POLYNOMIAL INDEX IN DEDEKIND RINGS

M.E. CHARKANI
Department of Mathematics, Faculty of Sciences Dhar-Mahraz, Morocco

A. DEAJIM
Department of Mathematics, King Khalid University, Saudi Arabia

Abstract. Let $R$ be a Dedekind ring, $p$ a nonzero prime ideal of $R$, $P \in R[X]$ a monic irreducible polynomial, and $K$ the quotient field of $R$. We give in this paper a lower bound for the $p$-adic valuation of the index of $P$ over $R$ in terms of the degrees of the monic irreducible factors of the reduction of $P$ modulo $p$. As an important application, when the lower bound is greater than zero for some $p$, we conclude that no root of $P$ generates a power integral basis in the field extension of $K$ defined by $P$.

1. Introduction

It is well-known that the problem of studying the integral closure of a Dedekind ring $A$ in some finite separable extension of its quotient field is related to the problem of studying the integral closures of localizations of $A$ at its nonzero prime ideals. As such localizations are discrete valuation rings, we consider some tools and relevant results over discrete valuation rings.

Let $R$ be a discrete valuation ring and $p$ its nonzero prime ideal. An important notion which we need here is the notion of index of an irreducible polynomial over $R$, whose definition we recall below for the sake of completion (see [3] for a more general treatment).

If $M$ is a nonzero torsion $R$-module of finite type, then $M$ admits a composition series of submodules

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_t = M,$$

where, for each $i = 0, 1, \ldots, t - 1$, the quotient $R$-module $M_{i+1}/M_i$ is simple and is isomorphic to $R/p$. Note here that $t$ is an invariant of $M$ independent of the choice of composition series (see [1, Proposition 6.7] or [9, §11–Theorem 19]). Now, if $M$
is an $R$-module of finite type, we define the order ideal of $M$ over $R$ by (see [3]):

$$\text{ord}_R(M) := \begin{cases} R & \text{if } M = 0 \\ 0 & \text{if } M \text{ is not a torsion } R\text{-module} \\ p^t & \text{if } M \text{ is a nonzero torsion } R\text{-module.} \end{cases}$$

If $N \subseteq M$ are two projective $R$-modules of the same finite constant rank, then we define the index of $M$ over $N$ to be the ideal $\text{ord}_R(M/N)$, and we denote it by $[M : N]_R$. By definition, note that $M = N$ if and only if $[M : N]_R = R$.

Let $K$ be the quotient field of $R$, $L$ a finite separable extension of $K$, $O_L$ the integral closure of $R$ in $L$, $\alpha \in O_L$ a primitive element of $L$, and $P \in R[X]$ the minimal polynomial of $\alpha$ over $R$. As $R[\alpha] \subseteq O_L$ are projective $R$-modules of the same constant rank, $[O_L : R[\alpha]]_R$ is well defined. We call $[O_L : R[\alpha]]_R$ the index of $P$ (or of $\alpha$) and denote it by $\text{Ind}_R(P)$ (see [2] for instance). This notion of index is generalized to the case when $R$ is a Dedekind domain (see [3]). Now recall the generalized discriminant-index formula (see [3])

$$\text{Disc}_R(P) = \text{Ind}_R(P)^2 D_R(O_L),$$

where $\text{Disc}_R(P) = \text{disc}(P)R$ is the principal ideal of $R$ generated by the usual discriminant of $P$, and $D_R(O_L)$ is the relative discriminant of $O_L$ over $R$ in the sense of [3] (see also [5]).

If $R$ is a Dedekind ring, $p$ a nonzero prime ideal of $R$, and $P(X) \in R[X]$ is a monic irreducible polynomial defining a separable field extension $L$ over the quotient field of $R$, then our main result, Theorem 1.1 below, gives a lower bound on the $p$-adic valuation of $\text{Ind}_R(P)$ in terms of the degrees of the monic irreducible factors of the reduction of $P$ modulo $p$. An important application of this theorem is to conclude, when the lower bound is greater than zero for some $p$, that a root of $P(X)$ in $L$ does not generate a power basis for the integral closure of $R$ in $L$.

**Theorem 1.1.** Let $R$ be a Dedekind ring, $K$ its quotient field, $L$ a finite separable extension of $K$, $O_L$ the integral closure of $R$ in $L$, $L = K(\alpha)$ for some $\alpha \in O_L$, $P \in R[X]$ the minimal polynomial of $\alpha$ over $K$, and $A = R[\alpha]$. Let $p$ be a nonzero prime ideal of $R$, $\overline{P} = \prod_{i=0}^r \overline{P}_i^{t_i}$ the monic irreducible factorization of $P$ modulo $p$, and $P_i \in R[X]$ a monic lift of $\overline{P}_i$ for each $i$. Suppose that $T \in R[X]$ with $\overline{T}$ nonzero and $P = \prod_{i=0}^r P_i^{t_i} + aT$ for $a \in p - p^2$. Let $t_i$ be the highest power of $\overline{P}_i$ that divides $\overline{T}$ and set $s_i = \min\{\frac{t_i}{2}, t_i\}$. Then,

$$\nu_p(\text{Ind}_R(P)) \geq \sum_{i=1}^r s_i \deg(P_i) = \deg(\prod_{i=1}^r P_i^{s_i}).$$
2. Lemmas

For a nonzero fractional ideal \( \mathfrak{a} \) of an integral domain \( R \), denote by \( \text{Stab}_K(\mathfrak{a}) \) the fractional ideal

\[
(\mathfrak{a} :_K \mathfrak{a}) := \{ x \in K \mid x \mathfrak{a} \subseteq \mathfrak{a} \},
\]

where \( K \) is the quotient field of \( R \). We call \( \text{Stab}_K(\mathfrak{a}) \) the \( K \)-stabilizer of \( \mathfrak{a} \). Note that \( R \subseteq \text{Stab}_K(\mathfrak{a}) \). It is known that \( \text{Stab}_K(\mathfrak{a}) \) is the largest subring \( B \) of \( K \) such that \( \mathfrak{a} \) is a \( B \)-module. Further, if \( R \) is noetherian and \( \overline{R} \) is the integral closure of \( R \) in \( K \), then \( \overline{R} = \bigcup \mathfrak{a} \text{Stab}_K(\mathfrak{a}) \), where \( \mathfrak{a} \) runs over all nonzero fractional ideals \( \mathfrak{a} \) of \( R \) (see [8, Proposition 2.4.8]).

By \((\ldots)\) (resp. \([\ldots]\)) we mean the usual notation for the greatest common divisor (resp. least common multiple), and by \([\ldots]\) we mean the integral part of a number.

Now let \( R \) be a discrete valuation ring, \( \pi \) a uniformizer of \( R \), \( \mathfrak{p} = \pi R \) the prime ideal of \( R \), \( k = R/\mathfrak{p} \) the residue field of \( R \), \( K \) the quotient field of \( R \), \( L \) a finite separable extension of \( K \), \( O_L \) the integral closure of \( R \) in \( L \), \( L = K(\alpha) \) for some \( \alpha \in O_L \), \( P(X) \in R[X] \) the minimal polynomial of \( \alpha \) over \( R \), and \( A = R[\alpha] \). For a polynomial \( f(X) = \sum_{i=0}^{t} a_i X^i \in R[X] \), by \( \overline{f}(X) \) we mean the polynomial \( \sum_{i=0}^{t} \overline{a_i} X^i \in k[X] \) resulting from reducing all coefficients of \( f(X) \) modulo \( \mathfrak{p} \).

**Lemma 2.1.** Keep the notation as above. Let \( W \in R[X] \) be monic such that \( \overline{W} \) divides \( \overline{P} \) in \( k[X] \). Then \( M = A + (W(\alpha)/\pi) A \) is a free \( R \)-module with \([M : A]_R = \mathfrak{p}^{n-m}\), where \( n = \deg(P) \) and \( m = \deg(W) \).

**Proof.** Since \( R \) is a discrete valuation ring and \( A \) is a free \( R \)-module of finite rank \( n \) and \( \pi M \subseteq A \subseteq M \), it follows that \( \pi M \) and, thus, \( M \) are free \( R \)-modules of rank \( n \) as well. Since \( A/\pi M \cong k[X]/(\overline{W}) \cong k^m = (R/\mathfrak{p})^m \) as \( R \)-modules and \([A : \pi M]_R = \text{ord}_R(A/\pi M)\), \([A : \pi M]_R = \text{ord}_R((R/\mathfrak{p})^m) = \mathfrak{p}^m\). On the other hand, as \([M : A]_R [A : \pi M]_R = [M : \pi M]_R = \text{ord}(M/\pi M) = \mathfrak{p}^n\), it follows that \([M : A]_R = \mathfrak{p}^{n-m}\) as claimed.

**Lemma 2.2.** Keep the notation of Lemma 2.1. Let \( \mathfrak{a} = \pi A + f(\alpha) A \) for some monic \( f \in R[X] \) such that \( \overline{f} \) divides \( \overline{P} \) in \( k[X] \). Let \( g, T \in R[X] \) be such that \( P = fg + \pi T \) with \( \overline{T} \) nonzero, and \( D, h, U \in R[X] \) such that \( \overline{D} = (\overline{f}, \overline{g}, \overline{T}) \), \( \overline{h} = \overline{f}/(\overline{f}, \overline{T}) \), and \( \overline{U} = \overline{T}/\overline{D} \). Then we have the following:

(i) \( \overline{U} = [\overline{h}, \overline{f}] \).

(ii) \( \text{Stab}_L(\mathfrak{a}) = A + \frac{U(\alpha)}{\pi} A \subseteq O_L \).

(iii) \( \text{Stab}_L(\mathfrak{a}) \) is a free \( R \)-submodule of \( O_L \) and \([\text{Stab}_L(\mathfrak{a}) : A]_R = \mathfrak{p}^{\deg(D)}\).

**Proof.**

(i) \( \overline{U} = \frac{\overline{g} \overline{\overline{f}}}{(\overline{g}, \overline{f}, \overline{T})} = \frac{\overline{g} \overline{\overline{h}(\overline{f}, \overline{T})}}{(\overline{g}, (\overline{f}, \overline{T}))} = \overline{h}[\overline{g}, (\overline{f}, \overline{T})] = [\overline{h} \overline{g}, \overline{h}(\overline{f}, \overline{T})] = [\overline{h} \overline{g}, \overline{f}]. \)
(ii) Note, first, that \( a \) is a nonzero fractional ideal of \( A \). So, \( \text{Stab}_L(a) \subseteq O_L \) follows from the fact that \( O_L = \bigcup_a \text{Stab}_L(a), \) where \( a \) runs over all nonzero fractional ideals of \( A \) (see the paragraph preceding this lemma). It remains to show the proposed equality. By part (i), \( U = [h, r, f] \). So, it suffices to show that if \( x = Q(\alpha)/\pi \) for some \( Q \in R[X], \) then \( x \in \text{Stab}_L(a) \) if and only if both \( f \) and \( g(h) \) divide \( \overline{Q} \). Indeed, as \( x \in \text{Stab}_L(a) \) if and only if \( \pi x, xf(\alpha) \in a \), proving the equality will be complete by showing that \( \pi x \in a \) if and only if \( f \) divides \( \overline{Q} \), and \( xf(\alpha) \in a \) if and only if \( g(h) \) divides \( \overline{Q} \).

On the one hand, we see that \( \pi x \in a \) if and only if there exist \( F, G \in R[X] \) such that
\[
Q(\alpha) f(\alpha) = \pi(\pi Q_1(\alpha) + f(\alpha)Q_2(\alpha)).
\]
Since \( P \) is the minimal polynomial of \( \alpha \) over \( R \), (1) is equivalent to the existence of \( Q_3 \in R[X] \) such that
\[
Q f = \pi(\pi Q_1 + f Q_2) + P Q_3.
\]
Reducing modulo \( p \) we get that \( \overline{Q} = \overline{Q_3 f} \). Let now \( Q_4 \in R[X] \) be such that
\[
Q = \pi Q_4 + Q_3 g.
\]
Substituting in (2), we get
\[
Q_3(fg - P) = \pi(\pi Q_1 + f Q_2 - f Q_4).
\]
Now letting \( Q_5 = Q_4 - Q_2 \in R[X], \) we get that \( xf(\alpha) \in a \) if and only if there exist \( Q_1, Q_3, Q_5 \in R[X] \) such that
\[
Q_3 T = f Q_5 - \pi Q_1.
\]
Reducing modulo \( p \) again, we get \( \overline{Q_3 T} = \overline{f Q_5}. \) This is equivalent to saying that \( \overline{f} \) divides \( \overline{T} \overline{Q_3} \) or, equivalently, \( \overline{h} \) divides \( \overline{Q_3} \) since \( \overline{T} \) is nonzero. So \( xf(\alpha) \in a \) if and only if there exist \( Q_6, Q_7 \in R[X] \) such that
\[
Q_3 = h Q_6 + \pi Q_7.
\]
Substituting in (3) we get
\[ Q = \pi(Q_4 + gQ_7) + ghQ_6 \]
\[ = \pi Q_8 + ghQ_6, \]
where \( Q_8 = Q_4 + gQ_7 \in R[X]. \) It finally follows that \( xf(\alpha) \in a \) if and only if \( gh \) divides \( Q. \)

(iii) Apply Lemma 2.1 with \( U = W. \)

**Remark.** It should be noted here that Lemma 2.2 generalizes Lemma 6.1.5 of [4]. Furthermore, choosing \( f \) to be the radical of the square part of \( \overline{P} \) would give a refinement of Theorem 6.1.5 of [4] (by the radical of a polynomial over \( K \) we mean the product of all its distinct irreducible factors, and by the square part of a polynomial over \( K \) we mean the quotient upon dividing the polynomial by its radical).

3. **Lower Bounds of** \( \nu_p(\text{Ind}_R(P)) \)

**Proposition 3.1.** Keep the notation and assumptions of Lemma 2.2. Then
\[ \nu(\text{Ind}_R(P)) \geq \text{deg}(D). \]

**Proof.** Indeed, \( A \subseteq \text{Stab}_L(a) \subseteq O_L \) and, therefore, \( [\text{Stab}_L(a) : A]_R \) divides \( [O_L : A]_R = \text{Ind}_R(P). \) Now, using Lemma 2.2 (ii) yields the claim.

**Proposition 3.2.** Keep the notation and assumptions of Lemma 2.2. If \( O_L = A, \) then \( (\overline{f}, \overline{h}, \overline{T}) = \overline{1}. \)

**Proof.** It follows from Lemma 2.2 that \( \text{Stab}_L(a) = O_L \) and \( \text{deg}(D) = 0. \)

Now the proof of Theorem 1.1.

**Proof.** (Theorem 1.1) We localize at \( p \) and apply Proposition 3.1 to a suitable choice of a divisor \( \overline{f} \) of \( \overline{P}; \) namely, \( \overline{f} = \prod_{i=1}^r P_i^{s_i}. \) Let \( f = \prod_{i=1}^r P_i^{s_i} \) and \( h = \prod_{i=1}^r P_i^{l_i-s_i}. \) Then, \( P = fh + \pi T \) and, in this case, \( \overline{D} = (\overline{f}, \overline{h}, \overline{T}) = \prod_{i=1}^r P_i^{m_i}, \) where \( m_i = \min\{s_i, l_i-s_i, t_i\}. \) Since \( m_i = \min\{\frac{l_i}{2}, t_i\} = s_i, \) the assertion now follows from Proposition 3.1.

**Example.**

Let \( R \) be a Dedekind ring, \( K \) the quotient field of \( R, \) \( p = \pi R \) a nonzero principal prime ideal of \( R, \) and \( P(X) = g(X)^n + ag(X)^m + b \in R[X] \) irreducible over \( R, \) with \( g(X) \in R[X] \) monic, \( \overline{g}(X) \) irreducible modulo \( p, \) \( n > 1, n \geq m \geq 1, \nu_p(a) = 1, \) and \( \nu_p(b) \geq 2 \) (e.g. \( P(X) = X^3 + \sqrt{3}X^2 + 3 \in \mathbb{Z}[\sqrt{3}][X] \) with \( p = \sqrt{3}\mathbb{Z}[\sqrt{3}]). \) Then, \( \overline{P}(X) \equiv \overline{g}(X)^n \) modulo \( p. \) For \( T(X) = g(X)^m + b/\pi \in R[X], \) it is clear that \( \overline{T}(X) = \overline{g}(X)^m \) is nonzero and \( \overline{T}(X) \) divides \( \overline{P}(X) \) modulo \( p. \) As \( l = n > 1 \) and...
\( t = m \geq 1, \ s = \min\{\lfloor \frac{n}{2} \rfloor, m\} \geq 1. \) Thus, \( \nu_p(\text{Ind}_R(P)) \geq (1)\deg(g(X)) \geq 1. \) Hence, a root \( \alpha \) of \( P \) never generates a power basis for the integral closure of \( R \) in \( K(\alpha) \).

**Remark.** It was shown in [7, Theorem 1.1 and Corollary 1.2] that if \( P(X) = X^n + aX^m + b \in \mathbb{Z}[X] \) is irreducible with \( m|n, \ p|a, \ p^2|b \) for a prime integer \( p \), then \( p|\text{Ind}_\mathbb{Z}(P) \). This is a special case that follows from the example above without even requiring that \( m|n \).

**References**

[1] M. Atiyah and I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Company, 1969.

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

[3] M.E. Charkani and A. Deajim, *Relative index in extensions of Dedekind rings*, JP J. Algebra, Number Theory and Appl 27 (2012), 73–84.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag, 1996.

[5] L. El Fadil and M.E. Charkani, *Generalization of the discriminant and applications*, Arab. J. Sci. Eng. 29 (2004), 93–98.

[6] A. Fröhlich and M. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics 27, 1993.

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

[8] I. Swanson and C. Huneke, *Integral Closure of Ideals, Rings, and Modules*, Cambridge University Press, 2006.

[9] O. Zariski and P. Samuel, *Commutative Algebra – V. 1*, GTM 28, Springer-Verlag, 1958.

(M.E. Charkani) Department of Mathematics, Faculty of Sciences Dhar-Mahraz, B.P. 1796, Fes, Morocco  
E-mail address: mcharkani@gmail.com

(A. Deajim) Department of Mathematics, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia  
E-mail address: deajim@kku.edu.sa, deajim@gmail.com