INVARIANTS OF DEFECTLESS IRREDUCIBLE POLYNOMIALS

RON BROWN AND JONATHAN L. MERZEL

Abstract. Defectless irreducible polynomials over a valued field (F, v) have been studied by means of strict systems of polynomial extensions and complete distinguished chains. Strong connections are developed here between these two approaches and applications made to both. In the tame case where a root α of an irreducible polynomial f generates a tamely ramified extension of (F, v), simple formulas are given for the Krasner constant, the Brink separant and the diameter of f. Applications are made to analyze situations where f has an approximate root in an extension field, where a polynomial is close to f, and where α is the first coordinate of a minimal pair. A key technical result is a computation in the tame case of the Newton polygon of $f(x + \alpha)$. Invariants of defectless polynomials are discussed and the existence of defectless polynomials with given invariants is proven. Khanduja's characterization of the tame polynomials whose Krasner constants equal their diameters is generalized to arbitrary defectless polynomials over Henselian fields.

2000 *Mathematics Subject Classification.* Primary: 12J20, 12E05 ; Secondary: 12J10 .

Key words and phrases. valued field, Henselian field, irreducible polynomial, Krasner constant, diameter, separant, Newton polygon, tamely ramified, defectless, strict system of polynomial extensions, complete distinguished chain, minimal pair.

Contents

1. Introduction

Throughout this paper (F, v) will denote a valued field of arbitrary rank with value group vF and residue class field $\overline{F}$. We investigate a number of invariants of the elements of a large class $\mathcal{P}(F)$ of defectless polynomials in $F[x]$. (A polynomial $h \in F[x]$ is *defectless* over (F, v) if it has a root α such that $\deg h$ is the product of the ramification index and the residue class degree of some extension of v to $F[\alpha]$.) If (F, v) is a maximal field, then $\mathcal{P}(F)$ is the set of all monic nonlinear irreducible polynomials over F, and if (F, v) is discrete rank one, then $\mathcal{P}(F)$ is the set of monic nonlinear polynomials over F which are irreducible over the completion of (F, v) [8, Remark 6(C)]. The class $\mathcal{P}(F)$ of polynomials arose in a study of the extensions of v to the rational function field $F(x)$ [6, Theorem 5.10 and Section 6]. (This study was closely related to an earlier one of MacLane [12].) Another approach to the study of extensions of v to $F(x)$, particularly for local fields, was developed by N. Popescu and several collaborators (e.g., see [13]) and then generalized and extended by S. Khanduja and her collaborators (e.g., see [1], [3], [14]). Both feature certain sequences of irreducible polynomials. In this paper we will establish strong connections between the two approaches and use them to make applications to both. In particular we will give a simple characterization of the elements of $\mathcal{P}(F)$ in the case that (F, v) is Henselian. We will also study invariants of defectless polynomials which are developed in both approaches; they are often essentially identical. Particular attention is paid to tame polynomials in $F[x]$. (A polynomial $h \in F[x]$ is *tame* if it is defectless and admits a root α such that the characteristic of $\overline{F}$ does not divide the ramification index of the field extension $F[\alpha]/F$, and the residue class field extension of $F[\alpha]/F$ is separable.) For such polynomials we give simple formulas for some basic invariants, such as their Krasner constants [10, p. 226], and give some applications of these formulas. (The Krasner constant of a tame irreducible polynomial can be regarded as the Krasner constant of any of its roots.)

The definition of $\mathcal{P}(F)$ will be recalled in Section 2, following the simplified approach of [8, §2] using strict systems of polynomial extensions. We will also state our main theorem for tame polynomials in §2. We show that it can be regarded as a description of the Newton polygon of $f(x + \alpha)$ (cf. Remark 3.1) where α can be any root of f. Although this theorem is easily stated, it is somewhat technical. The reader desiring more motivation could turn directly to the applications of the theorem starting in Section 4.

The main theorem for tame polynomials will be proved in Section 3. We use there the analysis of $\mathcal{P}(F)$ in Proposition 5 of [8] and the very useful observation of Brink [5] that for any $f \in F[x]$ and α in F^a, the values $v^a(\alpha - \beta)$, where β ranges over the roots of f, are exactly the slopes of the Newton polygon of $f(x + \alpha)$ with respect to v^a.

In Section 4 we will apply the main theorem to calculate some familiar invariants of a tame polynomial $f \in \mathcal{P}(F)$. In particular we give simple formulas for the Krasner constant and the separant [5, §3] of

f as well as for another invariant of f studied by Ax [2] and later by Khanduja [9] which we call the *diameter* of f.

The formula for the Krasner constant will be applied in Section 5 to generalize to arbitrary tame polynomials in $\mathcal{P}(F)$ a criterion [7, Theorem 1] for when the existence of an approximate root of a generalized Schönemann polynomial $h \in F[x]$ in an extension field K of F guarantees the existence of an exact root of h in K. In Section 6 we give a criterion for when a monic polynomial $c \in F[x]$ is close enough to a tame polynomial $h \in \mathcal{P}(F)$ to guarantee that it is also tame and in $\mathcal{P}(F)$ and that its roots give exactly the same simple extensions of F as do those of h. This result is inspired by a rather general theorem of Brink [5, Theorem 1], but our theorem deals with polynomials whose coefficients are not necessarily integral and when both theorems apply, the one here generally gives a stronger result.

Each element of $\mathcal{P}(F)$ comes equipped with some noncanonical structure (a strict system of polynomial extensions, c.f. Definition 2.1). This structure facilitates induction arguments. In Section 7 we show that many quantities defined in terms of a strict system of polynomial extensions associated with an element of $\mathcal{P}(F)$ are actually invariants of that element. The existence of polynomials with prescribed invariants is proved in Section 8.

In Section 9 we prove that if (F, v) is Henselian, then the complete distinguished chains of [13] and [1] uniquely determine strict systems (of polynomial extensions). We use this fact to show that if (F, v) is Henselian, then $\mathcal{P}(F)$ is exactly the set of nonlinear monic defectless polynomials over (F, v). From this we obtain in the tame case a simple characterization (which can also be derived easily from work of Singh and Khanduja [14, Theorem 1.1]) of the minimal pairs of [13] and [1]. We prove that in the tame case strict systems canonically give rise to complete distinguished chains; we do not know if this is true in general. We also discuss briefly in this section the connection between the invariants we constructed in the previous section from strict systems and the invariants constructed in [13] and [1] from complete distinguished chains. Finally, in Section 10 we characterize the defectless polynomials of length one; this generalizes a characterization of Khanduja of the tame polynomials whose Krasner constants equal their diameters [10, Theorem 1.1].

This paper is relatively self-contained except for the last two sections where we rely heavily on the concepts and results (many from earlier papers) presented in [1] and [3].

2. The main theorem for tame polynomials

We first recall the set $\mathcal{P}(F)$ of polynomials over F as defined in [8, Definition 2]. As in that paper we adopt the convention that if w (respectively, w_i) denotes an extension of v to a valuation on the polynomial ring $F[x]$ [4, Definition 1, p.101], possibly with $w^{-1}(\infty)$ a nontrivial ideal of $F[x]$, then the corresponding place is denoted by $\tau : F[x] \longrightarrow k \cup \{\infty\}$ (respectively, by $\tau_i : F[x] \longrightarrow k_i \cup \{\infty\}$). We also let $\mathbb{Q}vF$ denote a fixed divisible hull of vF and let $\mathcal{E}$ denote the set of extensions of v to a valuation on $F[x]$ mapping into $\mathbb{Q}vF \cup \{\infty\}$.

2.1. **Definition.** Suppose that $n \geq 0$. A *strict system of polynomial extensions over* (F, v) *of length* $n+1$ is a sequence

$$g = ((g_0, w_0, \gamma_0), \ldots, (g_{n+1}, w_{n+1}, \gamma_{n+1}))$$

of elements of $F[x] \times \mathcal{E} \times (\mathbb{Q}vF \cup \{-\infty\})$ such that for some $a \in F$ and all $0 \leq i \leq n$:

(A) $g_0 = x - a$, $\gamma_0 = -\infty$, and $w_0(g_0) = \infty$;

(B) $\deg g_{i+1} > \deg g_i$;

(C) $\gamma_{i+1} = w_i(g_{i+1})$;

(D) $w_{i+1}(g_{i+1}) = \infty$;

(E) $w_i(A_r)/(d_i - r) \geq w_i(A_0)/d_i > \gamma_i$ for all $r < d_i$, where $g_{i+1} = g_i^{d_i} + \sum_{r<d_i} A_r g_i^r$ is the g_i–expansion of g_{i+1} (so $\deg A_r < \deg g_i$ for all $r < d_i$); and

(F) if $e_i > 0$ is least with $e_i w_i(A_0) \in d_i w_i F[x]$ and $f_i = d_i/e_i$, then the polynomial

$$Y^{f_i} + \sum_{r<f_i} \tau_i(s^{f_i - r} A_{e_i r}) Y^r \tag{2.1}$$

is irreducible over k_i for all $s \in F[x]$ with $w_i(A_0 s^{f_i}) = 0$.

As noted in [8, §2] the polynomial (2.1) makes sense, i.e., $0 < f_i \in \mathbb{Z}$ and all the coefficients are finite, and the irreducibility of the polynomial (2.1) over k_i is independent of the choice of s. Of course the A_r in (E) and (F) above depend on the value of i.

2.2. **Notation.** We let $\mathcal{P}(F)$ denote the set of all polynomials h with $h = g_{n+1}$ for some strict system g as in Definition 2.1. Given such a system g we set (for each $0 \leq r \leq n$)

$$m_r = \gamma_{r+1} - \sum_{i=0}^{r} \left(1 - \frac{1}{d_i}\right) \gamma_{i+1} \,. \tag{2.2}$$

A simple recursion formula for m_r is given in Eq. (3.3). For the remainder of this paper we will assume that h is a polynomial over $F[x]$ and that α is a root of h in an algebraic closure F^a of F; we will let v^a denote an extension of v to F^a. For the first seven sections of the paper we will also assume that $h \in \mathcal{P}(F)$ with $h = g_{n+1}$ for some strict system g as in Definition 2.1.

We can now state our main theorem for tame polynomials.

2.3. **Theorem.** *Suppose that h is tame. Then for each integer r with $0 \le r \le n$, the set*

$$\mathcal{S}_r = \left\{\beta \in F^a : v^a(\alpha - \beta) = m_r,\ h(\beta) = 0\right\}$$

has $(d_r - 1) \prod_{i=r+1}^{n} d_i$ elements.

In the above theorem the empty product $\prod_{i=n+1}^{n} d_i$ is assigned the value 1.

There is a computation in [14, Theorem 1.2] of the number of roots β of h such that $v^a(\alpha - \beta)$ takes on some particular value; the deeper part of Theorem 2.3 is that these values are exactly the elements m_i (cf. Remark 3.1 below, which shows how to interpret the above theorem as a description of the Newton polygon of $h(x+\alpha)$ with respect to (F^a, v^a)).

3. Proof of the main theorem for tame polynomials

Recall that $h = g_{n+1}$ with g as in Definition 2.1 and that α is a root of h in F^a.

We will write $q_i = \gamma_{i+1}/d_i$ for all $0 \le i \le n$. For $0 \le i \le n$ we have

$$d_i q_i = \gamma_{i+1} = w_i(g_{i+1}) = w_i(A_0) > d_i \gamma_i \tag{3.1}$$

where A_0 is as in Definition 2.1; hence

$$q_i > \gamma_i, \text{ so if } i < n \text{ then } q_{i+1} > d_i q_i \,. \tag{3.2}$$

Also $m_0 = q_0$ and an easy computation shows that if $0 \le i < n$ then

$$m_{i+1} = m_i + q_{i+1} - d_i q_i > m_i \,. \tag{3.3}$$

We first interpret Theorem 2.3 in terms of Newton polygons. This interpretation will be used in the (inductive) proof of the theorem.

3.1. **Remark.** Let $|A|$ denote the number of elements in any finite set A. Theorem 2.3 implies that

$$\big|\{\alpha\}\big| + \sum_{r=0}^{n} |\mathcal{S}_r| = d_0 \cdots d_n = \deg h \,.$$

Since the m_r are all distinct (cf. formula (3.3)), the sets $\mathcal{S}_r$ are pairwise disjoint and hence Theorem 2.3 also implies that

$$\{\beta \in F^a : \; h(\beta) = 0\} = \{\alpha\} \cup \mathcal{S}_0 \cup \cdots \cup \mathcal{S}_n \,. \tag{3.4}$$

As β ranges over the roots of h in F^a the differences $\beta - \alpha$ are exactly the roots of $h(x+\alpha)$, and therefore the values $v^a(\beta - \alpha)$ are exactly the slopes of the Newton polygon of $h(x+\alpha)$, regarded as a polynomial over the valued field (F^a, v^a), i.e., of the convex hull of the points $(i, v^a(b_{D-i}))$ where we set $D = \deg h$ and write $h(x+\alpha) = \sum_{i=0}^{D} b_i x^i$ (cf. [5, Section 2]). Hence Theorem 2.3 describes the Newton polygon of

$h(x+\alpha)$ (with respect to v^a) as consisting of $n+2$ segments of slopes

$$m_0 < m_1 < m_2 < \cdots < m_n < \infty$$

whose projections onto the "X–axis" have respective lengths

$$(d_0-1)\prod_{i=1}^{n} d_i,\ (d_1-1)\prod_{i=2}^{n} d_i,\ \ldots,\ (d_{n-1}-1)d_n,\ d_n-1,\ 1\,.$$

We next state a proposition [8, Proposition 5 and Remark 7] which is needed for the proof of Theorem 2.3. We write $J_0 = \{0\}$ and $g^0 = 1$. When $0 < i \le n+1$ we write $J_i = \prod_{0\le j<i} \{0,1,\ldots,d_j-1\}$; for $\sigma \in J_i$ we set $\sigma = (\sigma(0),\ldots,\sigma(i-1))$ and $g^\sigma = \prod_{0\le j<i} g_j^{\sigma(j)}$. For each $m \ge 1$ let $F[x]_m = \{c \in F[x] : \deg c < m\}$. If w is an extension of v to $F[x]$, then by a *valuation basis* for w on $F[x]_m$ we mean a basis $\{b_1,\cdots,b_m\}$ for $F[x]_m$ as an F-space such that for all $a_i \in F$ we have $w(\Sigma_{i\le m} a_i b_i) = \min_{i\le m} w(a_i b_i)$.

3.2. **Proposition.** *Suppose that w is an extension of v to a valuation on $F[x]$ with $w(g_{n+1}) > \gamma_{n+1}$. Then for all i with $0 \le i \le n$,*

(A) $w(g_i) = w_{i+1}(g_i) = q_i$;

(B) $\{g^\sigma : \sigma \in J_{i+1}\}$ is a valuation basis for w on $F[x]_{\deg g_{i+1}}$;

(C) g_{i+1} is irreducible over F and w_{i+1} is the unique extension of v to $F[x]$ with $w_{i+1}(g_{i+1}) = \infty$;

(D) the ramification index of w_{i+1}/v is $e_0\cdots e_i$ and $w_{i+1}F[x] = vF + \sum_{0\le j\le i} \mathbb{Z}q_j$;

(E) there is an $\overline{F}$– homomorphism $\Phi_{i+1} : k_{i+1} \longrightarrow k$ with

$$\Phi_{i+1}\tau_{i+1}\big(cg_0^{\sigma_0}\cdots g_i^{\sigma_i}\big) = \tau\big(cg_0^{\sigma_0}\cdots g_i^{\sigma_i}\big)$$

for all $c \in F$ and nonnegative σ_j with $w\big(cg_0^{\sigma_0}\cdots g_i^{\sigma_i}\big) \geq 0$; and if we use Φ_{i+1} and Φ_i (where Φ_0 denotes the natural map $\overline{F} \to k$) to identify k_i and k_{i+1} with subfields of k, then k_{i+1} is generated as an extension of k_i by the root $\tau_{i+1}(sg_i^{e_i})$ of the polynomial (2.1) of Definition 2.1.

Parts (D) and (E) of the above proposition imply that the residual degree of w_{i+1}/v is $f_0\cdots f_i$, and that $\deg g_{i+1}$ is the product of this residual degree and the ramification index of w_{i+1}/v. The proposition does not assume g_{n+1} is tame; by parts (C), (D) and (E) and the above observations, g_{n+1} is tame if and only if none of the e_i are divisible by the characteristic of $\overline{F}$ and each of the polynomials in display (2.1) (for $0 \leq i \leq n$) is separable over k_i.

Suppose that $0 \leq i \leq n$ and that w is as in the above proposition. Since both $w_{i+1}(g_{i+1})$ and $w(g_{i+1})$ are larger than γ_{i+1}, we can apply parts (A) and (B) of the above proposition to deduce that w and w_{i+1} agree on $F[x]_{\deg g_{i+1}}$. We can also apply part (C) of the proposition to deduce that

$$w_{n+1}(f) = v^a(f(\alpha)) \tag{3.5}$$

for all $f \in F[x]$ (cf. Notation 2.2). We will use both these facts frequently (and often only implicitly) below.

The proof of Theorem 2.3 will also require:

3.3. **Lemma.** *Suppose that g_{n+1} is tame over (F, v). Let w be an extension of v to $F[x]$ with $w(g_{n+1}) > \gamma_{n+1}$. If $1 \le i \le n+1$, then:*

(A) $w(g_i') = d_{i-1}q_{i-1} - m_{i-1}$; and

(B) $w(f') \ge w(f) - m_{i-1}$ for any $f \in F[x]$ which is a product of elements of $F[x]_{\deg g_i}$.

Proof. We will show that (A) and (B) hold whenever $0 \le i \le n+1$ where we pick d_{-1}, q_{-1} and m_{-1} so that $d_{-1}q_{-1} = m_{-1} < q_0$. With these choices formula (3.3) also holds if $i = -1$. Both (A) and (B) are obvious if $i = 0$ since then $g_i' = 1$ and f is a constant. Now suppose they hold for all $i \le j$ where $0 \le j \le n$; it suffices to show they hold for $i = j+1$. We first prove (B) in this case. By the product rule it suffices to consider the case that $\deg f < \deg g_{j+1}$. Write $f = \sum_{\sigma \in J_{j+1}} c_\sigma g^\sigma$ where each $c_\sigma \in F$, so that $w(f) = \min_{\sigma \in J_{j+1}} w(c_\sigma g^\sigma)$ (cf. Proposition 3.2(B)). Then by the product rule f' is a sum of terms of the form $c_\sigma (g^\sigma / g_r) g_r'$ (where $0 \le r \le j$, $\sigma \in J_{j+1}$, and $\sigma(r) \ne 0$). By our induction hypotheses each such term has value at least

$$w(c_\sigma g^\sigma) - q_r + d_{r-1}q_{r-1} - m_{r-1} \ge w(f) - m_r \ge w(f) - m_{i-1}$$

as required.

We now prove (A) for $i = j+1$. We may write

$$g_{j+1} = g_j^{d_j} + \sum_{r<d_j} A_r g_j^r$$

where each A_r is in $F[x]_{\deg g_j}$. By Proposition 3.2 there exist $c \in F$ and $\sigma \in J_j$ with $w(s) = -(e_j/d_j)w(A_0)$ where $s = cg^\sigma$. Also write $f = f_j$ and

$$G(Y) = Y^f + \sum_{r<f} (s^{f-r} A_{re_j}) Y^r$$

(in the polynomial ring $F[x][Y]$ over $F[x]$). Then

$$s^f g_{j+1} = G(sg_j^{e_j}) + \sum_{e_j \nmid r} s^f A_r g_j^r, \tag{3.6}$$

and by Definition 2.1(F)

$$\tau_j(G(Y)) = Y^f + \sum_{r<f} \tau_j(s^{f-r} A_{re_j}) Y^r$$

is irreducible over k_j, which we regard as a subfield of k (cf. Proposition 3.2(E)). Moreover by Proposition 3.2(E), $\tau(sg_j^{e_j})$ is a root of this polynomial. By the remarks just after the statement of Proposition 3.2, since g_{n+1} is tame, therefore $\tau G(Y)$ is separable and hence $(\tau G')(\tau(sg_j^{e_j})) \neq 0$. Thus

$$w(G'(sg_j^{e_j})) = 0\,.$$

Therefore by the condition (A) (with $i = j$) we have

$$\begin{aligned} &w(G'(sg_j^{e_j})s\frac{d}{dx}g_j^{e_j}) \\ &\quad = w(s) + (e_j - 1)w(g_j) + w(g_j') \\ &\quad = w(s) + (e_j - 1)w(g_j) + d_{j-1}q_{j-1} - m_{j-1} \\ &\quad = -e_jq_j + (e_j - 1)q_j + d_{j-1}q_{j-1} - m_{j-1} = -m_j\,. \end{aligned}$$

(Note that $w(e_j) = 0$ since g_{n+1} is tame.) Similarly, condition (B) (with $i = j + 1$) shows that

$$w(G'(sg_j^{e_j})s'g_j^{e_j}) \geq w(s) - m_{j-1} + e_jq_j > -m_j\,.$$

Also when $e_j \nmid r$ condition (B) (with $i = j + 1$) says that

$$w\left(\frac{d}{dx}(s^fA_rg_j^r)\right) \geq w(s^fA_rg_j^r) - m_j > -m_j$$

and similarly (B) with our hypothesis implies that

$$w\left(g_{j+1}\frac{d}{dx}s^f\right) > \gamma_{j+1} + w(s^f) - m_{j-1} = -m_{j-1} > -m_j\,.$$

Applying the chain and product rules to Eq. (3.6) we see that

$$\begin{aligned} s^fg_{j+1}' = {}& G'(sg_j^{e_j})s\frac{d}{dx}g_j^{e_j} \\ &+ G'(sg_j^{e_j})s'g_j^{e_j} + \sum_{e_j\nmid r}\frac{d}{dx}(s^fA_rg_j^r) - g_{j+1}\frac{d}{dx}s^f\,. \end{aligned}$$

Thus the above calculations show that $w(g_{j+1}') = -m_j - w(s^f) = d_jq_j - m_j$ which completes the proof of condition (A) for $i = j+1$, and hence the proof of the lemma. □

We now turn directly to the proof of Theorem 2.3, which will occupy the remainder of this section. We first argue that we may assume without loss of generality that (F, v) is Henselian. There is a Henselization (F', v') of (F, v) contained in (F^a, v^a). Since (F', v') is an immediate extension of (F, v), adjoining any root of h in F^a to either F or F' yields the same value group and residue class field extensions (Proposition 3.2 implies that such extensions are defectless of degree $\deg h$). Hence h is tame over (F', v'). Similarly each of the valuations w_i has a unique extension w'_i to $F'[x]$ also extending v' with $w'_i(g_i) = \infty$. Replacing each w_i by w'_i converts g to a strict system of polynomial extensions over (F', v') with exactly the same sets of integers m_r and sets of roots $\mathcal{S}_r$.

For the remainder of this section we will assume that (F, v) is Henselian and denote the unique extension of v to F^a by v.

To facilitate an application in Section 5 we isolate part of the proof of Theorem 2.3 in:

3.4. **Lemma.** *Suppose that $v(h(\delta)) > \gamma_{n+1}$ for some $\delta \in F^a$. Then $h(x + \alpha)$ and $h(x + \delta)$ have the same Newton polygon except that over the interval $[\deg h - 1, \deg h]$ the Newton polygon of $h(x+\alpha)$ has infinite slope, while that of $h(x + \delta)$ has slope $m_n + v(h(\delta)) - d_n q_n$.*

In the remainder of this section we give a single induction argument proving both Lemma 3.4 and Theorem 2.3. In this proof we will regard the singleton sequence $((g_0, w_0, \gamma_0))$ as a strict system of polynomial extensions over (F, v) of length 0 and define m_{-1}, q_{-1} and d_{-1} as in the beginning of the proof of Lemma 3.3, so formula (3.3) is valid with $i = -1$. Then Lemma 3.4 is trivially true if g is a strict system of length 0 (note that $h = x - \alpha$ in this case), and Theorem 2.3 is vacuously true. We now assume inductively that Lemma 3.4 and Theorem 2.3 are valid for the sequence $\widehat{g} = ((g_i, w_i, \gamma_i))_{i \le n}$. The roots of g_{n+1} in F^a will be denoted by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_D$ and those of g_n by $\beta_1 = \beta, \beta_2, \ldots, \beta_{\widehat{D}}$ (so D and $\widehat{D}$ denote the degrees of g_{n+1} and g_n, respectively). Applying Eq. (3.5) with $f = g_n$ we have $v(g_n(\alpha)) = q_n > \gamma_n$. Hence the hypothesis that Lemma 3.4 is valid for $\widehat{g}$ implies that the Newton polygons for $g_n(x + \alpha)$ and $g_n(x + \beta)$ are identical except over the interval $[\deg g_n - 1, \deg g_n]$ where the Newton polygon for $g_n(x + \alpha)$ has slope

$$v(g_n(\alpha)) + m_{n-1} - d_{n-1}q_{n-1} = m_{n-1} + (q_n - d_{n-1}q_{n-1}) = m_n \, .$$

Indeed, this Newton polygon has slope m_n only over this interval of length 1, so there is a unique root $\beta_i - \alpha$ of $g_n(x+\alpha)$ with $v(\beta_i - \alpha) = m_n$. That is, we have a well–defined map $\pi : \{\alpha_1, \alpha_2, \ldots\} \longrightarrow \{\beta_1, \beta_2, \ldots\}$ assigning to each α_i the unique β_j with $v(\alpha_i - \beta_j) = m_n$.

We may assume that the β_i are indexed so that $\pi(\alpha) = \beta$. By Proposition 3.2(C) for any β_i there is an F–automorphism σ of F^a mapping β to β_i. Then $\sigma(\alpha) = \alpha_j$ for some j and hence since (F, v) is Henselian,

$$v(\beta_i - \alpha_j) = v(\sigma(\beta - \alpha)) = v(\beta - \alpha) = m_n\,,$$

so $\pi(\alpha_j) = \beta_i$. Thus π is surjective; we now show it is $d_n : 1$. Our assumption that Theorem 2.3 is valid for $\widehat{g}$ implies that

$$v(\alpha - \beta) = m_n > m_{n-1} = \max_{i>1} v(\beta - \beta_i)\,,$$

so by Krasner's Lemma we have $F[\beta] \subseteq F[\alpha]$. (Note that g_n is separable because it is tame.) By Proposition 3.2(C) we have $[F[\alpha] : F[\beta]] = d_n$, so there are d_n homomorphisms $F[\alpha] \longrightarrow F^a$ fixing $F[\beta]$, say $\sigma_1, \ldots, \sigma_{d_n}$. We may assume the α_i are indexed so that $\sigma_i(\alpha) = \alpha_i$ for all $i \leq d_n$. Then since (F, v) is Henselian,

$$v(\alpha_i - \beta) = v(\sigma_i(\alpha - \beta)) = v(\alpha - \beta) = m_n$$

so $\pi(\alpha_i) = \beta$ for all $i \leq d_n$. Thus $|\pi^{-1}(\beta)| \geq d_n$. Since π is surjective we may conclude that $|\pi^{-1}(\beta_j)| \geq d_n$ for all j. In fact none of these inequalities can be strict since otherwise

$$\deg g_{n+1} = \sum_j |\pi^{-1}(\beta_j)| > d_n \deg g_n = \deg g_{n+1}\,.$$

Thus π is indeed $d_n : 1$. In particular, we have $\pi^{-1}(\beta) = \{\alpha_1, \ldots, \alpha_{d_n}\}$.

Recall that for each $k \leq n$ we set $\mathcal{S}_k = \{\alpha_i : v(\alpha - \alpha_i) = m_k\}$; similarly for $k < n$ set $\widehat{\mathcal{S}}_k = \{\beta_j : v(\beta - \beta_j) = m_k\}$. The proof that Theorem 2.3 holds for the sequence g reduces to the proof of the

Claim. If $k < n$ then $\mathcal{S}_k = \pi^{-1}\big(\widehat{\mathcal{S}}_k\big)$, so that by induction on n

$$|\mathcal{S}_k| = d_n\big|\widehat{\mathcal{S}}_k\big| = (d_k - 1)\prod_{i=k+1}^{n} d_i,$$

and $\mathcal{S}_n = \pi^{-1}(\beta) \setminus \{\alpha\}$, so that $|\mathcal{S}_n| = d_n - 1$.

First suppose that $k < n$. Then if $\alpha_i \in \mathcal{S}_k$ we have

$$v(\pi(\alpha_i) - \beta) = v(\pi(\alpha_i) - \alpha_i + \alpha_i - \alpha + \alpha - \beta) = m_k$$

since $v(\pi(\alpha_i) - \alpha_i) = v(\alpha - \beta) = m_n > m_k$. Thus $\mathcal{S}_k \subseteq \pi^{-1}\big(\widehat{\mathcal{S}}_k\big)$. On the other hand if $\alpha_i \in \pi^{-1}\big(\widehat{\mathcal{S}}_k\big)$, then

$$v(\alpha - \alpha_i) = v(\alpha - \beta + \beta - \pi(\alpha_i) + \pi(\alpha_i) - \alpha_i) = m_k\,,$$

so $\alpha_i \in \mathcal{S}_k$. Thus $\mathcal{S}_k = \pi^{-1}\big(\widehat{\mathcal{S}}_k\big)$.

It remains to show that $\mathcal{S}_n = \pi^{-1}(\beta) \setminus \{\alpha\}$. By our induction hypothesis we may assume that

$$\{\beta_i : i > 1\} = \bigcup_{k<n} \widehat{\mathcal{S}}_k$$

(cf. formula (3.4)). Then

$$\begin{aligned}\{\alpha_i : i > d_n\} &= \{\alpha_i : i \geq 0\} \setminus \pi^{-1}(\beta)\\ &= \pi^{-1}\big(\{\beta_i : i > 1\}\big) = \bigcup_{k<n} \pi^{-1}\big(\widehat{\mathcal{S}}_k\big) = \bigcup_{k<n} \mathcal{S}_k\,.\end{aligned}$$

Since $\mathcal{S}_n$ is disjoint from $\bigcup_{k<n} \mathcal{S}_k$ we have

$$\mathcal{S}_n \subseteq \{\alpha_2, \ldots, \alpha_{d_n}\} = \pi^{-1}(\beta) \setminus \{\alpha\}.$$

Now suppose that $2 \leq i \leq d_n$. Then

$$v(\alpha - \alpha_i) = v(\alpha - \beta + \beta - \alpha_i) \geq m_n \,. \tag{3.7}$$

It now suffices to prove that

$$\sum_{i=2}^{d_n} v(\alpha - \alpha_i) = (d_n - 1)m_n \tag{3.8}$$

since this implies that none of the inequalities of (3.7) can be strict, so $\alpha_i \in \mathcal{S}_n$ for all $2 \leq i \leq d_n$.

We begin the proof of Eq. (3.8) with an inductive proof that for all nonnegative integers $s \leq n$ we have

$$(d_s - 1)m_s = d_s q_s - m_s - \sum_{j=0}^{s-1} m_j d_s (d_j - 1) \prod_{i=j+1}^{s-1} d_i \,. \tag{3.9}$$

This is clear if $s = 0$ (where it says that $(d_0 - 1)q_0 = d_0 q_0 - q_0 - 0$) or $s = 1$ (since $(d_1 - 1)m_1 = d_1 q_1 - m_1 - m_0 d_1 (d_0 - 1)$). Suppose that (3.9) is true for some $s < n$; we prove it for $s + 1$. Multiplying (3.9) by d_{s+1} yields

$$\begin{aligned} 0 &= \sum_{j=0}^{s-1} m_j d_{s+1} (d_j - 1) \prod_{i=j+1}^{s} d_i + m_s d_{s+1} (d_s - 1) - d_{s+1}(d_s q_s - m_s) \\ &= \sum_{j=0}^{s} m_j d_{s+1} (d_j - 1) \prod_{i=j+1}^{s} d_i \ + \ (d_{s+1} - 1)m_{s+1} - d_{s+1} q_{s+1} + m_{s+1} \end{aligned}$$

since $m_{s+1} = m_s + q_{s+1} - d_s q_s$. This completes the proof of Eq. (3.9).

Since we are assuming that Theorem 2.3 is valid for $\widehat{g}$, formula (3.9) with $s = n$ can be written in the form

$$(d_n - 1)m_n = d_n q_n - m_n - \sum_{j<n} d_n \big|\widehat{S}_j\big| m_j$$

which since π is a $d_n : 1$ mapping from $\mathcal{S}_j$ onto $\widehat{\mathcal{S}}_j$ equals

$$d_n q_n - m_n - \sum_{j<n} |S_j| m_j \,.$$

By the definition of $\mathcal{S}_j$ and Lemma 3.3(A) this equals

$$d_n q_n - m_n - \sum_{j>d_n} v(\alpha_j - \alpha)$$

$$= \; v(g'_{n+1}(\alpha)) + \sum_{j=2}^{d_n} v(\alpha_j - \alpha) - \sum_{j\geq 2} v(\alpha_j - \alpha) \,. \tag{3.10}$$

By the product rule the last summation in Eq. (3.10) is $v(g'_{n+1}(\alpha))$. This completes the proof of formula (3.8) and hence of the Claim. Thus Theorem 2.3 is valid for g; it remains to show that Lemma 3.4 is valid for g.

Because F might have prime characteristic it is convenient to express the Taylor series for polynomials in $F[x]$ using the linear operators $\Delta_m : F[x] \longrightarrow F[x]$ (for $m \geq 0$) with $\Delta_m(x^r) = \binom{r}{m} x^{r-m}$ for all $r \geq m$ and $\binom{r}{m} = 0$ if $r < m$. The binomial theorem implies that for any

$f(x) = \sum_{m=0}^{t} a_m x^m \in F[x]$ and $b \in F^a$,

$$f(x+b) \quad = \quad \sum_{m=0}^{t} a_m \sum_{k=0}^{m} \binom{m}{k} b^{m-k} x^k = \sum_{k=0}^{t} (\Delta_k(f)(b)) x^k \, .$$

Thus in particular we have

$$h(x+\alpha) = h(\alpha) + \Delta_1(h)(\alpha)x + \Delta_2(h)(\alpha)x^2 + \cdots$$

and

$$h(x+\delta) = h(\delta) + \Delta_1(h)(\delta)x + \Delta_2(h)(\delta)x^2 + \cdots \, .$$

Let w denote the extension of v to $F[x]$ with $w(f) = v(f(\delta))$ for all $f \in F[x]$. For each $j > 0$

$$\deg \Delta_j(h) < \deg h \quad \text{and} \quad w(h) = v(h(\delta)) > \gamma_{n+1} \, ,$$

so by (A) and (B) of Proposition 3.2 and Eq. (3.5) we have

$$v(\Delta_j(h)(\alpha)) \quad = \quad w_{n+1}(\Delta_j(h)) = w(\Delta_j(h)) = v(\Delta_j(h)(\delta)) \, .$$

Moreover the line segment joining the points $(\deg h - 1, v(\Delta_1(h)(\delta)))$ and $(\deg h, v(h(\delta)))$ by hypothesis and Lemma 3.3(A) has slope

$$\begin{aligned} v(h(\delta)) - v(\Delta_1(h)(\delta)) &= v(h(\delta)) - d_n q_n + m_n \\ &> m_n > m_{n-1} > \cdots > m_0 \, . \end{aligned} \tag{3.11}$$

The Newton polygon of $h(x+\alpha)$ (which has been proven above to be as described in Theorem 2.3 and Remark 3.1) is therefore the convex hull of the same set of points as that of $h(x+\delta)$ except for the replacement of the point $(\deg h, \, v(h(\delta)))$ by $(\deg h, \infty)$. Thus the inequality (3.11) says that the Newton polygon of $h(x+\delta)$ indeed is the same as that of $h(x+\alpha)$ except that the last segment has slope $v(h(\delta)) - d_n q_n + m_n$. This completes the combined proof of Lemma 3.4 and Theorem 2.3. □

We record a useful corollary of the proof of Theorem 2.3 above.

3.5. **Corollary.** *For any root α of g_{n+1} there is a unique root β of g_n such that $v^a(\alpha-\beta) = m_n$.*

4. Invariants of tame polynomials

Recall that h denotes an element of $\mathcal{P}(F)$ and that $h = g_{n+1}$ where g is a strict system as in Definition 2.1. In this section we study some invariants associated with h in the case that h is tame over (F, v). In order to relate easily to some results in the literature we will assume that (F, v) is Henselian. This assumption is essentially without loss of generality since h is also in $\mathcal{P}(F')$ for any Henselization (F', v') of (F, v). (Further, if h is tame over (F, v), then it is also tame over (F', v').) The unique extension of v to F^a will be denoted by v.

As usual $\alpha \in F^a$ denotes a root of h. The *Krasner constant* of h, denoted $\omega_F(h)$, is the maximum of the set

$$\{v(\alpha - \alpha') : \alpha \neq \alpha' \in F^a \text{ and } h(\alpha') = 0\}.$$

(This set is independent of the choice of α, so $\omega_F(h)$ – often called the Krasner constant of α – is an invariant of h.) We call the minimum of the above set the *diameter* of h and denote it by $\Omega_F(h)$ (cf. [2], [9]). Finally, Brink [5] defines the *separant* of h to be the maximum of

$$\{v(h'(\alpha)(\alpha-\alpha')) : \alpha \neq \alpha' \in F^a, h(\alpha')=0\}.$$

4.1. **Theorem.** *If h is tame over (F,v), then the Krasner constant of h is m_n, the diameter is $m_0 = q_0$, and the separant is $\gamma_{n+1} = d_n q_n$.*

Proof. The first two assertions are immediate from Theorem 2.3. Applying Lemma 3.3(A), we calculate that the separant of h is

$$w_{n+1}(g'_{n+1}) + m_n = d_n q_n - m_n + m_n = \gamma_{n+1}.$$

□

Whether or not h is tame, the quantity γ_{n+1} is an invariant of h not depending on the choice of g, c.f. Theorem 7.1. We often denote it by γ_h. (See [8, Remark 6(B)] for some intrinsic characterizations of γ_h.)

5. Roots of tame polynomials

5.1. **Theorem.** *Suppose that (F,v) is Henselian and that $h \in \mathcal{P}(F)$ is tame. Suppose that $v^a(h(\delta)) > \gamma_h$ for some $\delta \in F^a$. Then there is a root of h in $F[\delta]$.*

This theorem generalizes Theorem 1 of [7] since if h is a generalized Schönemann polynomial in the sense of that paper, then $h \in \mathcal{P}(F)$ and

γ_h is exactly the "$v(\pi)$" appearing in the theorem cited above. Examples show that the above theorem is generally stronger than ones involving some simple applications of Hensel's Lemma [7, Remark 2(B)]. Theorem 5.1 is proved in [8] under the extra hypothesis that δ is taken from a tamely ramified extension of (F, v); the methods used in that proof are quite different from those in this paper or [7]. Khanduja showed us a proof of Theorem 5.1 in the case that h is integral of length 2 and $e_0 = f_1 = 1$; she uses the theory of lifting polynomials to calculate the Krasner constant of h.

Proof. As usual we assume that $h = g_{n+1}$ with g as in Definition 2.1. The roots of $h(x+\delta)$ have the form $\beta - \delta$ where β ranges over the roots of h. By Lemma 3.4 there is a root β of h with

$$v^a(\beta - \delta) = m_n + v^a(h(\delta)) - d_n q_n$$

which by hypothesis is larger than

$$m_n + \gamma_h - d_n q_n = m_n\,,$$

the Krasner constant of h (Theorem 4.1). Hence by Krasner's lemma, $F[\delta] \supseteq F[\beta]$. That is, $F[\delta]$ contains a root of h. □

5.2. **Remark.** The quantity γ_h in Theorem 5.1 is easily seen to be best possible [8, Remark 8]: for any h, a root δ of g_n has $v^a(h(\delta)) = \gamma_h$, but $F[\delta]$ has no root of h.

6. Brink's separable Hensel's lemma

In this section we assume that (F, v) is Henselian and that h is tame over (F, v). As usual we assume that $h \in \mathcal{P}(F)$, $h = g_{n+1}$ where g is as in Definition 2.1, and $\alpha \in F^a$ is a root of h. We let w denote w_{n+1}, the unique extension of v to $F[x]$ with $w(h) = \infty$. Recall that $\gamma_h = \gamma_{n+1}$ is the separant of h (Theorem 4.1).

6.1. **Theorem.** *Suppose that $c \in F[x]$ is monic of the same degree as h and that $w(h - c) > \gamma_h$. Let $\beta \in F^a$ be a root of c. Then:*

(A) c is a tame element of $\mathcal{P}(F)$;

(B) the Newton polygons of $c(x + \beta)$ and $h(x + \alpha)$ are identical;

(C) h and c have the same separant, Krasner constant and diameter;

(D) there exist $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_r$ in F^a with $h = \prod_{i \le r}(x - \alpha_i)$, $c = \prod_{i \le r}(x - \beta_i)$, and $F[\alpha_i] = F[\beta_i]$ for all $i \le r$.

We will clarify the connection between this theorem and Brink's "separable Hensel's lemma" [5, Theorem 1] after giving the proof of the theorem. One might note that γ_h is best possible in the above theorem since if $c = g_n^{d_n}$, then $w(h - c) = w(g_n^{d_n}) = \gamma_h$, but c is not even irreducible. The hypothesis that (F, v) is Henselian is not really needed in the above theorem except in part (D).

Proof. Write $g_{n+1} = g_n^{d_n} + \sum_{i<d_n} A_i g_n^i$ as usual and write $c = g_n^{d_n} + \sum_{i<d_n} B_i g_n^i$ where each B_i is in $F[x]_{\deg g_n}$. Proposition 3.2 implies that for each $i < d_n$ we have

$$w_n(A_i - B_i) = w((A_i - B_i)g_n^i) - iq_n \geq \min_j w((A_j - B_j)g_n^j) - iq_n$$
$$= w(h - c) - iq_n > \gamma_{n+1} - iq_n = (d_n - i)q_n \, . \qquad (6.1)$$

Let w^* be the extension of v to $F[x]$ with $w^*(m) = v^a(m(\beta))$ for all $m \in F[x]$ (so $w^*(c) = \infty$).

Let g^* be identical to the sequence g but with the last term (h, w, γ_h) of g replaced by (c, w^*, γ_h). We now show that g^* is a strict system over (F, v) with $w^* F[x] = wF[x]$ and with the residue class fields of w and w^* being $\overline{F}$–isomorphic. This will prove that c is a tame element of $\mathcal{P}(F)$. Conditions (A), (B) and (D) of Definition 2.1 are transparent. To check condition (C) just apply the inequality (6.1) with $i = 0$ to see that

$$w_n(h - c) = w_n(A_0 - B_0) > d_n q_n = \gamma_h \, ;$$

thus since $w_n(h) = \gamma_h$, therefore $w_n(c) = \gamma_h$. Again applying (6.1) we have that for all $r < d_n$

$$w_n(A_r - B_r) > (d_n - r)q_n = \frac{d_n - r}{d_n} w_n(A_0),$$

so $w_n(A_0 - B_0) > w_n(A_0)$ and

$$w_n(B_r) \geq \frac{d_n - r}{d_n} w_n(A_0) = \frac{d_n - r}{d_n} w_n(B_0) > (d_n - r)\gamma_n \, .$$

Thus g^* satisfies condition (E) of Definition 2.1. Now pick $s \in F[x]$ with $d_n w_n(s) = -e_n w_n(A_0) = -e_n w_n(B_0)$. For each $r < f_n$ we have

$$w_n(s^{f_n-r}A_{re_n} - s^{f_n-r}B_{re_n}) > (f_n - r)\left(-\frac{1}{f_n}\right) w_n(A_0) + (d_n - re_n)q_n = 0\,.$$

This says that the polynomials of the form (2.1) of Definition 2.1 with $i = n$ are the same for the sequences g and g^*. Thus condition (F) of that definition is satisfied and g^* is indeed a strict system. Moreover, $wF[x] = w^*F[x]$ and w and w^* have $\overline{F}$–isomorphic residue class fields (Proposition 3.2, parts (D) and (E)). Hence $c \in \mathcal{P}(F)$, c is tame, and also $\gamma_h = \gamma_c$.

Part (B) of the Theorem now follows immediately from Remark 3.1. Thus part (C) follows from Theorem 4.1.

It remains to prove part (D) of the theorem.

Let us write $h = \prod_{i=1}^{r}(x - \alpha_i)$ where each α_i is in F^a. There exist F–automorphisms $\sigma_1, \ldots, \sigma_r$ of F^a with $\sigma_i(\alpha_1) = \alpha_i$ for all $i \le r$. Since

$$v^a(c(\alpha_1)) = v((h - c)(\alpha_1)) = w(h - c) > \gamma_h = \gamma_c\,,$$

therefore by Theorem 5.1 $F[\alpha_1]$ contains a root β_1 of c. Since h and c are irreducible of the same degree, we have $F[\alpha_1] = F[\beta_1]$. For each $i \le r$ let $\beta_i = \sigma_i(\beta_1)$. (Of course σ_1 fixes $F[\alpha_1]$ so $\sigma_1(\beta_1) = \beta_1$.) Thus $F[\alpha_i] = F[\beta_i]$ for all $i \le r$. It remains to show that the β_i are distinct, so that $c = \prod_{i \le r}(x - \beta_i)$. Suppose $\beta_i = \beta_j$. Then since $\sigma_i^{-1}\sigma_j(\beta_1) = \beta_1$, the map $\sigma_i^{-1}\sigma_j$ fixes $F[\beta_1] = F[\alpha_1]$, so $\alpha_i = \sigma_i(\alpha_1) = \sigma_j(\alpha_1) = \alpha_j$ and hence, because tame polynomials are separable, $i = j$. □

The following lemma will help clarify the connection between the above theorem and [5, Theorem 1]. We will let v (our valuation on F) also denote the Gaussian valuation on $F[x]$ (so $v(\Sigma b_i x^i) = \min v(b_i)$ for all $b_i \in F$).

6.2. **Lemma.** *If h is integral (i.e., $v(h) \ge 0$), then $w(c) \ge v(c)$ for all $c \in F[x]$.*

Proof. As usual α denotes a root of h in F^a, so $w(c) = v^a(c(\alpha))$ for all $c \in F[x]$. The monic polynomial h is integral. Hence α is integral and so $w(x) = v^a(\alpha) \ge 0$. Thus for any $c = \Sigma c_i x^i \in F[x]$ we have

$$w(c) \ge \min_i (iw(x) + v(c_i)) \ge \min_i v(c_i) = v(c)\,.$$

□

6.3. **Corollary.** *Suppose that $v(h) \ge 0$. Suppose that $c \in F[x]$ is monic with the same degree as h and with $v(c - h) > \gamma_h$. Then c is a tame element of $\mathcal{P}(F)$ and there exist $\alpha_1, \dots, \alpha_r$, $\beta_1, \dots, \beta_r \in F^a$ with $h = \prod(x - \alpha_i)$, $c = \prod(x - \beta_i)$, and with $F[\alpha_i] = F[\beta_i]$ for all $i \le r$.*

The Corollary follows from Theorem 6.1 since the lemma above tells us that $w(c-h) \geq v(c-h) > \gamma_h$.

Since tame polynomials are always separable and γ_h is the separant of h (Theorem 4.1), the last part of the above Corollary reduces to the special case of Brink's "separable Hensel's lemma" [5, Theorem 1] when the polynomial in question is tame. In this case Theorem 6.1 gives a stronger result than [5, Theorem 1] because it also applies to nonintegral polynomials and because the hypothesis that $w(h-c) > \gamma_h$ is generally weaker than the condition that $v(h-c) > \gamma_h$. For example if (F, v) is the valued field of p–adic numbers and $h = (x^2-p)^2 - p^2x$ (cf. [8, Example 3(D)]), then $v(px(x^2-p)) = 1$ and $w(px(x^2-p)) = 2.75$. Since $\gamma_h = 2\frac{1}{2}$, Theorem 6.1 applies to h and $c = h + px(x^2-p)$ but Brink's separable Hensel's lemma does not apply to h and c.

It is easy to show that in part (D) of Theorem 6.1 we have $v^a(\alpha_i - \beta_i) > \omega_F(h)$ for all $i \leq r$. This suggests the possibility of a sharp result on the continuity of the roots of a tame polynomial $h \in \mathcal{P}(F)$ in which the Gaussian valuation on $F[x]$ is replaced by w (cf. [11, Theorem 5.8]).

7. Invariants of defectless polynomials

Throughout this section h will denote a polynomial with $h = g_{n+1}$ for some strict system g as in Definition 2.1 and α will denote a root of h. By Proposition 3.2 any such polynomial is defectless and we will prove in Section 9.1 that if (F, v) is Henselian, then all monic nonlinear defectless polynomials are in $\mathcal{P}(F)$. We prove here that a number of sequences defined in terms of g are actually invariants of h, i.e., they are independent of the choice of g. Of course these invariants may depend on the choice of (F, v). All of these sequences are familiar except for one. We will let $G_i \in k_i[Y]$ denote the polynomial (2.1) of Definition 2.1 (for $0 \leq i \leq n$) and let $[G_i]$ denote the equivalence class of G_i, where we call two nonzero polynomials $b,\ c \in k_i[Y]$ *linearly equivalent* over k_i (or just *k_i-equivalent*) if there exists $\gamma \neq 0$ and δ in k_i such that $\gamma^t b(Y) = c(\gamma Y + \delta)$ where $t = \deg c$. For example, different choices of s in Definition 2.1 will lead to linearly equivalent polynomials (2.1) over k_i (see the proof of the next theorem).

7.1. **Theorem.** *The integer n and the sequences* $(\deg g_0, \ldots, \deg g_{n+1})$, $(d_0, \ldots, d_n)$, $(\gamma_1, \ldots, \gamma_{n+1})$, $(q_0, \ldots, q_n)$, $([G_0], \ldots, [G_n])$, $(e_0, \ldots, e_n)$, $(f_0, \ldots, f_n)$, $(w_0 F[x], \ldots, w_{n+1} F[x])$, *and* $(k_0, \ldots, k_{n+1})$ *are invariants of h (i.e., they are independent of the choice of g).*

In the above theorem we are identifying each group $w_iF[x]$ with a subgroup of our divisible hull $\mathbb{Q}vF$ of vF and we are identifying each residue class field k_i with a subfield of k_{n+1} (as in Proposition 3.2(E)). Here we can regard k_{n+1} as the residue class field of the unique $w \in \mathcal{E}(v)$ with $w(h) = \infty$.

The connection of these sequences of invariants with some sequences of invariants constructed in [13] and [1] from complete distinguished chains will be discussed in Remark 9.7.

7.2. **Remark and Definition.** Since the length $n+1$ of the strict system g is independent of g (so long as $h = g_{n+1}$), we may call $n+1$ the *length* of h. We will also call the invariant q_0 of h the *base invariant* of h with respect to (F, v), and denote it by $\beta_F(h)$. It is easy to see that the base invariant of h is the maximum value of $v(\alpha - b)$ as b ranges over F. The elements of $\mathcal{P}(F)$ of length one are described in Theorem 10.1; they turn out to be the monic nonlinear defectless polynomials whose base invariants equal their main invariants (in the sense of [1, p. 608]).

The proof of Theorem 7.1 will require the next lemma.

7.3. **Lemma.** *Suppose that* $0 \le m \le n+1$. *Suppose that* $w(g_{n+1}) > \gamma_{n+1}$ *for some extension* w *of* v *to* $F[x]$ *and that* c *is a nonzero product* *of elements of* $F[x]_{\deg g_m}$. *Then* $w(c)$ *is in* $w_m F[x]$ *and if* c *is integral with respect to* w, *then the residue class of* c *is in* k_m.

In this lemma we have identified k_m with a subfield of k (cf. Proposition 3.2(E)).

Proof. The first assertion follows immediately from Proposition 3.2. We may suppose that $m > 0$ and that c is a unit. By Proposition 3.2(B) c is a sum of units and infinitesimals of the form ag^σ where $a \in F$ and $\sigma = (\sigma(0), \cdots, \sigma(m-1))$. Thus we may assume without loss of generality that c is a unit of the form ag^σ. Since c is a unit we must have $e_{m-1}i = \sigma(m-1)$ for some integer $i > 0$. There exist $t, u \in F[x]_{\deg g_{m-1}}$ with tu and $tg_{m-1}^{e_{m-1}}$ units. By Proposition 3.2(E) and induction on m the residue classes of both tu and

$$(tu)^i c = (u^i a \prod_{j<m-1} g_j^{\sigma(j)})(tg_{m-1}^{e_{m-1}})^i$$

are in k_m. The lemma follows immediately. □

7.4. **Remark.** Lemma 7.3 is part of a more conceptual result. With hypotheses as in the previous lemma let M denote the maximal ideal of w and let $\Gamma_m = \{b(1+M) : 0 \neq b \in F[x]_{\deg g_m}\}$. Then Γ_m is a group under multiplication and we have a natural exact sequence

$$1 \to k_m^\bullet \to \Gamma_m \to w_m F[x] \to 0\,.$$

We can now give the

Proof of Theorem 7.1. Let $w = w_{n+1}$, the unique extension of v to $F[x]$ mapping h to ∞. For each $m \geq 0$ let E_m be the subfield of k generated by all the residue classes of all integral products of elements of $F[x]_m$, and let Γ_m denote the subgroup generated by $\{w(s) : s \in F[x]_m, w(s) \neq \infty\}$. The above lemma implies that if $\deg g_i < m \leq \deg g_{i+1}$, then $E_m = k_{i+1}$ and $\Gamma_m = w_{i+1}F[x]$. Also, if $m > \deg h$, then $E_m = k$ and $\Gamma_m = wF[x]$. Thus the sequence of ordered pairs

$$((E_m, \Gamma_m))_{1 \leq m}$$

is nonconstant (i.e., $(E_m, \Gamma_m) \neq (E_{m+1}, \Gamma_{m+1})$) exactly at the values $m = \deg g_i$ for $i = 0, \ldots, n$. Thus n and the sequences $(\deg g_0, \ldots, \deg g_{n+1})$, $(k_0, \ldots, k_{n+1})$ and $(w_0F[x], \ldots, w_{n+1}F[x])$ are invariants of h. Hence the sequence of indices $e_i = (w_{i+1}F[x] : w_iF[x])$ and the sequences of quotients $d_i = \deg g_{i+1}/\deg g_i$ and $f_i = d_i/e_i$ are invariants of h.

It remains to prove that the sequences $(q_0, \ldots, q_n)$ and $([G_0], \ldots, [G_n])$ are invariants of h. (The definition of q_i for $0 \leq i \leq n$, cf. formula (3.1), would then say that $(\gamma_1, \ldots, \gamma_{n+1})$ is also an invariant of h.) Suppose that $g^* = ((g_i^*, w_i^*, \gamma_i^*))_{i \leq n+1}$ is a second strict system of polynomial extensions with $g_{n+1}^* = h$. We adapt the notation introduced for g to the sequence g^* in the obvious way, by adding superscript *'s.

Thus, for example, d_i^* will denote $\deg g_{i+1}^*/\deg g_i^*$ and q_i^* will denote $\gamma_{i+1}^*/d_i^* = w(g_i^*)$.

Suppose that $m \leq n$. Since g_m and g_m^* are monic of the same degree, by Proposition 3.2(B) we can write $g_m^* = g_m + \Sigma_{\sigma\in J_m} b_\sigma g^\sigma$ for some $b_\sigma \in F$ and then

$$q_m^* = w(g_m^*) = \min(q_m, w(\Sigma_{\sigma\in J_m} b_\sigma g^\sigma)) \leq q_m\,.$$

Similarly, $q_m \leq q_m^*$. Hence $q_m = q_m^*$ for all $m \leq n$.

We now show that G_m and G_m^* are linearly equivalent over k_m. This will prove that the sequence of equivalence classes $[G_i]$ is an invariant of h. We assume that G_m is defined with respect to some choice of $s \in F[x]_{\deg g_m}$ and similarly that G_m^* is defined with respect to some $s^* \in F[x]_{\deg g_m}$. By the above paragraph we have $w(s) = w(s^*) = -e_m q_m$. There exists $u \in F[x]_{\deg g_m}$ with us and us^* both units. Let us write $G_m = Y^{f_m} + \Sigma_{i<f_m}\tau(A_{ie_m} s^{f_m-i})Y^i$. One checks that

$$G(\tau(su)\tau(s^*u)^{-1}Y) = (\tau(su)\tau(s^*u)^{-1})^{f_m}(Y^{f_m}+\Sigma_{i<f_m}\tau(A_{ie_m} {s^*}^{f_m-i})Y^i)\,.$$

Thus without loss of generality we may assume that $s = s^*$ and indeed that $s = bg^\sigma$ for some $b \in F$ and $\sigma \in J_m$. If $\tau(sg_m^{e_m})$, which has irreducible polynomial G_m, equals $\tau(s{g_m^*}^{e_m})$, then $G_m = G_m^*$ and we are finished. Otherwise, $s(g_m^{e_m} - {g_m^*}^{e_m})$ is a unit and so $w(g_m^{e_m} - {g_m^*}^{e_m}) =$

$e_m q_m \in w_m F[x]$. We can write

$$g_m^{e_m} - g_m^{*\ e_m} = \Sigma_{i<e_m} \Sigma_{\sigma \in J_m} a_{i,\sigma} g^\sigma g_m^i$$

for some $a_{i,\sigma} \in F$ and

$$e_m q_m = \min_{i,\sigma} w_m(a_{i,\sigma} g^\sigma) + i q_m\,.$$

Thus by the definition of e_m every term $a_{i,\sigma} g^\sigma g_m^i$ of the above sum with value $e_m q_m$ must have $i = 0$ and hence by the previous lemma the residue class of $s(g_m^{e_m} - g_m^{*\ e_m})$ is in k_m. Hence

$$G_m^*(Y) = G_m(Y + \tau(s(g_m^{e_m} - g_m^{*\ e_m})))$$

since both polynomials are monic irreducible over k_m with the same root $\tau(s g_m^{*\ e_m})$. Thus G_m and G_m^* are linearly equivalent over k_m, as was to be shown. □

8. Polynomials with prescribed invariants

Note that all of the sequences of invariants of elements of $\mathcal{P}(F)$ described in Theorem 7.1 can be derived from just the pair of sequences $(q_0, \ldots, q_n)$ and $([G_0], \ldots, [G_n])$. We now show that subject to obviously necessary conditions all such pairs of sequences are invariants of some element of $\mathcal{P}(F)$. A technical problem must be dealt with before we can do this. One can speak of a sequence $(q_0, \ldots, q_n)$ of elements of $\mathbb{Q}vF$, but in order to speak abstractly of a sequence $([G_0], \ldots, [G_n])$ of equivalence classes of polynomials one must have fields specified over which they are polynomials. These considerations suggest the following definition.

8.1. **Definition.** An *abstract system of polynomial invariants* over (F, v) is a triple of sequences

$$\big((q_0, \dots, q_n), ([G_0], \dots, [G_n]), (k_0, \dots, k_{n+1})\big)$$

such that the q_i are in $\mathbb{Q}vF$, the k_i are fields with $k_0 = \overline{F}$, and the $[G_i]$ are k_i-equivalence classes of monic irreducible polynomials $G_i \in k_i[x]$ such that if $i \le n$ then k_{i+1} is a field extension of k_i generated by a root of G_i. If

$$\big((q_0^*, \dots, q_n^*), ([G_0^*], \dots, [G_n^*]), (k_0^*, \dots, k_{n+1}^*)\big)$$

is another such triple, we regard the two as *equivalent* if $q_i = q_i^*$ for all $i \le n$ and there exists an isomorphism $\theta : k_{n+1} \to k_{n+1}^*$ such that for all $i \le n$, $\theta(k_i) = k_i^*$ and θ takes the k_i-equivalence class of G_i to the k_i^*-equivalence class of G_i^*.

Let us denote by Φ_F the map assigning to each $h \in \mathcal{P}(F)$ the equivalence class of the abstract system of polynomial invariants

$$\big((q_0, \dots, q_n), ([G_0], \dots, [G_n]), (k_0, \dots, k_{n+1})\big)$$

of Theorem 7.1.

8.2. **Theorem.** *Φ_F maps $\mathcal{P}(F)$ surjectively onto the set of all equivalence classes of abstract systems of polynomial invariants*

$$\big((q_0, \dots, q_n), ([G_0], \dots, [G_n]), (k_0, \dots, k_{n+1})\big) \tag{8.1}$$

over (F, v) such that if $0 \le i \le n$, then

$$e_i f_i > 1 \text{ and if } i < n, \text{ then } q_{i+1} > e_i f_i q_i \tag{8.2}$$

where $f_i = [k_{i+1} : k_i]$ and $e_i = (vF + \Sigma_{j \le i} \mathbb{Z} q_j : vF + \Sigma_{j<i} \mathbb{Z} q_j)$.

Proof. That the abstract systems of polynomial invariants arising from elements of $\mathcal{P}(F)$ satisfy the two conditions (8.2) follows immediately from Definition 2.1(B) and formula (3.2). Now suppose that we are given an abstract system of polynomial invariants (8.1) satisfying these two conditions. By induction on n we may assume without loss of generality that there exists a strict system of polynomial extensions $g^* = ((g_i, w_i, \gamma_i))_{i \le n}$ such that $\Phi_F(g^*)$ is the equivalence class of

$$\big((q_0, \dots, q_{n-1}), ([G_0], \dots, [G_{n-1}]), (k_0, \dots, k_n)\big)\,. \tag{8.3}$$

(If $n = 0$ let g^* be the sequence with just the one element (g_0, w_0, γ_0) where $g_0 = x,\ \gamma_0 = -\infty$ and $w_0(c) = v(c(0))$ for all $c \in F[x]$.) We will use all the notation of Sections 2 and 3 as they apply to g^*; we are *not* assuming that we are given a strict system of polynomial extensions g. By Proposition 3.2 there exist $s, t \in F[x]_{\deg g_n}$ with $w_n(s) = -w_n(t) = -e_n q_n$. Let us write $G_n = Y^{f_n} + \sum_{i<f_n} a_i Y^i$. For each $i < f_n$ pick $B_i \in$

$F[x]_{\deg g_n}$ with $\tau_n(B_i) = a_i\tau_n(st)^{i-f_n}$ and let $A_i \in F[x]_{\deg g_n}$ denote the remainder when $B_i t^{f_n-i}$ is divided by g_n. Then $w_n(A_i - B_i t^{f_n-i}) = \infty$. Set $g_{n+1} = g_n^{e_n f_n} + \sum_{i<f_n} A_i g_n^{ie_n}$. Let w_{n+1} be any element of $\mathcal{E}(v)$ with $w_{n+1}(g_{n+1}) = \infty$ and let $\gamma_{n+1} = w_n(g_{n+1})$. Then the sequence $((g_i, w_i, \gamma_i))_{i\leq n+1}$ satisfies the first four conditions of Definition 2.1 for being a strict system. It satisfies condition (E) (for $i = n$) since for all $r < f_n$ our hypothesis (8.2) implies that

$$w_n(A_r)/(e_nf_n - e_nr) = w_n(B_rt^{f_n-r})/(e_nf_n - e_nr)$$

$$\geq w_n(t)/e_n = w_n(A_0)/e_nf_n = q_n > \gamma_n\,.$$

Finally condition (F) is satisfied since both $A_i s^{f_n-i}$ and $B_i(st)^{f_n-i}$ map under τ_n to a_i. Thus g is a strict system of polynomial extensions over (F, v) and the residue class field of w_{n+1} is k_n-isomorphic to the given field k_{n+1} in display (8.1) (both extensions are generated by a root of G_n); hence $\Phi_F(g_{n+1})$ is the equivalence class of the system (8.1). □

8.3. **Remark.** All elements of $\mathcal{P}(F)$ can be obtained from a variant of the construction in the previous proof. Let us add to the construction of g_{n+1} in that proof a final step in which we replace g_{n+1} by its sum with any polynomial c of smaller degree with $w_{n+1}(c) > \gamma_{n+1}$; the resulting sum has the same image under Φ_F. By varying at each stage of the inductive construction of g_{n+1} our choice of the representative G_i and of s and c, we can generate all elements of $\mathcal{P}(F)$ whose image under Φ_F is the equivalence class of the abstract system in display (8.1).

9. Complete distinguished chains

Throughout this section we assume that (F, v) is Henselian and we do *not* assume that $h = g_{n+1}$ for some g as in Definition 2.1. We will denote the unique extension of v to the algebraic closure F^a also by v.

In this section we will show that if (F, v) is Henselian, then every complete (often called "saturated") distinguished chain of polynomials in $F[x]$ in the sense of [13], [1] is a strict system of polynomial extensions. The first application of this theorem will be to show that if (F, v) is Henselian, then $\mathcal{P}(F)$ consists precisely of the monic nonlinear defectless polynomials over (F, v).

Generalizing the language of [13, p. 109] (which assumes that one is working over a local field) to the more general context of [1], we will say that a sequence $h_1, \cdots, h_m$ of monic irreducible polynomials in $F[x]$ is a *complete distinguished chain* with respect to (F, v) if the polynomials have respective roots $\alpha_1, \cdots, \alpha_m$ in F^a which form a complete distinguished chain in the sense of [1, p. 608]; that is, $\deg h_1 > \cdots > \deg h_m = 1$ and for all $i < m$ if $c \in F^a$ and $[F[c] : F] < \deg h_{i+1}$, then $v(\alpha_{i+1} - c) \leq v(\alpha_{i+1} - \alpha_i)$, with equality only if $[F[c] : F] \geq \deg h_i$.

9.1. **Theorem.** *Suppose that* $(g_{n+1}, \cdots, g_0)$ *is a complete distinguished chain over* (F, v)*. Let* $\gamma_0 = -\infty$*. For each* $0 \leq i \leq n+1$ *let* w_i *denote the unique extension of* v *to* $F[x]$ *with* $w_i(g_i) = \infty$ *and for each* $0 \leq i \leq n$ *set* $\gamma_{i+1} = w_i(g_{i+1})$*. Then the sequence* $g = ((g_i, w_i, \gamma_i))_{i \leq n+1}$ *is a strict system of polynomial extensions over* (F, v)*.*

The proof below of Theorem 9.1 owes a debt to the arguments of the proof of Theorem 3.2 in [13]. It will in particular use the notion of a "minimal pair" over (F, v), i.e., an ordered pair $(\theta, \delta) \in F^a \times \mathbb{Q}vF$ such that $[F[\theta] : F] \leq [F[b] : F]$ for all $b \in F^a$ with $v(\theta - b) \geq \delta$. Such a minimal pair has associated with it a valuation $w_{\theta,\delta}$ on $F^a(x)$ which is given on $F^a[x]$ by the formula

$$w_{\theta,\delta}(\sum a_i(x-\theta)^i) = \min_i v(a_i) + i\delta\,.$$

If c is the irreducible polynomial of θ over F, then the restriction of $w_{\theta,\delta}$ to $F[x]$ is given by the formula

$$w_{\theta,\delta}(\sum A_i c^i) = \min_i v(A_i(\theta)) + i\gamma \tag{9.1}$$

where the A_i above are in $F[x]_{\deg c}$ and where

$$\gamma = w_{\theta,\delta}(c) = \sum \min(\delta, v(\theta - \beta))$$

(the last sum above is taken over all roots β of c) [1, Theorem A], [3, Theorem A].

In the proof of Theorem 9.1 and in the next lemma we will often write $c \equiv d \pmod{u}$ (or just $c \equiv d$) if $u(c-d) > u(c)$ where c and d are nonzero elements of $F^a(x)$ and u is a valuation on $F^a(x)$. Note that if $s \equiv t$ and $c \equiv d$, then we have $sc \equiv td$ and $1/c \equiv 1/d$. Moreover if $u(c) = u(d) = 0$, then $c \equiv d$ if and only if c and d have the same residue class. When using this notation we will of course specify explicitly the valuation u involved.

9.2. **Lemma.** *Suppose that (α, δ) is a minimal pair over (F, v) and that α is a root of g_{n+1} for some g as in Definition 2.1. Then $w_{\alpha,\delta}(g_{n+1}) > \gamma_{n+1}$.*

Proof. We let $\overline{\beta}$ denote residue class of any unit β with respect to the valuation $w_{\alpha,\delta}$.

Note that $w_{\alpha,\delta}$ and w_{n+1} agree on $F[x]_{\deg g_{n+1}}$ (they both map any $c \in F[x]_{\deg g_{n+1}}$ to $v(c(\alpha))$). Hence if we write

$$g_{n+1} = \sum_{r \le d_n} A_r g_n^r$$

where each A_r is in $F[x]_{\deg g_n}$ and $A_{d_n} = 1$, then we have

$$\gamma_{n+1} = d_n q_n = \min_r \{ w_{n+1}(A_r g_n^r) \} \le w_{\alpha,\delta}(g_{n+1})\,.$$

We must show that the above inequality is strict; just suppose that it is not. Then $w_{\alpha,\delta}(g_{n+1}) \in vF[\alpha]$ and hence there exists $c \in F[x]_{\deg g_{n+1}}$

with $w_{\alpha,\delta}(g_{n+1}/c) = 0$. As usual if e_n does not divide i then $w_{\alpha,\delta}(A_i g_n^i) = w_{n+1}(A_i g_n^i) > d_n q_n$. Thus by [3, Lemma 2.1(i)]

$$\overline{g_{n+1}/c} = \overline{g_n^{d_n}/c}\ \overline{1 + \sum_{j<f_n} A_{je_n}/g_n^{d_n - je_n}}$$
$$= \overline{g_n^{d_n}(\alpha)/c(\alpha)}\ \overline{1 + \sum_{j<f_n} A_{je_n}(\alpha)/g_n^{d_n - je_n}(\alpha)} \in \overline{F[\alpha]}\,.$$

(The last equality above uses the multiplicativity of the relation $\equiv$ defined with respect to $w_{\alpha,\delta}$.) This contradicts the fact that $\overline{g_{n+1}/c}$ is transcendental over $\overline{F}$ [3, Theorem A (ii)]. □

We now turn directly to the

Proof of Theorem 9.1. The sequence g is easily checked to satisfy conditions (A), (B), (C), and (D) of Definition 2.1. It remains to show that it satisfies (E) and (F).

We will regard the singleton sequence $((g_0,\ w_0,\ \gamma_0))$ as a strict system of length 0. We may then assume by induction on n that $\widehat{g} := ((g_i,\ w_i,\ \gamma_i))_{i \leq n}$ is a strict system. We will use the notation of Sections 2 and 3 as they apply to the strict system $\widehat{g}$.

By hypothesis (g_{n+1}, g_n) is a distinguished pair, so (α, α_n) is a distinguished pair for some roots α and α_n of g_{n+1} and g_n, respectively. By the definition of distinguished pairs $\delta := v(\alpha - \alpha_n)$ is the main invariant $\delta_F(\alpha)$ of α [1, p. 608]. Thus (α_n, δ) is a minimal pair [1, Lemma 2.2]; the associated valuation is $w := w_{\alpha_n,\delta}$. Set $\gamma := w(g_n)$ (cf. Eq. 9.1).

For any unit $\beta \in F^a[x]$ we let $\overline{\beta}$ denote its residue class with respect to w. The residue class field of any subfield E of F^a with respect to the restriction of v to E will be denoted by $\overline{E}$. The relation $\equiv$ will be defined with respect to the valuation w. We will use repeatedly the facts that for any nonzero $c \in F[x]_{\deg g_n}$ we have $c(\alpha) \equiv c(\alpha_n) \equiv c$ (and hence $v(c(\alpha)) = v(c(\alpha_n)) = w_n(c))$ [3, Lemma 2.1], and for any $c \in F[x]_{\deg g_{n+1}}$ we have $v(c(\alpha)) = w(c)$ [1, Lemma 2.2]. In particular $\gamma = w(g_n) = v(g_n(\alpha))$. Thus by [1, Theorem 1.1] we have

$$vF[\alpha] = vF[\alpha_n] + \mathbb{Z}\gamma \,, \tag{9.2}$$

and $\overline{F[\alpha]} \supseteq \overline{F[\alpha_n]}$. Let

$$e = (vF[\alpha] : vF[\alpha_n]) \quad \text{and} \quad f = [\overline{F[\alpha]} : \overline{F[\alpha_n]}\ ] \,.$$

Since g_{n+1} and g_n are defectless [1, Theorem 1.2], therefore

$$\begin{aligned} \deg g_{n+1} &= [\overline{F[\alpha]} : \overline{F}](vF[\alpha] : vF) \\ &= ef[\overline{F[\alpha_n]} : \overline{F}](vF[\alpha_n] : vF) \\ &= ef \deg g_n \,. \end{aligned}$$

Thus we can write

$$g_{n+1} = g_n^{ef} + \sum_{r<ef} A_r g_n^r$$

where each A_r is in $F[x]_{\deg g_n}$.

Let us write $g_n = \prod_{i=1}^{\deg g_n}(x-\beta_i)$ and $g_{n+1} = \prod_{i=1}^{\deg g_{n+1}}(x-\rho_i)$. Since (F,v) is by hypothesis Henselian,

$$\begin{aligned}\frac{\gamma}{\deg g_n} &= \frac{v(g_n(\alpha))}{\deg g_n} = \frac{v(\prod_{i=1}^{\deg g_{n+1}} g_n(\rho_i))}{\deg g_n \deg g_{n+1}} \\ &= \frac{v(\prod_{i=1}^{\deg g_{n+1}}\prod_{j=1}^{\deg g_n}(\rho_i-\beta_j))}{\deg g_n \deg g_{n+1}} = \frac{v(\prod_{j=1}^{\deg g_n} g_{n+1}(\beta_j))}{\deg g_n \deg g_{n+1}} \\ &= \frac{v(g_{n+1}(\alpha_n))}{\deg g_{n+1}} = \frac{v(A_0(\alpha_n))}{\deg g_{n+1}} = \frac{w(A_0)}{\deg g_{n+1}}\,.\end{aligned}$$

Hence $w(A_0) = ef\gamma$. Since $\sum A_i g_n^i$ has smaller degree than g_{n+1}, we have

$$\begin{aligned}&w(\sum_{i<ef} A_i g_n^i) = v(\sum_{i<ef} A_i(\alpha) g_n(\alpha)^i) \\ &= v(g_n^{ef}(\alpha)) = ef v(g_n(\alpha)) = ef\gamma\,,\end{aligned}$$

so by formula (9.1) for all $j < ef$, we have $w(A_j) + j\gamma \geq ef\gamma$, and hence

$$\frac{w_n(A_j)}{(ef-j)} = \frac{w(A_j)}{(ef-j)} \geq \gamma = \frac{w(A_0)}{ef} = \frac{w_n(A_0)}{ef}\,.$$

Since $\gamma > \gamma_n$ (apply Lemma 9.2 to $\widehat{g}$ in the nontrivial case that $n > 0$), this completes the argument that condition (E) of Definition 2.1 is satisfied.

From formula (9.2) we see that there exists $s \in F[x]_{\deg g_n}$ with $w_n(s) = w(s) = -e\gamma$, so that $w(sg_n^e) = 0$. One checks that for each $i < f$ we have $w_n(A_{ie}s^{f-i}) = w(A_{ie}s^{f-i}) \geq 0$ and also that if $i < ef$ and e does not divide i, then $w(s^f A_i g_n^i) > 0$. Thus if e does not divide

i, then $v(A_i(\alpha)s^f(\alpha)g_n(\alpha)^i) > 0$, so

$$0 = \overline{s^f(\alpha)g_{n+1}(\alpha)} = (\overline{s(\alpha)g_n^e(\alpha))}^f + \sum_{i<f} \overline{A_{ie}(\alpha)s^{f-i}(\alpha)}\ \overline{(s(\alpha)g_n^e(\alpha))}^i ,$$

so that $\overline{s(\alpha)g_n^e(\alpha)}$ is a root of

$$\begin{aligned} Y^f + \sum_{i<f} \overline{A_{ie}(\alpha)s^{f-i}(\alpha)}Y^i &= Y^f + \sum_{i<f} \overline{A_{ie}s^{f-i}}Y^i \\ &= Y^f + \sum_{i<f} \overline{A_{ie}(\alpha_n)s^{f-i}(\alpha_n)}Y^i . \end{aligned} \tag{9.3}$$

This is a polynomial over $\overline{F[\alpha_n]}$. Now consider any unit in $F[\alpha]$, say $c(\alpha)$ where $\deg c < \deg g_{n+1}$. If we write $c = \sum_{i<ef} B_i g_n^i$ (where $B_i \in F[x]_{\deg g_n}$ for all i), then for each $i < ef$

$$w(B_i(\alpha)g_n(\alpha)^i) = w(B_i g_n^i) \geq w(c) = v(c(\alpha)) = 0$$

with equality only if $i = je$ for some j, whence

$$\overline{B_i(\alpha)g_n^i(\alpha)} = \overline{g_n^e(\alpha)s(\alpha)}^j\, \overline{B_i(\alpha)/s^j(\alpha)} = \overline{g_n^e(\alpha)s(\alpha)}^j\, \overline{B_i(\alpha_n)/s^j(\alpha_n)} .$$

This shows that $\overline{F[\alpha]} = \overline{F[\alpha_n]}[\overline{g_n^e(\alpha)s(\alpha)}]$. Since $[\overline{F[\alpha]} : \overline{F[\alpha_n]}] = f$, the polynomial (9.3) is irreducible over $\overline{F[\alpha_n]}$. Since $w(g_n) = \gamma > \gamma_n$, we can apply part (E) of Proposition 3.2 to w to conclude that the polynomial (2.1) of Definition 2.1 with $i = n$ is irreducible over k_n. (The map Φ_n of (E) maps the polynomial (2.1) in Definition 2.1 to that of formula (9.3) and the field k_n to $\overline{F[\alpha_n]}$.) Thus the sequence g satisfies condition (F) of that definition. Hence g is a strict system. □

9.3. **Theorem.** *If* (F, v) *is Henselian, then* $\mathcal{P}(F)$ *consists exactly of the monic nonlinear defectless polynomials over* (F, v)*.*

Proof. That every polynomial in $\mathcal{P}(F)$ is defectless follows from Proposition 3.2. Now suppose that h is monic, nonlinear and defectless. Aghigh and Khanduja prove that any root α of h is the first element of a complete distinguished chain of elements of F^a over (F, v) [1, Theorem 1.2]; the corresponding sequence of irreducible polynomials is by Theorem 9.1 a strict system of polynomial extensions whose polynomial of highest degree is h. Thus, $h \in \mathcal{P}(F)$. □

As an application we now give in the tame case a characterization of minimal pairs; this result is also a corollary of [14, Theorem 1.1].

9.4. **Theorem.** *Suppose that* $F[\alpha]$ *is a proper tame extension of the Henselian field* (F, v)*. Then for any* $\delta \in \mathbb{Q}vF$*, the pair* (α, δ) *is a minimal pair with respect to* (F, v) *if and only if* $\delta > \omega_F(\alpha)$*.*

Proof. The sufficiency of the condition follows from Krasner's Lemma. Now suppose that (α, δ) is a minimal pair. By Theorem 9.3 the irreducible polynomial h of α over F equals g_{n+1} for some g as in Definition 2.1. By Corollary 3.5 and Theorem 4.1 there exists a root β of g_n with $v(\alpha - \beta) = m_n = \omega_F(\alpha)$. Since (α, δ) is a minimal pair and $\deg \alpha > \deg \beta$, therefore $\delta > v(\alpha - \beta) = \omega_F(\alpha)$.

□

9.5. **Problems.** (A) Is Theorem 9.3 valid without the hypothesis that (F, v) is Henselian? This is indeed the case when (F, v) is discrete rank one [8, Remark 6(C)].

(B) Suppose that (F, v) is Henselian and that g is a strict system as in Definition 2.1. Is the sequence $(g_{n+1}, \cdots, g_0)$ a complete distinguished chain? It is easy to see that the answer is yes if g has length one. We will show next that this is also the case if the polynomials g_i are tame.

9.6. **Theorem.** *Suppose that g as in Definition 2.1 is a strict system and that $h = g_{n+1}$ is tame over (F, v). Then the sequence $(g_{n+1}, \cdots, g_0)$ is a complete distinguished chain over (F, v).*

Proof. By Corollary 3.5 for any root θ_0 of h there is a unique root θ_1 of g_n with $v(\theta_0 - \theta_1) = m_n$. Hence by Theorem 4.1 and [3, Theorem C] we have $v(\theta_0 - \theta_1) = \delta_F(\theta_0)$. Note that

$$[F[\theta_0] : F] = \deg g_{n+1} > \deg g_n = [F[\theta_1] : F].$$

Moreover, if $\beta \in F^a$ and $[F[\beta] : F] < [F[\theta_1] : F]$, then

$$v(\theta_0 - \beta) < v(\theta_1 - \theta_0)$$

since otherwise

$$v(\theta_1 - \beta) = v(\theta_1 - \theta_0 + \theta_0 - \beta) \geq m_n > m_{n-1} = \omega_F(g_n),$$

so $F[\beta] \supset F[\theta_1]$, a contradiction. Thus (θ_0, θ_1) is a distinguished pair in the sense of [1, p. 608]. Applying the above argument to each of the pairs of polynomials (g_{i+1}, g_i) we see that we have associated with h and its root θ_0 a canonical complete distinguished chain $\theta_0,\ \theta_1,\ \cdots,\ \theta_{n+1} = a$ where for each $i \geq 0$ we have $v(\theta_{i+1} - \theta_i) = m_i$. The associated complete distinguished chain of polynomials is exactly the sequence $(g_{n+1},\ \cdots,\ g_0)$. □

9.7. **Remark.** Extending work of [13, Proposition 4.3], Aghigh and Khanduja use complete distinguished chains to construct a number of sequences of invariants of defectless polynomials over (F, v) [1, Theorem 1.5]. One can apply Theorem 9.1 to deduce the invariance of most of these sequences (and some others) from Theorem 7.1; the obvious exception is the sequence of main invariants. To deduce (most of) Theorem 7.1 from [1, Theorem 1.5] would appear to require supplying an affirmative answer to Problem 9.5(B).

10. Polynomials of length one

We now describe the polynomials of length one.

As in the previous section we will assume that (F, v) is Henselian and denote the unique extension of v to F^a by v. The residue class of any integral element b of F^a and the residue class field of any subfield L

of F^a will be denoted by $\overline{b}$ and $\overline{L}$, respectively. As usual h will denote an element of $\mathcal{P}(F)$ with a root $\alpha \in F^a$.

10.1. **Theorem.** *The following are equivalent:*

(A) h has length one;

(B) the main invariant of h equals its base invariant;

(C) there exists $a \in F$ such that if $e > 0$ is least with $ev(a-\alpha) = -v(s)$ for some $s \in F$, then

$$e = (vF[\alpha] \ : vF) \quad \textit{and} \quad \overline{F}\left[\,\overline{(a-\alpha)^e s}\,\right] = \overline{F[\alpha]}\,.$$

This theorem generalizes and is inspired by Khanduja's characterization in the tame case of the polynomials whose Krasner constants equal their diameters [10, Theorem 1.1]. Of course in the tame case the base invariant is the diameter and the Krasner constant is the main invariant (cf. Definition 7.2, Theorem 4.1, and [3, Theorem C]). Condition (iii) of Khanduja's theorem cited above is our condition (C) above. The proof below that (A) and (C) are equivalent will not use the hypothesis that (F, v) is Henselian.

Proof. We first show that (A) implies (B). Since h is defectless, there is a complete distinguished chain, say of length n, with first element h and last element of the form $x - a$ [1, Theorem 1.2]. This chain gives the sequence of polynomials in a strict system of polynomial extensions

g as in Definition 2.1 (Theorem 9.1) which also must have length one (Theorem 7.1). Thus $(h, x-a)$ is a distinguished pair, and so $\delta_F(h) = v(\alpha - a) = q_0 = \beta_F(h)$.

We next argue the converse, that (B) implies (A). There is a complete distinguished chain of the form $(\alpha, \alpha_n, \cdots, \alpha_0)$. If $n = 0$, then we are finished since there would be a strict system of length one with h as its polynomial of maximum degree (Theorem 9.1). Suppose that $n > 0$. Since (α, α_n) is a distinguished pair, we have

$$v(\alpha - \alpha_n) = \delta_F(\alpha) = \beta_F(\alpha) = v(\alpha - a)$$

for some $a \in F$, and hence $1 = [F[a] : F] \geq [F[\alpha_n] : F] > 1$, a contradiction.

That (A) implies (C) follows immediately from Proposition 3.2 (parts (D) and (E)). (Note that if $h = g_{n+1}$ for some g as in Definition 2.1, then $n = 0$ and $\tau_0((x-a)^e s)$ is a root of the polynomial (2.1) of Definition 2.1(F) with $i = 0$, where the s in Definition 2.1 is taken to be the s of part (C) of Theorem 10.1.)

We now prove that (C) implies (A). Pick a and s as in (C). Let $f = \left[\overline{F[\alpha]} : \overline{F}\right]$, so $\deg h = \left[\overline{F[\alpha]} : \overline{F}\right](vF[\alpha] : vF) = ef$. Pick $B_i \in F$, each either zero or a unit, with $Y^f + \sum_{i<f} \overline{B_i} Y^i$ the irreducible

polynomial of $\overline{(\alpha-a)^e s}$ over $\overline{F}$. Set

$$T = (x-a)^{ef} + \sum_{i<f} B_i s^{i-f}(x-a)^{ie}\,.$$

There exist extensions w_0, w, and w' of v to $F[x]$ with

$$w_0(x-a) = w(h) = w'(T) = \infty\,.$$

One can check as in the proof of Theorem 8.2 that

$$((x-a, w_0, -\infty), (T, w', -fv(s)))$$

is a strict system of polynomial extensions over (F, v). (Since $s \in F$ we can take $t = s^{-1}$ in the argument proving Theorem 8.2.) By the choice of the B_i we have

$$\begin{aligned} w(T) &= w\left(s^{-f}(((x-a)^e s)^f + \sum B_i((x-a)^e s)^i)\right) \\ &> -w(s^f) = \gamma_T \end{aligned}$$

so by Proposition 3.2, the valuations w and w' agree on $F[x]_{ef}$, and so for any $c_i \in F$,

$$w\left(\sum_{i<ef} c_i(x-a)^i\right) = \min_{i<ef}\left(v(c_i) - \frac{i}{e}v(s)\right).$$

Now write $h = \sum c_i(x-a)^i$ and $T = \sum c_i'(x-a)^i$ where each c_i, $c_i' \in F$. Since deg $(T-h) < ef$, for all $j < ef$ we have

$$\left(\frac{j}{e} - f\right)v(s) < w(T) + \frac{j}{e}v(s) = w(T-h) + \frac{j}{e}v(s)$$

$$= \min_{i<ef} v(c_i' - c_i) - \frac{i}{e}v(s) + \frac{j}{e}v(s) \le v(c_j' - c_j)\,.$$

If $c'_j \neq 0$ we have $j = ei$ for some integer i and $c'_j = B_i s^{i-f}$ where B_i is a unit, so

$$v(c'_j) = \left(\frac{j}{e} - f\right) v(s) < v(c'_j - c_j),$$

and hence $v(c_j) = v(c'_j)$. In particular $v(c_0) = v(c'_0) = -fv(s)$. Of course if $c'_j = 0$ then $v(c_j) > \left(\frac{j}{e} - f\right) v(s)$. It follows that

$$((x - a, w_0, \ -\infty), \ (h, w, -fv(s)))$$

is a strict system of polynomial extensions over (F, v), so that h is indeed an element of $\mathcal{P}(F)$ of length 1. (In verifying that condition (F) of Definition 2.1 holds, we may assume the element denoted "s" in the definition is the s in condition (C) of Theorem 10.1.) $\square$

References

[1] K. Aghigh and S. K. Khanduja, On chains associated with elements algebraic over a Henselian valued field, *Algebra Colloq.* **12** (2005) 607—616.

[2] J. Ax, Zeros of polynomials over local fields – the Galois action, *J. Algebra* **15** (1970) 417–428.

[3] S. Bhatia and S. K. Khanduja, On extensions generated by roots of lifting polynomials, *Mathematika* **49** (2002) 107–118.

[4] N. Bourbaki, *Algèbre Commutative*, Chapitre VI, "Valuations," (Hermann, Paris, 1964).

[5] D. Brink, New light on Hensel's lemma, *Expos. Math.* **24** (2006), 291–306.

[6] R. Brown, Valuations, primes and irreducibility in polynomial rings and rational function fields, *Trans. Amer. Math. Soc.* **174** (1972) 451–488.

[7] R. Brown, Roots of generalized Schönemann polynomials in Henselian extension fields, *Indian J. of Pure and Applied Math.* **39** (2008) 403–410.

[8] R. Brown, Roots of irreducible polynomials in tame Henselian extension fields, *Comm. Alg.* to appear.

[9] S. K. Khanduja, A note on a result of J. Ax, *J. Algebra* **140** (1991) 360–361.

[10] S. K. Khanduja, On Krasner's constant, *J. Algebra* **213** (1999) 225–230.

[11] F.-V. Kuhlmann, *Valuation Theory*, 2008 draft available at http://math.usask.ca/∼ fvk/Fvkbook.htm.

[12] S. MacLane, A construction for absolute values on polynomial rings, *Trans. Amer. Math. Soc.* **40** (1936) 363–395.

[13] N. Popescu and A. Zaharescu, On the structure of the irreducible polynomials over local fields, *J. Number Theory* **52** (1995) 98–118.

[14] A. Singh and S. K. Khanduja, On finite tame extensions of valued fields, *Comm. Alg.* **33** (2005) 1095–1105.

Department of Mathematics, University of Hawaii, 2565 McCarthy Mall, Honolulu, HI 96822

E-mail address: ron@math.hawaii.edu

Department of Mathematics, Soka University of America, One University Drive, Aliso Viejo, CA 92656

E-mail address: jmerzel@soka.edu