Journal of Algebraic Systems
Vol. 11, No. 2, (2024), pp 83-91

A CLASSIFICATION OF EXTENSIONS GENERATED BY A ROOT OF AN EISENSTEIN-DUMAS POLYNOMIAL

A. NIKSERESHT

Abstract. It is known that for a discrete valuation v of a field K with value group $\mathbb{Z}$, an valued extension field (K', v') of (K, v) is generated by a root of an Eisenstein polynomial with respect to v having coefficients in K if and only if the extension $(K', v')/(K, v)$ is totally ramified. The aim of this paper is to present the analogue of this result for valued field extensions generated by a root of an Eisenstein-Dumas polynomial with respect to a more general valuation (which is not necessarily discrete). This leads to classify such algebraic extensions of valued fields.

1. Introduction and preliminaries

The earliest and probably best known irreducibility criterion is the Eisenstein irreducibility criterion:

Eisenstein criterion [3]**.** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with coefficients in the ring $\mathbb{Z}$ of integers. Suppose that there exists a prime number p such that

(i) a_n is not divisible by p,
(ii) a_i is divisible by p for $0 \leq i \leq n-1$,
(iii) a_0 is not divisible by p^2.

Then $f(x)$ is irreducible over the field $\mathbb{Q}$ of rational integers.

DOI: 10.22044/JAS.2022.11808.1603.
MSC(2010): Primary: 12F05; Secondary: 12J10, 12E05.
Keywords: Algebraic field extensions; Valued fields; Polynomials in general fields.
Received: 7 April 2022, Accepted: 21 October 2022.

The second best known irreducibility criterion based on divisibility of the coefficients by a prime is the so called Dumas irreducibility criterion, due to Gustave Dumas:

Dumas criterion [2]**.** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with coefficients in $\mathbb{Z}$. Suppose that there exists a prime p whose exact power p^{r_i} dividing a_i (where r_i is the largest with this property and $r_i = \infty$ if $a_i = 0$), $0 \leq i \leq n$, satisfy

(i) $r_n = 0$,
(ii) $\frac{r_i}{n-i} \geq \frac{r_0}{n}$ for $0 \leq i \leq n-1$,
(iii) $\gcd(r_0, n) = 1$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

Example. $x^3 + 3x^2 + 9x + 9$ is irreducible over $\mathbb{Q}$ by applying Dumas criterion.

We note that Eisenstein's criterion is a special case of Dumas criterion with $r_0 = 1$.

In 1923, Joseph Kürschák extended Dumas criterion to polynomials over more general fields by employing the notion of valuation [8]. He was the first who formulated the formal definition of valuation on a field in 1912 [9]. It is now well-known that valuations are the basic and the most important concept in valuation theory. They were first introduced as "p-adic valuations" over the field $\mathbb{Q}$ and later extended to arbitrary fields.

p-adic valuation of $\mathbb{Q}$. For a given prime number p, let v_p stand for the surjective map $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ defined as follows. Write any non-zero rational number $x = p^r \frac{a}{b}$, $p \nmid ab$. Set $v_p(x) = r$. Then

(i) $v_p(xy) = v_p(x) + v_p(y)$,
(ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Set $v_p(0) = \infty$ where (by convention) ∞ is a symbol satisfying

$$\infty + \infty = \infty + \gamma = \gamma + \infty = \infty,$$

for every $\gamma \in \mathbb{Z}$. Then v_p is called the p-adic valuation of (or on) $\mathbb{Q}$.

By the above definition for a non-zero integer n and a prime p, $v_p(n)$ stands for the largest integer i such that $p^i | n$. This leads to the following expression of Dumas criterion:

Dumas criterion (by using p-adic valuations). Let

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

be a polynomial with coefficients in $\mathbb{Z}$. Suppose there exists a prime number p such that

(i) $v_p(a_n) = 0$,
(ii) $\frac{v_p(a_i)}{n-i} \geq \frac{v_p(a_0)}{n}$ for $0 \leq i \leq n-1$,
(iii) $\gcd(v_p(a_0), n) = 1$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

In 1932, Krull generalized the notion of valuations over arbitrary fields [6] as follows:

Krull valuation of a field K. Let K be a field and $G(K)$ be a totally ordered additive abelian group. A surjective map

$$v : K \longrightarrow G(K) \cup \{\infty\}$$

satisfying

(i) $v(xy) = v(x) + v(y)$,
(ii) $v(x+y) \geq \min\{v(x), v(y)\}$,
(iii) $v(0) = \infty$,

is called a (Krull) valuation of (or on) K; and the pair (K, v) is called a valued field. Moreover, $G(K)$ is called the value group of (K, v).

For a valued field (K, v), the subring $\mathcal{O}_v = \{x \in K |\ v(x) \geq 0\}$ of K is called the valuation ring of v. It has a unique maximal ideal given by $\mathcal{M}_v = \{x \in K |\ v(x) > 0\}$. $\mathcal{O}_v/\mathcal{M}_v$ is called the residue field of v and denoted by $R(K)$.

A valuation is said to be discrete if its value group is isomorphic to $\mathbb{Z}$. p-adic valuations of $\mathbb{Q}$ are the most famous examples of discrete valuations. With the above definitions and notations, we are now in a position to present a generalization of Eisenstein irreducibility criterion by applying discrete valuations of an arbitrary field K (see [10, Chapter 3, C]):

Theorem 1.A. *Let K be a field and v be a discrete valuation of K. If*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathcal{O}_v[x]$$

is such that $a_i \in \mathcal{M}_v$ for every $0 \leq i \leq n-1$ and $a_0 \notin {\mathcal{M}_v}^2$, then $f(x)$ is irreducible over K.

Eisenstein polynomial with respect to v. A polynomial which satisfies the hypothesis of Theorem 1.A is called an Eisenstein polynomial with respect to v (or (K, v)).

Another generalization of Eisenstein irreducibility criterion, which is more general and strengthened than the above one, was provided by

Khanduja and Saha in 1997 [5]. They presented the following test over arbitrary valued fields (not necessarily discrete) [5, Corollary 1.2]:

Theorem 1.B. *Let v be a valuation of a field K and*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

be a polynomial over K. If

(i) $\frac{v(a_i)}{n-i} \geq \frac{v(a_0)}{n} > 0$ *for* $0 \leq i \leq n-1$, *and*
(ii) *there does not exist any integer $d > 1$ dividing n such that* $\frac{v(a_0)}{d} \in G(K)$,

then $f(x)$ is irreducible over K.

The foregoing result led to the definition of Eisenstein-Dumas polynomial with respect to an arbitrary (Krull) valued field (see [1]):

Eisenstein-Dumas polynomial with respect to v. A polynomial which satisfies the assumption of Theorem 1.B is called an Eisenstein-Dumas polynomial with respect to v (or (K, v)).

In order to explain the main result of this paper, we also need to remark some notions about extension of valued fields in valuation theory.

Let K'/K be a field extension, v a valuation of K and v' a valuation of K'. We say that (K', v') is an extension of (K, v) (or v' is an extension of v to K') if $v'|_K = v$ (i.e., v is the restriction of v' to K) and denote it by $(K', v')/(K, v)$ (or briefly by K'/K whenever the valuations are clear from the context).

A valued field (K, v) is said to be henselian if it has a unique extension to the algebraic closure $\widetilde{K}$ of K, or equivalently, if it admits a unique extension of the valuation to every algebraic extension field. Henselian valuations have a prominent position in valuation theory (see for example [4, Chapter 4] or [10, Section 3.2]).

For a valued field extension $(K', v')/(K, v)$, $G(K)$ is a subgroup of $G(K')$ and also $R(K)$ is a subfield of $R(K')$ (see [4, Section 3.2]). When K'/K is finite, the extension $(K', v')/(K, v)$ is called totally ramified if $[K' : K] = [G(K') : G(K)]$.

In [10, Chapter 4, H], it is provided a characterization of finite extensions generated by a root of some Eisenstein polynomial with respect to a discrete valuation. More precisely, it is proved that a finite extension (K', v') of a discrete valued field (K, v) is generated by a root of some Eisenstein polynomial with respect to v having coefficients in K if and only if the extension $(K', v')/(K, v)$ is totally ramified. Here we present a similar characterization of the extensions generated by a

root of some Eisenstein-Dumas polynomial with respect to a (Krull) henselian valuation. Indeed, it is shown that

Theorem 1.1. *Let (K, v) be a henselian valued field and K'/K be a finite extension of fields. Denote by $\widetilde{K}$ the algebraic closure of K. Then the following statements are equivalent:*

(i) *$K' = K(\theta)$ for some $\theta \in \widetilde{K}$, where the minimal polynomial of θ over K is an Eisenstein-Dumas polynomial with respect to v.*
(ii) *The extension K'/K is totally ramified and the quotient group $G(K')/G(K)$ is cyclic.*

2. Defectless extensions

This section is devoted to provide some definitions and preliminary results related to the concept of defectless extensions needed in the last section.

Take an arbitrary extension of valued fields $(K', v')/(K, v)$. As we have mentioned in the introduction, the value group $G(K)$ is a subgroup of the value group $G(K')$ and the residue field $R(K)$ is a subfield of the residue field $R(K')$. Accordingly, the index $[G(K') : G(K)]$ is called the ramification index of this extension and the degree $[R(K') : (K)]$ is called its inertia degree (see [4, Section 3.2]). The following result gives an important relation between the degree of a finite extension, its ramification indexes and its inertia degrees (see [4, Theorem 3.3.4] or [7, Theorem 7.49]).

Theorem 2.1. (Fundamental inequality) *Let (K, v) be a valued field and K' a finite extension of K. Let $v_1, \dots, v_r$ be all distinct extensions of v to K'. Then we have the fundamental inequality*

$$[K' : K] \geq \sum_{i=1}^{r} [G_i'(K') : G(K)][R_i'(K') : R(K)], \tag{2.1}$$

where $G_i'(K')$ and $R_i'(K')$ are respectively the value group and the residue field of the valued field (K', v_i') for every $1 \leq i \leq r$.

A valued field (K, v) is called defectless in a finite extension K' of K if equality holds in (2.1).

From the multiplicativity of extension degree, ramification index and inertia degree, we obtain the multiplicativity of the defectlessness.

Proposition 2.2. [7, Lemma 11.6] *Let (K, v) be a valued field, L/K a finite extension and K'/K a subextension of L/K. Let $v_1, \dots, v_r$ be all extensions of v from K to K'. Then (K, v) is defectless in L if and*

only if (K,v) *is defectless in* K' *and* (K',v_i) *is defectless in* L *for every* $1 \leq i \leq r$.

Finally we remark some facts about henselian valued fields needed in the proof of Theorem 1.1. Take a henselian valued field (K,v). We always fix a unique extension of v to the algebraic closure $\widetilde{K}$ of K and denote it by $\tilde{v}$. For every algebraic extension K' of K, the unique extension of v to K' is the restriction of $\tilde{v}$ to K', denoted again by $\tilde{v}$. In this case, we mostly drop the valuation on K'; and hence express the extension $(K',\tilde{v})/(K,v)$ by K'/K. Thus, by the property of being henselian and the above notions, a finite extension K'/K of henselian valued fields is said to be defectless if

$$[K':K] = [G(K'):G(K)][R(K'):R(K)].$$

Accordingly, we can present an immediate consequence of Proposition 2.2 for henselian valued field extensions:

Corollary 2.3. *Suppose that* (K,v) *is a henselian valued field,* L/K *is a finite extension and* K'/K *is a subextension of* L/K. *Then* (K,v) *is defectless in* L *if and only if* (K,v) *is defectless in* K' *and* $(K',\tilde{v})$ *is defectless in* L.

3. Proof of Theorem 1.1

Set $[K':K] = n$ and consider the unique extension of v to the algebraic closure $\widetilde{K}$ of K by $\tilde{v}$.

To prove (i)⇒(ii), suppose that $K' = K(\theta)$ for some $\theta \in \widetilde{K}$ with the minimal polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in K[x]$$

being an Eisenstein-Dumas polynomial with respect to v. Let $\theta = \theta_1, \ldots, \theta_n \in \widetilde{K}$ be the roots of $f(x)$. Since $\tilde{v}$ is henselian, we have $\tilde{v}(\theta_1) = \cdots = \tilde{v}(\theta_n)$ (see [4, Proposition 3.2.16]). This implies that

$$v(a_0) = v((-1)^n\theta_1 \cdots \theta_n) = v(\theta_1 \cdots \theta_n) = n\tilde{v}(\theta).$$

Denote $\tilde{v}(\theta) = \frac{v(a_0)}{n}$ by δ. It is clear that

$$G(K) \subseteq G(K) + \mathbb{Z}\delta \subseteq G(K(\theta)). \tag{3.1}$$

We claim that the order of $\delta + G(K)$ in the quotient group $\frac{G(K)+\mathbb{Z}\delta}{G(K)}$ is equal to n. It is obvious that $n(\delta+G(K)) = v(a_0)+G(K) = G(K)$; and n is the smallest positive integer with this property because if (otherwise) there would exist $r < n$ $(r \mid n)$ with $r\delta \in G(K)$, then there would also exist $d > 1$ dividing n such that $\frac{v(a_0)}{d} \in G(K)$, which contradicts to the hypothesis that $f(x)$ is an Eisenstein-Dumas polynomial with

respect to v. Therefore, one has $[G(K)+\mathbb{Z}\delta : G(K)] = n$; hence the fundamental inequality (2.1) together with (3.1) implies that

$$\begin{aligned} n = [K' : K] = [K(\theta) : K] &\geq [G(K(\theta)) : G(K)] \\ &\geq [G(K)+\mathbb{Z}\delta : G(K)] \\ &= n. \end{aligned}$$

So one obtains $[K(\theta) : K] = [G(K(\theta)) : G(K)]$, showing that $K(\theta)/K$ (or K'/K) is totally ramified. Moreover, the equation

$$[G(K(\theta)) : G(K)] = [G(K)+\mathbb{Z}\delta : G(K)]$$

together with (3.1) shows that $G(K(\theta)) = G(K)+\mathbb{Z}\delta$. Since the quotient group $\frac{G(K)+\mathbb{Z}\delta}{G(K)}$ is cyclic, we deduce that $\frac{G(K(\theta))}{G(K)}$ (or $\frac{G(K')}{G(K)}$) is cyclic too, which completes the proof.

For (ii)⇒(i), since the extension K'/K is totally ramified, one observes

$$n = [K' : K] = [G(K') : G(K)]. \tag{3.2}$$

Keeping in mind the hypothesis that $\frac{G(K')}{G(K)}$ is cyclic, so there exists $\theta \in K'$ such that $\tilde{v}(\theta) + G(K)$ is a generator of the quotient group $\frac{G(K')}{G(K)}$ of order n. Hence by the properties of the valuation $\tilde{v}$ (i.e., $\tilde{v}(\theta^{-1}) = -\tilde{v}(\theta)$ (see [4, Section 2.1])), we may assume that $\tilde{v}(\theta) > 0$.

We first show that $K' = K(\theta)$. Since $\theta \in K'$, one sees that

$$G(K(\theta)) \subseteq G(K').$$

Besides, $\tilde{v}(\theta) + G(K) \in \frac{G(K(\theta))}{G(K)}$ is a generator of $\frac{G(K')}{G(K)}$; hence

$$G(K') \subseteq G(K(\theta)).$$

Therefore,

$$G(K') = G(K(\theta)). \tag{3.3}$$

On the other hand, by the fundamental inequality (2.1), one has

$$[K' : K] \geq [G(K') : G(K)][R(K') : R(K)].$$

This together with the assumption that K'/K is totally ramified (the equation (3.2)) yields $R(K') = R(K)$. Since $\theta \in K'$, we see that $R(K) \subseteq R(K(\theta)) \subseteq R(K')$. Hence the equality $R(K') = R(K)$ implies that

$$R(K') = R(K(\theta)). \tag{3.4}$$

Again by applying the assumption of K'/K being totally ramified, we conclude that K'/K is defectless, and hence using Corollary 2.3, $K'/K(\theta)$ is also defectless. So

$$[K' : K(\theta)] = [G(K') : G(K(\theta))][R(K') : R(K(\theta))].$$

Therefore, by virtue of (3.3) and (3.4), one obtains $K' = K(\theta)$, as desired.

Now consider $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ as the minimal polynomial of θ over K. The proof of the theorem is complete once we show that $f(x)$ is an Eisenstein-Dumas polynomial with respect to v. As pointed out in the proof of (i)⇒(ii), $v(a_0) = n\tilde{v}(\theta) > 0$. Moreover, we can claim that there exist at least two indices j and k with $0 \leq j < k \leq n$ such that

$$\min_{0\leq i\leq n}\{\tilde{v}(a_i\theta^i)\} = \tilde{v}(a_j\theta^j) = \tilde{v}(a_k\theta^k), \tag{3.5}$$

because (otherwise) there would exist one j, $0 \leq j \leq n$, such that

$$\min_{0\leq i\leq n}\{\tilde{v}(a_i\theta^i)\} = \tilde{v}(a_j\theta^j).$$

So by the strong triangle law (see [4, page 28]),

$$\infty = \tilde{v}(g(\theta)) = \tilde{v}(\sum_{i=0}^{n} a_i\theta^i) = \min_{0\leq i\leq n}\{\tilde{v}(a_i\theta^i)\} = \tilde{v}(a_j\theta^j).$$

Therefore, $\infty = v(a_j)+j\tilde{v}(\theta)$; and hence $\infty = v(a_j)+j\frac{v(a_0)}{n}$. One would conclude from $a_0 \neq 0$ that $a_j = 0$, a contradiction. This completes the proof of the claim and verifies (3.5).

According to (3.5), $v(a_j) + j\tilde{v}(\theta) = v(a_k) + k\tilde{v}(\theta)$; and hence

$$(k-j)\tilde{v}(\theta) = v(a_j) - v(a_k) \in G(K).$$

From the fact that n is the smallest positive integer such that $n\tilde{v}(\theta) \in G(K)$, one sees that $j = 0$ and $k = n$. Consequently, for every $0 \leq i \leq n$, (3.5) becomes

$$v(a_0) = n\tilde{v}(\theta) \leq v(a_i) + i\tilde{v}(\theta).$$

This shows that for every $0 \leq i \leq n-1$,

$$\frac{v(a_i)}{n-i} \geq \frac{v(a_0)}{n} = \tilde{v}(\theta) > 0.$$

It remains to show that there does not exist any integer $d > 1$ dividing n such that $\frac{v(a_0)}{d} \in G(K)$. This can be easily obtained because if (otherwise) there would exist $d_0 > 1$ dividing n such that $\frac{v(a_0)}{d_0} \in G(K)$, then there would exist a positive integer $r < n$ such that $r\tilde{v}(\theta) \in G(K)$, contradicting the assumption that $\tilde{v}(\theta) + G(K)$ is a generator of the quotient group $\frac{G(K')}{G(K)}$ of order n.

References

1. R. Brown, Roots of generalized Schönemann polynomials in henselian extension fields, *Indian J. Pure Appl. Math.*, **39** (2008), 403–410.
2. G. Dumas, Sur quelques cas d'irreductibilité des polynômes á coefficients rationnels, *Journal de Math. Pure et Appl.*, **2** (1906), 191–258.
3. G. Eisenstein, Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, *J. Reine Angew. Math.*, **39** (1850), 160–182.
4. A. J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, Berlin, 2005.
5. S. K. Khanduja and J. Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika*, **44**(1) (1997), 37–41.
6. W. Krull, Allgemeine bewertungstheorie, *Journ. f. d. reine u. angewandte Math.*, **167** (1932), 160–196.
7. F.-V. Kuhlmann, *Valuation theory of fields, abelian groups and modules*, monograph in preparation, preliminary versions of several chapters are available on the web site http //: math.usask.ca/ fvk/Fvkbook.htm
8. J. Kürschák, Irreduzible formen, *J. Reine Angew. Math.*, **152** (1923), 180–191.
9. J. Kürschák, Über Limesbildung und allgemeine Körpertheorie, *Proceedings of the 5th International Congress of Mathematicians Cambridge 1912*, **1** (1913), 285–289.
10. P. Ribenboim, *The Theory of Classical Valuations*, Springer Monographs in Mathematics, Springer-Verlag, New York, 1999.

Azadeh Nikseresht
Department of Mathematics, Ayatollah Boroujerdi University, Boroujerd, Iran.
Email: a.nikseresht@abru.ac.ir; a.nikseresht@alumni.kntu.ac.ir

Journal of Algebraic Systems

A ClASSIFICATION OF EXTENSIONS GENERATED BY A ROOT OF AN EISENSTEIN-DUMAS POLYNOMIAL

A. NIKSERESHT

یک رده‌بندی از توسیع‌های تولیدشده به‌وسیلهٔ ریشه‌ای از یك چندجمله‌ای آیزنشتاین-دوماس

آزاده نیک‌سرشت

گروه ریاضی، دانشکده علوم پایه، دانشگاه آیت الله بروجردی (ره)، بروجرد، ایران

واضح است که براي یک ارزیاب گسسته v از یك میدان K با گروه ارزیاب $\mathbf{Z}$، یک میدان توسیع ارزیابی (K', v') از (K, v) به‌وسیله‌ی ریشه‌ای از یک چندجمله‌ای آیزنشتاین نسبت به v که ضرایبش در K می‌باشد، تولید می‌شود اگر و فقط اگر توسیع $(K', v')/(K, v)$ تماماً منشعب باشد. هدف اصلی این مقاله ارائه‌ی مشابه این نتیجه برای توسیع‌های میدان ارزیابی تولیدشده به‌وسیله‌ی ریشه‌ای از یک چندجمله‌ای آیزنشتاین-دوماس نسبت به یک ارزیاب کلی‌تر (که الزاماً گسسته نیست) می‌باشد. حصول این نتیجه منجر به ارائه‌ی رده‌بندی از چنین توسیع‌های جبری از میدان‌های ارزیابی می‌شود.

کلمات کلیدی: توسیع‌های میدان جبری، میدان‌های ارزیابی، چندجمله‌ای‌ها در میدان‌های کلی.