fields of arbitrary rank (cf. [Jh-Kh1, Theorem 1.2]). All these generalizations of Ore's results for factorization are proved using ϕ-Newton polygons which later came to be known as Newton polygons of order one. In 2012, Guàrdia, Montes and Nart [G-M-N] introduced the notion of Newton polygons of higher order to extend the method of factorization of Ore in a different direction in the classical case when the polynomial $G_{S_j}(y)$ mentioned above has repeated irreducible factors over $\mathbb{F}_q$. In this thesis, we have extended the notion of Newton polygons of higher order to polynomials with coefficients in henselian valued fields of arbitrary rank (see Definition 1.1.K). We use k-th order Newton polygons to give a factorization for such polynomials for each $k \geq 1$. In fact the factorization for $k = 1$ in the classical case corresponds to the one given by Ore. At the end, we give examples to illustrate our main results (see Examples 5.4.1-5.4.3). These examples show that factorization of certain polynomials into irreducible factors can be obtained more quickly using first, second or third order Newton polygons with respect to residually transcendental prolongations than applying the method of factorization of Ore (in the generalized form) given in [Jh-Kh1] (cf. Remark 5.4.4). The main motivation behind this chapter is [G-M-N]; however our approach is different from [G-M-N] and involves residually transcendental prolongations of a given valuation V_0 of K to a simple transcendental extension $K(x)$ of K. For stating the major results of this chapter we need a few definitions and notations.

Let V_0 be a Krull valuation of a field K with value group G_0 and μ be an element of a totally ordered abelian group containing G_0 as an ordered subgroup. Then the function V_1 defined on the polynomial ring $K[x]$ by

$$V_1(\sum c_i x^i) = \min_i \{V_0(c_i) + i\mu\}$$

gives a valuation of $K(x)$ (cf. [En-Pr, Theorem 2.2.1]) and will be denoted by $V_1 = [V_0, V_1 x = \mu]$. As in [Mac], [Moy], it will be referred to as a first stage valuation of $K(x)$. In 1936, MacLane [Mac] described a method by which any valuation W of $K(x)$ can be augmented to yield another valuation of $K(x)$ by means of a key polynomial which is already introduced in Definition 1.1.I.

Let $\phi(x)$ be a key polynomial over a valuation W of $K(x)$ having value group G and $\mu > W(\phi(x))$ be an element of a totally ordered abelian group containing G as an ordered subgroup. Then the function V defined for any $f(x) \in K[x]$ having ϕ-expansion $\sum\limits_{i=0}^{n} f_i(x)\phi(x)^i$ with $\deg(f_i(x)) < \deg(\phi(x))$ by

$$V(f) = \min_i \{W(f_i(x)) + i\mu\}, \tag{5.1.1}$$

gives a valuation of $K(x)$ (cf. [Mac, Theorem 4.2], [Moy, p. 103]). The valuation V is called the augmented valuation over W associated with ϕ, μ and will be denoted by $V = [W, V\phi = \mu]$. With this notation, we now introduce the notion of k-th stage commensurable inductive valuation.

A k-th stage inductive valuation V_k is a valuation of $K(x)$ obtained by a finite sequence of valuations $V_1, V_2, \cdots, V_k$ of $K(x)$ where $V_1 = [V_0, V_1 x = \mu_1]$ is a first stage valuation obtained from a valuation V_0 of K and each $V_i = [V_{i-1}, V_i\phi_i = \mu_i]$ is obtained by augmenting V_{i-1} with the key polynomial $\phi_i(x)$ satisfying the following two conditions for $2 \leq i \leq k$:

(i) $\phi_1(x) = x$, $\deg(\phi_i(x)) \geq \deg(\phi_{i-1}(x))$;

(ii) $\phi_i(x)$ is not equivalent to $\phi_{i-1}(x)$ in V_{i-1}.

As in [Mac], the valuation V_k will be symbolized as $V_k = [V_0, V_1 x = \mu_1, V_2\phi_2 = \mu_2, \cdots, V_k\phi_k = \mu_k]$. The above valuation V_k with value group G_k is called commensurable if G_k/G_0 is a torsion group; G_0 being the value group of V_0. As shown in

Corollary 5.1.2, the residue field of a commensurable inductive valuation V_k is a transcendental extension of the residue field of V_0. It is known that (cf. [A-P-Z2, Theorem 2.2]) residually transcendental prolongations of V_0 to $K(x)$ are given by minimal pairs (see Definition 1.1.F). In what follows, we retain the notations as in Notation 1.1.E. and introduce some more which shall be used later.

Notation 5.1.A. Let V_0 be a henselian valuation of arbitrary rank of a field K. For a finite extension (K', V_0') of the valued field (K, V_0), the (henselian) defect to be denoted by $\mathrm{def}(K'/K)$ is defined to be $[K' : K]/e'f'$ where e', f' are the ramification index and the residual degree of V_0'/V_0.

The following theorem which plays a great role in the proof of the main result of this chapter relates minimal pairs with key polynomials.

Theorem 5.1.1. *Let (K, V_0), $G_0, \widetilde{G}_0$ be as in Notation 1.1.E. Let W be a valuation of $K(x)$ extending V_0 and $\phi(x)$ be a key polynomial over W. Let $V = [W, V\phi = \mu]$ with $\mu \in \widetilde{G}_0$ be an augmented valuation over W associated with ϕ, μ. Then V is a residually transcendental extension of V_0 to $K(x)$. Moreover there exists $\delta \in \widetilde{G}_0$ such that for any root α of $\phi(x)$, (α, δ) is a (K, V_0)-minimal pair and $V = w_{\alpha,\delta}$.*

The above theorem quickly yields the following corollary.

Corollary 5.1.2. *Let (K, V_0) be as in Notation 1.1.E and $V_k = [V_0, V_1 x = \mu_1, V_2\phi_2 = \mu_2, \cdots, V_k\phi_k = \mu_k]$ be a k-th stage commensurable inductive valuation. Then V_k is a residually transcendental extension of V_0 to $K(x)$. Moreover $V_k = w_{\alpha_k,\delta_k}$ where α_k is a root of ϕ_k with (α_k, δ_k) a (K, V_0)-minimal pair.*

The following corollary to be used in the sequel will be deduced from Theorem 5.1.1. It is of independent interest as well.

Corollary 5.1.3. *Let V_k be as in the above corollary with value group G_k. Let $\phi(x)$ be a key polynomial for an inductive valuation over V_k having a root α in $\widetilde{K}$, then $G_k = G(K(\alpha))$.*

With α as in Corollary 5.1.3, the following theorem gives the degree of the extension $\overline{K(\alpha)}/\overline{K}$ and quickly implies that the (henselian) defect of $K(\alpha)/K$ is 1.

Theorem 5.1.4. *Let $V_k, \phi(x), \alpha$ be as in Corollary 5.1.3. For $1 \leq j \leq k$, let $V_j = [V_0, V_1 x = \mu_1, V_2\phi_2 = \mu_2, \cdots, V_j\phi_j = \mu_j]$ stand for the j-th stage inductive valuation and τ_j be the smallest positive integer such that $\tau_j\mu_j$ belongs to the value group G_{j-1} of V_{j-1}. Then degree of the extension $\overline{K(\alpha)}/\overline{K}$ equals* $\deg(\phi(x))/\prod_{j=1}^{k}\tau_j$.

It is known that if $W = w_{\alpha',\delta'}$ is a residually transcendental prolongation of V_0 to $K(x)$ defined by a (K, V_0)-minimal pair (α', δ'), then the minimal polynomial of α' over K is a key polynomial over W (cf. [Po-Po, Corollary 4.3]). We shall avoid working with such trivial key polynomials and use nontrivial key polynomials (see Definition 1.1.I).

Remark 5.1.5. *It may be pointed out that in the particular case when V_k is as in Corollary* 5.1.2 *and $\phi(x)$ is a key polynomial for an inductive valuation over V_k, then $\phi(x)$ is a nontrivial key polynomial because in view of Corollary* 5.1.2, *we have $V_k = w_{\alpha_k,\delta_k}$ with α_k a root of $\phi_k(x)$ and $\phi(x)$ is not equivalent to $\phi_k(x)$ in V_k by the definition of inductive valuation.*

In this chapter, our main aim is to prove:

Theorem 5.1.6. *Let (K, V_0) be a henselian valued field of arbitrary rank with value group G_0, residue field $\overline{K}$ and $(\widetilde{K}, \widetilde{V_0})$ be as in Notation 1.1.E. Let W be a residually transcendental extension of V_0 to $K(x)$ and $\phi(x)$ be a nontrivial key polynomial of degree m over W having a root $\alpha \in \widetilde{K}$. Let $F(x)$ belonging to $K[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$, $A_s(x) = 1$. Suppose that the ϕ-Newton polygon of $F(x)$ with respect to W consists of r sides $S_1, \ldots, S_r$ having positive slopes $\lambda_1, \ldots, \lambda_r$. Then the following hold:*

(i) $F(x) = F_1(x) \cdots F_r(x)$, where each $F_i(x)$ belonging to $K[x]$ is a monic polynomial of degree ml_i whose ϕ-Newton polygon with respect to W has a single side which is a translate of S_i and l_i is the length of the horizontal projection of S_i.

(ii) If θ_i is a root of $F_i(x)$, then $\widetilde{V_0}(\phi(\theta_i)) = W(\phi(x)) + \lambda_i = \mu'_i$ (say) and $G(K(\alpha)) \subseteq G(K(\theta_i))$. The index $[G(K(\theta_i)) : G(K(\alpha))]$ is divisible by e_i, where e_i is the smallest positive integer such that $e_i\mu'_i \in G(K(\alpha))$. The degree $[\overline{K(\theta_i)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}]$.

(iii) $F_i(x)$ *is a lifting of a monic polynomial* $T_i(y) \in \overline{K(\alpha)}[y]$ *not divisible by* y *of degree* l_i/e_i *with respect to* $\phi(x), \mu_i'$.

(iv) If $U_{i1}(y)^{a_{i1}} \cdots U_{in_i}(y)^{a_{in_i}}$ *is the factorization of* $T_i(y)$ *into powers of distinct monic irreducible polynomials over* $\overline{K(\alpha)}$*, then* $F_i(x)$ *factors as* $F_{i1}(x) \cdots F_{in_i}(x)$ *over* K*, each* $F_{ij}(x)$ *is a lifting of* $U_{ij}(y)^{a_{ij}}$ *with respect to* $\phi(x), \mu_i'$ *with degree* $me_i a_{ij} \deg U_{ij}$ *and* $\widetilde{V}_0(\phi(\theta_{ij})) = \mu_i'$*. If some* $a_{ij} = 1$*, then* $F_{ij}(x)$ *is irreducible over* K *and for any root* θ_{ij} *of* $F_{ij}(x)$*, the index* $[G(K(\theta_{ij})) : G(K(\alpha))] = e_i$ *and the degree* $[\overline{K(\theta_{ij})} : \overline{K}] = \deg U_{ij}(y)[\overline{K(\alpha)} : \overline{K}]$ *in this case.*

It may be pointed out that Theorem 1.2 of [Jh-Kh1] is a special case of the above theorem because in view of Example 1.1.J a monic polynomial $\phi(x) \in R_0[x]$ with $\bar{\phi}(x)$ irreducible over $\overline{K}$ is a nontrivial key polynomial over the Gaussian prolongation V_0^x defined by (1.1.3) when $\bar{\phi}(x) \neq x$; in case $\bar{\phi}(x) = x$, then $\phi(x) = x - a$ (say) is a nontrivial key polynomial over the residually transcendental prolongation $w_{a+1,0}$ corresponding to the minimal pair $(a+1, 0)$.

Keeping in mind Corollary 5.1.3, Theorem 5.1.4 and Remark 5.1.5, the following theorem can be easily deduced from the above theorem. It generalizes Theorems 3.1, 3.7 of [G-M-N] which are proved for the polynomials with coefficients in finite extensions of the field of p-adic numbers. It also extends Corollary 3.8 of [G-M-N] in view of equation (5.3.7).

Theorem 5.1.7. *Let* (K, V_0) *be a henselian valued field of arbitrary rank with value group* G_0*, residue field* $\overline{K}$ *and* $(\widetilde{K}, \widetilde{V}_0)$ *be as in Notation 1.1.E. Let* $V_k, \phi(x), \alpha, \tau_j$ *be as in Theorem 5.1.4 and* G_k *denote the value group of* V_k*. Let* $F(x)$ *belonging to* $K[x]$ *be a monic polynomial not divisible by* $\phi(x)$ *with* ϕ*-expansion* $\sum_{i=0}^{s} A_i(x)\phi(x)^i$, $A_s(x) = 1$*. Suppose that the* ϕ*-Newton polygon of* $F(x)$ *with respect to* V_k *consists of* r *sides* $S_1, \dots, S_r$ *having positive slopes* $\lambda_1, \dots, \lambda_r$*. Then the following hold:*

(i) $F(x) = F_1(x) \cdots F_r(x)$*, where each* $F_i(x)$ *belonging to* $K[x]$ *is a monic polynomial of degree* $l_i(\deg(\phi(x))$ *whose* ϕ*-Newton polygon with respect to* V_k *has a single side which is a translate of* S_i *and* l_i *is the length of the horizontal projection of* S_i.

(ii) If θ_i *is a root of* $F_i(x)$*, then* $\widetilde{V}_0(\phi(\theta_i)) = V_k(\phi(x)) + \lambda_i$ *and* $G_k \subseteq G(K(\theta_i))$*. The*

index $[G(K(\theta_i)) : G_0]$ *is divisible by* $e_i \prod_{j=1}^{k} \tau_j$, *where* e_i *is the smallest positive integer such that* $e_i\lambda_i \in G_k$. *The degree* $[\overline{K(\theta_i)} : \overline{K}]$ *is divisible by* $[\overline{K(\alpha)} : \overline{K}] = \frac{\deg(\phi(x))}{\prod_{j=1}^{k}\tau_j}$.

(iii) $F_i(x)$ *is a lifting of a monic polynomial* $T_i(y) \in \overline{K(\alpha)}[y]$ *not divisible by* y *of degree* l_i/e_i *with respect to* $\phi(x), V_k(\phi(x)) + \lambda_i$.

(iv) If $U_{i1}(y)^{a_{i1}} \cdots U_{in_i}(y)^{a_{in_i}}$ *is the factorization of* $T_i(y)$ *into powers of distinct monic irreducible polynomials over* $\overline{K(\alpha)}$, *then* $F_i(x)$ *factors as* $F_{i1}(x) \cdots F_{in_i}(x)$ *over* K, *each* $F_{ij}(x)$ *is a lifting of* $U_{ij}(y)^{a_{ij}}$ *with respect to* $\phi(x), V_k(\phi(x)) + \lambda_i$ *with degree* $e_i a_{ij} \deg U_{ij} \deg \phi$ *and* $\widetilde{V}_0(\phi(\theta_{ij})) = V_k(\phi(x)) + \lambda_i$. *If some* $a_{ij} = 1$, *then* $F_{ij}(x)$ *is irreducible over* K *and for any root* θ_{ij} *of* $F_{ij}(x)$, *the index* $[G(K(\theta_{ij})) : G_0] = e_i\tau_1\tau_2\cdots\tau_k$ *and the degree* $[\overline{K(\theta_{ij})} : \overline{K}] = \frac{\deg(U_{ij}(y))\deg(\phi(x))}{\tau_1\tau_2\cdots\tau_k}$ *in this case.*

The following result which is already known in the particular case when W is the Gaussian prolongation V_0^x (cf. [Jh-Kh4, Theorem 1.5]), will be deduced from Theorem 5.1.6.

Corollary 5.1.8. *Let* $(K, V_0), \phi(x), m, W$ *and* α *be as in Theorem 5.1.6. Let* $F(x)$ *belonging to* $K[x]$ *be a polynomial having* ϕ*-expansion* $\sum_{i=0}^{s} A_i(x)\phi(x)^i$ *with* $A_s(x) = 1$, $A_i(x) \neq 0$ *for some* $i < s$ *and assume that all the sides in the* ϕ*-Newton polygon of* $F(x)$ *with respect to* W *have positive slopes. If* l *is the smallest non-negative integer for which* $\min_{0\le i\le s-1}\left\{\frac{W(A_i(x)\phi(x)^i) - W(\phi(x)^s)}{s-i}\right\} = \frac{W(A_l(x)\phi(x)^l) - W(\phi(x)^s)}{s-l}$ *and* $\frac{W(A_l(x))}{d}$ *does not belong to* $G(K(\alpha))$ *for any number* $d > 1$ *dividing* $s-l$, *then for any factorization* $G(x)H(x)$ *of* $F(x)$ *over* K, $\min\{\deg G(x), \deg H(x)\} \le lm$.

Note that in the special case when $W = V_0^x$ and $G_0 = \mathbb{Z}$, then it can be easily seen that for $A(x) \in K[x]$, the condition $V_0^x(A(x)) \notin dG_0$ for any number $d > 1$ dividing $s-k$ is equivalent to saying that $V_0^x(A(x))$ and $s-k$ are coprime. So the above corollary yields the following corollary which extends Schönemann Irreducibility Criterion (cf. [Rib, 3.1.D]).

Corollary 5.1.9. *Let* V_0 *be a valuation of a field* K *with value group* $\mathbb{Z}$. *Let* $\phi(x)$ *be a monic polynomial of degree* m *which is irreducible over* $\overline{K}$. *Let* $F(x)$

belonging to $K[x]$ *be a polynomial having* ϕ*-expansion* $\sum_{i=0}^{s} A_i(x)\phi(x)^i$ *with* $A_s(x) = 1$, $A_i(x) \neq 0$ *for some* $i < s$. *Let* l *be the smallest non-negative integer such that* $\min_{0 \le i \le s-1} \left\{ \frac{V_0^x(A_i(x))}{s-i} \right\} = \frac{V_0^x(A_l(x))}{s-l} > 0$ *and* $V_0^x(A_l(x))$, $s-l$ *are coprime, then for any factorization* $F(x) = G(x)H(x)$ *of* $F(x)$ *over* K, *one has*

$$\min\{\deg G(x), \deg H(x)\} \le lm.$$

5.2 Proof of Theorem 5.1.1, Corollary 5.1.3.

Proof of Theorem 5.1.1. Let t be a positive integer such that $t\mu \in G_0$, say $t\mu = V_0(a), a \in K$. Then the V-residue of $\phi(x)^t/a$ is transcendental over the residue field of V_0, for otherwise there exist $a_0, a_1, \cdots, a_n$ in the valuation ring R_0 of V_0 with a_n a unit in R_0 such that $V\big(\sum_{i=0}^{n} a_i \big(\frac{\phi(x)^t}{a}\big)^i\big) > 0$, which is impossible because by definition of V, we have

$$V\left(\sum_{i=0}^{n} a_i \left(\frac{\phi(x)^t}{a}\right)^i\right) = \min_{0 \le i \le n} \{V_0\left(\frac{a_i}{a^i}\right) + it\mu\} = \min_{0 \le i \le n} \{V_0(a_i)\} = 0.$$

This proves that V is a residually transcendental prolongation of V_0 to $K(x)$. So by Theorem 2.1 of [K-P-R], there exists a (K, V_0)-minimal pair $(\beta, \delta) \in \widetilde{K} \times \widetilde{G}_0$ such that $V = w_{\beta,\delta}$.

We claim that there exists a root α of $\phi(x)$ such that $\widetilde{V}_0(\alpha - \beta) \ge \delta$. Suppose to the contrary, the claim is false. Then for each root α_i of $\phi(x)$, we have

$$\widetilde{V}_0(\alpha_i - \beta) < \delta. \tag{5.2.1}$$

On writing $\phi(x)/\phi(\beta)$ as $\prod_i (1 + \frac{x-\beta}{\beta-\alpha_i})$ and using (5.2.1), we see that the $\widetilde{w}_{\beta,\delta}$-residue of $\phi(x)/\phi(\beta)$ equals 1 and hence the $w_{\beta,\delta}$-residue, i.e., the V-residue of $\phi(x)^t/a$ will be same as the $\widetilde{w}_{\beta,\delta}$-residue of $\phi(\beta)^t/a$, which is impossible because as shown above the former is transcendental over the residue field of V_0, whereas the latter is not so. This contradiction proves the claim.

It is immediate from the claim and the definition of minimal pair that $[K(\beta) : K] \le [K(\alpha) : K] = \deg(\phi(x)) = m$ (*say*). Now we prove that

$$[K(\beta) : K] = m. \tag{5.2.2}$$

Suppose that (5.2.2) is false. Let $G(x)$ be the minimal polynomial of β over K. By the division algorithm, write $\phi(x) = q(x)G(x) - A(x)$, with $\deg(A(x)) < \deg(G(x)) < m$, so that

$$q(x)G(x) = \phi(x) + A(x) \tag{5.2.3}$$

is the ϕ-expansion of $q(x)G(x)$. Keeping in mind that both $q(x), G(x)$ are of degree less than m and using formula (5.1.1), we see that

$$W(q(x)G(x)) = V(q(x)G(x)) = \min\{V(\phi(x)), W(A(x))\}.$$

Thus we have $W(A(x)) \geq W(q(x)G(x))$. Indeed $W(A(x)) = W(q(x)G(x))$, for otherwise $W(A(x)) = W(q(x)G(x)-\phi(x)) > W(q(x)G(x))$ which would imply that $\phi(x)$ is not equivalence irreducible in W, contradicting that $\phi(x)$ is a key polynomial over W. It now follows from (5.2.3) and the triangle law that $W(\phi(x)) \geq W(A(x))$. Keeping in mind that $V = w_{\beta,\delta}$ is an augmented valuation associated with ϕ, μ and using Theorem 1.1.$G(ii)$, the last inequality can be rewritten as

$$\widetilde{V}_0(A(\beta)) = w_{\beta,\delta}(A(x)) = V(A(x)) = W(A(x)) \leq W(\phi(x)) < V(\phi(x)) = \mu. \tag{5.2.4}$$

Substituting $x = \beta$ in (5.2.3), we obtain $\phi(\beta) = -A(\beta)$ as $G(\beta) = 0$. So it follows from (5.2.4) that $\widetilde{V}_0(\phi(\beta)) < \mu$; this is impossible because if $\phi(x) = \prod\limits_{i=1}^{m}(x - \alpha_i)$, then using (1.1.4), we have

$$\mu = w_{\beta,\delta}(\phi(x)) = \sum_{i=1}^{m} \widetilde{w}_{\beta,\delta}(x-\alpha_i) = \sum_{i=1}^{m} \min(\delta, \widetilde{V}_0(\beta-\alpha_i)) \leq \sum_{i=1}^{m} \widetilde{V}_0(\beta-\alpha_i) = \widetilde{V}_0(\phi(\beta)).$$

This contradiction proves (5.2.2).

Now we show that (α, δ) is a (K, V_0)-minimal pair, where α is a root of $\phi(x)$ with $\widetilde{V}_0(\alpha-\beta) \geq \delta$. Let γ be an element of $\widetilde{K}$ with $[K(\gamma) : K] < [K(\beta) : K]$. Since (β, δ) is a (K, V_0)-minimal pair and $[K(\beta) : K] = m$ by (5.2.2), we have $\widetilde{V}_0(\beta - \gamma) < \delta$; consequently by strong triangle law $\widetilde{V}_0(\alpha - \gamma) = \min\{\widetilde{V}_0(\alpha - \beta), \widetilde{V}_0(\beta - \gamma)\} = \widetilde{V}_0(\beta - \gamma) < \delta$, which proves that (α, δ) is a (K, V_0)-minimal pair. Since (K, V_0) is henselian, it can be easily seen that for any root α' of $\phi(x)$, (α', δ) is a (K, V_0)-minimal pair; further $V = w_{\beta,\delta} = w_{\alpha,\delta} = w_{\alpha',\delta}$ by virtue of Theorem 2.1 of [K-P-R].

Proof of Corollary 5.1.3. Fix an element $\mu > V_k(\phi(x))$ in the divisible closure $\widetilde{G}_0$

of G_0. Let V denote the augmented valuation $V = [V_k, V\phi = \mu]$. By Theorem 5.1.1, there exists $\delta \in \widetilde{G}_0$ such that (α, δ) is a (K, V_0)-minimal pair and $V = w_{\alpha,\delta}$. Note that for any polynomial $A(x) \in K[x]$ with $\deg(A(x)) < \deg(\phi(x)) = m$ (say), in view of Theorem 1.1.$G(ii)$, we have

$$\widetilde{V}_0(A(\alpha)) = w_{\alpha,\delta}(A(x)) = V(A(x)) = V_k(A(x)); \tag{5.2.5}$$

consequently $G(K(\alpha)) \subseteq G_k$. To prove that $G_k \subseteq G(K(\alpha))$, it is enough to show that $V_k(\phi_k(x)) = \mu_k$ (say) belongs to $G(K(\alpha))$, because for any polynomial $g(x) \in K[x]$ with ϕ_k-expansion $\sum_i g_i(x)\phi_k(x)^i$, on using (5.2.5) and the fact that $\deg(\phi_k(x)) \leq m$ by definition of inductive valuation, we have

$$V_k(g(x)) = \min_i\{V_k(g_i(x)) + i\mu_k\} = \min_i\{\widetilde{V}_0(g_i(\alpha)) + i\mu_k\}.$$

If $\deg(\phi_k(x)) < m$, then again in view of (5.2.5), $\mu_k = V_k(\phi_k(x)) = \widetilde{V}_0(\phi_k(\alpha)) \in G(K(\alpha))$. So assume that $\deg(\phi_k(x)) = m$. In this situation, $\phi(x)$ has ϕ_k-expansion $\phi(x) = \phi_k(x) + r(x)$. By hypothesis $\phi(x)$ is a key polynomial for an inductive valuation over V_k and hence $\phi(x)$ is not equivalent to $\phi_k(x)$ in V_k, i.e., $V_k(\phi(x) - \phi_k(x)) \leq V_k(\phi_k(x))$. Indeed $V_k(r(x)) = V_k(\phi_k(x))$, for otherwise $V_k(r(x)) < V_k(\phi_k(x)) = V_k(\phi(x) - r(x))$ which implies that $\phi(x)$ is equivalent to $r(x)$ in V_k; this is impossible because $\phi(x)$ is a key polynomial over V_k and $\deg(r(x)) < m$. Therefore by virtue of (5.2.5), we see that $V_k(\phi_k(x)) = V_k(r(x)) = \widetilde{V}_0(r(\alpha))$ belongs to $G(K(\alpha))$.

5.3 Preliminary results and Proof of Theorem 5.1.4.

In this section, we first prove three preliminary results viz. Theorems 5.3.1-5.3.3 which play a crucial role for the proof of Theorem 5.1.6 and are of independent interest as well. We use Theorem 5.3.1 in the proof of Theorem 5.1.4 which is also proved in this section. At the end of this section, we prove some lemmas needed for the proof of the main theorem. Throughout this section (K, V_0), (α, δ), $f(x)$, $w_{\alpha,\delta}$, μ are as in Theorem 1.1.G. For a non-zero polynomial $F(x)$ belonging to $K[x]$ with f-expansion $\sum\limits_i A_i(x)f(x)^i$, we shall denote by $I_{\alpha,\delta}(F(x))$, $S_{\alpha,\delta}(F(x))$ respectively the minimum and the maximum integers belonging to the set $\{i \mid w_{\alpha,\delta}(F(x)) = \widetilde{V}_0(A_i(\alpha))+i\mu\}$. It is known that for any non-zero polynomials $F(x), G(x)$ belonging to $K[x]$, one has (cf. [Kh-Ku2, Lemma 2.1])

$$I_{\alpha,\delta}(FG) = I_{\alpha,\delta}(F) + I_{\alpha,\delta}(G); \quad S_{\alpha,\delta}(FG) = S_{\alpha,\delta}(F) + S_{\alpha,\delta}(G). \tag{5.3.1}$$

With 'def' as introduced in Notation 5.1.A, we now prove

Theorem 5.3.1. *Let (K, V_0), $(\alpha, \delta), f(x), m, w_{\alpha,\delta}$, μ, e are as in Theorem 1.1.G and $F(x) \in K[x]$ be a lifting of a monic polynomial $T(y)$ not divisible by y of degree $t > 0$ belonging to $\overline{K(\alpha)}[y]$ with respect to (α, δ). Let θ be any root of $F(x)$. Then the following hold :*
(i) $G(K(\alpha)) \subseteq G(K(\theta))$ and the degree $[\overline{K(\alpha)} : \overline{K}]$ divides $[\overline{K(\theta)} : \overline{K}]$;
(ii) $\mathrm{def}(K(\alpha)/K)$ *divides* $\mathrm{def}(K(\theta)/K)$*;*
(iii) In the particular case when $T(y)$ is irreducible over $\overline{K(\alpha)}$, then $F(x)$ is irreducible over K, $[G(K(\theta)) : G(K(\alpha))] = e$ and $[\overline{K(\theta)} : \overline{K}] = t[\overline{K(\alpha)} : \overline{K}]$.

The theorems stated below are already known (see [Jh-Kh1, Theorem 2.B] for Theorem 5.3.A and [Kh-Sa, Theorem 1.1] for Theorem 5.3.B); these will be used in the proof of the above theorem.

Theorem 5.3.A. *Let $(K, V_0), (\alpha, \delta), f(x), m, \mu, F(x), T(y), e$ and t be as in the above theorem and $h(x)$ be as in Theorem 1.1.G(iii). Then (i) $\widetilde{V}_0(\theta - \alpha) \leq \delta$ for each root θ of $F(x)$. (ii) Given any root θ of $F(x)$, there exists a K-conjugate θ' of θ such that $\widetilde{V}_0(\theta' - \alpha) = \delta$ and $\widetilde{V}_0(f(\theta')) = \widetilde{V}_0(f(\theta)) = \mu$. (iii)* If θ' is as in *(ii)*, then the $\widetilde{V}_0$- residue of $f(\theta')^e/h(\alpha)$ is a root of $T(y)$.
Theorem 5.3.B. Let $(K, V_0), (\widetilde{K}, \widetilde{V}_0)$ be as in Notation 1.1.E. Let α, θ belonging to $\widetilde{K}$ be such that $\widetilde{V}_0(\alpha - \theta) > \widetilde{V}_0(\alpha - \beta)$ for every $\beta \in \widetilde{K}$ satisfying $[K(\beta) : K] < [K(\alpha) : K]$. Then $G(K(\alpha)) \subseteq G(K(\theta))$, $\overline{K(\alpha)} \subseteq \overline{K(\theta)}$ and $\mathrm{def}(K(\alpha)/K)$ divides $\mathrm{def}(K(\theta)/K)$.
Proof of the Theorem 5.3.1. By Theorem 5.3.A(ii), there exists a K-conjugate θ' of θ such that $\widetilde{V}_0(\theta' - \alpha) = \delta$. Since (α, δ) is a (K, V_0)-minimal pair, in view of Definition 1.1.F we have $\widetilde{V}_0(\alpha - \beta) < \delta = \widetilde{V}_0(\theta' - \alpha)$ for every $\beta \in \widetilde{K}$ satisfying

$[K(\beta) : K] < [K(\alpha) : K]$. Therefore it follows from Theorem 5.3.B and the henselian property of (K, V_0) that $G(K(\alpha)) \subseteq G(K(\theta')) = G(K(\theta))$, $\overline{K(\alpha)} \subseteq \overline{K(\theta')}$ and $\text{def}(K(\alpha)/K)$ divides $\text{def}(K(\theta')/K) = \text{def}(K(\theta)/K)$. It only remains to prove the last assertion of the theorem. Assume that $T(y)$ is irreducible over $\overline{K(\alpha)}$. We have

$$etm = \deg(F(x)) \geq [K(\theta) : K] = [\overline{K(\theta')} : \overline{K}][G(K(\theta)) : G_0]\text{def}(K(\theta)/K).$$

As $\text{def}(K(\alpha)/K)$ divides $\text{def}(K(\theta)/K)$ and $\overline{K(\alpha)} \subseteq \overline{K(\theta')}$, the above inequality implies

$$etm \geq [K(\theta) : K] \geq [\overline{K(\theta')} : \overline{K(\alpha)}][G(K(\theta)) : G(K(\alpha))][K(\alpha) : K]. \qquad (5.3.2)$$

Recall that $[K(\alpha) : K] = m$ and by Theorem 5.3.A(ii), $\mu = \widetilde{V}_0(f(\theta)) \in G(K(\theta))$; hence e divides $[G(K(\theta)) : G(K(\alpha))]$. Further keeping in mind Theorem 5.3.A(iii) and the fact that $T(y)$ is irreducible over $\overline{K(\alpha)}$, we see that the degree of the extension $\overline{K(\theta')}/\overline{K(\alpha)}$ is at least t. It now follows that (5.3.2) is possible only when $[K(\theta) : K] = etm$, $[G(K(\theta)) : G(K(\alpha))] = e$ and $[\overline{K(\theta')} : \overline{K(\alpha)}] = t$, which completes the proof of the theorem.

Now we prove the following theorem to be used in the proof of Theorem 5.3.3.

Theorem 5.3.2. *Let $\phi(x)$ be a nontrivial key polynomial of degree m over a residually transcendental extension W of V_0 to $K(x)$. Let $F(x) \in K[x]$ be a monic polynomial of degree sm which is equivalent to $\phi(x)^s$ in W. Then each factor of $F(x)$ over K has degree a multiple of m.*

The two theorems stated below will be used in the proof of the above theorem. Theorem 5.3.C is proved in [Jh-Kh1, Corollary 2.2]. Theorem 5.3.D is essentially proved in [Po-Po, Theorem 4.6]; for reader's convenience, we sketch the proof of the latter.

Theorem 5.3.C. Let $F(x)$ belonging to $K[x]$ be a monic polynomial which is a lifting of a monic polynomial $T(y)$ not divisible by y belonging to $\overline{K(\alpha)}[y]$ with respect to a (K, V_0)-minimal pair (α, δ). Then any monic polynomial $G(x) \in K[x]$

dividing $F(x)$ is a lifting of a monic polynomial dividing $T(y)$ with respect to (α, δ).

Theorem 5.3.D. If $\phi(x)$ is a key polynomial over a residually transcendental prolongation w_{α_1,δ_1} of V_0 to $K(x)$ with (α_1, δ_1) a (K, V_0)-minimal pair such that $\phi(x)$ is not equivalent to the minimal polynomial of α_1 over K, then $\phi(x)$ is a lifting of an irreducible polynomial $\psi(y) \neq y$ belonging to $\overline{K(\alpha_1)}[y]$ with respect to (α_1, δ_1).

Proof of Theorem 5.3.D. Let n_1 denote the degree of the minimal polynomial $f_1(x)$ of α_1 over K and W the valuation w_{α_1,δ_1}. In view of Proposition 4.1 of [Po-Po], $\deg(\phi(x)) \geq n_1$. When $\deg(\phi(x)) > n_1$, then by Theorem 4.6 of [Po-Po], $\phi(x)$ is a lifting of an irreducible polynomial $\psi(y) \neq y$ belonging to $\overline{K(\alpha_1)}[y]$ with respect to (α_1, δ_1). So we need to prove the theorem when $\deg(\phi(x)) = n_1 = \deg(f_1(x))$. In this case write $\phi(x) = f_1(x) + r_0(x)$, $\deg(r_0(x)) < n_1$. In view of Theorem 1.1.G, we have

$$W(\phi(x)) = \min\{W(f_1(x)), W(r_0(x))\}. \tag{5.3.3}$$

As $\phi(x)$ is not equivalent to $f_1(x)$ in W, we see that $W(r_0(x)) = W(\phi(x) - f_1(x)) \leq W(f_1(x))$. It now follows from (5.3.3) that $W(\phi(x)) = W(r_0(x))$. We show that $W(\phi(x)) = W(f_1(x))$. By virtue of (5.3.3), we have $W(f_1(x)) \geq W(\phi(x))$. If $W(f_1(x)) > W(\phi(x))$, then $W(f_1(x)) = W(\phi(x) - r_0(x)) > W(\phi(x))$, which is impossible because $\phi(x)$ is key polynomial over W and $\deg(r_0(x)) < \deg(\phi(x))$. Therefore we have $W(\phi(x)) = W(f_1(x)) = W(r_0(x))$ which immediately implies that $\phi(x)$ is a lifting of the linear polynomial $y + \bar{1}$ with respect to (α_1, δ_1) on taking $h(x) = r_0(x)$. This completes the proof of the theorem.

The converse of Theorem 5.3.D stated below as Theorem 5.3.E is proved in [Po-Po, Theorem 4.6]. It will be used to construct examples.

Theorem 5.3.E. Let w_{α_1,δ_1} be a residually transcendental prolongation of V_0 to $K(x)$ with (α_1, δ_1) a (K, V_0)-minimal pair. If $\phi(x) \in K[x]$ is a monic polynomial which is a lifting of an irreducible polynomial $\psi(y) \neq y$ belonging to $\overline{K(\alpha_1)}[y]$ with respect to (α_1, δ_1) such that $deg(\phi(x))$ is strictly greater than the degree of the minimal polynomial of α_1 over K, then $\phi(x)$ is a key polynomial over w_{α_1,δ_1}.

Proof of Theorem 5.3.2. Let $g(x)$ be a monic polynomial in $K[x]$ dividing $F(x)$. Since $\phi(x)$ is a nontrivial key polynomial over W, there exists a (K, V_0)-minimal pair (α_1, δ_1) such that $W = w_{\alpha_1,\delta_1}$ where $f_1(x)$ is the minimal polynomial of α_1 over K of degree n_1 (say) and $\phi(x)$ is not equivalent to $f_1(x)$ in W. By Theorem 5.3.D, $\phi(x)$ is a lifting of an irreducible polynomial $\psi(y) \in \overline{K(\alpha_1)}[y]$ different from y with respect to (α_1, δ_1). As $F(x)$ is equivalent to $\phi(x)^s$ in W, it follows that $F(x)$ is a lifting of $\psi(y)^s$ with respect to (α_1, δ_1). By Theorem 5.3.C, $g(x)$ is a lifting of $\psi(y)^d$ with respect to (α_1, δ_1) for some $d \leq s$. If e_1 denotes the smallest positive integer such that $e_1 w_{\alpha_1,\delta_1}(f_1(x)) \in G(K(\alpha_1))$, then in view of Definition 1.1.H of lifting, $\deg(g(x)) = de_1n_1(\deg(\psi(y)) = d\deg(\phi(x))$ as desired.

The following theorem which we now prove for all residually transcendental prolongations W is proved in [Jh-Kh1, Theorem 3.1] in the particular case when W is V_0^x defined by (1.1.3).

Theorem 5.3.3. *Let $\phi(x)$ be a nontrivial key polynomial of degree m over a residually transcendental extension W of V_0 to $K(x)$ having a root $\alpha \in \widetilde{K}$. Let $V = [W, V\phi = \lambda + W\phi]$ be the augmented valuation over W associated with $\phi, \mu = \lambda + W\phi$ and (α, δ) be a (K, V_0)-minimal pair such that $V = w_{\alpha,\delta}$. Let e be the smallest positive integer such that $e\mu \in G(K(\alpha))$ and $F(x)$ belonging to $K[x]$ be a monic polynomial of degree sm which is equivalent to $\phi(x)^s$ in W. If $I_{\alpha,\delta}(F) = 0$ and $S_{\alpha,\delta}(F) = l > 0$, then $F(x)$ has a monic factor $G(x) \in K[x]$ of degree lm such that $S_{\alpha,\delta}(G) = l$. Further $G(x)$ is a lifting of a monic polynomial of degree l/e not divisible by y belonging to $\overline{K(\alpha)}[y]$ with respect to (α, δ).*

The following two already known lemmas will be used in the proof of the above theorem (see [Jh-Kh1, Lemma 2.3] for Lemma 5.3.F and [Kha, Lemma 2.3] for Lemma 5.3.G).

Lemma 5.3.F. *Let $(K, V_0), (\alpha, \delta), f(x), \mu$ be as in Theorem 1.1.G. If $g(x) \in K[x]$ is a monic polynomial for which $I_{\alpha,\delta}(g) = 0$ and $S_{\alpha,\delta}(g)$ is positive, then $\widetilde{V}_0(\theta - \alpha) \leq \delta$ for each root θ of $g(x)$; there exists a root θ' of $g(x)$ with $\widetilde{V}_0(\theta' - \alpha) = \delta$ and $\widetilde{V}_0(f(\theta')) = \mu$ for such a root θ'.*

Lemma 5.3.G. *Let $g(x)$ and $g_1(x)$ be two monic irreducible polynomials over a henselian valued field (K, V_0) of degrees n, n_1 respectively such that $g(\beta) = g_1(\beta_1) = 0$ for some $\beta, \beta_1 \in \widetilde{K}$. Then $n_1\widetilde{V}_0(g(\beta_1)) = n\widetilde{V}_0(g_1(\beta))$.*

Proof of Theorem 5.3.3. Let $g_1(x), \cdots, g_r(x)$ be all the monic irreducible factors of $F(x)$ over K, counted with multiplicity (if any) for which $S_{\alpha,\delta}(g_i) > 0$, say $S_{\alpha,\delta}(g_i) = l_i$. Set $G(x) = \prod_{i=1}^{r} g_i(x)$. By (5.3.1), $S_{\alpha,\delta}(G) = \sum_{i=1}^{r} l_i = l$. Let $g_i(x) = \sum_{j=0}^{d_i} g_{ij}(x)\phi(x)^j$ be the ϕ-expansion of $g_i(x)$ with $g_{id_i}(x) \neq 0$. Then in view of Theorem 5.3.2, the degree of $g_i(x)$ is a multiple of m and hence $\deg(g_i(x)) = d_i m$. Clearly the first assertion of the theorem is proved once we show that

$$d_i = l_i, \quad 1 \leq i \leq r. \tag{5.3.4}$$

Since $I_{\alpha,\delta}(F) = 0$, we have $I_{\alpha,\delta}(g_i) = 0$. Also $S_{\alpha,\delta}(g_i) > 0$. Applying Lemma 5.3.F, there exists a root θ_i of $g_i(x)$ such that $\widetilde{V}_0(\phi(\theta_i)) = \mu$. By Lemma 5.3.G, $\widetilde{V}_0(g_i(\alpha)) = d_i\widetilde{V}_0(\phi(\theta_i)) = d_i\mu$. Therefore keeping in mind that $I_{\alpha,\delta}(g_i) = 0$, we see that

$$w_{\alpha,\delta}(g_i(x)) = w_{\alpha,\delta}(g_{i0}(x)) = \widetilde{V}_0(g_{i0}(\alpha)) = \widetilde{V}_0(g_i(\alpha)) = d_i\mu,$$

which shows that $S_{\alpha,\delta}(g_i) = d_i$ and (5.3.4) is proved. Keeping in view the above equation, we see that $d_i\mu \in G(K(\alpha))$. So $d_i = l_i$ is divisible by e and hence $g_i(x)$ is a lifting of a monic polynomial not divisible by y of degree l_i/e belonging to $\overline{K(\alpha)}[y]$ with respect to (α, δ) which implies that $G(x) = \prod_{i=1}^{r} g_i(x)$ is a lifting of a polynomial of degree l/e.

The following generalized version of Hensel's lemma proved in [Jh-Kh1, Theorem 1.1] will be used in the proof of Theorem 5.1.6.

Theorem 5.3.H. *Let (K, V_0) be a henselian valued field of arbitrary rank. Let (α, δ) be a (K, V_0)-minimal pair and $h(x) \in K[x]$ be as in Theorem 1.1.G(iii). If a monic polynomial $F(x) \in K[x]$ is a lifting of a product of two coprime polynomials $U_1(y), U_2(y)$ belonging to $\overline{K(\alpha)}[y]$ with respect to (α, δ) and $h(x)$, then there exist* *monic polynomials $F_1(x), F_2(x)$ in $K[x]$ such that $F(x) = F_1(x)F_2(x)$ and $F_i(x)$ is a lifting of $U_i(y)$ with respect to $(\alpha, \delta), h(x)$.*

Using Theorems 5.3.D and 5.3.1, we now prove Theorem 5.1.4 :

Proof of Theorem 5.1.4. Denote $\phi(x)$ by $\phi_{k+1}(x)$ and α by α_{k+1}. By Corollary 5.1.2, $V_j = w_{\alpha_j,\delta_j}$ where α_j is a root of $\phi_j(x)$ with (α_j, δ_j) a (K, V_0)-minimal pair. In view of Corollary 5.1.3, the value group G_j of V_j equals $G(K(\alpha_{j+1}))$. So τ_j is the smallest positive integer such that $\tau_j w_{\alpha_j,\delta_j}(\phi_j(x)) = \tau_j V_j(\phi_j(x)) = \tau_j \mu_j$ belongs to $G_{j-1} = G(K(\alpha_j))$. Since $\phi_{j+1}(x)$ is a lifting of an irreducible polynomial $\psi_j(y)$ belonging to $\overline{K(\alpha_j)}[y]$ of degree t_j (say) with respect to (α_j, δ_j) in view of Theorem 5.3.D, it now follows from Definition 1.1.H that

$$\deg(\phi_{j+1}(x)) = \tau_j t_j \deg(\phi_j(x)). \tag{5.3.5}$$

Applying the last assertion of Theorem 5.3.1 to the polynomial $\phi_{j+1}(x)$, we obtain

$$[\overline{K(\alpha_{j+1})} : \overline{K}] = t_j[\overline{K(\alpha_j)} : \overline{K}]. \tag{5.3.6}$$

Keeping in mind that $\alpha = \alpha_{k+1}$, $\alpha_1 = 0$ and using (5.3.6) for $1 \leq j \leq k$, we see that

$$[\overline{K(\alpha)} : \overline{K}] = [\overline{K(\alpha_{k+1})} : \overline{K}] = \prod_{j=1}^{k} t_j. \tag{5.3.7}$$

The desired equality is obtained on substituting for t_j from (5.3.5) in (5.3.7).

In what follows in this section, W is a residually transcendental prolongation of V_0 to $K(x)$, $\phi(x)$ is a key polynomial over W and the ϕ-Newton polygon of any polynomial is taken with respect to W. With notations as in Notation 1.1.E, the following lemmas establish the close analogy between the concept of ϕ-Newton polygon with respect to W and the phenomenon of lifting with respect to minimal pairs corresponding to an augmented valuation over W.

Lemma 5.3.4. *Let (K, V_0) be a henselian valued field of arbitrary rank. Let W be a residually transcendental prolongation of V_0 to $K(x)$ and $\phi(x)$ be a key polynomial over W having a root $\alpha \in \widetilde{K}$. Let $V = [W, V\phi = \mu]$ be the augmented valuation of*

W with $\mu \in \widetilde{G}_0$ and (α, δ) be a (K, V_0)-minimal pair such that $V = w_{\alpha,\delta}$. Let e be the smallest positive integer such that $e\mu$ belongs to $G(K(\alpha))$ and $\lambda = \mu - W(\phi(x))$. If $F(x) \in K[x]$ is a lifting with respect to (α, δ) of a monic polynomial $T(y)$ belonging to $\overline{K(\alpha)}[y]$ not divisible by y having degree t, then the ϕ-Newton polygon of $F(x)$ with respect to W consists of a single side which has slope λ and the length of its horizontal projection is et.

Proof. Note that if a polynomial $A(x) \in K[x]$ has degree strictly less than $\deg(\phi(x))$, then keeping in mind Theorem 1.1.G(ii), (5.1.1) and the fact that $V = w_{\alpha,\delta}$, one has

$$\widetilde{V}_0(A(\alpha)) = w_{\alpha,\delta}(A(x)) = V(A(x)) = W(A(x)). \tag{5.3.8}$$

Let $F(x) = \phi(x)^s + A_{s-1}(x)\phi(x)^{s-1} + \cdots + A_0(x)$ be the ϕ-expansion of $F(x)$. Since $F(x)$ is a lifting of $T(y)$ of degree t not divisible by y, in view of Definition 1.1.H of lifting, we have $s = et$ and $w_{\alpha,\delta}(F(x)) = s\mu = \widetilde{V}_0(A_0(\alpha))$. Using (5.3.8), we see that $w_{\alpha,\delta}(F(x)) = \min_i\{W(A_i(x)) + i\mu\} = s\mu = W(A_0(x))$. Substituting $\mu = \lambda + W(\phi(x))$ in the last equation, it follows that

$$\frac{W(A_i(x)\phi(x)^i) - W(\phi(x)^s)}{s-i} \geq \lambda = \frac{W(A_0(x)) - W(\phi(x)^s)}{s},$$

for $1 \leq i \leq s-1$, which shows that the ϕ-Newton polygon of $F(x)$ (with respect to W) has a single side whose slope is λ and the length of its horizontal projection is $s = et$.

The next result is the converse of the above lemma.

Lemma 5.3.5. *Let $(K, V_0), W, \phi(x)$ and α be as in above lemma. Assume that the ϕ-Newton polygon with respect to W of a polynomial $F(x) \in K[x]$ not divisible by $\phi(x)$ having ϕ-expansion $\phi(x)^s + A_{s-1}(x)\phi(x)^{s-1} + \cdots + A_0(x)$ consists of a single side with slope $\lambda > 0$. Let $V = [W, V\phi = \lambda + W\phi]$ be the augmented valuation over W associated with $\phi, \mu = \lambda + W\phi$ and (α, δ) be a (K, V_0)-minimal pair such that $V = w_{\alpha,\delta}$. Let e be the smallest positive integer such that $e\mu \in G(K(\alpha))$. Then s/e is an integer and $F(x)$ is a lifting of a monic polynomial $T(y)$ not divisible by y of degree s/e belonging to $\overline{K(\alpha)}[y]$ with respect to (α, δ).*

Proof. In view of the hypothesis regarding the ϕ-Newton polygon of $F(x)$, we have

$$\frac{W(A_i(x)\phi(x)^i) - W(\phi(x)^s)}{s-i} \geq \lambda = \frac{W(A_0(x)) - W(\phi(x)^s)}{s},$$

for $1 \leq i \leq s-1$, i.e., $W(A_i(x)\phi(x)^i) + i\lambda \geq s(W(\phi(x)) + \lambda) = W(A_0(x))$ which shows that $V(F(x)) = \min_i \{W(A_i(x)) + i\mu\} = W(A_0(x)) = s\mu$. Keeping in mind that $V = w_{\alpha,\delta}$ and $W(A_i(x)) = \widetilde{V}_0(A_i(\alpha))$, we see that

$$w_{\alpha,\delta}(F(x)) = \min_i \{\widetilde{V}_0(A_i(\alpha)) + i\mu\} = \widetilde{V}_0(A_0(\alpha)) = s\mu. \tag{5.3.9}$$

Since e is the smallest positive integer for which $e\mu \in G(K(\alpha))$, say $e\mu = \widetilde{V}_0(h(\alpha))$, $h(x) \in K[x]$, $\deg(h(x)) < \deg(\phi(x))$, it follows from (5.3.9) that $s = et$ for some integer t and $\widetilde{V}_0(A_i(\alpha)) + i\mu > s\mu = \widetilde{V}_0(h(\alpha)^t)$ when i is not divisible by e. Therefore using Theorem 1.1.G(ii) and denoting the $w_{\alpha,\delta}$-residue of $\frac{\phi(x)^e}{h(x)}$ by z, we see that the $w_{\alpha,\delta}$-residue of $F(x)/h(x)^t$ equals $z^t + \big(\overline{\frac{A_{e(t-1)}(\alpha)}{h(\alpha)}}\big) z^{t-1} + \cdots + \big(\overline{\frac{A_0(\alpha)}{h(\alpha)^t}}\big) = T(z)$ (say). This proves that $F(x)$ is a lifting of $T(y)$ with respect to (α, δ).

Lemma 5.3.6. *Let $(K, V_0), W, \phi(x)$ and α be as in Lemma 5.3.4 and $F(x)$ belonging to $K[x]$ be a polynomial not divisible by $\phi(x)$ having ϕ-expansion $A_s(x)\phi(x)^s + A_{s-1}(x)\ \phi(x)^{s-1} + \cdots + A_0(x)$, $A_s(x) \neq 0$. Suppose that a side of the ϕ-Newton polygon of $F(x)$ with respect to W has slope $\lambda > 0$ with interval of horizontal projection starting at $s-k$ and ending at $s-j$. Let $V = [W, V\phi = \lambda + W\phi]$ be the augmented valuation over W associated with $\phi, \mu = \lambda + W\phi$ and (α, δ) be a (K, V_0)-minimal pair such that $V = w_{\alpha,\delta}$. Then $I_{\alpha,\delta}(F) = j$ and $S_{\alpha,\delta}(F) = k$.*

Proof. Since $V = w_{\alpha,\delta}$ and $W(A_i(x)) = \widetilde{V}_0(A_i(\alpha))$ in view of (5.3.8), we see that $w_{\alpha,\delta}(F(x)) = \min_i \{W(A_i(x)) + i\mu\}$. So the lemma is proved once we show that j, k are respectively the smallest and the largest indices at which the minimum of the set $M = \{W(A_i(x)) + i\mu, 0 \leq i \leq s\}$ is attained. For the sake of convenience, denote $W(A_i(x)\phi(x)^i)$ by γ_i. As $[s-k, s-j]$ is the interval of horizontal projection of the side of the ϕ-Newton polygon of $F(x)$ having slope λ, in view of Definition 1.1.K, it follows that for all indices i lying in the interval $[j, k]$ we have $\lambda \leq \frac{\gamma_i - \gamma_k}{k-i}$ and this inequality becomes equality when $i = j$. Substituting for γ_i, γ_k and $\mu = W(\phi(x)) +$

λ, the above inequality can be rewritten as $W(A_i(x)) + i\mu \geq W(A_k(x)) + k\mu$ with equality when $i = j$. Therefore for proving the lemma, it is enough to prove that

$$W(A_i(x)) + i\mu > W(A_j(x)) + j\mu, \quad \text{when} \quad i < j \tag{5.3.10}$$

and

$$W(A_i(x)) + i\mu > W(A_k(x)) + k\mu, \quad \text{when} \quad i > k. \tag{5.3.11}$$

Keeping in mind that the slopes of the edges are in increasing order, for any index $i < j$, we have $\frac{\gamma_i - \gamma_j}{j-i} > \lambda = \mu - W(\phi(x))$, which immediately gives (5.3.10) when we substitute for γ_i, γ_j. To prove (5.3.11), fix an index $i > k$ and let $[s - k_1, s - k_2]$ denote the interval of horizontal projection of the side of the ϕ-Newton polygon of $F(x)$ which contains $s - i$. Then by Definition 1.1.K, $\frac{\gamma_i - \gamma_{k_1}}{k_1 - i} \geq \frac{\gamma_{k_2} - \gamma_{k_1}}{k_1 - k_2}$. A simple calculation shows that the above inequality is same as saying

$$\frac{\gamma_{k_2} - \gamma_i}{i - k_2} \leq \frac{\gamma_{k_2} - \gamma_{k_1}}{k_1 - k_2}. \tag{5.3.12}$$

Note that if $k_2 = k$, then the slope λ of r-th edge (say) of the ϕ-Newton polygon of $F(x)$ is strictly greater than the slope $\frac{\gamma_k - \gamma_{k_1}}{k_1 - k}$ of its previous edge. Therefore when $k_2 = k$, the inequality in (5.3.12) implies that $\frac{\gamma_k - \gamma_i}{i-k} < \lambda$, which on substituting for γ_i, γ_k and $\mu = W(\phi(x)) + \lambda$ immediately gives inequality (5.3.11). In general when $k_2 > k$, let $k_1 > k_2 > \cdots > k_t = k$ be integers such that each of the interval $[s - k_r, s - k_{r+1}]$ is an interval of horizontal projection of a side of the ϕ-Newton polygon of $F(x)$. Since the slopes of the respective edges are increasing, we have by (5.3.12)

$$\frac{\gamma_{k_2} - \gamma_i}{i - k_2} < \frac{\gamma_{k_3} - \gamma_{k_2}}{k_2 - k_3} < \cdots < \frac{\gamma_{k_t} - \gamma_{k_{t-1}}}{k_{t-1} - k_t} < \lambda$$

which implies that $\frac{\gamma_{k_t} - \gamma_i}{i - k_t} < \frac{\gamma_{k_t} - \gamma_{k_{t-1}}}{k_{t-1} - k_t} < \lambda$ in view of a basic inequality (which says that whenever $\frac{A_1}{B_1} < \frac{A_2}{B_2} < \cdots < \frac{A_r}{B_r}$ with $B_i > 0$, then $\frac{A_1 + \cdots + A_r}{B_1 + \cdots + B_r} < \frac{A_r}{B_r}$). So we have $\frac{\gamma_k - \gamma_i}{i-k} < \lambda = \mu - W(\phi(x))$ which immediately gives (5.3.11). This completes the proof of the lemma.

Lemma 5.3.7. *Let $(K, V_0), W$ and $\phi(x)$ be as in Lemma 5.3.4. Let $F(x), G(x)$ belonging to $K[x]$ be two monic polynomials not divisible by $\phi(x)$. Suppose that the*

ϕ-Newton polygons of $F(x), G(x)$ with respect to W consist of k, t sides respectively having positive slopes $\lambda_1 < \cdots < \lambda_k$ and $\lambda'_1 < \cdots < \lambda'_t$. Let l_i, l'_i denote the lengths of the horizontal projection of the sides with slopes λ_i, λ'_i respectively. Then the distinct elements of the set $\{\lambda_i, \lambda'_j, 1 \leq i \leq k, 1 \leq j \leq t\}$ arranged in ascending order are all the slopes of the ϕ-Newton polygon of $F(x)G(x)$. If $\lambda_i = \lambda'_j$ for some pair (i, j), then the length of horizontal projection of the side of the ϕ-Newton polygon of $F(x)G(x)$ with slope λ_i will be $l_i + l'_j$; in case $\lambda_i \neq \lambda'_j$, then the length of horizontal projection of the side of the ϕ-Newton polygon of $F(x)G(x)$ with slope λ_i (respectively λ'_j) is l_i (respectively l'_j).

Proof. Let $F(x) = \sum_{i=0}^{s} A_i(x)\phi(x)^i$, $G(x) = \sum_{i=0}^{t} B_i(x)\phi(x)^i$ be the ϕ-expansions of $F(x)$ and $G(x)$ with $A_s(x)B_t(x) \neq 0$. Let $\lambda > 0$ be the slope of an edge S of the ϕ-Newton polygon of $F(x)$ having horizontal projection $[s-k, s-j]$. Let $V = [W, V\phi = \mu = \lambda + W\phi]$ be the augmented valuation over W and α be a root of $\phi(x)$, then by Theorem 5.1.1 there exists $\delta \in \widetilde{G}_0$ such that (α, δ) is a (K, V_0)-minimal pair and $V = w_{\alpha,\delta}$. So by Lemma 5.3.6, $I_{\alpha,\delta}(F(x)) = j, S_{\alpha,\delta}(F(x)) = k$. We first show that the ϕ-Newton polygon of $F(x)G(x)$ with respect to W has a side of slope λ and also find the length of the horizontal projection of this side. Two cases arise:

Case I. λ is not the slope of any side of the ϕ-Newton polygon of $G(x)$.

In this case, in view of Lemma 5.3.6, $I_{\alpha,\delta}(G(x)) = S_{\alpha,\delta}(G(x)) = l$ (say). By (5.3.1), $I_{\alpha,\delta}(F(x)G(x)) = I_{\alpha,\delta}(F(x)) + I_{\alpha,\delta}(G(x)) = j + l$ and $S_{\alpha,\delta}(F(x)G(x)) = k + l$. Therefore the ϕ-Newton polygon of $F(x)G(x)$ has a side with slope λ having the length of horizontal projection equal to that of S.

Case II. λ is the slope of some side of the ϕ-Newton polygon of $G(x)$.

Suppose that the side S' of the ϕ-Newton polygon of $G(x)$ of slope λ has interval of horizontal projection $[t - k_1, t - j_1]$. Therefore by virtue of Lemma 5.3.6, $I_{\alpha,\delta}(G(x)) = j_1, S_{\alpha,\delta}(G(x)) = k_1$. Using (5.3.1), $I_{\alpha,\delta}(F(x)G(x)) = j + j_1, S_{\alpha,\delta}(F(x)G(x)) = k + k_1$. So the ϕ-Newton polygon of $F(x)G(x)$ has a side of slope λ whose length of horizontal projection is equal to the sum of the lengths of the horizontal projections of S and S'.

The proof of the lemma is complete once we show that if $\lambda > 0$ is the slope of a side S'' of the ϕ-Newton polygon of $F(x)G(x)$, then either the ϕ-Newton polygon of $F(x)$ or of $G(x)$ has a side with slope λ. If l denotes the length of the horizontal projection of S'', then by Lemma 5.3.6, $S_{\alpha,\delta}(F(x)G(x)) - I_{\alpha,\delta}(F(x)G(x)) = l > 0$. So in view of (5.3.1), either $S_{\alpha,\delta}(F(x)) - I_{\alpha,\delta}(F(x)) > 0$ or $S_{\alpha,\delta}(G(x)) - I_{\alpha,\delta}(G(x)) > 0$ which proves that the ϕ-Newton polygon of either $F(x)$ or $G(x)$ has a side of slope $\lambda > 0$.

5.4 Proof of Theorem 5.1.6, Corollary 5.1.8 and examples.

Proof of Theorem 5.1.6. We prove assertions $(i), (ii), (iii)$ of the theorem by induction on r = the number of sides of the ϕ-Newton polygon of $F(x)$ (with respect to W). For $r = 1$, let $\lambda' > 0$ denote the slope of the single side of the ϕ-Newton polygon of $F(x)$. Let $V' = [W, V'\phi = \lambda' + W\phi]$ be the augmented valuation over W associated with $\phi, \mu' = \lambda' + W\phi$. By Theorem 5.1.1, there exists $\delta' \in \widetilde{G}_0$ such that (α, δ') is a (K, V_0)-minimal pair and $V' = w_{\alpha,\delta'}$. Let e' be the smallest positive integer such that $e'\mu' \in G(K(\alpha))$. By Lemma 5.3.5, $F(x)$ is a lifting of a polynomial not divisible by y belonging to $\overline{K(\alpha)}[y]$ with respect to (α, δ') of degree s/e'. Therefore by Theorem 5.3.1, for each root θ of $F(x)$, $G(K(\alpha)) \subseteq G(K(\theta))$ and the degree $[\overline{K(\alpha)} : \overline{K}]$ divides $[\overline{K(\theta)} : \overline{K}]$. Also by Theorem 5.3.A, $\widetilde{V}_0(\phi(\theta)) = \mu'$. So $\mu' \in G(K(\theta))$; consequently e' divides the index $[G(K(\theta)) : G(K(\alpha))]$. Thus the first three assertions of the theorem are proved when $r = 1$.

Suppose that $r \geq 2$ and let $0 < \lambda_1 < \lambda_2 < \cdots < \lambda_r$ be the slopes of the ϕ-Newton polygon of $F(x)$. Denote λ_r by λ. Let $V = [W, V\phi = \lambda + W\phi]$ be the augmented valuation over W associated with $\phi, \mu = \lambda + W\phi$. By Theorem 5.1.1, there exists $\delta \in \widetilde{G}_0$ such that (α, δ) is a (K, V_0)-minimal pair and $V = w_{\alpha,\delta}$. Let e be the smallest positive integer such that $e\mu \in G(K(\alpha))$. Let $[s - l, s]$ denote the interval of horizontal projection of the side of the ϕ-Newton polygon of $F(x)$ with slope $\lambda_r = \lambda$. Therefore in view of Lemma 5.3.6 we have $S_{\alpha,\delta}(F) = l$,

$I_{\alpha,\delta}(F) = 0$. Claim is that $F(x)$ is equivalent to $\phi(x)^s$ in W. Since all sides of the ϕ-Newton polygon of $F(x)$ with respect to W have positive slopes, we see that $W(A_i(x)\phi(x)^i) > W(\phi(x)^s)$ for $0 \leq i < s$ and hence we have

$$W(F(x) - \phi(x)^s) = W(\sum_{i=0}^{s-1} A_i(x)\phi(x)^i) \geq \min_i\{W(A_i(x)\phi(x)^i)\} > W(\phi(x)^s),$$

which proves the claim. It now follows that Theorem 5.3.3 is applicable to $F(x)$ and hence $F(x)$ has a monic factor $F_r(x)$ (say) belonging to $K[x]$ of degree lm which is a lifting of a monic polynomial belonging to $\overline{K(\alpha)}[y]$ not divisible by y of degree l/e with respect to ϕ, μ. If θ_r is a root of $F_r(x)$, then in view of Theorem 5.3.A, $\widetilde{V}_0(\phi(\theta_r)) = \mu$. By Lemma 5.3.4, the ϕ-Newton polygon of $F_r(x)$ with respect to W consists of single side which has slope λ and length of its horizontal projection is equal to l. Applying Lemma 5.3.7, we see that the ϕ-Newton polygon of the polynomial $F(x)/F_r(x)$ consists of $r-1$ sides with slopes $0 < \lambda_1 < \cdots < \lambda_{r-1}$. Therefore by induction hypothesis applied to $F(x)/F_r(x)$, assertions (i)–(iii) of the theorem follow. Assertion (iv) is obtained on applying Theorem 5.3.H to polynomials $F_i(x)$ and then using the last assertion of Theorem 5.3.1.

Proof of Corollary 5.1.8. In view of the hypothesis, the side with the smallest slope of the ϕ-Newton polygon of $F(x)$ with respect to W has interval of horizontal projection $[0, s-l]$ and has slope $\dfrac{W(A_l(x)\phi(x)^l) - W(\phi(x)^s)}{s-l} = \lambda_1$ (say). Therefore by assertions $(i), (iii)$ of Theorem 5.1.6, $F(x)$ has a monic factor $F_1(x)$ belonging to $K[x]$ of degree $(s-l)m$ which is a lifting of a monic polynomial $T_1(y) \in \overline{K(\alpha)}[y]$ not divisible by y with respect to $\phi(x)$, $\mu = W(\phi(x)) + \lambda_1$. Let θ_1 be a root of $F_1(x)$. Then by Theorem 5.1.6 (ii), $\widetilde{V}_0(\phi(\theta_1)) = W(\phi(x)) + \lambda_1$. Substituting for λ_1, we see that $\widetilde{V}_0(\phi(\theta_1)) = \dfrac{W(A_l(x))}{s-l}$. Keeping in mind the hypothesis $\frac{W(A_l(x))}{d} \notin G(K(\alpha))$ for any number $d > 1$ dividing $s-l$, it follows from assertion (ii) of Theorem 5.1.6 that the index $[G(K(\theta_1)) : G(K(\alpha))]$ is divisible by $s-l$; also by the same assertion the degree $[\overline{K(\theta_1)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}]$. Therefore we have

$$\begin{aligned}(s-l)m \geq [K(\theta_1) : K] &= [G(K(\theta_1)) : G_0][\overline{K(\theta_1)} : \overline{K}]\mathrm{def}(K(\theta_1)/K) \\ &\geq (s-l)[G(K(\alpha)) : G_0][\overline{K(\alpha)} : \overline{K}]\mathrm{def}(K(\theta_1)/K).\end{aligned}$$

By Theorem 5.3.1, def$(K(\alpha)/K)$ divides def$(K(\theta_1)/K)$; consequently

$$(s-l)m \geq [K(\theta_1) : K] \geq (s-l)[G(K(\alpha)) : G_0][\overline{K(\alpha)} : \overline{K}]\text{def}(K(\alpha)/K) = (s-l)m.$$

Therefore the polynomial $F_1(x)$ of degree $(s-l)m$ is irreducible over K. Consequently for any factorization $G(x)H(x)$ of $F(x)$ over K, $F_1(x)$ will divide at least one of $G(x)$ or $H(x)$, say $F_1(x)$ divides $G(x)$. Then $\deg G(x) \geq (s-l)m$. Hence $\deg H(x) \leq lm$ as desired.

We now give examples to illustrate Theorems 5.1.6, 5.1.7. These examples occur in [J-K-S4]. As pointed out in Remark 5.4.4, in each of the examples the factorization of the polynomial $F(x)$ under consideration into irreducible factors over the base field cannot be obtained by already known results in this direction.

Example 5.4.1. *Let V_0 be a henselian valuation of arbitrary rank of a field K whose value group has a smallest positive element $\lambda_0 = V_0(\pi)$ for some π in the valuation ring R_0 of V_0. Let $\phi(x) \in R_0[x]$ be a monic polynomial with $\overline{\phi}(x) \neq x$ irreducible over the residue field of V_0. We factorize the polynomial $F(x) = (\phi(x)^s + \pi)^s + a\phi(x)$ into irreducible factors over K, where $V_0(a) = t\lambda_0$ and $t \geq s \geq 2$ are integers. Let V_2 denote the second stage inductive valuation defined by $V_2 = [V_0, V_1 x = 0, V_2\phi = \lambda_0/s]$. Take $\phi_3(x) = \phi(x)^s + \pi$. Keeping in mind Corollary 5.1.2, it can be easily verified using Theorem 5.3.E that $\phi_3(x)$ is a key polynomial over V_2. Further $\phi_3(x)$ is not equivalent to $\phi(x)$ in V_2 because $V_2(\phi_3(x)) = \lambda_0 > V_2(\phi(x)) = \frac{\lambda_0}{s}$. So $\phi_3(x)$ is a key polynomial for an inductive valuation over V_2. Since $F(x)$ has ϕ_3-expansion $\phi_3(x)^s + a\phi(x)$, the ϕ_3-Newton polygon of $F(x)$ with respect to V_2 consists of a single side with slope $\lambda = \frac{(t-s)\lambda_0}{s} + \frac{\lambda_0}{s^2}$. If e denotes the smallest positive integer such that $e\lambda$ belongs to the value group $G_0 + \frac{\lambda_0\mathbb{Z}}{s}$ of V_2, then by virtue of the hypothesis that λ_0 is the smallest positive element of G_0, we have $e = s$. Let α be a root of $\phi_3(x)$. Using assertions (i),(iii) of Theorem 5.1.7, we see that $F(x)$ is a lifting of a linear polynomial $T(y) \in \overline{K(\alpha)}[y]$ not divisible by y with respect to $\phi_3(x)$, $\lambda_0 + \lambda$. Hence in view of Theorem 5.1.7(iv), $F(x)$ is irreducible over K and for any root θ of $F(x)$, $[G(K(\theta)) : G_0] = s^2$, $[\overline{K(\theta)} : \overline{K}] = \deg(\phi(x))$.*

Example 5.4.2. *Let w_0 be the 2-adic valuation of the field $\mathbb{Q}$ of rational numbers defined by $w_0(2) = 1$. Let w_y denote the valuation of the field $\mathbb{Q}(y)$ of rational functions with coefficients from $\mathbb{Q}$ in an indeterminate y defined for any polynomial $f(y)$ belonging to $\mathbb{Q}[y]$ by $w_y(f(y))$= the highest power of the monomial y dividing $f(y)$. For a nonzero polynomial $f(y) \in \mathbb{Q}[y]$, let f^* denote the constant term of the polynomial $f(y)/y^{w_y(f(y))}$. Let w be the mapping from $\mathbb{Q}[y]$ into the group $\mathbb{Z} \times \mathbb{Z}$ with lexicographic ordering defined for any nonzero polynomial $f(y)$ by $w(f(y)) = (w_y(f(y)), w_0(f^*))$ and $w(0) = \infty$. It can be easily checked that w satisfies $w(fg) = w(f) + w(g)$ and $w(f + g) \geq \min\{w(f), w(g)\}$ for all f, g in $\mathbb{Q}[y]$. So w gives a valuation of $\mathbb{Q}(y)$. Let (K, V_0) denote the henselization of $(\mathbb{Q}(y), w)$. Then the value group Γ_0 of V_0 is $\mathbb{Z} \times \mathbb{Z}$ (lexicographically ordered) with smallest positive element $(0, 1)$. Let $s \geq 2$ be any integer. Consider the polynomial $F(x) = x^{2^s} - a$ belonging to $K(x)$ with $V_0(a - 4) \geq (0, 5)$. We show that $F(x)$ factors into a product of two irreducible polynomials over K each of degree 2^{s-1}. Let V_1 stand for the first stage valuation defined by $V_1 = [V_0, V_1 x = (0, \frac{1}{2^{s-1}})]$. Applying Theorem 5.3.E, it can be easily checked that the polynomial $\phi_2(x) = x^{2^{s-1}} - 2$ is a key polynomial over V_1. Clearly $\phi_2(x)$ is not equivalent to x in V_1. Note that the ϕ_2-expansion of $F(x)$ is $(\phi_2(x))^2 + 4\phi_2(x) + 4 - a$. Denote $V_0(4 - a)$ by μ and recall that by hypothesis $\mu \geq (0, 5)$. So the ϕ_2-Newton polygon of $F(x)$ with respect to V_1 consists of two edges. The first edge has slope $\lambda_1 = (0, 1)$; the second edge has slope $\lambda_2 = \mu - (0, 3) \geq (0, 2)$. Let α be a root of $\phi_2(x)$. In view of assertions $(i), (iii)$ of Theorem 5.1.7, we see that $F(x) = F_1(x)F_2(x)$, where $F_i(x)$ belonging to $K[x]$ having degree 2^{s-1} is a lifting of a monic linear polynomial $T_i(y) \neq y$ belonging to $\overline{K(\alpha)}[y]$ with respect to $\phi_2(x)$,$\lambda_i + V_1(\phi_2) = \lambda_i + (0, 1)$. It now follows from Theorem 5.1.7(iv) that $F_i(x)$ is irreducible over K for $i = 1, 2$ and for any root θ_i of $F_i(x)$, $[G(K(\theta_i)) : \Gamma_0] = 2^{s-1}$. Thus for each root θ of $F(x)$, $K(\theta)$ is a totally ramified extension of (K, V_0).*

Example 5.4.3. *Let V_0 be a henselian valuation of arbitrary rank of a field K with value group Γ_0. Let a, b be elements of K such that $V_0(a) > \frac{V_0(b)}{2} > 0$ and $\frac{V_0(b)}{2} \notin \Gamma_0$. Let b_0, b_1, b_2 be elements of K with $V_0(b_0) = 0, V_0(b_1) \geq V_0(b)$ and $V_0(b_2) \geq 2V_0(b)$.*

We show that the polynomial $F(x) = (x^2+ax+b)^2 + b_2(x^2+ax+b) + b^2(b_0x+b_1)$ *is irreducible over* K*. Define* $V_1 = [V_0, V_1x = V_0(b)/2]$ *and* $\phi_2(x) = x^2+ax+b$*. Observe that* $\phi_2(x)$ *is a lifting of a linear polynomial with respect to the valuation* $V_1 = w_{0,\delta}$ *where* $\delta = V_0(b)/2$*. So by Theorem 5.1.E,* $\phi_2(x)$ *is a key polynomial over* V_1*. It is indeed a nontrivial key polynomial over* V_1 *because* $\phi_2(x)$ *is not equivalent to* x *in* V_1*. Let* α *be a root of* $\phi_2(x)$*. Since the* ϕ_2*-expansion of* $F(x)$ *is* $(\phi_2(x))^2 + b_2\phi_2(x) + b^2(b_0x+b_1)$*, it can be easily seen that its* ϕ_2*-Newton polygon with respect to* V_1 *consists of a single edge having slope* $\delta/2$*. Keeping in mind that* $V_1(\phi_2(x)) = 2\delta = V_0(b) \in \Gamma_0$ *and* $\delta \notin \Gamma_0$*, we conclude on applying Theorem 5.1.6(iii) that* $F(x)$ *is a lifting of a monic linear polynomial belonging to* $\overline{K(\alpha)}[y]$ *and hence is irreducible over* K *by Theorem 5.1.6(iv).*

Remark 5.4.4. *It may be pointed out that Theorem* 1.2 *of [Jh-Kh1] does not establish the irreducibility of* $F(x)$ *over* K *in Example 5.4.1 even when* $s = t = 2$*, for in this situation the* ϕ*-Newton polygon of* $F(x)$ *(with underlying valuation* V_0*) consists of a single edge having slope* $\frac{\lambda_0}{2}$ *with length of horizontal projection* 4*. So by Theorem* 1.2 *of [Jh-Kh1],* $F(x)$ *would be a lifting of a second degree polynomial belonging to* $\overline{K(\beta)}[y]$ *with respect to* $\phi(x), \frac{\lambda_0}{2}$*, where* β *is a root of* $\phi(x)$*. As regards Example 5.4.2,* $\phi(x) = x$ *is the only irreducible factor of* $F(x)$ *modulo the maximal ideal* M_0 *of the valuation ring of* V_0 *and the* ϕ*-Newton polygon of* $F(x)$ *consists of a single edge having slope* $(0, \frac{1}{2^{s-1}})$ *with length of horizontal projection* 2^s*. So* $F(x)$ *will be a lifting of a square of a linear polynomial belonging to* $\overline{K}[y]$ *with* $\overline{K}$ *being the field of two elements. Therefore Theorem* 1.2 *of [Jh-Kh1] does not give any information regarding the factorization of* $F(x)$ *in this situation.*

Bibliography

[A-P-Z1] V. Alexandru, N. Popescu, and A. Zaharescu, *A theorem of characterization of residual transcendental extension of a valuation*, J. Math. Kyoto Univ. **28** (1988), 579-592.

[A-P-Z2] V. Alexandru, N. Popescu, and A. Zaharescu, *Minimal pairs of definition of a residual transcendental extension of a valuation*, J. Math. Kyoto Univ. **30** (1990), 207-225.

[Bro] R. Brown, *Roots of generalized Schönemann polynomials in henselian extension fields*, Indian J. Pure Appl. Math. **39** (2008), 403-410.

[Ca-Fr] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1976.

[Ch-De] M. E. Charkani and A. Deajim, *Generating a power basis over a Dedekind ring*, J. Number Theory **132** (2012), 2267-2276.

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer - Verlag, Berlin-Heidelberg, 1993.

[C-M-S] S. D. Cohen, A. Movahhedi, and A. Salinier, *Factorization over local fields and the irreducibility of generalized difference polynomials*, Mathematika **47** (2000), 173-196.

[Ded] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen **23** (1878), 1-23.

[Dum] G. Dumas, *Sur quelques cas d'irréductibilité despolynomes à coefficients rationnels*, J. Math. Pures Appl. **6** (1906), 191–258.

[End] O. Endler, *Valuation Theory*, Springer-Verlag, Berlin Heidelberg, 1972.

[En-Pr] A. J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, New York, 2005.

[Ers] Y. L. Ershov, *A Dedekind criterion for arbitrary valuation rings*, Dokl. Math. **74** (2006), 650-652.

[Es-Mu] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory*, Second Edition, Springer, Inc. 2005.

[G-M-N] J. Guàrdia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), 361-416.

[Hen] K. Hensel, *Arithmetische Untersuchung über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math. **113** (1894), 128-160.

[Her] I. N. Herstein, *Topics in Algebra*, Second edition, John Wiley and Sons, 1975.

[Iya] S. Iyanaga, *The theory of numbers*, North-Holland Publishing Company, 1975.

[J-J-K-S] A. Jakhar, B. Jhorar, S. K. Khanduja, and N. Sangwan, *Discriminant as a product of local discriminants*, J. Algebra Appl. **16** (2017), 1750198 (7 pages).

[J-K-S1] A. Jakhar, S. K. Khanduja, and N. Sangwan, *On prime divisors of the index of an algebraic integer*, J. Number Theory **166** (2016), 47-61.

[J-K-S2] A. Jakhar, S. K. Khanduja, and N. Sangwan, *Characterization of primes dividing the index of an algebraic integer*, Int. J. Number Theory **13** (2017), 2505-2514.

[J-K-S3] A. Jakhar, S. K. Khanduja, and N. Sangwan, *On integrally closed simple extensions of valuation rings*, J. Pure Appl. Algebra **222** (2018), 889-899.

[J-K-S4] A. Jakhar, S. K. Khanduja, and N. Sangwan, *On factorization of polynomials in henselian valued fields*, Comm. Algebra, http://dx.doi.org/10.1080/00927872.2017.1407423.

[J-K-S5] A. Jakhar, S. K. Khanduja, and N. Sangwan, *On the compositum of integral closures of valuation rings*, J. Pure Appl. Algebra, http://dx.doi.org/10.2016/j.jpaa.2017.12.023.

[Jh-Kh1] B. Jhorar and S. K. Khanduja, *Reformulation of Hensel's Lemma and extension of a theorem of Ore*, Manuscr. Math. **151** (2016), No. 1, 223-241.

[Jh-Kh2] B. Jhorar, S. K. Khanduja, *When is $R[\theta]$ integrally closed?*, J. Algebra Appl. **15** (2016), 1650091 (7 pages).

[Jh-Kh3] B. Jhorar, S. K. Khanduja, *On power basis of a class of algebraic number fields*, Int. J. Number theory **12** (2016), 2317-2321.

[Jh-Kh4] B. Jhorar and S. K. Khanduja, *A generalization of Eisenstein-Dumas-Schönemann Irreducibility Criteria*, Proc. Edinburgh Math. Soc. **60** (2017), 937-945.

[Jh-Kh5] B. Jhorar, S. K. Khanduja, *On the Theorem of Index of Ore*, Manuscr. Math. **153** (2017), 299-313.

[Kha] S. K. Khanduja, *On Brown's constant associated with irreducible polynomials over henselian valued fields*, J. Pure Appl. Algebra, **214** (2010), 2294-2300.

[Kh-Kh] S. K. Khanduja and R. Khassa, *A generalization of Eisenstein-Schönemann Irreducibility Criterion*, Manuscr. Math. **134** (2011), 215-224.

[Kh-Ku1] S. K. Khanduja and M. Kumar, *On Dedekind criterion and simple extensions of valuation rings*, Comm. Algebra **38** (2010), 684-696.

[Kh-Ku2] S. K. Khanduja and M. Kumar, *Prolongations of valuations to finite extensions*, Manuscr. Math. **131** (2010), 323-334.

[Kh-Ku3] S. K. Khanduja and S. Kumar, *On prolongations of valuations via Newton polygons and liftings of polynomials*, J. Pure Appl. Algebra **216** (2012), 2648-2656.

[Kh-Ku4] S. K. Khanduja and S. Kumar, *A generalization of a theorem of Ore*, J. Pure Appl. Algebra **218** (2014), 1206-1218.

[Kh-Sa] S. K. Khanduja and J. Saha, *A generalized fundamental principle*, Mathematika **46** (1999), 83-92.

[K-P-R] S. K. Khanduja, N. Popescu, and K. W. Roggenkamp, *On minimal pairs and residually transcendental extensions of valuations*, Mathematika **49** (2002), 93-106.

[K-K-M] F.V. Kuhlmann, S. Kuhlmann, M. Marshall, Editors, *Valuation theory and its applications Volume I*, Fields Institute Communications, **32**, Amer. Math. Soc., Providence, RI, 2002.

[Kur] J. Kürchák, *Über Limesbildung und allgemeine Körpertheorie,* Proceedings of the 5th International Congress of Mathematicians Cambridge **1** (1913), 285-289.

[Mac] S. MacLane, *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. **40** (1936), 363-395.

[Mar] D. A. Marcus, *Number Fields*, Springer - Verlag, Berlin-Heidelberg, 1977.

[Moy] B. N. Moyls, *The structure of valuations of the rational function field $K(x)$*, Trans. Amer. Math. Soc. **71** (1951), 102-112.

[Nar] W. Narkiewicz, *Elementary and Analytical Theory of Algebraic Numbers*, Springer - Verlag, Berlin-Heidelberg, 2004.

[Ore1] Ø. Ore, *Zur Theorie der algebraischen Körper*, Acta Math. **44** (1923), 219-314.

[Ore2] Ø. Ore, *Weitere Untersuchungen zur Theorie der algebraischen Körper*, Acta Math. **45** (1924-25), 145-160.

[Ore3] Ø. Ore, *Bestimmung der Diskriminanten algebraischer Körper*, Acta Math. **45** (1925), 303-344.

[Ore4] Ø. Ore, *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*, Math. Ann. **96** (1926), 313-352.

[Ore5] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), 84-117.

[Ost1] A. Ostrowski, *Über sogenannte perfekte Körper*, J. Reine Angew. Math. **147** (1917), 191-204.

[Ost2] A. Ostrowski, *Über einige Lösungen der Functionalgleichung* $\phi(x)\phi(y) = \phi(xy)$, Acta Math. **41** (1918), 271-284.

[Ost3] A. Ostrowski, *Algebraische Funktionen von Dirichletschen Reihen*, Math. Zeitschr. **37** (1933), 98-133.

[Ost4] A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper (Die Theorie der Teilbarkeit in allgemeinen Körpern)*, Math. Zeitschr. **39** (1934), 269-404.

[Po-Po] L. Popescu and N. Popescu, *On the residual transcendental extensions of a valuation, key polynomials and augmented valuation*, Tsukuba J. Math. **15** (1991), No.1 , 57-78.

[Po-Za] N. Popescu and A. Zaharescu, *On the structure of the irreducible polynomials over local fields*, J. Number Theory **52** (1995), 98-118.

[Rib] P. Ribenboim, *The Theory of Classical Valuations*, Springer-Verlag, New York, 1999.

[Swa] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099-1106.

[Uch] K. Uchida, *When is $\mathbb{Z}[\alpha]$ the ring of the integers ?*, Osaka J. Math. **14** (1977), 155-157.