Journal of Pure and Applied Algebra 218 (2014) 1206–1218

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

A generalization of a theorem of Ore ☆

Sudesh K. Khanduja [a,*], Sanjeev Kumar [b]

[a] Indian Institute of Science Education and Research (IISER, Mohali), Sector-81, S.A.S. Nagar, 140306, Punjab, India
[b] Department of Mathematics, Panjab University, Chandigarh, 160014, India

ARTICLE INFO

Article history:
Received 14 July 2013
Received in revised form 4 October 2013
Available online 18 November 2013
Communicated by R. Parimala

Dedicated to Professor Peter Roquette on his 85th birthday

MSC:
12J10; 12J25; 12E05

ABSTRACT

Let (K, v) be a discrete rank one valued field with valuation ring R_v. Let L/K be a finite extension such that the integral closure S of R_v in L is a finitely generated R_v-module. Under a certain condition of v-regularity, we obtain some results regarding the explicit computation of R_v-bases of S, thereby generalizing similar results that had been obtained for algebraic number fields in El Fadil et al. (2012) [7]. The classical Theorem of Index of Ore is also extended to arbitrary discrete valued fields. We give a simple counter example to point out an error in the main result of Montes and Nart (1992) [12] related to the Theorem of Index and give an additional necessary and sufficient condition for this result to be valid.

0. Introduction

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring A_K of algebraic integers of K and let $F(x)$ be the minimal polynomial of θ 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 (see Definition 1.F). He used the factorization of the polynomial $\overline{F}(x)$ obtained on replacing each coefficient of $F(x)$ by its residue modulo p, say $\overline{F}(x) = \overline{\phi}_1(x)^{\nu_1} \cdots \overline{\phi}_r(x)^{\nu_r}$, 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 ϕ_i-Newton polygon of F for each i (definition given in 1.A). Moreover, to each side S of the ϕ_i-Newton polygon of F of positive slope, he associated a polynomial $(F)_S^{(\phi_i)}(Y)$ over the finite field $\mathbb{F}_{q_i}$, $q_i = p^{\deg \phi_i}$ in an indeterminate Y. If all these polynomials $(F)_S^{(\phi_i)}(Y)$ corresponding to various sides S_j, $1 \leqslant j \leqslant k_i$, $1 \leqslant i \leqslant r$ of the ϕ_i-Newton polygon of F have no repeated irreducible factor, then $F(x)$ is said to be p-regular with respect to $\phi_1(x), \ldots, \phi_r(x)$. In this situation, Ore (cf. [13,12]) proved that the p-adic valuation (denoted by v_p) of the index of $\mathbb{Z}[\theta]$ in A_K is given by

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

where $i_{\phi_j}(F)$ is $\deg \phi_j$ times the number of certain points with integral coordinates lying on or below the ϕ_j-Newton polygon of F (precise meaning of $i_{\phi_j}(F)$ is given by Eq. (3)). In 2012, using the results of Ore, El Fadil, Montes and Nart [7] 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

☆ The financial support by National Board for Higher Mathematics, Mumbai and CSIR (grant no. 09/135(0598)/2010-EMR-I) is gratefully acknowledged.
* Corresponding author.
E-mail addresses: skhanduja@iisermohali.ac.in (S.K. Khanduja), sanjeev_kumar_19@yahoo.co.in (S. Kumar).

0022-4049/$ – see front matter
http://dx.doi.org/10.1016/j.jpaa.2013.11.014

paper, we deal with the analogous problem for arbitrary Dedekind domains and replace the condition of p-regularity by a weaker one (see Theorem 1.3). The present paper extends the Theorem of Index of Ore [12] to arbitrary discrete valued fields without any restriction on the residue field. We give counterexamples to show that Criterion I on p. 326 of [12] is false (see Example 4.5) and that condition (iv) of the proposition on p. 328 of [12] does not imply the rest of the equivalent conditions (see Example 4.6). An extra necessary and sufficient condition has been given for these results to be true (cf. Theorems 1.5, 1.6). Our approach uses new ideas and involves residually transcendental prolongations of a valuation defined on a field L to a simple transcendental extension of L.

1. Definitions, notation and statement of results

Throughout v is a discrete valuation of a field K with value group $G_v = \mathbb{Z}$, valuation ring R_v, maximal ideal M_v and residue field R_v/M_v. Let π be a prime element of R_v. For an element ξ belonging to the valuation ring of v, $\bar{\xi}$ will denote its image under the canonical homomorphism from R_v onto R_v/M_v and for a polynomial $f(x)$ belonging to $R_v[x]$, $\bar{f}(x)$ will stand for the polynomial over R_v/M_v obtained on replacing each coefficient of $f(x)$ by its residue modulo M_v. We shall denote by v^x, the Gaussian valuation of the field $K(x)$ of rational functions in an indeterminate x which extends v and is defined on $K[x]$ by

$$v^x\left(\sum_i a_i x^i\right) = \min_i\{v(a_i)\}, \quad a_i \in K. \tag{1}$$

When (K, v) is a henselian valued field, then $\tilde{v}$ will stand for the unique prolongation of v to a fixed algebraic closure $\widetilde{K}$ of K whose value group is $G_{\tilde{v}} = \mathbb{Q}$. If L is a subfield of $\widetilde{K}$, then $\bar{L}, G(L)$ will denote respectively the residue field and the value group of the valuation of L obtained on restricting $\tilde{v}$. With the above notations, we introduce the concept of ϕ-Newton polygons.

Definition 1.A. Let $\phi(x)$ belonging to $R_v[x]$ be a monic polynomial of degree m with $\bar{\phi}(x)$ irreducible over R_v/M_v and $F(x)$ belonging to $K[x]$ be a polynomial not divisible by $\phi(x)$. Let $\sum_{i=0}^{n} A_i(x)\phi(x)^i$ with $\deg A_i(x) < m$, $A_n(x) \neq 0$ be the $\phi(x)$-expansion of $F(x)$ obtained on dividing it by successive powers of $\phi(x)$. The ϕ-Newton polygon of $F(x)$ (with respect to the underlying valuation v) is the polygonal path formed by the lower edges along the convex hull of the points $(j, v^x(A_{n-j}(x)))$, $0 \leqslant j \leqslant n$, $A_{n-j}(x) \neq 0$ with the slopes of edges increasing when calculated from left to right.

Definition 1.B. Let (K, v) be a henselian valued field. Let $\alpha \in \widetilde{K}$ be a root of a monic polynomial $\phi(x)$ belonging to $R_v[x]$ with $\bar{\phi}(x)$ irreducible over R_v/M_v. For any positive $\delta \in G_{\tilde{v}} = \mathbb{Q}$, let $\widetilde{w}_{\alpha,\delta}$ be the valuation on $\widetilde{K}$ extending $\tilde{v}$ defined by

$$\widetilde{w}_{\alpha,\delta}\left(\sum_i c_i(x-\alpha)^i\right) = \min_i\left\{\tilde{v}(c_i) + i\delta\right\}, \quad c_i \in \widetilde{K}. \tag{2}$$

The restriction of $\widetilde{w}_{\alpha,\delta}$ to $K(x)$ will be denoted by $w_{\alpha,\delta}$. The valuation $w_{\alpha,\delta}$ and its residue field are described by the following basic theorem proved in [1, Theorem 2.1].

Theorem 1.C. *Let (K, v) be a henselian valued field and $\phi(x)$, α, δ be as in Definition 1.B. Let m denote the degree of ϕ and (say) $w_{\alpha,\delta}(\phi(x)) = \lambda$. Then the following hold:*

(a) *For any polynomial $g(x)$ belonging to $K[x]$ with $\phi(x)$-expansion $\sum_i g_i(x)\phi(x)^i$, $\deg g_i(x) < m$, one has $w_{\alpha,\delta}(g(x)) = \min_i\{\tilde{v}(g_i(\alpha)) + i\lambda\}$.*
(b) *If $A(x)$ belonging to $K[x]$ is a polynomial of degree less than m, then the $\widetilde{w}_{\alpha,\delta}$-residue of $A(x)/A(\alpha)$ equals 1.*
(c) *Let e be the smallest positive integer such that $e\lambda \in \mathbb{Z}$, then the $w_{\alpha,\delta}$-residue Z of $\frac{\phi(x)^e}{\pi^{e\lambda}}$ is transcendental over $\overline{K(\alpha)}$ and the residue field of $w_{\alpha,\delta}$ is $\overline{K(\alpha)}(Z)$.*

The above theorem gives rise to the notion of liftings of polynomials with respect to the pair ϕ, λ given below.

Definition 1.D. Let $\phi(x)$, m, $w_{\alpha,\delta}$, λ, and e be as in Theorem 1.C. A monic polynomial $F(x)$ belonging to $K[x]$ is said to be a lifting of a monic polynomial $T(Y)$ belonging to $\overline{K(\alpha)}[Y]$ having degree $t \geqslant 1$ with respect to ϕ, λ if the following three conditions are satisfied: (i) $\deg F(x) = etm$; (ii) $w_{\alpha,\delta}(F(x)) = et\lambda$; (iii) the $w_{\alpha,\delta}$-residue of $F(x)/\pi^{et\lambda}$ is $T(Z)$, where Z is the $w_{\alpha,\delta}$-residue of $\phi(x)^e/\pi^{e\lambda}$.

The following already known result connects liftings of polynomials with ϕ-Newton polygons (see [9, Lemmas 2.1, 2.2]).

Proposition 1.E. *With the above notation, a monic polynomial $F(x)$ belonging to $R_v[x]$ having degree divisible by em is a lifting of a monic polynomial $T(Y)$ belonging to $\overline{K(\alpha)}[Y]$ not divisible by Y with respect to $\phi(x)$, λ if and only if the ϕ-Newton polygon of $F(x)$ has only one side and the side has slope λ.*