

On prolongations of rank one discrete valuations

LHOUSSAIN EL FADIL

Abstract. Let (K, ν) be a valued field, where ν is a rank one discrete valuation. Let R be its ring of valuation, \mathfrak{m} its maximal ideal, and L an extension of K , defined by a monic irreducible polynomial $F(X) \in R[X]$. Assume that $\overline{F}(X)$ factors as a product of r distinct powers of monic irreducible polynomials. In this paper a condition which guarantees the existence of exactly r distinct valuations of K extending ν is given, in such a way that it generalizes the results given in the paper “Prolongations of valuations to finite extensions” by S. K. Khanduja, M. Kumar (2010).

Keywords: discrete valuation; extension of valuation; prime ideal factorization

Classification: 13A18, 11S05

1. Introduction

Let K be a number field, defined by a monic irreducible polynomial $F(X) \in \mathbb{Z}[X]$, \mathbb{Z}_K its ring of integers, and $\text{ind}(\alpha) = [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ the index of $\mathbb{Z}[\alpha]$ in \mathbb{Z}_K . One of the most important problems in algebraic number theory is determining the factorization of a rational prime p into prime ideals of \mathbb{Z}_K . Due to Hensel’s theorem (see [5]), this problem is directly related to the factorization of $F(X)$ in $\mathbb{Q}_p[X]$.

If p does not divide the index $\text{ind}(\alpha)$, then a theorem of Kummer says that the factorization of $p\mathbb{Z}_K$ can be derived directly from the factorization of $\overline{F}(X)$ modulo p ; more precisely, if $\overline{F}(X) = \prod_{i=1}^r \overline{\varphi}_i(X)^{l_i}$ is the factorization of $\overline{F}(X)$ into the product of powers of distinct monic irreducible polynomials modulo p , then $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{p}_i^{l_i}$, where $\mathfrak{p}_i = (p, \varphi_i(\alpha))$ with ramification index $e(\mathfrak{p}_i/p) = l_i$ and residue degree $f(\mathfrak{p}_i/p) = \deg(\varphi_i)$. In this case, we say that the factorization of p in \mathbb{Z}_K is p -analogous to the factorization of $\overline{F}(X)$. So, in particular, there are exactly r distinct valuations of K extending ν_p . In 1878, R. Dedekind in [3] gave a criterion, which allows us to test if p does, or does not, divide the $\text{ind}(\alpha)$. In [6], S. Khanduja and M. Kumar showed that the condition “ p does not divide $\text{ind}(\alpha)$ ” is necessary for the existence of exactly r distinct prime ideals of \mathbb{Z}_K lying above p . They went on it in [7] to ask whether it is possible to find a weaker condition that guarantees the existence of exactly r distinct valuations of K extending ν_p with ramification indices and residue degrees all as above. In the same paper [7, Theorem 1.1], they gave a weaker sufficient condition. In [2], A. Deajim and

L. El Fadil improved [7, Theorem 1.1] in the context of number fields. The main goal of this paper is to give an improvement of [7, Theorem 1.1] and [2, Theorem 2.1] in the context of rank one discrete valuations.

2. Preliminaries

Throughout this paper, (K, ν) is a valued field, where ν is a rank one discrete valuation. By normalization, we can assume that the value group $G_\nu = \mathbb{Z}$. Let R be its ring of valuation, \mathfrak{m} its maximal ideal, and k_ν its residue field. Let K_ν be the ν -adic completion of K , R_ν its ring of valuation, and \mathfrak{m}_ν its maximal ideal. Let $\varphi \in R_\nu[X]$ be a monic polynomial whose reduction modulo \mathfrak{m}_ν is irreducible, \mathbb{F}_φ the finite field defined by \mathfrak{m}_ν and φ ; i.e, $\mathbb{F}_\varphi = R_\nu[X]/(\mathfrak{m}_\nu, \varphi) \simeq k_\nu[X]/\bar{\varphi}$ and let $\text{red}: R_\nu[X] \rightarrow \mathbb{F}_\varphi$ be the canonical projection. For any polynomial $F(X) \in R_\nu[X]$, by successive Euclidean division, $F(X)$ has a unique φ -adic expansion $F(X) = a_0(X)\varphi(X)^l + a_1(X)\varphi(X)^{l-1} + \dots + a_l(X)$ with for every $i := 0, \dots, l$ $a_i(X) \in R_\nu[X]$ and $\deg a_i(X) < \deg \varphi$ or $a_i(X) = 0$. The φ -Newton polygon of $F(X)$, with respect to the valuation ν , is first introduced by Ö. Ore when $\nu = \nu_p$ in [10] and developed by J. Guardia, J. Montes, and E. Nart in [4]. This notion was generalized to any discrete rank one valuation by D. Cohen, A. Movahhedi, and A. Salinier in their paper [1], and later by B. Jhorar and S. Khanduja in their paper [8], as the polygonal path formed by the lower edges along the convex hull of the points (i, u_i) , $u_i < \infty$, in the Euclidean plane, where $u_i = \nu(a_i(X))$. Geometrically, the φ -Newton polygon is represented by the process of joining all segments with an appropriate initial point with increasing slopes $\lambda_0 < \lambda_1 < \dots < \lambda_g$ when calculated from left to right. We shall write $N_\varphi(F) = S_0 + \dots + S_g$. The principal part of $N_\varphi(F)$, denoted by $N_\varphi^+(F)$, is the polygon determined by all sides of positive slopes of $N_\varphi(F)$. Since ν is a rank one discrete valuation, both of \mathfrak{m} and \mathfrak{m}_ν are principal ideals and generated by a common element with valuation 1, which we denote by p . For every $i = 0, \dots, n$, we attach to any abscissa the following residue coefficient $t_i \in \mathbb{F}_\varphi$ defined by

$$t_i = \begin{cases} 0 & \text{if } (i, u_i) \text{ lies strictly above } N_\varphi(F), \\ \text{red} \left(\frac{a_i(X)}{p^{u_i}} \right) \pmod{(p, \varphi(X))} & \text{if } (i, u_i) \text{ lies on } N_\varphi(F). \end{cases}$$

Let S be a side of $N_\varphi^+(F)$, with slope $\lambda = h/e$ such that h and e are positive coprime integers. Let $l = l(S)$ be the length of the projection of S to the x -axis and $d = l/e$ the degree of S . Note that, if s is the abscissa of the initial point of S , then S is divided into d segments by the points $(s, u_s), (s+e, u_s+h), \dots, (s+de, u_s+dh)$ of integer coordinates that lie on S . Let $F_S(Y) = t_s Y^d + t_{s+e} Y^{d-1} + \dots + t_{s+(d-1)e} Y + t_{s+de} \in \mathbb{F}_\varphi[Y]$ be the residual polynomial of $F(X)$ attached to S , where for every $i = 0, \dots, d$, t_{s+ie} is the residue coefficient. For more details see [1], [4], [8].

3. Main result

Throughout this section, $F(X) \in R[X]$ is a monic irreducible polynomial over K , α a root of $F(X)$ in an algebraic closure of K , L the field generated by α and K , \mathbb{Z}_L the integral closure of R in L , and we assume that $F(X) \equiv \prod_{i=1}^r \varphi_i^{l_i}(X) \pmod{\mathfrak{m}}$, where every $\varphi_i \in R[X]$ is a monic polynomial and whose reduction modulo \mathfrak{m} is irreducible. For every $i = 1, \dots, r$, let $F(X) = \sum_{j=0}^{L_i} a_j(X) \varphi_i^{L_i-j}(X)$ be the φ_i -adic expansion of $F(X)$ and $N_i = N_{\varphi_i}(F)$.

According to Newton polygon notations and terminology, [7, Theorem 1.1] can be reformulated as follows:

If for every $i = 1, \dots, r$, either $l_i = 1$, or $l_i \geq 2$ and N_i is only one side of degree $d_i = 1$, then there are exactly r distinct valuations ν_1, \dots, ν_r of L extending ν .

Recall that for any valued field (K, ν) , $(\widehat{K}, \widehat{\nu})$ is its ν -adic completion, let H be the separable closure of K in \widehat{K} . Then H is a Henselian field, called the Henselization of K with respect to ν (see [9, Chapter II, Section 6]).

Keep the same notation ν for the valuation of H extending ν and set R_H its ring of valuation. For any algebraic extension F of H , denote by ν_F the restriction to F of the unique extension of ν to the algebraic closure of H .

In order to improve this theorem, we need the following lemmas:

Lemma 3.1 ([7, Theorem 2.D]). *Let (K, ν) be a valued field, $K(\theta)$ an algebraic extension of K , $F(X)$ the minimal polynomial of θ over K , and H the Henselization of (K, ν) . Then, the valuations ν_1, \dots, ν_t of $K(\theta)$ extending ν are in one-to-one correspondence with the irreducible factors $F_1(X), \dots, F_t(X)$ of $F(X)$ in $H[X]$. Moreover, for any $i = 1, \dots, t$, the valuation ν_i attached to $F_i(X)$ is defined precisely by*

$$\nu_i \left(\sum_j a_j \theta^j \right) = \nu_H \left(\sum_j a_j \theta_i^j \right)$$

for any root θ_i of $F_i(X)$ and $a_j \in K$.

Lemma 3.2. *Assume that $F(X) \in R[X]$ is a monic irreducible polynomial which is congruent to a power of $\overline{\varphi}(X)$ with $\varphi(X) \in R[X]$ being monic, whose reduction modulo \mathfrak{m} is irreducible. Let α be a root of $F(X)$, $L = K(\alpha)$, \mathbb{Z}_L the integral closure of R in L . Then for every valuation ω of L extending ν , and for every polynomial $P(X) \in R[X]$, $\omega(P(\alpha)) \geq \nu(P(X))$. The equality holds if and only if $\overline{\varphi}(X)$ does not divide $\overline{P}_1(X)$, where $P_1(X) = P(X)/p^\nu$ and $\nu = \nu(P(X))$. In particular, if $\deg(P) < \deg(\varphi)$, then $\omega(P(\alpha)) = \nu(P(X))$.*

PROOF: Let ω be a valuation of L extending ν . Since α is integral over R and $P_1(X) \in R[X]$, $P_1(\alpha)$ is integral over R , and thus $\omega(P_1(\alpha)) \geq 0$. Thus, $\omega(P(\alpha)) \geq \nu = \nu(P(X))$. Since $\overline{F}(X)$ is congruent to a power of $\overline{\varphi}(X)$, $\omega(\varphi(\alpha)) > 0$. Let $\mathfrak{p} = m_\omega \cap \mathbb{Z}_L$, where m_ω is the maximal ideal of ω . Then \mathfrak{p} contains $\varphi(\alpha)$. Consider the following homomorphism $\psi: k_\nu[X] \rightarrow \mathbb{Z}_L/\mathfrak{p}$ of rings defined by $\psi(\overline{g}(X)) = \overline{g(\alpha)}$. Since $\omega(\varphi(\alpha)) > 0$, $\overline{\varphi}(X)$ is the minimal polynomial of $\overline{\alpha}$ over k_ν , $\text{Ker } \psi$ is the

principal ideal of $k_\nu[X]$ generated by $\bar{\varphi}(X)$. Let $P(X) \in R[X]$. If $\omega(P(\alpha)) > \nu$; $\omega(P_1(\alpha)) > 0$, then $P_1(\alpha) \equiv 0 \pmod{\mathfrak{p}}$, i.e., $\bar{\varphi}(X)$ divides $\overline{P_1(X)}$. \square

The following theorem gives us much weaker sufficient condition on $F(X)$ that guarantees the existence of exactly r distinct valuations ν_1, \dots, ν_r of L extending ν and for every extension ν_i , the ramification index $e(\nu_i)$ and the residue degree $f(\nu_i)$ are given too. In such a way it generalizes [2, Theorem 2.1] and [7, Theorem 1.1] in the context of discrete rank one valued fields.

Theorem 3.3. *If for every $i := 1, \dots, r$, either $l_i = 1$ or, $l_i \geq 2$, N_i is a single side, and $F_{N_i}(Y)$ is irreducible, then there are exactly r distinct valuations ν_1, \dots, ν_r of L extending ν . Moreover for every $i = 1, \dots, r$, $f(\nu_i) = m_i d_i$, and $e(\nu_i) = l_i / d_i$, where $m_i = \deg(\varphi_i)$, $d_i = \gcd(\nu(a_{L_i}(X)), l_i)$.*

PROOF: First, since H is a Henselian field and $F(X) \equiv \prod_{i=1}^r \varphi_i^{l_i}(X) \pmod{\mathfrak{m}}$, by Hensel's lemma, we can split $F(X) = \prod_{i=1}^r F_i(X)$ in $R_H[X]$, where for every $i = 1, \dots, r$, $F_i(X) \equiv \varphi_i^{l_i}(X) \pmod{\mathfrak{m}}$ and R_H is the ring of valuation of (H, ν_H) . So, by [9, Proposition 8.2], there are at least r distinct valuations ν_1, \dots, ν_r of L extending ν . If for every $i = 1, \dots, r$, $l_i = 1$, then every $F_i(X)$ is irreducible in $H[X]$ and there are exactly r distinct valuations ν_1, \dots, ν_r of L extending ν such that for every $i = 1, \dots, r$, $f(\nu_i) = m_i$, and $e(\nu_i) = l_i$. In this case since $l_i = 1$, $d_i = 1$ too. If there exists i such that $l_i \geq 2$, so again by [9, Proposition 8.2], it suffices to have every $F_i(X)$ irreducible in $H[X]$. Fix $i = 1, \dots, r$. By [1, Theorem 3.2, page 187] and by assumption, $N_{\varphi_i}(F_i) = N_{\varphi_i}(F) = N_i$ is a single side up to a translation and $F_{iN_i}(Y) = F_{N_i}(Y)$ up to multiplying by a nonzero constant. As $F_{N_i}(Y)$ is irreducible in $\mathbb{F}_{\varphi_i}[Y]$, $F_{iN_i}(Y)$ is irreducible too in $\mathbb{F}_{\varphi_i}[Y]$. So by [1, Theorem 1.6], $F_i(X)$ is irreducible in $H[X]$. Finally, for every $i = 1, \dots, r$, $F_i(X)$ is irreducible in $R_H[X]$, and there are exactly r distinct valuations ν_1, \dots, ν_r of L extending ν .

We next calculate the ramification index and the residue degree of each valuation ν_i . To simplify notations, fix $i = 1, \dots, r$ and set $f(X) = F_i(X)$, $\varphi(X) = \varphi_i(X)$, $l = l_i$, α a root of $f(X)$, $L = H(\alpha)$ the local field, \mathfrak{p} its maximal ideal, and \mathbb{Z}_L its ring of valuation. Let $f(X) = \varphi(X)^L + \dots + a_L(X)$ be the φ -adic expansion of $f(X)$. As $\bar{f}(X)$ is a power of $\bar{\varphi}(X)$ modulo \mathfrak{m}_ν , $L = l$. Let $\nu_l = \nu(a_l(X))$ and $p \in R$ such that $\nu(p) = 1$. As N_i is one side of slope λ , $\nu_l = l\lambda$. Since $\overline{\varphi(X)}$ is the minimal polynomial of $\bar{\alpha} \pmod{\mathfrak{m}_\nu}$ over k_ν and $\overline{\varphi(X)}$ does not divide $\overline{(a_l(X)/p^\nu)}$, by Lemma 3.2, we have $\overline{(a_l(\alpha)/p^\nu)} \neq \bar{0}$ modulo \mathfrak{m}_ν . Thus, $\nu_i(a_l(\alpha)) = \nu(a_l(X)) = l\lambda$. We now show that $\nu_i(\varphi(\alpha)) = \lambda$. Note that as N_i is a single side, $\nu(a_j(X)) \geq j\lambda$ for every $j = 1, \dots, l-1$. So $\nu_i(a_j(\alpha)) \geq j\lambda$ since α is integral over R_H . Thus, for every $j = 1, \dots, l-1$, $\nu_i(a_j(\alpha))\varphi(\alpha)^{l-j} \geq j\lambda + (l-j)u$, where $u = \nu_i(\varphi(\alpha))$. If $u \neq \lambda$, then it follows from the φ -adic expansion of $f(X)$ that $\nu_i(f(\alpha)) = \min\{lu, l\lambda\}$, which is impossible since $\nu_i(f(\alpha)) = \infty$. Thus, $u = \lambda$ as claimed.

Now let us show that the value group of ν_i is $\mathbb{Z}[\lambda]$, the subgroup of \mathbb{Q} generated by 1 and λ . For every $P(X) \in R[X]$, let the $P(X) = g_0(X)\varphi^l(X) + g_1(X)\varphi^{l-1}(X) + \dots + g_{l-1}(X)\varphi(X) + g_l(X)$ be the φ -adic expansion of $P(X)$.

Since $\nu_i(\varphi(\alpha)) = \lambda$ for each $j = 0, \dots, l$, $\nu_i(g_j(\alpha)\varphi^{l-j}(\alpha)) = n_j + (l - j)\lambda$, where $n_j = \nu_i(g_j(\alpha)) \in \mathbb{Z}$. Thus, $\nu_i(P(\alpha)) \in \mathbb{Z}[\lambda]$. As every element of K is of the form $P(\alpha)/b$ for some $P(X), b \in R[X] \times R^*$, the value group of ν_i is $\mathbb{Z}[\lambda]$. So, the ramification index $e(\nu_i)$ is the index $[\mathbb{Z}[\lambda] : \mathbb{Z}] = l/d$. As ν is discrete, the residue degree is $f(\nu_i) = (\deg(f))/e(\nu_i) = lm/e(\nu_i) = md$. □

Corollary 3.4. *Let R be a Dedekind domain with quotient field K and $L = K(\alpha)$, where $\alpha \in \bar{K}$ is a root of a monic irreducible polynomial $F(X) \in R[X]$.*

If for every $i := 1, \dots, r$, either $l_i = 1$ or, $l_i \geq 2$, N_i is only one side, and $F_{N_i}(Y)$ is irreducible, then there are exactly r distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of \mathbb{Z}_L lying above \mathfrak{m} and $\mathfrak{m}\mathbb{Z}_L = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, where for every $i = 1, \dots, r$, $f(\mathfrak{p}_i/\mathfrak{m}) = m_i d_i$, $e_i = l_i/d_i$, $m_i = \deg(\varphi_i)$, and $d_i = \gcd(\nu(a_{L_i}(X)), l_i)$.

4. Examples

The following examples show the advantage of Theorem 3.3 over the result of S.K. Khanduja and M. Kumar. The second and fourth examples present situations where Theorem 3.3 is not applicable.

Example 4.1. Let $R = \mathbb{F}_3[[X]]$ be the ring of formal power series over \mathbb{F}_3 , K its quotient field, and $F(Y) = Y^3 + XY^2 + X^2Y - X^3$. It is well known that K is a valued field according to the discrete valuation ν defined by $\nu(X) = 1$, R its ring of valuation, and $\mathfrak{m} = (X)$ its maximal ideal. Since $F(Y)$ is X -Eisenstein, $F(Y)$ is irreducible over R . Let $L = K(\alpha)$, where α is a root of $F(Y)$. Let $\varphi = Y$. Then $F(Y) \equiv \varphi^3 \pmod{\mathfrak{m}}$, $N_\varphi(F) = S$ is only one side with degree $d = 3$ such that $F_S(T) = T^3 + T^2 + T - 1$ is irreducible over \mathbb{F}_φ . Thus, there is only one valuation ν extending ν to L , where $e(\nu) = 1$, and $f(\nu) = 3$.

Example 4.2. Again $R = \mathbb{F}_3[[X]]$ be the ring of formal power series over \mathbb{F}_3 , K its quotient field, and $F(Y) = Y^3 + XY^2 + XY - X^3$. For the same reason, $F(X)$ is irreducible over K and $F(Y) \equiv \varphi^3 \pmod{\mathfrak{m}}$, where $\varphi = Y$. But $N_\varphi(F) = S_1 + S_2$ is two sides with respective slopes $1/2$ and 2 . Thus, there are at least two valuations of L extending ν , where $L = K(\alpha)$ and α is a root of $F(Y)$.

Example 4.3. Let ν_2 be the 2-adic valuation defined on \mathbb{Q} . Then (\mathbb{Q}, ν_2) is a valued field and $\mathbb{Z}_2 = \{a/b : (a, b) \in \mathbb{Z} \times \mathbb{N}, b \notin 2\mathbb{N}\}$ its ring of valuation. Consider $F(X) = X^6 + 12X^3 + 48 \in \mathbb{Z}[X]$. As $F(X)$ is 3-Eisenstein, it is irreducible over \mathbb{Q} . Let $L = \mathbb{Q}(\alpha)$ where α is a complex root of $F(X)$. Since $F(X) \equiv X^6 \pmod{2}$ and for $\varphi(X) = X$, $F(X) = \varphi(X)^6 + 12\varphi(X)^3 + 48$, $N_\varphi(F) = S$ is one side of slope $\lambda = 2/3$, $d = 2$, and $F_S(Y) = Y^2 + Y + 1$ which is irreducible over $\mathbb{F}_\varphi = \mathbb{F}_2$ (because $\deg(\varphi) = 1$). It follows that there is only one valuation ν_2 of L extending ν_2 , where $e(\nu_2) = 3$, and $f(\nu_2) = 2$.

Example 4.4. Let $F(X) = X^5 + 3X^3 + 6X^2 + 12X + 24 \in \mathbb{Z}[X]$. For the same reason, $F(X)$ is irreducible over \mathbb{Q} . Let $L = \mathbb{Q}(\alpha)$ where α is a complex root of $F(X)$. Since $F(X) \equiv X^3(X-1)^2 \pmod{2}$ and for $\varphi(X) = X$, $F(X) = \varphi(X)^5 + 3\varphi(X)^3 + 6\varphi^2 + 12\varphi + 24$. So, $N_\varphi^+(F) = S$ is one side of slope $\lambda = 1$, $d = 3$, and $F_S(Y) = Y^3 + Y^2 + Y + 1$ which is reducible over $\mathbb{F}_\varphi = \mathbb{F}_2$. It follows that there are at least 3 valuations of L extending ν_2 .

Acknowledgment. The author is very grateful to Professor Enric Nart for introducing him to Newton polygon techniques when he was a post-doc in 2007–2008 at CRM, Barcelona, Spain.

REFERENCES

- [1] Cohen S. D., Movahhedi A., Salinier A., *Factorization over local fields and the irreducibility of generalized difference polynomials*, *Mathematika* **47** (2000), no. 1–2, 173–196.
- [2] Deajim A., El Fadil L., *On the extensions of a discrete valuation in a number field*, *Math. Slovaca* **69** (2019), no. 5, 1009–1022.
- [3] Dedekind R., *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* **23** (1878), 3–38 (German).
- [4] Guàrdia J., Montes J., Nart E., *Newton polygons of higher order in algebraic number theory*, *Trans. Amer. Math. Soc.* **364** (2012), no. 1, 361–416.
- [5] Hensel K., *Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante*, *J. Reine Angew. Math.* **113** (1894), 61–83 (German).
- [6] Khanduja S. K., Kumar M., *On a theorem of Dedekind*, *Int. J. Number Theory* **4** (2008), no. 6, 1019–1025.
- [7] Khanduja S. K., Kumar M., *Prolongations of valuations to finite extensions*, *Manuscripta Math.* **131** (2010), no. 3–4, 323–334.
- [8] Khanduja S. K., Kumar M., *A generalization of a theorem of Ore*, *J. Pure Appl. Algebra* **218** (2014), no. 7, 1206–1218.
- [9] Neukirch J., *Algebraic Number Theory*, *Grundlehren der Mathematischen Wissenschaften*, 322, Springer, Berlin, 1999.
- [10] Ore Ö., *Newtonsche Polygone in der Theorie der algebraischen Körper*, *Math. Ann.* **99** (1928), no. 1, 84–117 (German).

L. El Fadil:

FACULTY OF SCIENCES DHAR-EL MAHRAZ, P. O. BOX 1796-ATLAS,
SIDI MOHAMED BEN ABDULLAH UNIVERSITY, FES, MOROCCO

E-mail: lhouelfadil2@gmail.com

(Received May 18, 2018, revised March 28, 2019)