Chapter 5

A generalization of a Theorem of Ore and related results

5.1 Statements of results

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta$ in the ring $A_K$ of algebraic integers of $K$ and $F(x)$ be the minimal polynomial of $\theta$ over the field $\mathbb{Q}$ of rational numbers. The computation of the discriminant of $K$ and the index of the subgroup $\mathbb{Z}[\theta]$ in $A_K$ are two intimately connected problems in algebraic number theory. In 1928, Ore attempted to solve this problem by giving a simple formula for determining the highest power of a given prime $p$ dividing $[A_K : \mathbb{Z}[\theta]]$ when $F(x)$ is $p$-regular (to be defined soon). He used the factorization of the polynomial $\overline{F}(x)$ obtained on replacing each coefficient of $F(x)$ by its residue modulo $p$, say $\overline{F}(x) = \overline{\phi_1}(x)^{r_1} \cdots \overline{\phi_r}(x)^{r_r}$, where $\overline{\phi_i}(x)$ are distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $\phi_i(x)$ monic. For this purpose, he considered the $\phi_i$-Newton polygon of $F$ for each $i$ (definition given in 1.5). Moreover to each side $S$ of the $\phi_i$-Newton polygon of $F$ of positive slope, he associated a polynomial $(F_i)_S(Y)$ over the finite field $\mathbb{F}_{q_i}$ for $q_i = p^\deg \phi_i$ in an indeterminate $Y$. If all these polynomials $(F_i)_S(Y)$ corresponding to various sides $S_i, 1 \leq j \leq k_i, 1 \leq i \leq r$, of the $\phi_i$-Newton polygon of $F$ have no repeated irreducible factor, then $F(x)$ is said to be $p$-regular with respect to...
\( \phi_1(x), \ldots, \phi_r(x) \) (precise definition given in 5.1). In this situation, Ore (cf. [Ore5], [Mo-Na, Theorem, p. 325]) proved a remarkable result (called Theorem of Index) that the \( p \)-adic valuation (denoted by \( v_p \)) of the index of \( \mathbb{Z}[\theta] \) in \( \mathbb{A}_K \) is given by

\[
v_p([\mathbb{A}_K : \mathbb{Z}[\theta]]) = \sum_{j=1}^{r} i_{\phi_j}(F),
\]

where \( i_{\phi_j}(F) \) is defined by equation (1.4). In 2012, using the results of Ore, El Fadil, Montes and Nart [F-M-N, Theorem 2.1] gave a method to determine explicitly a \( p \)-integral basis of \( K \) when \( F(x) \) is \( p \)-regular with respect to \( \phi_1, \ldots, \phi_r \). In this chapter, we deal with the analogous problems for arbitrary discrete valuation rings and replace the condition of \( p \)-regularity by a weaker one (see Theorem 5.1.3). We also extend the Theorem of Index of Ore to arbitrary discrete valued fields without any restriction on the residue field. Counter examples are given to show that Criterion I on page 326 and one of the equivalent statements of the Proposition on page 328 of [Mo-Na] are false (see Examples 5.5.4, 5.5.5). An extra necessary and sufficient condition has been given for these results to be true (cf. Theorems 5.1.5, 5.1.6). We state the results of this chapter after introducing some definitions.

**Definition 5.1.** Let \((\overline{K}, \overline{v})\) be the completion of a real valued field \((K, v)\). Let \( \phi(x) \in R_v[x] \) be a monic polynomial having a root \( \alpha \) with \( \overline{\phi}(x) \) irreducible over \( R_v/M_v \). Let \( G(x) \) belonging to \( R_v[x] \) be a monic polynomial not divisible by \( \phi(x) \) such that \( \overline{G}(x) = \overline{\phi}(x)^s \). Let \( 0 < \lambda_1 < \cdots < \lambda_k \) be the slopes of the \( \phi \)-Newton polygon of \( G(x) \). By Theorem 2.1.1, we can write \( G(x) = G_1(x) \cdots G_k(x) \), where \( G_i(x) \) belonging to \( R_v[x] \) is a lifting of \( T_i(Y) \) belonging to \( \overline{K}(\alpha)[Y] \), not divisible by \( Y \). If \( T_i(Y) \) is a product of distinct monic irreducible polynomials over \( \overline{K}(\alpha) \) for each \( i \), then \( G(x) \) is said to be \( \nu \)-regular with respect to \( \phi(x) \). In general, if \( F(x) \) belonging to \( R_v[x] \) is a monic polynomial and \( \overline{F}(x) = \overline{\phi}_1(x)^{\nu_1} \cdots \overline{\phi}_r(x)^{\nu_r} \) is its factorization into irreducible polynomials over \( R_v/M_v \) with each \( \phi_i(x) \) belonging to \( R_v[x] \) monic and \( \nu_i > 0 \), then by Hensel's Lemma, there exist \( F_1(x), \ldots, F_r(x) \) belonging to \( R_v[x] \) such
that \( F(x) = F_1(x) \cdots F_r(x) \) and \( \bar{F}_i(x) = \bar{\phi}_i(x)^{\nu_i} \). \( F(x) \) is said to be \( v \)-regular (with respect to \( \phi_1, \ldots, \phi_r \)) if each \( F_i(x) \) is \( v \)-regular with respect to \( \phi_i(x) \).

**Definition 5.2.** Let \( v \) be a discrete valuation of a field \( K \) with value group \( \mathbb{Z} \). Let \( F(x) \) belonging to \( R_v[x] \) be a monic irreducible polynomial over \( K \) of degree \( n \) having a root \( \theta \) and \( S \) be the integral closure of \( R_v \) in \( K(\theta) \). We define the index of \( F \) when \( S \) is a free \( R_v \)-module\(^1\). It is defined to be the \( v \)-valuation of the determinant of the transition matrix from an \( R_v \)-basis of \( S \) to \( \{1, \theta, \ldots, \theta^{n-1}\} \) and will be denoted by \( i(F) \). If \( G(x) = \prod_j G_j(x) \) is a monic polynomial belonging to \( R_v[x] \) with irreducible factors \( G_j(x) \) over \( R_v \) such that \( i(G_j) \) is defined for each \( j \), then we define the index of \( G \) by

\[
i(G) = \sum_j i(G_j) + \sum_{j < k} r(G_j, G_k), \tag{5.1}\]

where \( r(G_j, G_k) \) is the \( v \)-valuation of the resultant of \( G_j(x) \) and \( G_k(x) \). Note that \( i(G) = \infty \) only when \( G \) has repeated irreducible factors. Moreover, relation (5.1) holds for any decomposition of \( G(x) \), even when the factors are not necessarily irreducible.

**Remark 5.3.** It may be pointed out that with \( (K, v) \) as above, if \( F(x) \) belonging to \( R_v[x] \) is a monic separable irreducible polynomial having a root \( \theta \) which splits into irreducible factors over the completion of \( (K, v) \) as \( \prod_i \bar{F}_i(x) \), then the two meanings of \( i(F) \) described in the above definition are the same in view of the well known result relating the \( \text{disc}(K(\theta)/K) \) with local discriminants (cf. [Cas, Chapter 9, Lemma 3.2]) together with the relation \( v(\text{disc}(F)) = v(\text{disc}(K(\theta)/K)) + 2i(F) \) and similar relations for \( i(\bar{F}_i) \).

**Definition 5.4.** Let \( v \) be a real valuation of a field \( K \). Let \( F(x) \) belonging to \( R_v[x] \) be a monic polynomial with \( \bar{F}(x) = \bar{\phi}_1(x)^{\nu_1} \cdots \bar{\phi}_r(x)^{\nu_r} \), where \( \phi_i(x) \) are monic

\(^1\)If \( K(\theta)/K \) is a separable extension or \( (K, v) \) is complete, then \( S \) is finitely generated and hence free as \( R_v \)-module.
polynomials not dividing $F(x)$ which are distinct and irreducible modulo $M_v$ and $v_i$ are positive integers. When $v$ is discrete and $i(F)$ is defined, we say that $F(x)$ is weakly $v$-regular with respect to $\phi_1, \ldots, \phi_r$ if $i(F) = \sum_{j=1}^{r} i_{\phi_j}(F)$, where $i_{\phi_j}(F)$ is defined by (1.4) for $\phi = \phi_j$.

We are going to prove in Theorem 5.1.4 that the condition for $F(x)$ being weakly $v$-regular is indeed weaker than being $v$-regular.

Notation 5.5. Let $F(x)$, $\phi_i(x)$ be as in Definition 5.4. We shall denote by $m_i$, the degree of $\phi_i(x)$ and by $q_{i,j}(x), r_{i,j}(x)$ respectively the quotient and the remainder when $F(x)$ is divided by $\phi_i(x)^j$. The $\phi_i(x)$-expansion of $F(x)$ will be denoted by \[ \sum_{j=0}^{d_i} A_{i,j}(x)\phi_i(x)^j, \text{deg } A_{i,j}(x) < m_i, A_{i,d_i}(x) \neq 0. \] For $1 \leq j \leq d_i, y_{i,d_i-j}$ will stand for the ordinate of the point on the $\phi_i$-Newton polygon of $F$ with abscissa $d_i - j$.

With the above notations, in this chapter, we shall prove:

Theorem 5.1.1. Let $v$ be a real valuation of a field $K$. Let $F(x) \equiv \phi_1(x)^{\nu_1} \cdots \phi_r(x)^{\nu_r} \mod M_v$, $\phi_i(x), m_i, q_{i,j}(x)$ be as in Notation 5.5. Assume that $F(x)$ is irreducible over $K$ and has a root $\theta$. Then the set \[ \mathcal{B} = \{q_{i,j}(\theta)^{\nu_k} \mid 1 \leq i \leq r, 1 \leq j \leq \nu_i, 0 \leq k < m_i \} \] forms an $R_v$-basis of $R_v[\theta]$.

Theorem 5.1.2. Let $v$ be a discrete valuation of a field $K$ with value group $\mathbb{Z}$. Let $F(x) \equiv \phi_1(x)^{\nu_1} \cdots \phi_r(x)^{\nu_r} \mod M_v$ be a monic irreducible polynomial belonging to $R_v[x]$ with $\phi_i(x)$ as in Definition 5.4. If $i(F)$ is defined, then $i(F) \geq \sum_{j=1}^{r} i_{\phi_j}(F)$.

Theorem 5.1.3. Let $(K, v), F(x) \equiv \phi_1(x)^{\nu_1} \cdots \phi_r(x)^{\nu_r} \mod M_v$ be as in Theorem 5.1.2. Let $\theta$ be a root of $F(x)$ and $S$ be the integral closure of $R_v$ in $K(\theta)$. Let $m_i, q_{i,j}(x), y_{i,d_i-j}$ be as in Notation 5.5 and $\pi$ be a prime element of $R_v$. Let $z_{i,j}$
denote the greatest integer not exceeding \( y^{d_i-j} \). Assume that \( S \) is a free \( \mathbb{R}_v \)-module. Then the family 
\[
\mathcal{B}_1 = \left\{ \frac{g_{i,j}(\theta)\theta^k}{\pi^{i+i_j}} \mid 1 \leq i \leq n, 1 \leq j \leq d_i, 0 \leq k < m_i \right\}
\]
forms an \( \mathbb{R}_v \)-basis of \( S \) if and only if \( F(x) \) is weakly \( v \)-regular with respect to \( \phi_1, \ldots, \phi_r \).

**Theorem 5.1.4.** Let \( (K,v), F(x) \) and \( \phi_1(x), \ldots, \phi_r(x) \) be as in Theorem 5.1.2. If \( F(x) \) is separable and is \( v \)-regular with respect to \( \phi_1, \ldots, \phi_r \), then it is weakly \( v \)-regular with respect to \( \phi_1, \ldots, \phi_r \).

**Theorem 5.1.5.** Let \( v \) be a henselian discrete valuation of a field \( K \) with value group \( \mathbb{Z} \) and uniformizer \( \pi \). Let \( \phi(x), m, (\alpha, \delta), w_{\alpha, \delta}, \lambda \) and \( e \) be as in Lemma 2.2.1. Let \( F(x) \) belonging to \( K[x] \) be a monic polynomial of degree \( n \) which is a lifting of \( U(Y)^j \) of degree \( t \) with respect to \( \phi(x), \lambda \) and \( h = \pi^{\lambda \delta} \), where \( U(Y) \neq Y \) is a monic irreducible polynomial of degree \( d \) over \( \overline{K(\alpha)} \). Let \( \psi(x,Y) = \sum b_i(x)Y_i \) belonging to \( \mathbb{R}_v[x, Y] \) be such that \( b_d(x) = 1, \deg b_i(x) < m, \sum b_i(\alpha)Y^i = U(Y) \) and \( F^{(1)}(x) \in K[x] \) be the polynomial of degree less than \( n \) defined by

\[
F^{(1)}(x) = F(x) - \pi^{\delta \lambda} \left( \psi \left(x, \frac{\phi(x)^{\delta}}{\pi^{\lambda \delta}} \right)^j \right) = \sum c_j(x)\phi(x)^j, \deg c_j(x) < m. \tag{5.2}
\]

If \( s \) is the least index for which \( w_{\alpha, \delta}(F^{(1)}(x)) = w_{\alpha, \delta}(c_s(x)\phi(x)^s) \) and \( W(Z) \) denotes the \( w_{\alpha, \delta} \)-residue of \( \frac{F^{(1)}(x)}{c_s(x)\phi(x)^s} \), where \( Z \) is the \( w_{\alpha, \delta} \)-residue of \( \frac{\phi(x)^s}{\pi^{\lambda \delta}} \), then the following statements are equivalent:

(i) \( i(F) \) is defined and \( i(F) = i_{\phi}(F) \).

(ii) \( F(x) \) is irreducible over \( K \). If \( \theta \) is a root of \( F(x) \) and \( v' \) is the valuation of \( K(\theta) \) obtained by restricting \( \tilde{v} \) to \( K(\theta) \), then the set

\[
\mathcal{C} = \left\{ t \frac{\phi(\theta)^{j}}{\pi^{j \lambda}} \mid 0 \leq i \leq m - 1, 0 \leq j \leq et - 1 \right\}
\]

is an \( \mathbb{R}_v \)-basis of \( \mathbb{R}_v \); here \( [j \lambda] \) denotes the largest integer not exceeding \( j \lambda \).

(iii) \( F(x) \) is irreducible over \( K \). When \( \theta \) is a root of \( F(x) \) and \( v' \) is as in (ii), then
the index of ramification and the residual degree of \( v'/v \) are \( e_l, d_m \) respectively and
\[ v'\left( \psi \left( x, \frac{\phi(x)^e}{\pi^{e \lambda}} \right) \right) = \frac{1}{e l}. \]
(iv) Either \( l = 1 \) or \( l > 1, U(Y) \nmid W(Y) \) and \( w_{\alpha, \delta}(F^{(1)}(x)) = et\lambda + \frac{1}{e}. \)

**Theorem 5.1.6.** Let \((K, v)\) be a complete discrete valued field and \( \phi(x), m, (\alpha, \delta), \)
\( w_{\alpha, \delta}, \lambda, e \) and \( \pi \) be as in Theorem 5.1.5. Let \( F(x) \) belonging to \( K[x] \) be a polynomial
which is a lifting of the polynomial \( U_1(Y)^{l_1} \cdots U_r(Y)^{l_r} \) having degree \( t \) with respect
to \( \phi(x), \lambda \) and \( h = \pi^{e \lambda}, \) where \( U_i(Y) \neq Y \) are distinct monic irreducible polynomials
over \( K(\alpha) \). Let \( \psi_i(x, Y) \) be monic polynomials in \( Y \) belonging to \( R_\nu(x, Y) \) with
deg \( \psi_i(x, Y) < m \) such that \( \psi_i(\alpha, Y) = U_i(Y) \) for \( 1 \leq i \leq r. \) Let \( F^{(1)}(x) \) belonging
to \( K[x] \) be defined by
\[ F^{(1)}(x) = F(x) - \pi^{e \lambda} \left( \psi_1 \left( x, \frac{\phi(x)^e}{\pi^{e \lambda}} \right) \right)^{l_1} \cdots \left( \psi_r \left( x, \frac{\phi(x)^e}{\pi^{e \lambda}} \right) \right)^{l_r} = \sum c_i(x)\phi(x)^i. \]

If \( i_0 \) is the smallest non-negative integer such that \( w_{\alpha, \delta}(F^{(1)}(x)) = i_0\lambda + v(a_0) \) for
some \( a_0 \) belonging to \( K \) and \( W(Z) \) is the \( w_{\alpha, \delta}\) -residue of \( \frac{F^{(1)}(x)}{a_0\phi(x)^{i_0}} \) with \( Z \) as in
Theorem 5.1.5, then the following statements are equivalent:
(i) \( i(F) = i_0(F). \)
(ii) For each \( i, \) either \( l_i = 1 \) or \( l_i > 1, U_i(Y) \nmid W(Y) \) and \( w_{\alpha, \delta}(F^{(1)}(x)) = et\lambda + \frac{1}{e}. \)

It may be pointed out that Theorems 5.1.2, 5.1.4 extend the classical Theorem
of Index by Ore to arbitrary discrete valued fields. Theorem 5.1.1 besides being of
independent interest is used in the proof of Theorems 5.1.2, 5.1.3. Theorem 5.1.3
provides an \( R_\nu\)-basis of \( S \) when \( F(x) \) is weakly \( v\)-regular and extends Theorem 2.1
of [F-M-N]. In §5.5, Examples 5.5.4, 5.5.5 respectively point out an error each in
Criterion I on page 326 and in the Proposition on page 328 of [Mo-Na]. Theorems
5.1.5, 5.1.6 rectify these results and extend them to arbitrary complete discrete valued
fields. Theorem 5.1.5 can also be used to check the irreducibility of a polynomial
over a henselian discrete valued field as is done in Example 5.5.6.
5.2 Proof of Theorem 5.1.1

Lemma 5.2.1. Let \( v \) be a real valuation of a field \( K \). Let \( F(x) \equiv \phi_1(x)^{\nu_1} \cdots \phi_r(x)^{\nu_r} \mod M_v \) be as in Definition 5.4 and \( q_{i,j}(x), r_{i,j}(x), 1 \leq j \leq \nu_i \) be as in Notation 5.5. Then for every \( 1, 1 \leq l \leq r \), the highest power of \( \bar{\phi}_l(x) \) dividing \( \bar{q}_{i,j}(x) \) over \( R_v/M_v \) is \( \nu_l - j \) if \( l = i \) and \( \nu_l \) otherwise.

Proof. Let \( \sum_{j=0}^{d_i} A_{i,j}(x) \phi_l(x)^j, A_{i,j}(x) \neq 0 \) be the \( \phi_l(x) \) expansion of \( F(x) \). Then \( r_{i,j}(x) = A_{i,0}(x) + A_{i,1}(x) \phi_l(x) + \cdots + A_{i,j-1}(x) \phi_l(x)^{j-1} \) is the remainder obtained on dividing \( F(x) \) by \( \phi_l(x)^j \). Since \( F(x) \) is divisible by \( \bar{\phi}_l(x)^{\nu_l} \), it follows that for each pair \( (i, j) \), \( 1 \leq i \leq r, 1 \leq j \leq \nu_i \), \( r_{i,j}(x) = 0 \) and \( F(x) = (\bar{q}_{i,j}(x))^{\nu_l}(\bar{\phi}_l(x)^j) \). If \( \text{ord}_{\bar{\phi}_l}(\bar{q}_{i,j}(x)) \) denotes the highest exponent of \( \bar{\phi}_l(x) \) dividing \( \bar{q}_{i,j}(x) \), then it is clear that

\[
\nu_l = \text{ord}_{\bar{\phi}_l}(F(x)) = \text{ord}_{\bar{\phi}_l}(\bar{q}_{i,j}(x)) + j \text{ord}_{\bar{\phi}_l}(\bar{\phi}_l(x)).
\]

The above equality immediately proves the lemma because \( \text{ord}_{\bar{\phi}_l}(\bar{\phi}_l(x)) = 1 \) if \( i = l \) and \( 0 \) otherwise.

Proof of Theorem 5.1.1. We first prove that the family \( \mathcal{P} = \{q_{i,j}(x)x^k \mid 1 \leq i \leq r, 1 \leq j \leq \nu_i, 0 \leq k < m_i \} \) of polynomials belonging to \( \bar{K}[x] \) is linearly independent over \( \bar{K} = R_v/M_v \). Suppose that \( a_{i,j,k} \) are elements of \( R_v \) satisfying

\[
\sum_{i,j,k} a_{i,j,k} \bar{q}_{i,j}(x)x^k = 0 \quad (5.3)
\]

Define \( B_{i,j}(x) = \sum_{0 \leq k < m_i} a_{i,j,k} q_{i,j}(x)x^k \). Since \( q_{i,j}(x) \) are monic polynomials in \( R_v[x] \), \( \bar{B}_{i,j}(x) = 0 \) if and only if \( \bar{a}_{i,j,k} = 0 \) for \( 0 \leq k < m_i \). So the above assertion is proved once we show that \( \bar{B}_{i,j}(x) = 0 \) for every \( i, j \). We can rewrite (5.3) as

\[
\sum_{i,j} \bar{B}_{i,j}(x) = 0. \quad (5.4)
\]

\(^2\)The idea of the proof of this theorem has been taken from the proof of Theorem 2.1 of [F-M-N] proved for \( p \)-integral basis of number fields.
Suppose to the contrary that there exists an index \( l \) and a maximal index \( m, 1 \leq m \leq \nu_l \) such that \( \overline{B}_{l,m}(x) \neq \overline{0}, \overline{B}_{i,j}(x) = \overline{0} \) for \( j > m \). Rewrite (5.4) as

\[
-\overline{B}_{l,m}(x) = \sum_{i \neq l, 1 \leq j \leq \nu_l} \overline{B}_{i,j}(x) + \sum_{j \leq m-1} \overline{B}_{l,j}(x) . \tag{5.5}
\]

By definition \( \overline{B}_{i,j}(x) = \overline{q}_{i,j}(x)( \sum_{0 \leq k \leq m_i} \overline{a}_{i,j,k}x^k) \). Applying Lemma 5.2.1, we see that \( \text{ord}_{\overline{q}_{l,m}(x)} = \nu_l - m \) and that \( \text{ord}_{\overline{q}_{i,j}(x)} \) of each term on the right hand side of (5.5) is greater than or equal to \( \nu_l - m + 1 \). This contradiction proves that the family \( \mathcal{P} \) is linearly independent over \( \overline{K} \).

To prove the theorem we have to show that the transition matrix from \( \{1, \theta, \ldots, \theta^{n-1}\} \) to \( \mathcal{B} \) is invertible over \( R_v \). Rename the elements of \( \mathcal{B} \) as \( w_1, \ldots, w_n \). Let \( A \) denote the matrix over \( R_v \) such that \( [w_1, \ldots, w_n] = [1, \theta, \ldots, \theta^{n-1}]A \). Now suppose to the contrary that \( e(\det(A)) > 0 \). So there exists a non-zero vector \( [c_1, \ldots, c_n] \) with entries in \( R_v/M_v \) such that \( [c_1, \ldots, c_n]A^T = [0, \ldots, 0] \). Write \( [c_1, \ldots, c_n]A^T = [d_0, \ldots, d_{n-1}] \), then \( d_i \) belongs to \( M_v \) for every \( i \). Note that \( \sum_{i=1}^n c_iw_i = d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1} \). Rename \( c_1, \ldots, c_n \) as \( c_{i,j,k}, 1 \leq i \leq r, 1 \leq j \leq \nu_i, 0 \leq k < m_i \), so that

\[
\sum_{i=1}^n c_iw_i = \sum_{i,j,k} c_{i,j,k}q_{i,j}(\theta)\theta^k = d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1} .
\]

As \( \deg q_{i,j}(x)x^k < n \) for all triples \( (i,j,k) \) in the theorem, the above equation holds only when \( \sum_{i,j,k} c_{i,j,k}q_{i,j}(\theta)x^k = d_0 + d_1x + \cdots + d_{n-1}x^{n-1} \) which implies that

\[
\sum_{i,j,k} \overline{c}_{i,j,k}q_{i,j}(x)x^k = \overline{0} \quad \text{as} \quad d_i \in M_v .
\]

Since at least one \( c_{i,j,k} \) is a unit, this contradicts the linear independence of \( \mathcal{P} \) over \( R_v/M_v \) and hence the theorem is proved.

### 5.3 Proof of Theorems 5.1.2, 5.1.3

**Lemma 5.3.1.** Let \( v \) be a real valuation of a field \( K \) with valuation ring \( R_v \). Let \( \phi(x) \) belonging to \( R_v[x] \) be a monic polynomial such that \( \overline{\phi}(x) \) is irreducible over \( \overline{K} \).
the residue field of \( \nu \) and \( F(x) \) belonging to \( R_{\nu}[x] \) be a monic polynomial with \( \phi(x) \)-expansion \( \sum_{i=0}^{d} A_i(x)\phi(x)^i, A_0(x)A_d(x) \neq 0 \). Let \( S_1, \ldots, S_d \) be the sides of positive slopes of the \( \phi \)-Newton polygon of \( F(x) \) with slopes \( \lambda_1 < \ldots < \lambda_d \) respectively. If for any integer \( j, 0 \leq j \leq d, s_j \) is the smallest index such that the projection of the side \( S_{s_j} \) to the \( x \)-axis contains \( j \), then for any index \( k, 0 \leq k \leq u, y_k \geq y_j + \lambda_{s_j}(k - j) \), where \( y_j \) is the ordinate of the point with abscissa \( j \) lying on the \( \phi \)-Newton polygon of \( F(x) \).

**Proof.** In view of the convexity of the \( \phi \)-Newton polygon of \( F(x) \), it is clear that when \( j < k \), then the slope of the line segment joining \( (j, y_j) \) to \( (k, y_k) \) is greater than or equal to \( \lambda_{s_j}, \) i.e., \( \frac{y_k - y_j}{k - j} \geq \lambda_{s_j} \) as asserted. When \( j > k \), the slope of the line segment joining \( (k, y_k) \) to \( (j, y_j) \) is less than or equal to \( \lambda_{s_j} \) which also gives the desired inequality.

**Proposition 5.3.2.** Let \( (K, \nu), F(x) \equiv \phi_1(x)^{\nu_1} \cdots \phi_r(x)^{\nu_r} \mod M_\nu \) be as in Definition 5.4 and \( \theta \) be a root of \( F(x) \). Fix any \( \phi_i(x) \) and call it \( \phi(x) \). Let \( \sum_{i=0}^{d} A_i(x)\phi(x)^i \) be the \( \phi(x) \)-expansion of \( F(x) \) with \( A_d(x) \neq 0 \). If \( q_j(x) \) denotes the quotient obtained on dividing \( F(x) \) by \( \phi(x)^j \) and \( y_{d-j} \) denotes the ordinate of the point with abscissa \( d - j \) on the \( \phi \)-Newton polygon of \( F(x) \), then for any prolongation \( w \) of \( \nu \) to \( K(\theta) \), \( w(q_j(\theta)) \geq y_{d-j} \).

**Proof.** By the definition of the \( \phi \)-Newton polygon of \( F(x) \), it is clear that the point \( (d - i, v^\nu(A_i(x))) \) lies on or above it when \( v^\nu(A_i(x)) \neq 0 \). Therefore

\[
v^\nu(A_i(x)) \geq y_{d-i}, 0 \leq i \leq d. \tag{5.6}\]

Since \( \theta \) is integral over \( R_{\nu}, w(\theta) \geq 0 \). Hence in view of (5.6), we have

\[
w(A_i(\theta)) \geq v^\nu(A_i(x)) \geq y_{d-i}. \tag{5.7}\]
As \( q_j(x) = A_j(x) + A_{j+1}(x)\phi(x) + \cdots + A_d(x)\phi(x)^{d-j} \), it follows from (5.7) that
\[
 w(q_j(\theta)) \geq \min_{i \geq j} \{ w(A_i(\theta)\phi(\theta)^{j-i}) \} \geq \min_{i \geq 0} \{ y_{d-i} + (j-i)w(\phi(\theta)) \} \tag{5.8}
\]
We split the proof into two cases.

Case I. \( w(\phi(\theta)) = 0 \). In this case, it is clear from (5.8) that \( w(q_j(\theta)) \geq y_{d-j} \); the last equality holds because the slopes of the segments of the \( \phi \)-Newton polygon of \( F(x) \) are increasing from the initial point \((0, 0)\) to the terminal point \((d, w^*(A_d(x)))\).

Case II. \( w(\phi(\theta)) > 0 \). In this case applying Hensel’s Lemma and Theorem 2.1.1(ii), we see that \( w(\phi(\theta)) \) is the slope of a side of the \( \phi \)-Newton polygon of \( F(x) \), say \( w(\phi(\theta)) = \lambda_0 \). We retain the notation \( s_j \) introduced in Lemma 5.3.1 and split this case into two subcases.

Subcase (i). \( \lambda_0 \geq s_{d-j} \). In this situation, it follows from (5.8) that
\[
w(q_j(\theta)) \geq \min_{i \geq j} \{ y_{d-i} + (j-i)\lambda_0 \} = y_{d-k} + (k-j)\lambda_0 \tag{5.9}
\]
Applying Lemma 5.3.1 (with \( j \) and \( k \) replaced by \( d-j \) and \( d-k \) respectively), we see that
\[
w(q_j(\theta)) \geq y_{d-k} + (k-j)\lambda_0 \geq y_{d-j} + \lambda_{s_{d-j}}(j-k) + (k-j)\lambda_0.
\tag{5.9}
\]
In this subcase, \( \lambda_0 \geq s_{d-j} \), which implies that \( \lambda_0 \geq \lambda_{s_{d-j}} \). As \( k \geq j \), it now follows from (5.9) that \( w(q_j(\theta)) \geq y_{d-j} \).

Subcase (ii). \( \lambda_0 < s_{d-j} \). Recall that \( F(x) = q_j(x)\phi(x)^j + r_j(x) \), where \( r_j(x) = A_0(x) + A_1(x)\phi(x) + \cdots + A_{j-1}(x)\phi(x)^{j-1} \) and \( \theta \) is a root of \( F(x) \). So
\[
w(q_j(\theta)) + j\lambda_0 = w(r_j(\theta)).
\tag{5.10}
\]
Using (5.7), we see that
\[
w(r_j(\theta)) \geq \min_{0 \leq i \leq j-1} \{ w(A_i(\theta)\phi(\theta)^i) \} \geq \min_{0 \leq i \leq j-1} \{ y_{d-i} + i\lambda_0 \} = y_{d-k} + k\lambda_0 \tag{5.11}
\]
70
for some index \( k \). On applying Lemma 5.3.1 (with \( j \) and \( k \) replaced by \( d - j \) and \( d - k \) respectively), we obtain
\[
y_{d-k} \geq y_{d-j} + \lambda_{d-j}(j - k).
\]
This inequality together with (5.10) and (5.11) shows that
\[
w(q_j(\theta)) = w(r_j(\theta)) - j\lambda_0 \geq y_{d-j} + \lambda_{d-j}(j - k) + (k - j)\lambda_0.
\]
In the present subcase \( i_0 < s_{d-j} \) and hence \( \lambda_{i_0} \leq \lambda_{s_{d-j}} \). As \( k < j \), the above inequality gives \( w(q_j(\theta)) \geq y_{d-j} \).

**Proof of Theorems 5.1.2, 5.1.3.** Let \( \mathfrak{B} \) be as in Theorem 5.1.1 and \( M, M_1 \) denote respectively the \( R_v \)-modules with basis \( \mathfrak{B}, \mathfrak{B}_1 \). Arrange the elements of \( \mathfrak{B}, \mathfrak{B}_1 \) in increasing degrees of \( \theta \). Then the transition matrix from \( \mathfrak{B}_1 \) to \( \mathfrak{B} \) is a diagonal matrix with diagonal entries \( \pi^{i_0} \), each such entry repeated \( m_i \) times. Recall that by Theorem 5.1.1, \( M = R_v[\theta] \). So by Proposition 5.3.2, \( R_v[\theta] = M \subseteq M_1 \subseteq S \). Let \( \mu \) denote the \( v \)-valuation of the determinant of the transition matrix from an \( R_v \)-basis of \( S \) to \( \mathfrak{B}_1 \). Then \( i(F) = v \)-valuation of the determinant of the transition matrix from an \( R_v \)-basis of \( S \) to \( \mathfrak{B} \) is given by
\[
i(F) = \mu + \sum_i m_i \left( \sum_j z_{i,j} \right) = \mu + \sum_i i_{\phi_i}(F).
\]
Since \( \mu \geq 0 \), Theorem 5.1.2 is proved. Clearly \( \mathfrak{B}_1 \) is a basis of \( S \) if and only if \( \mu = 0 \), which in view of (5.12) holds if and only if \( i(F) = \sum_i i_{\phi_i}(F) \).

**5.4 Proof of Theorem 5.1.4**

For a valued field extension \((L, w)/(K, v)\), a subset \( \{x_i \mid i \in I\} \) of \( L \) is said to be valuation independent over \((K, v)\) if \( w(\sum_{i \in I} c_i x_i) = \min_{i \in I} \{w(c_i x_i)\} \) for every choice of coefficients \( c_i \in K \), only finitely many of them being non-zero. Note that if a set is valuation independent over \((K, v)\), then it is linearly independent over \( K \). The following basic result is well known (cf. [En-Pr, Lemma 3.2.2], [Kuhl, Lemma 2.6]).
Lemma 5.4.A. Let $v$ be a valuation of a field $K$ with value group $G_v$ and $w$ be a prolongation of $v$ to a finite extension $L$ of $K$. If $x_1, \ldots, x_r$ are elements of $L$ such that the cosets $w(x_i) + G_v$ are distinct and $y_1, \ldots, y_s$ in the valuation ring of $w$ are such that their $w$-residues are linearly independent over the residue field of $v$, then the set $\{x_iy_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$ is valuation independent over $(K, v)$.

Notation. In what follows, for a real number $p$, $[p]$ will stand for the greatest integer not exceeding $p$. For polynomials $f(x), g(x)$ belonging to $K[x], r(f, g)$ will stand for the $v$-valuation of the resultant of $f(x)$ and $g(x)$.

We retain the notations of Theorem 1.1.A, Definition 1.4 of the first chapter and prove some preliminary results.

Lemma 5.4.1. Let $v$ be a henselian discrete valuation of a field $K$ with value group $\mathbb{Z}$ and uniformizer $\pi$. Let $\phi(x), m, (\alpha, \delta), \lambda$ and $e$ be as in Lemma 2.2.1. Let $F(x)$ belonging to $K[x]$ be a polynomial which is a lifting of a monic irreducible polynomial $T(Y) \neq Y$ belonging to $\overline{K(\alpha)}[Y]$ with respect to $\phi(x), \lambda$ and $h(x)$. Then $i(F)$ is defined and equals $i_\phi(F)$.

Proof. Let $t$ denote the degree of $T(Y)$. The polynomial $F(x)$ being a lifting of an irreducible polynomial $T(Y)$ is irreducible over $K$ by virtue of [Kh-Sal, Theorem 2.2]. Let $\tilde{\theta}$ be a root of $F(x)$ with $\tilde{v}(\tilde{\theta} - \alpha) = \delta$; this is possible in view of Theorem 2.2.6. Set $\xi = \frac{\phi(\tilde{\theta})^\nu}{\pi e \lambda}$. Let $v'$ denote the prolongation of $v$ to $K(\tilde{\theta})$. By Theorem 2.2.6, $v'(\phi(\tilde{\theta})) = \lambda$ and $\frac{\phi(\tilde{\theta})^r}{h(\alpha)}$ is a root of $T(Y)$. So $\tilde{\xi}$ is a root of the irreducible polynomial $T\left(\frac{\phi(\tilde{\theta})^r}{h(\alpha)}Y\right) \in \overline{K(\alpha)}[Y]$. Keeping in mind that $\tilde{\theta} = \alpha$, it now follows that the set $\{\tilde{\theta}^i \xi^k \mid 0 \leq i \leq m - 1, 0 \leq k \leq t - 1\}$ is linearly independent over $R_v/M_v$. As $e$ is the smallest positive integer for which $e\lambda \in \mathbb{Z}$, the $v'$-valuation of the elements $\frac{\phi(\tilde{\theta})^j}{\pi^j \lambda}$ for $0 \leq j \leq e - 1$ lie in different cosets modulo $\mathbb{Z}$. Therefore in
view of Lemma 5.4.1, the set
\[ D = \left\{ \theta^j \left( \frac{\phi(\theta)^i}{\pi^{j\lambda}} \right)^k \mid 0 \leq i \leq m - 1, 0 \leq j \leq e - 1, 0 \leq k \leq t - 1 \right\} \]
is valuation independent over \((K, v)\). Since the \(v'\)-valuation of each element of \(D\) is less than 1, it follows that the elements of \(D\) form an \(R_v\)-basis of \(R_{v'}\). So \(i(F)\) is defined. We arrange the elements of \(D\) according to increasing degrees in \(\theta\), i.e., according to the lexicographic ordering on tuples \((k, j, i)\). Then the transition matrix from \(\{1, \theta, \ldots, \theta^{m-1}\}\) to \(D\) is a block triangular matrix with \(et\) blocks down the main diagonal, each block is a scalar matrix of order \(m \times m\) and the \(j\)th block down the main diagonal is a scalar matrix with each diagonal entry \(\pi^{-[j-1]\lambda}\). Therefore the \(v\)-valuation of the determinant of the transition matrix from \(\{1, \theta, \ldots, \theta^{m-1}\}\) to \(D\) is
\[-m \sum_{j=1}^{\eta t - 1} [j\lambda].\]
Since \(D\) is an \(R_{v'}\)-basis of \(R_{v'}\), it follows that \(i(F) = m \sum_{j=1}^{\eta t - 1} [j\lambda]\). Recall that by Lemma 2.2.1, the \(\phi\)-Newton polygon of \(F(x)\) is the straight line segment joining \((0, 0)\) to \((et, et\lambda)\). Therefore \(i_\phi(F) = m \sum_{j=1}^{\eta t - 1} [j\lambda] = i(F)\).

**Lemma 5.4.2.** Let \(v\) be a henselian real valuation of a field \(K\). Let \(\phi(x), m, (\alpha, \delta), \lambda\) and \(e\) be as in the above lemma. If \(F_1(x), F_2(x)\) belonging to \(K[x]\) are respectively the liftings with respect to \(\phi(x), \lambda\) and \(h(x)\) of two coprime monic polynomials \(T_1(Y), T_2(Y)\) belonging to \(K(\alpha)[Y]\) and not divisible by \(Y\), then \(i_\phi(F_1F_2) = i_\phi(F_1) + i_\phi(F_2) + t(F_1, F_2)\).

**Proof.** In view of Lemma 2.2.1, the \(\phi\)-Newton polygon of \(F_i(x), i = 1, 2\) is the line segment joining \((0, 0)\) to \((et, et\lambda)\) and that of \(F_1(x)F_2(x)\) is the line segment joining \((0, 0)\) to \((e(t_1 + t_2), e(t_1 + t_2)\lambda)\). Therefore
\[ i_\phi(F_1) = m \sum_{j=1}^{et_1 - 1} [j\lambda], i_\phi(F_2) = m \sum_{j=1}^{et_2 - 1} [j\lambda] \]
and a simple calculation shows that
\[ i_\phi(F_1F_2) = m \sum_{j=1}^{et_1 + et_2 - 1} [j\lambda] = m \sum_{j=1}^{et_1 - 1} [j\lambda] + m \sum_{j=et_1}^{et_1 + et_2 - 1} [j\lambda] = i_\phi(F_1) + i_\phi(F_2) + e^2m t_1 t_2 \lambda.\]
The lemma follows from the above equation once we show that

\[ r(F_1, F_2) = e^{2mt_1 t_2 \lambda}. \] (5.13)

We first show that for any roots \( \theta'_1 \) and \( \theta'_2 \) of \( F_1(x), F_2(x) \) respectively

\[ \hat{v}(\theta'_1 - \theta'_2) \leq \delta. \] (5.14)

Suppose to the contrary that \( \hat{v}(\theta'_1 - \theta'_2) > \delta \) for some roots \( \theta'_1, \theta'_2 \) of \( F_1(x), F_2(x) \) respectively. By Theorem 2.2.6, there exists a \( K \)-conjugate (say) \( \sigma(\theta'_1) \) of \( \theta'_1 \) such that \( \hat{v}(\sigma(\theta'_1) - \alpha) = \delta \). Since \( (K, v) \) is henselian, \( \hat{v}(\sigma(\theta'_1) - \sigma(\theta'_2)) = \hat{v}(\theta'_1 - \theta'_2) > \delta \). Consequently, \( \hat{v}(\sigma(\theta'_2) - \alpha) = \delta \). Replacing \( \theta'_1, \theta'_2 \) by \( \sigma(\theta'_1), \sigma(\theta'_2) \) respectively, we may assume without loss of generality that \( \hat{v}(\theta'_1 - \alpha) = \delta = \hat{v}(\theta'_2 - \alpha) \). Then \( \phi(\theta'_1) = \prod_{\alpha'}(\theta'_1 - \alpha')/\prod_{\alpha'}(\theta'_2 - \alpha' + \theta'_1 - \theta'_2) = \phi(\theta'_2)(1 + b) \) for some \( b \in \bar{K} \) with \( \hat{v}(b) > 0 \).

So \( \phi(\theta'_1)^{\hat{v}}/h(\alpha) = \phi(\theta'_2)^{\hat{v}}/h(\alpha) \) and \( \phi(\theta'_2)^{\hat{v}}/h(\alpha) \). This is a contradiction because in view of Theorem 2.2.6, \( \phi(\theta'_1)^{\hat{v}}/h(\alpha) \) and \( \phi(\theta'_2)^{\hat{v}}/h(\alpha) \) are respectively the roots of \( T_1(Y), T_2(Y) \) which are given to be coprime. This proves (5.14).

Since \( r(F_1, F_2) = \sum_{\theta'_1} \hat{v}(F_2(\theta'_1)) \), the desired equality (5.13) is proved once we show that for each root \( \theta'_1 \) of \( F_1(x) \)

\[ \hat{v}(F_2(\theta'_1)) = e^{t_2 \delta \lambda}. \] (5.15)

Fix a root \( \theta'_1 \) of \( F_1(x) \). By Theorem 2.2.6(v), there exists a \( K \)-conjugate \( \theta_1 \) of \( \theta'_1 \) such that \( \hat{v}(\theta_1 - \alpha) = \delta \). Note that if \( \theta'_2 \) is any root of \( F_2(x) \), then \( \hat{v}(\theta'_2 - \alpha) \leq \delta \) by Theorem 2.2.6(i) and \( \hat{v}(\theta_1 - \theta'_2) \leq \delta \) by (5.14). Therefore

\[ \hat{v}(\theta_1 - \theta'_2) = \min\{\hat{v}(\theta_1 - \alpha), \hat{v}(\alpha - \theta'_2)\} = \hat{v}(\alpha - \theta'_2); \]

consequently

\[ \hat{v}(F_2(\theta'_1)) = \hat{v}(F_2(\theta_1)) = \hat{v}(F_2(\alpha)). \]
The desired equality (5.15) now follows, for if \( \phi(x)^{et_2+1}+B_{et_2-1}(x)\phi(x)^{et_2-1}+\cdots+B_0(x) \) is the \( \phi(x) \)-expansion of \( F_2(x) \), then \( F_2(\alpha) = B_0(\alpha) \) and \( \tilde{\nu}(B_0(\alpha)) = et_2\lambda \) in view of the definition of lifting and the fact that \( T_2(Y) \) is not divisible by \( Y \).

**Lemma 5.4.3.** Let \( (K, v), \phi(x), m \) and \( \alpha \) be as in the above lemma. Let \( T(Y) \) belonging to \( K(\alpha)[Y] \) be a monic polynomial of degree \( t \) not divisible by \( Y \). If \( F_1(x), F_2(x) \) are liftings of \( T(Y) \) with respect to \( \phi(x), \lambda_1 \) and \( \phi(x), \lambda_2 \) respectively with \( \lambda_1 < \lambda_2 \), then \( i_\phi(F_1F_2) = i_\phi(F_1) + i_\phi(F_2) + r(F_1, F_2) \).

**Proof.** Let \( e_1, e_2 \) be the smallest positive integers such that \( e_1\lambda_1 \in \mathbb{Z} \) and \( e_2\lambda_2 \in \mathbb{Z} \). Applying Lemmas 2.2.4 and 2.2.1, we see that the \( \phi \)-Newton polygon of \( F_1(x)F_2(x) \) consists of two line segments, first from \((0,0)\) to \((e_1t, e_1t\lambda_1)\) and the other joining \((e_1t, e_1t\lambda_1)\) to \((e_1t + e_2t, e_1t\lambda_1 + e_2t\lambda_2)\). Therefore

\[
i_\phi(F_1F_2) = m \sum_{j=1}^{e_1t-1} [j\lambda_1] + m \left( \sum_{j=e_1t}^{e_1t+e_2t-1} [e_1t\lambda_1 + j\lambda_2 - e_1t\lambda_2] \right)
= m \sum_{j=1}^{e_1t-1} [j\lambda_1] + me_1t\lambda_1(e_2t) + m \sum_{j=e_1t+1}^{e_1t+e_2t-1} [j\lambda_2 - e_1t\lambda_2]
= i_\phi(F_1) + e_1e_2mt^2\lambda_1 + i_\phi(F_2).
\]

So the lemma is proved once we show that for each root \( \theta'_2 \) of \( F_2(x) \)

\[
\tilde{\nu}(F_1(\theta'_2)) = e_1t\lambda_1.
\] (5.16)

We first verify that

\[
\delta_1 < \delta_2.
\] (5.17)

Write \( \phi(x) = \sum_{i=1}^{m} c_i(x - \alpha)^i \), then by virtue of (1.3),

\[
w_{\alpha, \delta_1}(\phi(x)) = \min_{1 \leq i \leq m} \{ \tilde{\nu}(c_i) + i\delta_1 \} = \lambda_1
\]

which implies that \( \delta_1 = \max_{1 \leq i \leq m} \left\{ \frac{\lambda_1 - \tilde{\nu}(c_i)}{i} \right\} \). Similarly \( \delta_2 = \max_{1 \leq i \leq m} \left\{ \frac{\lambda_2 - \tilde{\nu}(c_i)}{i} \right\} \). As \( \lambda_1 < \lambda_2 \), (5.17) follows. Fix a root \( \theta'_2 \) of \( F_2(x) \), then there exists a \( K \)-conjugate.
\( \theta_2 \) of \( \theta'_2 \) with \( \check{v}(\theta_2 - \alpha) = \delta_2 \) (cf. Theorem 2.2.6(v)). For any root \( \theta'_1 \) of \( F_1(x) \), \( \check{v}(\theta'_1 - \alpha) \leq \delta_1 \); consequently using (5.17), we have

\[
\check{v}(\theta'_1 - \theta_2) = \min \{ \check{v}(\theta_2 - \alpha), \check{v}(\alpha - \theta'_1) \} = \min \{ \delta_2, \check{v}(\alpha - \theta'_1) \} = \check{v}(\alpha - \theta'_1).
\]

Hence \( \check{v}(F_1(\theta'_2)) = \check{v}(F_1(\theta_2)) = \check{v}(F_1(\alpha)) \). The desired equality (5.16) is now proved as \( \check{v}(F_1(\alpha)) = e_1 t \lambda_1 \) because \( F_1(x) \) is a lifting of \( T_1(Y) \) not divisible by \( Y \).

**Proof of Theorem 5.1.** Let \( \hat{(K, v)} \) denote the completion of \((K, v)\) and \( \alpha_i \) be a root of \( \phi_i(x) \). By virtue of Hensel’s Lemma, there exist monic polynomials \( F_i(x) \) belonging to \( R_v[x] \) with \( \hat{F}_i(x) = \hat{\phi}_i(x)^{n_i} \) such that \( F(x) = F_1(x) \cdots F_r(x) \). Keeping in mind Remark 5.3 and equation (5.1) holding for polynomials which are not necessarily irreducible together with the fact that \( \hat{F}_i(x), \hat{F}_j(x) \) are coprime for \( i \neq j \), we see that \( i(F) = \sum_{j=1}^{r} i(F_j) \).

Suppose that the \( \phi_i \)-Newton polygon of \( F_i(x) \) has \( n_i \) sides with positive slopes \( \lambda_{i1} < \cdots < \lambda_{i n_i} \). By Theorem 2.1.1(iii), we can write \( F_i(x) = \prod_{j=1}^{n_i} F_{ij}(x) \), where \( F_{ij}(x) \) belonging to \( \hat{K}[x] \) is a lifting of a polynomial \( T_{ij}(Y) \) belonging to \( \hat{K}(\alpha_i)[Y] \) with respect to \( \phi_i(x), \lambda_{ij} \). As \( F_i(x) \) is \( v \)-regular with respect to \( \phi_i(x) \), the polynomial \( T_{ij}(Y) \) is a product of distinct monic irreducible polynomials over \( \hat{K}(\alpha_i) \) for each pair \( (i, j), 1 \leq i \leq r, 1 \leq j \leq n_i \). Fix a pair \( (i, j) \) and write \( T_{ij}(Y) = \prod_k U_{ijk}(Y) \) as a product of distinct monic irreducible polynomials over \( \hat{K}(\alpha_i) \). In view of Theorem 2.1.1(iv), we can write \( F_{ij}(x) = \prod_k G_{ijk}(x) \), where \( G_{ijk}(x) \) belonging to \( \hat{K}[x] \) is a lifting of \( U_{ijk}(Y) \) with respect to \( \phi_i, \lambda_{ij} \). By Lemma 5.4.1, \( i(G_{ijk}) \) is defined and equals \( i_{\phi_i}(G_{ijk}) \). Since \( F_i(x) = \prod_{j,k} G_{ijk}(x) \), it follows from Lemmas 5.4.2, 5.4.3 that

\[
i(F_i) = i_{\phi_i}(F_i), \quad 1 \leq i \leq r.
\]

By virtue of Lemma 2.2.4, the \( \phi_i \)-Newton polygon of \( F(x) \) is a horizontal line segment.
followed by a translate of the $\phi$-Newton polygon of $F_i(x)$; consequently

$$i_{\phi_i}(F) = i_{\phi_i}(F_i).$$  \hfill (5.19)

Combining (5.18), (5.19) with what has been proved in the first paragraph, we conclude that

$$i(F) = \sum_{i=1}^{r} i(F_i) = \sum_{i=1}^{r} i_{\phi_i}(F_i) = \sum_{i=1}^{r} i_{\phi_i}(F).$$

This proves the theorem.

### 5.5 Proof of Theorems 5.1.5, 5.1.6

The following two propositions which are proved for arbitrary rank valuations will be used in the proof of Theorem 5.1.5; these are of independent interest as well.

**Proposition 5.5.1.** Let $(K, v)$ be a henselian valued field of arbitrary rank with valuation group $G_v$ and $\phi(x), m, (\alpha, \delta, \lambda)$ and $e$ be as in Lemma 2.2.1. Let $F(x)$ belonging to $K[x]$ be a monic polynomial having a root $\theta$ which is a lifting of a power of a monic irreducible polynomial $U(Y) \neq Y$ over $K(\alpha)$ with respect to $\phi(x), \lambda$ and $h(x)$ with $h(x) \in K[x]$ of degree less than $m$ such that $v(h(\alpha)) = e\lambda$. Let $G(x)$ belonging to $K[x]$ be a polynomial having $\phi(x)$-expansion $\sum G_i(x)\phi(x)^i$ with $j$ as the least index for which $w_{\alpha, \delta}(G(x)) = w_{\alpha, \delta}(G_j(x)\phi(x)^i).$ Let $Z$ denote the $w_{\alpha, \delta}$-residue of $h(x)$ and $W(Z)$ belonging to $K[\alpha][Z]$ be the $w_{\alpha, \delta}$-residue of $G(x)/G_j(x)\phi(x)^i.$ If $W(Y)$ is divisible by $U(Y)$, then $\hat{v}(G(\theta)) > w_{\alpha, \delta}(G(x)).$

**Proof.** In view of Theorem 2.2.6(v), replacing $\theta$ by its $K$-conjugate, we may assume that $\hat{v}(\theta - \alpha) = \delta.$ So by Lemma 3.2.1, for any polynomial $A(x) \in K[x]$ of degree strictly less than $m$, one has

$$\hat{v}(A(\theta)) = \hat{v}(A(\alpha)) = v^\sigma(A(x)).$$ \hfill (5.20)
Recall that $v(\phi(\theta)) = \lambda$ by Theorem 2.2.6(iii). Keeping in mind (5.20), Theorem 1.1.A, for any polynomial $H(x)$ belonging to $K[x]$ with $\phi(x)$-expansion $\sum_i H_i(x)\phi(x)^i$, we have

$$v(H(\theta)) \geq \min_i \{v(H_i(\theta)) + i\lambda\} = \min_i \{\psi^x(H_i(x)) + i\lambda\} = w_{a,\delta}(H(x)). \quad (5.21)$$

Write $W(Y) = U(Y)D(Y)$ for some $D(Y)$ belonging to $K(\alpha)[Y]$. Let $\psi(x, Y)$ belonging to $R_{\psi}[x, Y]$ be as in Theorem 5.1.5 and choose $D_1(x, Y) \in R_\psi[x, Y]$ such that $D_1(\overline{\alpha}, (\phi(x)^r_h)) = D(Z)$. The equality $W(Z) = U(Z)D(Z)$ implies that

$$w_{a,\delta}\left(\frac{G(x)}{G_j(x)\phi(x)^j}\psi\left(x, \frac{\phi(x)^r_h}{h}\right)D_1\left(x, \frac{\phi(x)^r_h}{h}\right)\right) > 0,$$

i.e.,

$$w_{a,\delta}\left(G(x) - G_j(x)\phi(x)^j\psi\left(x, \frac{\phi(x)^r_h}{h}\right)D_1\left(x, \frac{\phi(x)^r_h}{h}\right)\right) > w_{a,\delta}(G(x)).$$

Denote $\phi(\theta)^r_h(\theta)$ by $\eta$. In view of (5.21), the above inequality implies that

$$v(G(\theta) - G_j(\theta)\phi(\theta)^j\psi(\theta, \eta)D_1(\theta, \eta)) > w_{a,\delta}(G(x)). \quad (5.22)$$

By virtue of (5.20), $\tilde{v}(G_j(\theta)\phi(\theta)^j) = v^x(G_j(x)) + j\lambda = w_{a,\delta}(G(x))$. Also in view of Lemma 2.2.B(ii), $\tilde{\eta} = \left(\frac{\phi(\theta)^r_h}{h(\alpha)}\right)$, which is a root of $\tilde{v}(\tilde{\alpha}, Y) = U(Y)$ by Theorem 2.2.6(iv). So $\tilde{v}(\psi(\theta, \eta)) > 0$. As $\tilde{v}(D_1(\theta, \eta)) \geq 0$, the desired inequality now follows from (5.22) and the triangle inequality.

**Remark.** As shown in the fourth chapter, the converse of the above proposition is also true, i.e., if $\tilde{v}(G(\theta)) > w_{a,\delta}(G(x))$, then $U(Y)$ divides $W(Y)$ (see Proposition 4.2.1).

**Corollary 5.5.2.** Let $v$ be a henselian real valuation of a field $K$ with $\phi(x), m, (\alpha, \delta), w_{a,\delta}, \lambda, e$ as in the Proposition 5.5.1 and $U(Y)$ belonging to $K(\alpha)[Y]$ be a monic irreducible polynomial. If $F_1(x), F_2(x)$ are liftings of $U(Y)^{i_1}, U(Y)^{i_2}$ with respect to $\phi(x), \lambda$ respectively, then $i_\phi(F_1) < i_\phi(F_1) + i_\phi(F_2) + r(F_1, F_2)$. 78
Proof. Denote \( dl_1 \) by \( t_1 \) and \( dl_2 \) by \( t_2 \). Then
\[
i_\varphi(F_1 F_2) = m \sum_{j=1}^{e_t_1 + e_t_2 - 1} |j\lambda| = i_\varphi(F_1) + e^2 m t_1 t_2 \lambda + i_\varphi(F_2).
\]
Thus the corollary is proved once we show that
\[
r(F_1, F_2) = \sum_{\theta_i} \hat{v}(F_2(\theta_i)) > e^2 m t_1 t_2 \lambda,
\]
where \( \theta_i \) runs over roots of \( F_1(x) \). Fix a root \( \theta_1 \) of \( F_1(x) \). Applying Proposition 2.2.A (with \( F(x) \) and \( G(x) \) replaced by \( F_1(x) \) and \( F_2(x) \) respectively), we see that
\[
\hat{v}(F_2(\theta_1)) > w_{\alpha, \delta}(F_2(x)) = e \lambda t_2 \lambda
\]
and hence (5.23) is proved.

**Proposition 5.5.3.** Let \( v \) be a henselian valuation of arbitrary rank of a field \( K \) with value group \( G_v \). Let \( f(x), m, (\alpha, \delta), w_{\alpha, \delta}, \lambda, e \) and \( h(x) \) be as in Theorem 1.1.A. If \( F(x) \) is a lifting of a monic polynomial \( T(Y) \) not divisible by \( Y \) belonging to \( \overline{K(x)} \) with respect to \( (\alpha, \delta) \) and \( h(x) \), then so is each monic factor of \( F(x) \) in \( K[x] \).

Proof. Let \( t \) denote the degree of \( T(Y) \), so that \( \deg F(x) = etm \). Let \( G(x) \in K[x] \) be a monic polynomial dividing \( F(x) \) and write \( F(x) = G(x)H(x) \). Let \( \sum_{i=0}^{r} G_i(x)f(x)^i \), \( \sum_{i=0}^{s} H_i(x)f(x)^i \) be the \( f(x) \)-expansions of \( F(x), G(x) \) and \( H(x) \) respectively with \( G_r(x)H_s(x) \neq 0 \). As in Theorem 2.2.A, let \( I_{\alpha, \delta}(F) \) and \( S_{\alpha, \delta}(F) \) denote respectively the minimum and the maximum integers belonging to the set \( \{ i \mid w_{\alpha, \delta}(F(x)) = \hat{v}(F(x)) + i \lambda \} \). By Theorem 2.2.A,
\[
I_{\alpha, \delta}(F) = I_{\alpha, \delta}(G) + I_{\alpha, \delta}(H), \quad S_{\alpha, \delta}(F) = S_{\alpha, \delta}(G) + S_{\alpha, \delta}(H).
\]
(5.24)
Since \( T(Y) \) is not divisible by \( Y \), we have \( I_{\alpha, \delta}(F) = 0 \) which in view of (5.24) implies that \( I_{\alpha, \delta}(G) = I_{\alpha, \delta}(H) = 0 \). So we have
\[
w_{\alpha, \delta}(G(x)) = \hat{v}(G_0(\alpha)); \quad w_{\alpha, \delta}(H(x)) = \hat{v}(H_0(\alpha)).
\]
(5.25)
Also \( et = S_{\alpha, \delta}(F) = S_{\alpha, \delta}(G) + S_{\alpha, \delta}(H) \leq r + s \leq et \), which shows that \( S_{\alpha, \delta}(G) = r \) and \( S_{\alpha, \delta}(H) = s \). Using (5.25), we see that \( w_{\alpha, \delta}(G(x)) = \hat{v}(G_r(\alpha)) + r \lambda = \hat{v}(G_0(\alpha)) \).
Therefore \( r \lambda \in G(K(\alpha)) \) and hence \( e \parallel r \). Similarly \( e \parallel s \).

Since \( \deg F(x) = etm \) and \( r + s = et \), it follows that \( G_r(x) \) and \( H_s(x) \) are constants and in fact equal 1. So \( w_{\alpha, \beta}(G(x)) = r \lambda = er_1 \lambda, w_{\alpha, \beta}(H(x)) = s \lambda = es_1 \lambda \). On dividing \( F(x) \) by \( h(x)^t = h(x)^{r_1+s_1} \) and taking the \( w_{\alpha, \beta} \)-residues, we conclude that \( G(x) \) is a lifting of some factor of \( T(Y) \) of degree \( r_1 \).

**Remark.** If \((K, v), F(x), \phi(x), \lambda, U(Y)\) are as in Theorem 5.1.5 and if \( i(F) \) is defined, then \( i(F) \geq i_0(F) \) with strict inequality whenever \( F(x) \) is reducible over \( K \). To verify this, write \( F(x) = F_1(x) \cdots F_k(x) \) as a product of irreducible factors over \( K \). By Proposition 5.5.3, each \( F_i(x) \) is a lifting of a power of \( U(Y) \). In view of Corollary 5.5.2, \( i_0(F) = i_0(F_1) + \cdots + i_0(F_k) + \sum_{i<j} r(F_i, F_j) \) with strict inequality whenever \( k > 1 \). By virtue of Theorem 5.1.2, \( i_0(F_j) \leq i(F_j) \); consequently \( i_0(F) \leq i(F_1) + \cdots + i(F_k) + \sum_{i<j} r(F_i, F_j) = i(F) \) with strict inequality when \( k > 1 \).

**Proof of Theorem 5.1.5.** We prove that (i) \( \Rightarrow \) (ii) \( \Rightarrow \) (iii) \( \Rightarrow \) (iv) \( \Rightarrow \) (i).

(i) \( \Rightarrow \) (ii). In view of the above remark \( F(x) \) is irreducible over \( K \). Let \( \theta \) be a root of \( F(x) \). Now arrange the elements of \( \mathfrak{C} \) according to increasing degrees in \( \theta \), i.e., with respect to the lexicographic ordering on the pairs \((j, i)\), then the transition matrix from \( \{1, 0, \ldots, 0^{n-1}\} \) to \( \mathfrak{C} \) is a block triangular matrix with \( et \) blocks down the main diagonal, each block is a scalar matrix of order \( m \times m \) and the \( j^{th} \) block down the main diagonal is a scalar matrix with each diagonal entry \( \pi^{-(j-1)\lambda} \). Therefore the valuation of the determinant of the transition matrix from \( \mathfrak{C} \) to \( \{1, \theta, \ldots, \theta^{n-1}\} \) is \( m^{et-1} \sum_{j=1}^{et-1} [j\lambda] = i_0(F) \). Since \( i_0(F) = i(F) \) by hypothesis of (i), so \( \mathfrak{C} \) is an \( R_\theta \)-basis of \( S \).

(ii) \( \Rightarrow \) (iii). In view of Theorem 2.2.6, on replacing \( \theta \) by a suitable conjugate, we may assume that \( \hat{\delta}(\theta - \alpha) = \delta \). Let \( v' \) be the restriction of \( \hat{\delta} \) to \( K(\theta), e(v'/v) \) and \( f(v'/v) \) stand respectively for the index of ramification and the residual degree of \( v'/v \). We denote \( \frac{\phi(\theta)^{r}}{\pi^{e\lambda}} \) by \( \xi \) in the proof of this theorem. As the family \( \mathfrak{C} \) is an \( R_\theta \)-basis of \( R_{v'} \), every element in the residue field of \( v' \) can be expressed as

80
So the residue field of \( v' \) is generated over the residue field of \( v \) by \( \tilde{\theta}, \tilde{\xi} \). Since \( \tilde{\xi} \) is a root of \( U(Y) \) by virtue of Theorem 2.2.6, it now follows that the residual degree \( f(v'/v) = dm \). By hypothesis \( R_{v'} \) is a free \( R_v \)-module, so \( (K(\theta), v')/(K, v) \) is a defectless extension by [End, Theorem 18.6], i.e., \( [K(\theta) : K] = e(v'/v)f(v'/v) \) and hence \( e(v'/v) = el \). We now show that \( \tilde{v}(\psi(\theta, \xi)) = \frac{1}{el} \). Let \( i_0 \) be the index \( 0 \leq i_0 \leq e - 1 \) such that \( \frac{\phi(\theta)^{i_0}}{\pi^{[a\lambda]}} = \frac{e - 1}{e} \). Consider an element \( \gamma \) of \( R_{v'} \) defined by \( \gamma = \phi(\theta)^{j_0} (\psi(\theta, \xi))^{i-1} \). When we express \( \gamma \) as an \( R_v \)-linear combination of the elements of \( \mathcal{E} \), then the term with the highest degree in \( \theta \), which is \( \phi(\theta)^{j_0} (\phi(\theta)^{\xi})^{d(l-1)} = \phi(\theta)^{j_0} \pi^{[a\lambda]} \), with \( j_0 = ed(l-1) + i_0 \) has coefficient 1. Therefore \( 0 < \tilde{v}(\gamma) < v(\pi) = 1 \), which implies that

\[
\frac{e - 1}{e} + (l - 1)\tilde{v}(\psi(\theta, \xi)) < 1, \quad i.e., \quad \tilde{v}(\psi(\theta, \xi)) < \frac{1}{el(l - 1)}.
\]

Since \( e(v'/v) = el \), we conclude that \( \tilde{v}(\psi(\theta, \xi)) = 1/el \).

\((iii) \implies (iv)\). On replacing \( \theta \) by its \( K \)-conjugate, it may be assumed that \( \tilde{v}(\theta - \alpha) = \delta \). As the \( w_{a,\delta} \)-residues of \( F(x) \) and \( \big( \psi(\theta, \phi(\theta)^{e})^\xi \big)^{i} \) are the same, we see that \( w_{a,\delta}(\psi(F^{(1)}(x)) > 0 \). Keeping in mind that the value group of \( w_{a,\delta} \) is \( \mathbb{Z} + \mathbb{Z}\lambda = \mathbb{Z} \frac{1}{e} \) in view of Theorem 1.1.A, it now follows that

\[
w_{a,\delta}(F^{(1)}(x)) \geq et\lambda + \frac{1}{e}.
\] (5.26)

Substituting \( x = \theta \) in (5.2) and then taking \( \tilde{v} \)-valuation, keeping in view the hypothesis \( \tilde{v}(\psi(\theta, \xi)) = \frac{1}{el} \), we see that

\[
\tilde{v}(F^{(1)}(\theta)) = et\lambda + \tilde{v}(\psi(\theta, \phi(\theta)^{e})) = et\lambda + \frac{1}{e},
\]

which in view of (5.21) implies that

\[
w_{a,\delta}(F^{(1)}(x)) \leq \tilde{v}(F^{(1)}(\theta)) = et\lambda + \frac{1}{e}.
\] (5.27)

81
Comparing (5.26) and (5.27), we have \( w_{v_{\alpha}}(F^{(1)}(x)) = v(F^{(1)}(\theta)) = \epsilon t \lambda + \frac{1}{e} \). So by Proposition 5.5.1, \( U(Y) \) does not divide \( W(Y) \).

\((iv) \implies (i)\). In view of Lemma 5.4.1, we need to consider the case when \( l > 1 \).

Let \( \theta \) be a root of \( F(x) \) with \( v(\theta - \alpha) = \delta \) and \( v', e(v'/v), f(v'/v), \xi \) be as in the proof of \((ii) \implies (iii)\). We first prove that \( e(v'/v) = el, f(v'/v) = dm \). Since \( U(Y) \) does not divide \( W(Y) \), it follows from Proposition 4.2.1 and the hypothesis that \( \tilde{v}(F^{(1)}(\theta)) = w_{v_{\alpha}}(F^{(1)}(x)) = \epsilon t \lambda + \frac{1}{e} \). So on substituting \( x = \theta \) in (5.2) and then taking \( \tilde{v} \)-valuation, we see that

\[
\epsilon t \lambda + \frac{1}{e} = \tilde{v}(F^{(1)}(\theta)) = \epsilon t \lambda + l \tilde{v}(\psi(\theta, \xi)).
\]

Consequently

\[
\tilde{v}(\psi(\theta, \xi)) = 1/el \tag{5.28}
\]

and hence \( e(v'/v) \geq el \). As \( \tilde{\xi} \) is a root of \( U(Y) \), therefore \( f(v'/v) \geq dm \). In view of the Fundamental Inequality, \( [K(\theta) : K] \geq e(v'/v)f(v'/v) \geq delm = \deg F(x) \). So \( F(x) \) is irreducible over \( K \) and \( e(v'/v) = el, f(v'/v) = dm \).

Consider the set

\[
\mathcal{E}_1 = \left\{ \theta^i \left( \frac{\phi(\theta)^j}{\pi^{[\pi]}} \right) \xi^k(\psi(\theta, \xi))^q \mid 0 \leq i < m, 0 \leq j < e, 0 \leq k < d, 0 \leq q < l \right\}.
\]

Note that the \( v' \)-valuation of the elements \((\phi(\theta)^j/\pi^{[\pi]})(\psi(\theta, \xi))^q, 0 \leq j < e, 0 \leq q < l \) lie in distinct cosets modulo \( Z \) in view of (5.28). So by Lemma 5.4.1, \( \mathcal{E}_1 \) is valuation independent over \( (K, v) \). Since the \( v' \)-valuation of each element of \( \mathcal{E}_1 \) is less than 1, it follows that \( \mathcal{E}_1 \) forms an \( R_{v'} \)-basis of \( R_{v'} \) and hence \( i(F) \) is defined.

We arrange elements of \( \mathcal{E}_1 \) according to increasing degrees in \( \theta \), i.e., with respect to the lexicographic ordering of the tuples \((q, k, j, i)\). The transition matrix from \( \{1, \theta, \ldots, \theta^{n-1}\} \) to \( \mathcal{E}_1 \) is a block triangular matrix with \( \epsilon t \) blocks down the main diagonal, each block is a scalar matrix of order \( m \times m \) and the \( j^{th} \) block down the main diagonal is a scalar matrix with each diagonal entry \( \pi^{-[j-1]^{[\pi]}} \). Therefore the
valuation of the determinant of the transition matrix from $\mathfrak{C}_i$ to \{1, $\theta$, \ldots, $\theta^{n-1}$\} is $m \sum_{j=1}^{d-1} [j\lambda]$. As $\mathfrak{C}_i$ is a basis of $R_{et}$, we see that $i(F) = m \sum_{j=1}^{d-1} [j\lambda] = i_\phi(F)$ which completes the proof of the theorem.

Proof of Theorem 5.1.6. By Lemma 2.2.1, the $\phi$-Newton polygon of $F$ is the straight line segment joining (0, 0) to $(et, et\lambda)$. So by Theorem 2.1.1(iv), $F(x)$ can be written as $F_1(x) \cdots F_r(x)$, where $F_i(x)$ is a lifting of $U_i(Y)^{t_i}$ having degree $t_i$ (say) with respect to $\phi(x), \lambda$. We shall write $\psi_i$ for $\psi_i\left(x, \frac{\phi(x)^{t_i}}{\pi\epsilon^\lambda}\right)$ and $F^{(1)}_i(x)$ for the polynomial $F_i(x) - \pi^{et_i\lambda}\psi_i^{t_i}$. Let $W_i(Z)$ have the same meaning as $W(Z)$ in Theorem 5.1.5 when $F^{(1)}_i(x)$ is replaced by $F^{(1)}_i(x)$ in (5.2). By virtue of equation (5.1), $i(F) = \sum_i i(F_i) + \sum_{i<j} r(F_i, F_j)$, even when $F_i$ are not irreducible over $K$. Also in view of Lemma 5.4.2, $i_\phi(F) = \sum_i i_\phi(F_i) + \sum_{i<j} r(F_i, F_j)$. By the remark after Proposition 5.5.3, $i(F_i) \geq i_\phi(F_i)$, so it is clear that

$$i(F) = i_\phi(F) \iff i(F_i) = i_\phi(F_i) \text{ for } 1 \leq i \leq r. \quad (5.29)$$

Write $F^{(1)}(x) = F(x) - \pi^{et_i\lambda}\psi_i^{t_i} \cdots \psi_r^{t_r}$ as

$$F^{(1)}(x) = \sum_{i=1}^r \left( F_i(x) - \pi^{et_i\lambda}\psi_i^{t_i} \right) \left( \prod_{j \neq i, j \neq k \leq i} \left( \pi^{et_j\lambda}\psi_j^{t_j} F_k(x) \right) \right), \quad F_0(x) = 1. \quad (5.30)$$

Since $w_{\alpha, \delta}(F_i(x) - \pi^{et_i\lambda}\psi_i^{t_i}) > w_{\alpha, \delta}(F_i(x)) = et_i\lambda$ and the value group of $w_{\alpha, \delta}$ is $\mathbb{Z} + \mathbb{Z}\lambda = \mathbb{Z} + \frac{1}{e}$, it follows that

$$w_{\alpha, \delta}(F_i(x) - \pi^{et_i\lambda}\psi_i^{t_i}) \geq et_i\lambda + \frac{1}{e}. \quad (5.31)$$

We now prove (i) $\implies$ (ii). Assume that some $l_i$, say $l_i > 1$. We first show that

$$w_{\alpha, \delta}(F^{(1)}(x)) = et\lambda + \frac{1}{e}. \quad (5.32)$$

By virtue of (5.29), $i(F_i) = i_\phi(F_i)$ for each $i$. So by Theorem 5.1.5(i), each $F_i(x)$ is irreducible over $K$. Let $\theta$ be a root of $F_i(x)$ with $\bar{\phi}(\theta - \alpha) = \delta$. We denote $\frac{\phi(\theta)^{t_i}}{\pi\epsilon^\lambda}$ by

83
\( \xi \). By assertions (iii), (iv) of Theorem 5.1.5, we have
\[
\bar{\nu}(\psi_1(\xi, \xi)) = \frac{1}{e_l}, \quad U_1(Y) \nmid W_1(Y), \quad w_{\alpha, \delta}(F_1(\xi)) = e\lambda + \frac{1}{e}.
\] (5.33)

Note that \( \bar{\nu}(\psi_j(\xi, \xi)) = 0 \) when \( j \neq 1 \), for otherwise \( \bar{\xi} \) will be a root of \( \bar{\psi}_j(\bar{\alpha}, Y) = U_j(Y) \) which is not so as \( \bar{\xi} \) is a root of \( U_1(Y) \) in view of Theorem 1.1.6. Since \( \theta \) is a root of \( F_1(x) \), on substituting \( x = \theta \) in (5.30), we see that
\[
P^{(1)}(\theta) = \pi^{e\lambda \psi_1(\theta, \xi)} \prod_{j>1} (\pi^{e\lambda \psi_j(\theta, \xi)})^{\delta_j}.
\]

Keeping in mind the first equality in (5.33), it now follows that \( \bar{\nu}(F^{(1)}(\theta)) = e\lambda + \frac{1}{e} \). Therefore in view of (5.21), \( w_{\alpha, \delta}(F^{(1)}(x)) \leq \bar{\nu}(F^{(1)}(\theta)) = e\lambda + \frac{1}{e} \). Since \( w_{\alpha, \delta}(F^{(1)}(x)) > w_{\alpha, \delta}(F(x)) = e\lambda \) and the value group of \( w_{\alpha, \delta} \) is \( \mathbb{Z} + \mathbb{Z} \chi = \mathbb{Z} \), we conclude that (5.32) holds.

Recall that \( i_0 \) is the smallest non-negative integer such that \( w_{\alpha, \delta}(F^{(1)}(x)) = i_0 \lambda + \nu(a_0) \) for some \( a_0 \) belonging to \( K \) and \( Z \) is the \( w_{\alpha, \delta} \)-residue of \( \frac{\phi(x)^e}{\pi^{e\lambda}} \). Keeping in mind (5.31) together with Theorem 1.1.6(b), on dividing both sides of (5.30) by \( a_0 \phi^j \) and then taking the \( w_{\alpha, \delta} \)-residue, it can be easily seen that
\[
W(Z) = \sum_{i=1}^{r} Z^j A_i(\alpha) W_i(Z) \left( \prod_{j \neq i} U_j(Z)^{\delta_j} \right),
\] (5.34)

where \( j_i \) are integers and \( A_i(\alpha) \in K(\alpha) \) is non-zero or zero according as \( w_{\alpha, \delta}(F_1^{(1)}(x)) = e\lambda + \frac{1}{e} \) or not. By virtue of (5.33), \( A_i(\alpha) \neq 0 \) and \( U_1(Z) \neq Z \) does not divide \( W(Z) \). So \( U_1(Z) \nmid W(Z) \) in view of (5.34); this together with (5.32) proves (i) \( \implies \) (ii).

(ii) \( \implies \) (i). In view of Lemma 5.4.1 and (5.29), it is enough to prove that \( i(F_i) = i_0(F_i) \) whenever \( l_i > 1 \). For simplicity of notation, we prove it for \( i = 1 \) with \( l_1 > 1 \). By hypothesis, (5.32) holds and hence by what has been shown in the above paragraph, (5.34) holds. As \( U_1(Z) \) does not divide \( W(Z) \), it follows from (5.34) that \( A_i(\alpha) \neq 0 \) and \( U_1(Z) \nmid W_1(Z) \). So \( w_{\alpha, \delta}(F_1(x) - \pi^{e\lambda \psi_1(\xi)}) = e\lambda + \frac{1}{e} \). Therefore hypothesis in statement (iv) of Theorem 5.1.5 is satisfied. Hence in view of this theorem, \( i(F_1) = i_0(F_1) \).
Remark. We wish to point out that in assertion (iv) of Theorem 5.1.5, the condition $\omega_{a,b}(F^{(1)}(x)) = \epsilon \lambda + \frac{1}{\epsilon}$ cannot be dispensed with when $l > 1$ even when the base field is the field of $p$-adic numbers as the following example shows.

Example 5.5.4. Consider $F(x) = x^4 + 2px^2 - p^2x^2 + p^2$ over the field $K = \mathbb{Q}_p$ of $p$-adic numbers with the $p$-adic valuation $v_p, p \neq 2$. Take $\phi(x) = x$. The $\phi$-Newton polygon of $F(x)$ is a straight line segment joining $(0,0)$ to $(4,2)$. Take $\alpha = 0$ and $\delta = \frac{1}{2}$. Let $\omega_{a,b}$ be the valuation defined by (1.3). It can be easily checked that $\omega_{a,b}(F(x)) = 2$ and that the $\omega_{a,b}$-residue of $\frac{F(x)}{p^2}$ is $(Z + 1)^2$, where $Z$ is the $\omega_{a,b}$-residue of $\frac{x^2}{p}$ and is transcendental over the field with $p$ elements in view of Theorem 1.1.A. So $F(x)$ is a lifting of $U(Y) = (Y + 1)^2$ with respect to the minimal pair $(0,1/2)$. Define $F^{(1)}(x) = F(x) - p^2 \left(\frac{x^2}{p} + 1\right)^2 = -p^2x^2$. Note that $\omega_{a,b}(F^{(1)}(x)) = 3$ and the $\omega_{a,b}$-residue of $\frac{F^{(1)}(x)}{p^2}$ is $-Z = W(Z)$ (say). So $U(Y)$ and $W(Y)$ are coprime. We show that $i(F) \neq i_{\phi}(F)$. Note that $i_{\phi}(F) = 2$. Write $F(x) = (x^2 + px + p)(x^2 - px + p) = G(x)H(x)$ (say). The $\phi$-Newton polygons of $G(x)$ and $H(x)$ are single line segments joining $(0,0)$ to $(2,1)$. So $i_{\phi}(G) = i_{\phi}(H) = 0$. Since $G(x)$ and $H(x)$ are both liftings of $Y + 1$ with respect to the minimal pair $(0,1/2)$, it follows from Lemma 5.4.1 that $i(G) = i_{\phi}(G) = 0, i(H) = i_{\phi}(H) = 0$.

By definition $i(F) = i(G) + i(H) + r(G,H) = r(G,H)$, where $r(G,H)$ is the $p$-adic valuation of the resultant of $G(x)$ and $H(x)$. Since $G(x), H(x)$ are both liftings of $Y + 1$ with respect to the minimal pair $(0,1/2)$, therefore applying Proposition 5.5.1, we see that for any root $\theta_2$ of $H(x), \bar{v}(\theta_2) > \omega_{a,b}(G(x)) = 1$. Consequently $i(F) = r(G,H)) > 2 = i_{\phi}(F)$.

The following example shows that one of the equivalent versions of the Proposition on page 328 of [Mo-Na] is false.
Example 5.5.5. Consider \( F(x) = x^3 + 9cx^2 + 27cx - 27b^3 \) with \( b, c \) in \( \mathbb{Z} \) and \( b \equiv 2 \) (modulo 9) and \( c \equiv 1 \) (modulo 9) over the field \( K = \mathbb{Q}_3 \) of the 3-adic numbers with 3-adic valuation denoted by \( v \). Take \( \phi(x) = x \). The \( \phi \)-Newton polygon of \( F(x) \) is a straight line segment joining \((0, 0)\) to \((3, 3)\). So by Theorem 2.1.1, for each root \( \theta \) of \( F(x) \), \( v(\theta) = 1 \). We claim that \( F(x) \) is irreducible over \( K \). Let \( w_{0,1} \) be the valuation of \( K(x) \) with respect to the minimal pair \((0, 1)\). Clearly \( w_{0,1}(F(x)) = 3 \). Take \( \pi = 3b \).

The \( w_{0,1} \)-residue of \( \frac{F(x)}{(3b)^3} \) is given by

\[
\left( \frac{F(x)}{27b^3} \right) = \left( \frac{x}{3b} \right)^3 - 1 = Z^3 - 1 = (Z - 1)^3 = U(Z)^3 \text{ (say)},
\]

where \( Z \) is the \( w_{0,1} \)-residue of \( \frac{x}{3b} \). A simple calculation shows that

\[
F^{(1)}(x) = F(x) - (3b)^3 \left( \frac{x}{3b} - 1 \right)^3 = 9(c + b)x^2 + 27(c - b^2)x.
\]

(5.35)

Keeping in mind the choice of the choice of \( b, c \), it can be easily seen that \( w_{0,1}(F^{(1)}(x)) = 5 \) and the \( w_{0,1} \)-residue of \( \frac{F^{(1)}(x)}{27(c - b^2)x} = \frac{b(c + b)}{c - b^2} \left( \frac{x}{3b} \right) + 1 \) is \( Z + 1 \) which is coprime to \( U(Z) \). So by virtue of Proposition 4.2.1, \( v(F^{(1)}(\theta)) = w_{0,1}(F^{(1)}(x)) = 5 \) for any root \( \theta \) of \( F(x) \). It now follows from the first equality of (5.35) that \( \bar{v}(F^{(1)}(\theta)) = 3 \left( 1 + \bar{v} \left( \frac{\theta}{3b} - 1 \right) \right) = 5 \) and hence \( \bar{v} \left( \frac{\theta}{3b} - 1 \right) = \frac{2}{3} \). So \( [K(\theta) : K] \geq 3 \) which implies that \( F(x) \) is irreducible over \( K \). Thus \( F(x) \) satisfies the hypothesis of equivalent statement (iv) of the proposition on page 328 of [Mo-Na]. We claim that statement (ii) of this proposition does not hold, i.e., the set \( \mathcal{B} = \left\{ \frac{\theta^j}{\pi^{|j|}} \mid 0 \leq j \leq 2 \right\} = \left\{ 1, \frac{\theta}{3b}, \left( \frac{\theta}{3b} \right)^2 \right\} \) is not an \( R_\pi \)-basis of the integral closure of \( R_\pi \) in \( K(\theta) \). By what has been shown above, \( \bar{v} \left( \left( \frac{\theta}{3b} - 1 \right)^2 \right) = \frac{4}{3} \) which implies that \( \bar{v} \left( \frac{1}{3} \left( \frac{\theta}{3b} \right)^2 - \frac{2}{3} \left( \frac{\theta}{3b} \right) + \frac{1}{3} \right) = \frac{1}{3} > 0 \) proving the claim.

The following example shows that Theorem 5.1.3 can be used to determine a \( p \)-integral basis of an algebraic number field \( K = \mathbb{Q}(\theta) \) when the minimal polynomial \( F(x) \) of \( \theta \) over \( \mathbb{Q} \) is not \( p \)-regular.

86
Example 5.5.6. Let \( F(x) = x^6 + 3x^5 + 9x^4 + 9x^3 + 27x^2 + 27x + 27 \). We will prove that it is irreducible over the field \( \mathbb{Q}_3 \) of 3-adic numbers with 3-adic valuation \( v \) by showing that all the conditions of Theorem 5.1.5(iv) are satisfied. Consider \( \phi(x) = x \). The \( \phi \)-Newton polygon of \( F(x) \) with respect to \( v \) is the straight line segment joining \((0,0)\) to \((6,3)\). Take \( \alpha = 0 \) and \( \delta = 1/2 \). The \( w_{\alpha,\delta} \)-valuation of \( F(x) \) is 3 and the \( w_{\alpha,\delta} \)-residue of \( \frac{F(x)}{3^3} \) is easily seen to be \( Z^3 + 3Z^2 + 3Z + 1 = (Z + 1)^3 \), \( Z \) being the \( w_{\alpha,\delta} \)-residue of \( x^2/3 \). Take \( U(Z) = Z + 1 \) and define \( F^{(1)}(x) = F(x) - 3^3 \left( \frac{x^2}{3} + 1 \right)^3 = 3x^5 + 9x^3 + 27x \).

Note that \( w_{\alpha,\delta}(F^{(1)}(x)) = 7/2 \) and the \( w_{\alpha,\delta} \)-residue of \( \frac{F^{(1)}(x)}{27x} \) is \( Z^2 + Z + 1 = W(Z) \). Clearly \( U(Z) \) and \( W(Z) \) are coprime. Also \( w_{\alpha,\delta}(F^{(1)}(x)) = 7/2 = 3 + 1/2 = \eta \lambda + 1/\epsilon \).

So by assertions (ii), (i) of Theorem 5.1.5, \( F(x) \) is irreducible over \( \mathbb{Q}_3 \) and \( F(x) \) is weakly \( v \)-regular with respect to \( \phi(x) = x \) but clearly it is not \( v \)-regular. Applying Theorem 5.1.3, the set \( \mathfrak{B}_1 = \{ q_j(\theta)/3^j \mid 1 \leq j \leq 6 \} \) forms a 3-integral basis of the algebraic number field \( \mathbb{Q}(\theta) \), where \( q_j(x), z_j \) have the same meaning as in Proposition 5.3.2 and \( \theta \) is a root of \( F(x) \). It can be easily checked that

\[
\frac{q_1(\theta)}{3^{j_1}} = \frac{\theta^5 + 3\theta^4 + 9\theta^3 + 9\theta^2 + 27\theta + 27}{9}, \quad \frac{q_2(\theta)}{3^{j_2}} = \frac{\theta^4 + 3\theta^3 + 9\theta^2 + 9\theta + 27}{9},
\]

\[
\frac{q_3(\theta)}{3^{j_3}} = \frac{\theta^3 + 3\theta^2 + 9\theta + 9}{3}, \quad \frac{q_4(\theta)}{3^{j_4}} = \frac{\theta^2 + 3\theta + 9}{3},
\]

\[
\frac{q_5(\theta)}{3^{j_5}} = \theta + 3, \quad \frac{q_6(\theta)}{3^{j_6}} = 1.
\]

Therefore \( \mathfrak{B}_1 \) and hence \( \{ 1, \theta, \frac{\theta^2}{3}, \frac{\theta^3}{3}, \frac{\theta^4 + 3\theta^3}{9}, \frac{\theta^5 + 3\theta^4}{9} \} \) is a 3-integral basis of \( \mathbb{Q}(\theta) \).