TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 174, December 1972

VALUATIONS, PRIMES AND IRREDUCIBILITY IN POLYNOMIAL RINGS AND RATIONAL FUNCTION FIELDS

BY

RON BROWN[1]

ABSTRACT. The set of extensions of the valuation v on a linearly compact (i.e. maximal) field F to the polynomial ring $F[x]$ is shown to depend only on the value group and residue class field of v. By a method related to Mac Lane's construction of (rank one) valuations on polynomial rings, a determining invariant is associated with each such extension, called its "signature". Very roughly, a signature is a pair of sequences, one in the algebraic closure of the residue class field of v and one in the divisible closure of the value group of v. Signatures are also associated with various mathematical objects by means of the extensions of the above sort which naturally arise from them. For example, the set of nonconstant monic irreducible polynomials in $F[x]$, the set of all finite Harrison primes of the polynomial ring of a global field, and the set of equivalence classes of valuations on the field of rational functions over a global field are each shown to be bijective with a simple set of signatures. Moreover, these objects are studied by means of their associated signatures. For example, necessary and sufficient conditions for irreducibility in $F[x]$ are given, independent of the language of signatures.

1. **Introduction.** Let v be a discrete rank one valuation on a field F. We study the extensions of v to a valuation on the polynomial ring $F[x]$, assigning to each extension a determining invariant. (For valuations on commutative rings see, for example, Bourbaki [2, p. 101].) Our approach has considerable overlap with Mac Lane's construction of the (rank one) valuations on $F[x]$ extending v [15]. In particular, the underlying method consists of approximating a valuation on $F[x]$ by means of the valuations on an associated sequence of simple algebraic extensions of F.

We call the determining invariant associated with an extension of v to $F[x]$ its "signature". Abstractly, signatures are defined entirely in terms of the residue

Presented to the Society, August 28, 1969 under the title *Valuations, primes and irreducibility in rings of polynomials and rational functions*; received by the editors November 19, 1970.

AMS (MOS) subject classifications (1970). Primary 12J10, 12E05, 12B05, 13A15; Secondary 12A20, 12F05, 12F20, 12B10, 12J20, 13F20.

Key words and phrases. Valuation, Harrison prime, discrete rank one valuation, polynomial ring, rational function field, irreducibility, Legendre polynomial, Eisenstein criterion, key polynomial, complete field, Henselian field, linearly compact field, maximal field, global field, algebraic extension, ramification, inductive value, limit value.

(1) Work on this paper was done over an extended period during which the author was variously an NSF fellow and an NAS-ONR research associate at the University of Oregon, and a postdoctoral fellow (partially supported by the Canadian NRC) at Simon Fraser University.

class field and value group of v; roughly, a signature consists of two sequences, one in the algebraic closure of the residue class field of v and one in the divisible closure of the value group of v. An axiomatic approach is used for assigning signatures to extensions; this allows a rapid exposition of our main results. In order that the axioms not appear too unmotivated we present in §2 a leisurely sketch of the construction of the signatures associated with an important set of valuations on $Q[x]$ (Q = rational numbers), namely those associated with finite Harrison primes [10, p. 18]. The definitions and axioms for "associated signatures" appear in §3, along with the statement of a lemma fundamental to our approach and having no analogue in [15]. Given an irreducible polynomial f and an extension w of v to $F[x]$, it describes when the value of w at f determines the value of w at every polynomial of degree less than that of f.

In §4 we prove that when F is topologically complete in the valuation topology of v (abbreviated, *complete*), then the set of extensions of v to $F[x]$ is bijective with an easily described set of signatures depending only on the residue class field and value group of v. We further describe how to recover an extension from its associated signature.

Our first applications are based on the observation that for any prime ideal $\mathfrak{p}$ of $F[x]$, the extensions w of v to $F[x]$ with $\mathfrak{p} = w^{-1}(\infty)$ are naturally bijective with the extensions of v to the field of fractions of $F[x]/\mathfrak{p}$. From the case $\mathfrak{p} = \{0\}$, we obtain a characterization in terms of signatures of the extensions of v to the field of rational functions $F(x)$. From the case $\mathfrak{p} \neq \{0\}$ (so that $F[x]/\mathfrak{p}$ is an algebraic extension of F), we develop several of the basic known facts about algebraic extensions of complete fields as corollaries to our description of valuations on $F[x]$.

Similar reasoning gives, again for F complete, a bijection from the set of nonconstant monic irreducible polynomials in $F[x]$ to a certain easily described set of signatures. This bijection is applied to give necessary and sufficient conditions for irreducibility in $F[x]$ which are independent of the language of associated signatures. While closely related to Mac Lane's generalizations of "polygonal irreducibility criteria" (e.g. Eisenstein's irreducibility criterion) [17, §3], our conditions do not apparently follow from them without the fundamental lemma. Our remarks about irreducibility and algebraic extensions appear in §5; we also make some remarks there about the not necessarily complete case.

In §6 we compute the extensions of v to $F[x]$ no longer assuming that F is complete. In applications, the valuations and finite Harrison primes of $F[x]$ and $F(x)$ are computed in terms of signatures for F a global field. We also compute the finite Harrison primes of $R[x]$ where R is a subring of a global field (e.g. $R = Z$, the integers).

All the results of §§3, 4 and 5 about fields complete at a discrete rank one valuation generalize fully to arbitrary linearly compact (alias, maximal) fields. This generalization is sketched in §7. Incidentally, it would have been possible to proceed initially in great generality, starting only with an arbitrary valuation on a commutative ring (see [3, p. 78] for an example of grotesque generality). Most of the results developed, however, would be more easily obtained as corollaries to the theory developed here, just as the noncomplete case in §6 is developed as a corollary of the complete case in §4. An example of such an application occurs in §9, where we take the briefest look at polynomials in several variables.

In §8 we give a proof of the fundamental lemma for linearly compact fields.

We have delayed until our tenth and last section giving detailed acknowledgements of, and connections with, Mac Lane's work ([15], [16], [17]). This was mainly for expository reasons: the connections are somewhat technical and emerge most clearly from a developed theory. This is the only section for which [15] is a prerequisite.

We now list for reference some notations that will be used throughout; most will be reintroduced before being used again.

"deg f" denotes the degree of a polynomial f. $F^\times$ denotes the multiplicative group of nonzero elements of a field F.

Let n be a nonnegative integer or ∞. The symbol $\langle a_i\rangle_{0\le i<n}$ (or, more compactly, $\langle a_i\rangle_{i<n}$) denotes the *sequence* defined on the set of nonnegative integers less than n whose value at i is a_i; we call n the *length* of the sequence. We allow the sequence of length zero, i.e. the "empty sequence". If $n<\infty$, $\langle a_i\rangle_{i\le n}$ has the obvious meaning.

We use additive notation for valuations. For any ring valuation $v\colon R \to \Gamma \cup \{\infty\}$ [2, p. 101] we call

$A_v = \{a \in R \mid v(a) \ge 0\}$ the *valuation ring* of v,

$\mathfrak{p}_v = \{a \in R \mid v(a) > 0\}$ the *prime ideal* of v,

$\Gamma_v = \Gamma \cap v(R)$ the *value monoid* of v,

$k_v = A_v/\mathfrak{p}_v$ the *residue class ring* of v,

$v^{-1}(\infty)$. the *infinity ideal* of v.

The valuation v is *equivalent* to a valuation v' on R if and only if there is an order isomorphism from $\Gamma_v \cup \{\infty\}$ to $\Gamma_{v'} \cup \{\infty\}$ whose composition with v is v'.

Note that ∞ is used both as an index for sequences and as an infinity for valuations, depending on context.

It is a great pleasure to thank D. K. Harrison and Hoyt Warner for reading various versions of this paper and pointing out many slips and obscurities. I am further in debt to D. K. Harrison for encouragement and generously given advice. This paper has considerable overlap with the author's doctoral dissertation [3], to which we occasionally refer for material peripheral to the main argument.

2. **Prototype example**: $Q[x]$. This paper originated in the study of this example, so it is germinal as well as prototypal. Q denotes the rational numbers, either as a field or as an additive ordered group, depending on context.

We will compute the valuations on $Q[x]$ whose value monoids are groups and whose residue class rings are locally finite fields (i.e. are fields which are the union of their finite subfields). We call such valuations *prime valuations* since the mapping $w \mapsto \mathfrak{p}_w = \{a \in Q[x] \mid w(a) > 0\}$ induces a bijection from the set of equivalence classes of prime valuations on $Q[x]$ to the set of finite Harrison primes of $Q[x]$ (cf. [10, p. 18]).

So let w be a prime valuation on $Q[x]$. Let v denote the restriction of w to Q; if p denotes the characteristic of the residue class field k_w, then v is the p-adic valuation on Q.

We wish initially to construct a sequence $S(w) = \langle \theta_i, q_i \rangle_{i<n}$ of ordered pairs in $k_w^\times \times \Gamma_w$. (Strictly speaking we should write $\langle\langle \theta_i, q_i \rangle\rangle_{i<n}$ but our abbreviation should cause no confusion.) One's first thought might be to set $q_i = w(x^i)$ and $\theta_i = x^i + \mathfrak{p}_w$ for each $i < \infty$. However, the resulting sequence, even when it made sense, would not in general tell one much about w. Rather, using a construction due to Mac Lane [15], we replace the sequence $\langle x^i \rangle_{i<\infty}$ implicitly used above by a sequence $g(w)$ of polynomials which reflects the additional structure that w puts on $Q[x]$ (much as the Gram-Schmidt orthogonalization process replaces a linear basis on an inner product space by one which reflects the inner product). We then use $g(w)$ to define $S(w)$.

Let $g_0 = x, g_1, \cdots, g_m$ be a finite sequence of nonconstant polynomials with $\deg g_s$ dividing $\deg g_{s+1}$ for all $s < m$. Each $f \in Q[x]$ has a unique expansion

$$\sum a_{i_0 \cdots i_m} g_0^{i_0} \cdots g_m^{i_m} \tag{1}$$

where the coefficients $a_{i_0 \cdots i_m}$ are in Q and

$$0 \le i_s < (\deg g_{s+1})/(\deg g_s) \qquad (0 \le s < m). \tag{2}$$

(This is because for each integer $n \ge 0$ there are unique i_s as in (2) with $n = \Sigma\, i_s \deg g_s$, i.e. with

$$g_0^{i_0} \cdots g_m^{i_m} \tag{3}$$

of degree exactly n.) We say that the polynomial (1) is *w-homogeneous in*

$\langle g_i\rangle_{i\le m}$ if and only if every nonzero term in the expansion (1) has the same value, and each coefficient $a_{i_0\cdots i_m}$ is the product of an integral power of p with an element of $\{0, 1, \cdots, p-1\}$. (The *value* of an element of a valued ring is its image under the valuation.)

We now define $g(w) = \langle g_i\rangle_{i<n}$ to be the unique sequence of polynomials of maximal length n (where $0 \le n \le \infty$) such that each polynomial has finite value, $g_0 = x$ if $0 < n$, and for any positive integer $m + 1 < n$,

(I) $\deg g_{m+1}$ is divisible by $\deg g_m$;

(II) g_{m+1} is monic and w-homogeneous in $\langle g_i\rangle_{i\le m}$;

(III) $w(g_{m+1})$ is greater than the value of any of the nonzero terms of g_{m+1}, when g_{m+1} is expanded as in (1);

(IV) g_{m+1} is a polynomial of minimal degree satisfying (III).

The uniqueness of the sequence $g(w)$ is easily verified. (If $0 < m + 1 < n$, then the difference of any two distinct candidates for g_{m+1} would be a polynomial of degree less than $\deg g_{m+1}$ satisfying (III); but this contradicts (IV).) Notice that by (IV), the value of any polynomial of degree less than $\deg g_{m+1}$ is equal to the minimum of the values of its terms, when expanded as in (1). Thus, while $g(w)$ is not a basis for $F[x]$ as an F-module, for each $0 < m < n$ the set of products (3) approximates an "orthobasis" in the sense of MacKenzie-Whaples [14].

Note that we allow $n = 0$ above; this case arises when $w(x) = \infty$.

Before constructing $S(w)$, it is helpful to notice

Lemma. *There is a unique order isomorphism of Γ_w into Q which maps $w(p)$ to 1. Here, Q denotes the additive ordered group of rational numbers.*

Proof (sketch). We first identify the cyclic subgroup of Γ_w generated by $w(p)$ with the integers, Z. It then suffices to show that each element of Γ_w is "commensurable with Z", i.e. has a nonzero integral multiple in Z. Just suppose that there is a polynomial f of least degree whose value is finite and not commensurable with Z. One then can verify that $w(f)$ cannot have an inverse in Γ_w, contradicting that Γ_w is a group. (Use here the fact that by the choice of f the value of a polynomial

$$\sum r_i f^i \qquad (\deg r_i < \deg f)$$

must equal the minimum of the values of its terms.)

We now construct $S(w)$. For each $i < n$, set $q_i = w(g_i)$. If $w(g_i) = w(p^s)$, it is natural to set $\theta_i = p^{-s}g_i + \mathfrak{P}_w$. To proceed in general, we first set (recall $v = w \mid Q$ and Z = integers)

$$\Gamma_m = \Gamma_v + \sum_{i<m} Z \cdot q_i \qquad (0 \le m \le n).$$

Notice that w gives a bijection between Γ_n and the set of all finite products

(5) $$p^{r_n} \prod_{i<n} g_i^{r_i}$$

where only finitely many of the integers r_i are nonzero and

$$0 \leq r_i < (\Gamma_{i+1} : \Gamma_i) \qquad (i < n).$$

Here $(\Gamma_{i+1} : \Gamma_i)$ denotes the index of Γ_i in Γ_{i+1}. We then set $\theta_m = t_m g_m + \wp_w$ for each $m < n$, where t_m is the unique product (5) with $w(t_m) = -w(g_m)$. We call $S(w) = \langle \theta_i, q_i \rangle_{i<n}$ the "presignature" of w.

A technical point. By strict analogy with the definition of the Γ_m, we define

$$k_m = k_v[\{\theta_i \mid i < m\}] \qquad (0 \leq m \leq n).$$

Note that the degree $[k_{m+1} : k_m]$ of each extension k_{m+1}/k_m is finite since k_w is a locally finite field. The fact that $(\Gamma_{m+1} : \Gamma_m)w(g_m) \in \Gamma_m$ and that $\theta_m = t_m g_m + \wp_w$ satisfies a polynomial of degree $[k_{m+1} : k_m]$ over k_m can be shown (nontrivially!) to imply that for $0 < m + 1 < n$

(6) $$\deg g_{m+1} = [k_{m+1} : k_m](\Gamma_{m+1} : \Gamma_m) \deg g_m$$

and hence by induction

(I′) $$\deg g_m = [k_m : k_v](\Gamma_m : \Gamma_v) \qquad (m < n).$$

Notice that the sequence $\langle \theta_i, q_i \rangle_{i<n}$ can be defined in the above manner assuming only that each polynomial in the sequence $\langle g_i \rangle_{i<n}$ has finite value. With this understanding, (I) and (IV) in the definition of $g(w)$ above can be replaced by (I′). Condition (III) then becomes

(7) $$q_{m+1} > [k_{m+1} : k_n](\Gamma_{m+1} : \Gamma_m) q_m$$

or equivalently

(III′) $\langle q_i/[k_i : k_v](\Gamma_i : \Gamma_v) \rangle_{i<n}$ is strictly increasing.

This is because the right-hand side of (7) is precisely the value of $g_m^{[k_{m+1} : k_m](\Gamma_{m+1} : \Gamma_m)}$ which by (6) is one of the nonzero terms of g_{m+1} when expanded as in (1).

One more step. We free $S(w)$ from its dependence on the notation of w (recall $S(w)$ is a sequence of pairs in $k_w^\times \times \Gamma_w$). The values q_i are no problem since by the lemma above they can be uniquely identified with rational numbers. In order to regard the θ_i as lying is some fixed algebraic closure of Z_p (= the field with p elements), call it Z_p^{alg}, we must choose an isomorphism of k_w into Z_p^{alg}. Since any two such isomorphisms differ by an automorphism of Z_p^{alg}, $S(w)$ determines a unique "p-signature" in the sense of the following definition.

Definition. A *p-signature* is an equivalence class ("equivalence" defined below) of sequences $\langle \theta_i, q_i \rangle_{i<n}$ of ordered pairs in $(Z_p^{\text{alg}})^\times \times Q$ which satisfy

(III′) above (with the obvious notation). Two such sequences $\langle \theta_i, q_i \rangle_{i<n}$ and $\langle \theta_i', q_i' \rangle_{i<n'}$ are *equivalent* if and only if $n = n'$, $q_i = q_i'$ for all $i < n$, and there is an automorphism of Z_p^{alg} carrying each θ_i to θ_i'.

We avoid developing the ideas of this section further until we can proceed in greater generality, except to state

Theorem. *Assigning to each prime valuation of $Q[x]$ its corresponding p-signature induces a bijection from the set of equivalence classes of prime valuations on $Q[x]$ to the set of p-signatures, where p ranges over all prime numbers.*

The proof of this theorem will give both an internal picture of the valuation associated with a given p-signature and an external picture of the space of all such valuations (e.g. see (6.8) below).

We close this section with a concrete example. Let $v: Q \to Z \cup \{\infty\}$ be the p-adic valuation and let

$$w : f \mapsto v(f(\alpha)) \qquad (f \in Q[x])$$

be the valuation induced by v and an element α of Q, say with p-adic expansion $\sum a_i p^i$ $(0 \le a_i < p$ for all $i)$. Let n be the number of nonzero terms of $\sum a_i p^i$, and for each $i < n$, let $a_{\sigma(i)} p^{\sigma(i)}$ be the $(i+1)$th such term. Then

$$g(w) = \left\langle x + \sum_{i<m} a_{\sigma(i)} p^{\sigma(i)} \right\rangle_{m<n} \quad \text{and} \quad S(w) = \langle a_{\sigma(i)} + pZ, \sigma(i) \rangle_{i<n}.$$

3. **Signatures and the Fundamental Lemma.** We now generalize the notion of a p-signature introduced in §2. In this generalization we allow "sequences of length $\infty + 1$", i.e. sequences of the form $\langle a_i \rangle_{i \le \infty}$ or, equivalently, $\langle a_i \rangle_{i<\infty+1}$. We are regarding ∞ and $\infty + 1$ as formal symbols with $n < \infty < \infty + 1$ for all integers n. (In §7 we will regard sequences as defined on initial segments of the ordinal numbers. In that context sequences of length $\infty + 1$ appear more naturally as sequences defined on the set of ordinal numbers less than the successor of the first infinite ordinal number.)

Let k be a field and Γ be a linearly ordered abelian group (abbreviated, *ordered group*). A *presignature* over (k, Γ) is a sequence of ordered pairs $S = \langle \theta_i, q_i \rangle_{i<n}$ where $0 \le n \le \infty + 1$ and where the θ_i all lie in some field containing k and the q_i all lie in some ordered group containing Γ. Given such a presignature S, we define nondecreasing sequences of integral domains and ordered semigroups

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n = k_S, \qquad \Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \cdots \subseteq \Gamma_n = \Gamma_S, \tag{8}$$

where, for each $m \le n$, k_m is the ring extension of k generated by $\{\theta_i \mid i < m\}$ and Γ_m is the semigroup extension of Γ generated by $\{q_i \mid i < m\}$. If $S' =$

$\langle \theta_i', q_i' \rangle_{i<n'}$ is a second presignature over (k, Γ), we say it is *equivalent* to S if $n = n'$ and, with the obvious notation,

(i) there is an order isomorphism of Γ_S onto $\Gamma_{S'}$ leaving Γ elementwise fixed and taking each q_i to q_i';

(ii) there is an isomorphism of k_S onto $k_{S'}$ leaving k elementwise fixed and taking each θ_i to θ_i'.

Notice that the isomorphisms of (i) and (ii) above are uniquely determined. An equivalence class of presignatures will usually be denoted by one of its members.

(3.1) **Definition.** A *signature over* (k, Γ) is an equivalence class of presignatures S over (k, Γ) with (notation for S as above)

(i) if $i < n$, then $[k_i : k](\Gamma_i : \Gamma) < \infty$, and the sequence

$$\langle q_i/[k_i : k](\Gamma_i : \Gamma) \rangle_{i<n} \tag{9}$$

is strictly increasing;

(ii) if $i < n$, then θ_i is nonzero if and only if q_i is "commensurable with Γ" (i.e. for some positive integer n, $nq_i \in \Gamma$).

Recall that $[k_i : k]$ denotes the dimension of k_i over k and $(\Gamma_i : \Gamma)$ denotes the index of Γ in Γ_i. The elements of the sequence (9) are regarded as lying in the "divisible closure" of Γ_S, in the following sense.

(3.2) **Lemma (and definition).** *Let Λ be a submonoid of an ordered group. There is a divisible ordered group containing Λ, which we denote by Λ^{div} and call the divisible closure of Λ, such that every element of Λ^{div} is commensurable with Λ, i.e. has an integral multiple which is equal to the difference of two elements of Λ. Λ^{div} is unique up to a (uniquely determined) isomorphism leaving Λ elementwise fixed.*

Proof [21, p. 8]. Actually, we may set $\Lambda^{\mathrm{div}} = \Lambda \otimes_Z Q$.

Let $S = \langle \theta_i, q_i \rangle_{i<n}$ be a signature over (k, Γ). Notice that each θ_i is nonzero and algebraic over k, except possibly the last one (if there is a last one). Similarly, each q_i is commensurable with Γ except possibly a last one. Further, θ_i is zero if and only if the corresponding q_i is not commensurable with Γ. If $n = \infty + 1$, then q_∞ is larger than every element of Γ and hence is not commensurable with Γ. For any m, if $0 < m + 1 < n$, then

$$q_{m+1} > [k_{m+1} : k_m](\Gamma_{m+1} : \Gamma_m) q_m.$$

The reader can now check that the conditions on S listed in this paragraph are sufficient to guarantee that the equivalence class of a presignature satisfying them be a signature. In particular, the p-signatures of §2 may be identified with certain of the signatures over (Z_p, Z).

Incidentally, it is easy to verify that the collection of signatures over (k, Γ) form a set (use the paragraph above). Indeed one can construct a field $k' \supset k$ and an ordered group $\Gamma' \supset \Gamma$ such that every presignature satisfying (i) of (3.1) is equivalent to a presignature with values in $k' \times \Gamma'$.

We introduce a useful variant of Definition (3.1).

(3.3) **Definition.** Let $S = \langle \theta_i, q_i \rangle_{i<n}$ be a presignature over (k, Γ). We call $[k_S : k](\Gamma_S : \Gamma)$ the *degree* of S, denoted "deg S". If deg $S = \infty$, we set aug S $= S$. If deg $S < \infty$, we set aug $S = \langle \theta_i, q_i \rangle_{i \le n}$ where $\theta_n = 0$ and $q_n = \infty$. If S' is a second presignature over (k, Γ), we say aug S is *equivalent* to aug S' if S is equivalent to S'. If the equivalence class of S is a signature, we call the equivalence class of aug S an *augmented signature over* (k, Γ). Finally, we write $k_{\text{aug } S} = k_S$, $\Gamma_{\text{aug } S} = \Gamma_S$, and deg (aug S) = deg S.

As with signatures, augmented signatures will usually be denoted by a representative "augmented presignature". Notice that any augmented signature has the form $\langle \theta_i, q_i \rangle_{i<n}$ where $n \le \infty + 1$ (for if the signature S has length $\infty + 1$, it must have infinite degree—see the paragraph following (3.2)). We may define the sequences of Γ_m and k_m (see (8)) for augmented signatures over (k, Γ) at least when $m < n$. (Thus Γ_n is not defined when $q_{n-1} = \infty$.)

Note that the map $S \mapsto$ aug S gives a bijection from signatures to augmented signatures.

Now let v be a discrete rank one valuation on a field F. We shall define when a signature over (k_v, Γ_v) is "associated" with an extension of v to $F[x]$. This definition will depend on the choice, *which we now make once and for all*, of a system A of representatives in $F^\times$ for Γ_v (so v maps A bijectively onto Γ_v) and a system B of coset representatives in $F^\times$ for $F^\times/(1 + \mathfrak{p}_v)$. *We further assume for convenience that* $1 \in A \cap B$.

In §2 where v was the p-adic valuation on Q, we implicitly took A to be the set of integral powers of p and B to be $\{sp^t \mid s$ and t integers with $0 < s < p\}$.

The important group $F^\times/(1 + \mathfrak{p}_v)$ will be discussed further below.

Recall a concept introduced in §2. Suppose w is an extension of v to $F[x]$. Let $g_0 = x, g_1, \cdots, g_m$ be a finite sequence in $F[x] \setminus F$ with deg g_s dividing deg g_{s+1} for all $s < m$. Each element of $F[x]$ has a unique expansion

$$\sum b_i g_0^{i_0} \cdots g_m^{i_m} \qquad (i = (i_0, \cdots, i_m)) \tag{10}$$

where the coefficients b_i are in F and $0 \le i_s < (\deg g_{s+1})/(\deg g_s)$ $(0 \le s < m)$. Following Mac Lane [15], we say a polynomial is *w-homogeneous in* $\langle g_i \rangle_{i \le m}$ if when expanded as in (10), each coefficient b_i is either zero or in B and each nonzero term of (10) has the same value. (The *value* of an element of a valued ring is its image under the valuation.)

We use the notation for signatures above, setting $(k, \Gamma) = (k_v, \Gamma_v)$.

(3.4) **Definition.** Let w be an extension of v to a valuation on $F[x]$. We say a (possibly augmented) signature $S = \langle \theta_i, q_i \rangle_{i<n}$ is *associated with* w if and only if there is a sequence $\langle g_i \rangle_{i<n}$ of monic polynomials in $F[x]$ (which we call a *generating sequence for* w *and* S) with

(i) if $0 < n$, then $g_0 = x$;

(ii) if $m < n$, $\deg g_m = [k_m : k_v](\Gamma_m : \Gamma_v)$;

(iii) if $0 < m + 1 < n$, then g_{m+1} is w-homogeneous in $\langle g_i \rangle_{i \leq m}$;

(iv) if $m < n$, then $q_m = w(g_m)$;

(v) if $m < n$ and q_m is finite and commensurable with Γ_v, then we can write

$$\theta_m = \left(a \prod_{i \leq m} g_i^{r_i} \right) g_m + \wp_w$$

where $a \in A$ and $0 \leq r_i < (\Gamma_{i+1} : \Gamma_i)$ for $i \leq m$.

Also, we say a sequence of monic polynomials $\langle g_i \rangle_{i<n}$ in $F[x]$ is a *generating sequence for* w if and only if there exists a (possibly augmented) signature S such that $\langle g_i \rangle_{i<n}$ is a generating sequence for w and S.

The above definition says that if S is associated with w, then a representative presignature for S can be found with the q_i in Γ_w and the θ_i in k_w.

Notice that for each $m < n$ with q_m finite and commensurable with Γ_v, the corresponding choice of a and r_i $(i \leq m)$ in (v) of (3.4) above is uniquely determined by $v(a) + \Sigma r_i q_i = -q_m$ (this must be true since $\theta_m \neq 0$). Further, if q_m is not finite and commensurable with Γ_v, then $\theta_m = 0$ (cf. (3.1)). Hence (iv) and (v) of (3.4) guarantee that w and $\langle g_i \rangle_{i<n}$ completely determine S. Something much stronger is true. The next lemma says that S determines $\langle g_i \rangle_{i<n}$ *independently of* w, and that for each $m < n$, the fact that $\langle \theta_i, q_i \rangle_{i<m}$ is associated with w can be deduced from the fact that w assigns to g_m a sufficiently large value.

(3.5) **Fundamental Lemma.** *Suppose F is complete. Let $S = \langle \theta_i, q_i \rangle_{i<n}$ be any signature over (k_v, Γ_v) of finite degree (cf. (3.1) and (3.3)). Then there exists a unique monic nonconstant polynomial $f \in F[x]$ such that, for any extension w of v to $F[x]$, the following are equivalent (with the usual notation):*

(i) *S is associated with w;*

(ii) *w has a unique generating sequence of length $n + 1$ and f is its nth term;*

(iii) *$w(f) > [k_S : k_i](\Gamma_S : \Gamma_i) q_i$ for all $i < n$.*

We call f the *generator* of S.

(3.6) **Examples.** (A) x is the generator of the sequence of length zero.

(B) Suppose $f = \Sigma b_i x^i$ is a monic nonconstant polynomial all of whose nonzero coefficients are in $\{b \in B \mid v(b) = 0\}$. If $\Sigma (b_i + \wp_v) x^i$ is an irreducible

polynomial over k_v with a nonzero root α in some extension of k_v, then f is the generator of the signature of length one whose only term is $(\alpha, 0)$.

(C) Suppose $v(b)$ is the least positive element of Γ_v, $b \in B$, and $b^{-1} \in A$. Then for any positive integer n, $x^n + b$ is the generator of the signature of length one whose only term is $(-1, v(b)/n)$.

The proof of (3.5) is a complicated but basically straightforward counting argument. In order to proceed directly to the main results of this paper, we refer the reader to §8 for its proof.

A final remark. All of the above definitions make sense when v is the trivial valuation on F. Since F is linearly compact for the trivial valuation, all of our results hold in this case as well as the discrete rank one case (cf. §7). These results are in every case familiar, e.g. Lemma (3.5) above becomes the usual bijection between the monic nonconstant irreducible polynomials over F and the F-conjugacy classes of elements in the algebraic closure of F. (For another example, compare Corollary (4.3) below with [8, p. 46].)

4. **Valuations on the polynomial ring and rational function field of a complete field.** *Throughout this section F will denote a field complete at a discrete rank one valuation v.* A and B again denote systems of representatives for Γ_v and $F^\times/(1 + \mathfrak{p}_v)$, respectively, with $1 \in A \cap B$. Associated signatures and generating sequences are implicitly assumed to be defined with respect to the choice of A and B.

(4.1) **Main Theorem.** *Each extension of v to $F[x]$ has associated with it a unique augmented signature over (k_v, Γ_v). This association induces a bijection from the set of equivalence classes of extensions of v to $F[x]$ onto the set of augmented signatures over (k_v, Γ_v).*

Recall that two valuations on a ring are equivalent if they differ by an isomorphism of their value monoids (cf. §1).

This section is devoted to the proof of (4.1) and its "supplement" (4.2), which describes how to recover a valuation from its augmented signature. As a corollary, we also compute in terms of signatures the set of extensions of v to the field of rational functions $F(x)$.

(4.2) **Supplement to the Main Theorem.** *Let $S = \langle \theta_i, q_i \rangle_{i<n}$ be an augmented signature over (k_v, Γ_v). For each $m < n$, let g_m denote the generator of the signature $\langle \theta_i, q_i \rangle_{i<m}$ (cf. (3.5)).*

(A) *Let D_S denote the set of all products*

$$\prod_{i<n} g_i^{r_i} \tag{11}$$

where only a finite number of the r_i *are nonzero and*

$$0 \leq r_i < [k_{i+1} : k_i](\Gamma_{i+1} : \Gamma_i) \qquad (0 < i + 1 < n). \tag{12}$$

Then D_S *is a basis for* $F[x]$ *as an* F*-module. Indeed, for any nonnegative number* n *there are unique* r_i *as in* (12) *such that the product* (11) *has degree exactly* n *(since the right-hand side of* (12) *equals* $(\deg g_{i+1})/(\deg g_i)$*).*

(B) *For any product* (11) *above, let us set*

$$v_S\left(\prod_{i<n} g_i^{r_i}\right) = \sum_{i<n} r_i q_i.$$

(v_S *is well defined by the last sentence of* (A) *above.) Then the map*

$$w\colon \sum a_f f \mapsto \min\{v(a_f) + v_S(f) \mid f \in D_S\} \tag{13}$$

(the coefficients $a_f \in F$ *indexed over* $f \in D_S$*) is the unique valuation on* $F[x]$ *with* S *an associated augmented signature.*

(C) *Moreover,* $k_w = k_S$ *and* $\Gamma_w = \Gamma_S$. $w^{-1}(\infty) = (0)$ *if* S *has infinite degree, and* $w^{-1}(\infty) = (f)$ *if* S *has finite degree and* f *is the generator of the unique signature* S_0 *with* $\operatorname{aug} S_0 = S$.

(4.3) **Corollary.** *Assign to each extension of* v *to* $F(x)$ *the augmented signature associated with its restriction to* $F[x]$. *This induces a bijection from the set of equivalence classes of extensions of* v *to* $F(x)$ *to the set of all signatures over* (k_v, Γ_v) *with infinite degree.*

Recall that a signature is an augmented signature if and only if it has infinite degree.

Proof of (4.3). Each extension of v to $F(x)$ is uniquely determined by its restriction to $F[x]$ (after all, $w(a/b) = w(a) - w(b)$ for any field valuation w). A valuation on $F[x]$ extends to a valuation on $F(x)$ if and only if it has trivial infinity ideal. The corollary now follows from Theorem (4.1) and (C) of (4.2).

Suppose w and S correspond in the bijection of (4.3) above. Supplement (4.2) gives a picture of w on $F[x]$, and hence on $F(x)$. In particular, it is easy to show that k_w is the field of fractions of k_S and Γ_w is the group generated by Γ_S (use (4.2B) to apply (4.2C)).

The remainder of this section is devoted to proving (4.1) and (4.2).

Let w be an extension of v to $F[x]$. There is associated with w a (possibly augmented) signature of maximal length. Hence there is associated with w a unique generating sequence of maximal length (apply "(i) implies (ii)" of (3.5), together with the definitions). Hence w admits a unique (possibly augmented) signature of maximal length (reason as in the paragraph preceding (3.5)). This possibly augmented signature must in fact be augmented, for otherwise we apply (3.5) to obtain a generating sequence of greater length. This proves the first

sentence of (4.1). Since equivalent extensions of v to $F[x]$ clearly have the same generating sequences and associated (augmented) signatures, the second sentence of (4.1) follows from (4.2), which we now prove.

In the next two lemmas we suppose $S = \langle \theta_i, q_i \rangle_{i<n}$, with corresponding generating sequence $\langle g_i \rangle_{i<n}$, is a signature over (k_v, Γ_v) associated with an extension w of v to $F[x]$. For each $m \leq n$, let A_m denote the multiplicative submonoid of $F[x]$ generated by F and $\{g_i | \ i < m\}$. Note that w maps A_m onto $\Gamma_m \cup \{\infty\}$.

Lemma A. *Suppose $m \leq n$ and $w(t) \geq 0$ for some $t \in A_m$. Then $t + \mathfrak{p}_w \in k_m$.*

Proof. By induction it suffices to suppose the lemma holds for some $m < n$, and prove it for $m + 1$. So suppose we have $w(tg_m^s) = 0$ for some integer $s \geq 0$ and $t \in A_m$. Clearly, there is an integer s' with $s = (\Gamma_{m+1} : \Gamma_m)s'$. There exist a and b in A_m with

$$w(a^{s'}b) = 0 \quad \text{and} \quad \theta_m = ag_m^{(\Gamma_{m+1} : \Gamma_m)} + \mathfrak{p}_w.$$

Rearranging terms and using that k_m is a field, we have

$$tg_m^s + \mathfrak{p}_w = (a^{s'}b + \mathfrak{p}_w)^{-1}(tb + \mathfrak{p}_w)\theta_m^{s'}$$

which is clearly in k_{m+1}. Done.

Let D_S denote the set of products $\Pi_{i<n} g_i^{r_i}$ where only finitely many of the r_i are nonzero and

$$0 \leq r_i < [k_{i+1} : k_i](\Gamma_{i+1} : \Gamma_i) \qquad (0 \leq i < n).$$

This notation is consistent with our earlier use of D_S (cf. (4.2A)).

Lemma B. *Let $b_f \in F$ $(f \in D_S)$. Then*

$$w\left(\sum b_f f\right) = \min_f w(b_f f).$$

Proof. By induction we may suppose the lemma is true for all signatures of length m, where $m + 1 = n$. Set

$$\gamma = \min\{w(b_f f) | \ f \in D_S\}.$$

We may assume (throwing away all terms $b_f f$ with value greater that γ and then dividing out the highest power of g_m occurring in the remaining terms) that $\gamma \in \Gamma_m$ and $w(b_f f) = \gamma$ for all $f \in D_S$ with $b_f \neq 0$. In particular, we may assume that q_m is commensurable with Γ_v, so $(\Gamma_{m+1} : \Gamma_m) < \infty$ and $\theta_m \neq 0$. Pick a and b in A_m with

$$\gamma = -w(ba^{[k_{m+1} : k_m]}) \quad \text{and} \quad \theta_m = ag_m^{(\Gamma_{m+1} : \Gamma_m)} + \mathfrak{p}_w.$$

Let $S^* = \langle \theta_i, q_i \rangle_{i<m}$. Each $f \in D_S$ can be uniquely written in the form $f^* g_m^{if}$ where $f^* \in D_{S^*}$. Now θ_m is a zero of no polynomial of degree less than $[k_{m+1} : k_m]$ over k_m. Hence

$$0 \neq \sum \Big(\sum b a^{[k_{m+1} : k_m] - i} b_f f^* + \mathfrak{p}_w \Big) \theta_m^i$$

(the outer sum is over i with $0 \leq i < [k_{m+1} : k_m]$, and for each such i, the inner sum is over $f \in D_S$ with $i_f = (\Gamma_{m+1} : \Gamma_m) i$. Use Lemma A and the induction hypothesis to show the coefficients of θ_m^i are in k_m and are not all zero). Hence $ba^{[k_{m+1} : k_m]} \sum b_f f + \mathfrak{p}_w \neq 0$ so $w(\sum b_f f) = -w(ba^{[k_{m+1} : k_m]}) = \gamma$. The lemma is proved.

Now suppose S and $\langle g_i \rangle_{i<n}$ are as in Supplement (4.2). We claim that it suffices to show that S is associated with some extension of v to $F[x]$. First, (4.2A) follows immediately from (ii) of Definition (3.4) (prove the second sentence first). Notice that Lemma B holds for augmented signatures S, using the D_S of (4.2) (this is a corollary of Lemma B as it is stated). Then any extension of v to $F[x]$ must be given by the formula of (4.2B). Finally, (4.2C) follows from (4.2B) and Lemma A.

First suppose $n \neq \infty$, so $n = m + 1$ for some $m \geq 0$. One checks (or see Bourbaki [2, p. 160]) that the map

$$w_0 : \sum a_i g_m^i \mapsto \min_i (v(a_i) + i q_m) \qquad (a_i \in F)$$

defines a valuation on $F[g_m]$. w_0 extends to a valuation w on $F[x]$ (apply [19, Proposition 7] to the extension $F[x]/F[g_m]$ if $q_m = \infty$ and to the extension $F(x)/F(g_m)$ if $q_m \neq \infty$). By the Fundamental Lemma (3.5) ((iii) implies (i)), $\langle \theta_i, q_i \rangle_{i<m}$ is associated with w. If q_m is not finite and commensurable with Γ_v, we are done. (For then, by (3.4), S is associated with w.) Now suppose q_m is commensurable with Γ_v; then since S is augmented, θ_m must be transcendental over k_m. Therefore it suffices to show that for any $a \in A_m$ (A_m defined as above) and $t > 0$ with $w(a g_m^t) = 0$, we have $a g_m^t + \mathfrak{p}_w$ transcendental over k_m. Using Lemma A we see this is the same as showing that $a g_m^t + \mathfrak{p}_w$ is transcendental over k_v for $a \in F$ and $t > 0$ with $w(a g_m^t) = 0$. If this is not true, then for some $b_i \in A_v$ (and $v(b_i) = 0$ for at least one i) we have

$$\sum (b_i + \mathfrak{p}_w)(a g_m^t + \mathfrak{p}_w)^i = 0,$$

i.e. $w(\sum a^i b_i g_m^{ti}) > 0$, which contradicts that w is an extension of w_0.

It remains to consider the case $n = \infty$. For each $m < \infty$ let w_m denote the unique extension associated with aug $\langle \theta_i, q_i \rangle_{i<m}$ (existence of w_m is proved in the preceding paragraph). For any $f \in F[x]$, the sequence $\langle w_i(f) \rangle_{i<\infty}$ becomes constant as soon as deg $g_m >$ deg f (notice that deg $S = \infty$, so deg $g_m \to \infty$). The map

$$f \mapsto \lim_{i \to \infty} w_i(f) \qquad (f \in F[x]) \tag{14}$$

gives a well-defined extension of v to $F[x]$, and S is associated with it (use the Fundamental Lemma).

The main theorem and its supplement are now proved. Notice that we have shown that, with notation as in (4.2), $\{\langle\theta_i, q_i\rangle_{i<m} \mid m \leq n\}$ is the set of all (possibly augmented) signatures associated with w. Also notice that we nowhere used in the proof of Lemmas A or B that F was complete.

5. **Irreducible polynomials and simple algebraic extensions.** *Throughout this section F denotes a field complete at a discrete rank one valuation v.* Associated signatures and generating sequences are again defined with respect to fixed systems A and B of representatives for Γ_v and $F^\times/(1+\mathfrak{p}_v)$. As earlier, we assume $1 \in A \cap B$.

The following theorem will be applied to study the irreducible polynomials and algebraic extensions of F.

(5.1) **Theorem.** *Assigning to each signature over (k_v, Γ_v) of finite degree its generator (cf. (3.5)) gives a bijection from the set of such signatures to the set of nonconstant monic irreducible polynomials in $F[x]$.*

Proof. Let f be the generator of a signature S. Let w be the unique extension of v to $F[x]$ with aug S associated with w (cf. (4.1)). By (3.5) and (4.2C), f generates the prime ideal $w^{-1}(\infty)$. Hence f is irreducible.

Conversely, suppose f is a nonconstant monic irreducible polynomial. There exists an extension w of v to $F[x]$ with $w(f) = \infty$ (since there exists an extension of v to $F[x]/(f)$). Then f must be in the generating sequence of w (apply (4.2C), recalling that $w^{-1}(\infty)$ can contain at most one monic irreducible polynomial). The theorem is proved.

For the remainder of this section, f will denote a nonconstant monic irreducible polynomial in $F[x]$, say with corresponding signature $S = \langle\theta_i, q_i\rangle_{i\leq n}$. As in the proof of (5.1), we let w denote the unique extension of v to $F[x]$ with $w(f) = \infty$ (or equivalently, with aug S associated with w). Notice that if θ is a zero of f in some extension of F, then there is a unique extension u of v to $F[\theta]$ ($\cong F[x]/(f)$). u and w are related by

$$u(h(\theta)) = w(h) \qquad (h \in F[x]) \tag{15}$$

and have naturally isomorphic residue class fields and value groups. It is well known that u (and hence w) can also be computed in terms of the norm map from $F[\theta]$ to F (cf. [21, p. 53]).

(5.2) **Corollary.** *Let E be an algebraic extension of F. Then v has a unique extension to E.*

Proof. For each $\alpha \in E$, apply the above remarks to the irreducible polynomial of α over F.

(5.3) **Corollary.** *Let E be a finite dimensional extension of F. Then E is complete with respect to the unique extension of v to E.*

Proof. Without loss of generality, we may suppose $E = F[x]/(f)$ (since any extension may be obtained by a sequence of simple extensions). Let $\langle g_i \rangle_{i<n}$ be the generating sequence of w and define D_S as in Lemma B, §4. Then $\{\overline{h} + (f) | h \in D_S\}$ is a basis for E/F (indeed, an "orthobasis" in the sense of MacKenzie-Whaples [14]). Any Cauchy sequence in E, $\langle \Sigma\, b_{i,h}\, h + (f) \rangle_{i<\infty}$ (for each i, the $b_{i,h} \in F$ are indexed over $h \in D_S$), converges to $\Sigma\, b_h\, h + (f)$, where, for each $h \in D_S$, b_h is the limit of the (Cauchy!) sequence $\langle b_{h,i} \rangle_{i<\infty}$.

The above two corollaries are of course well known, as is the next, at least for algebraic extensions.

(5.4) **Corollary.** *Let E be any field extension of F, and let z be an extension of v to E. Then*

$$[E : F] = [k_z : k_v](\Gamma_z : \Gamma_v). \tag{16}$$

Proof. If E/F is transcendental, we show that the right-hand side of (16) is infinite by the method of Corollary (4.3). If E/F is algebraic, we again may assume $E = F[x]/(f)$, whence (16) follows from the equality of deg S and deg f.

Notice that (16) holding for all extensions E/F is necessary *and sufficient* for F to be complete (use [12, Theorem 4]).

We now illustrate how to use (5.1) to study the irreducible polynomials over F. Since these results are peripheral to our main argument, we will only sketch proofs and refer the reader to [3] for a full discussion. Proofs tend to be long but straightforward computations with generating sequences.

(5.5) **Lemma and Definition.** *There exists a least element of $\Gamma_v^{\text{div}} \cup \{-\infty\}$, call it γ_f, such that, for every extension z of v to $F[x]$, if $z(f) > \gamma_f$ then z and w agree on all polynomials of degree less than* deg f.

The above lemma makes sense if we identify Γ_w and Γ_v^{div} with their canonical images in Γ_z^{div} (cf. (3.2)). Equivalently, given $\alpha \in \Gamma_z$ and $\beta \in \Gamma_w \cup \Gamma_v^{\text{div}}$ (so $m\beta \in \Gamma_v$ for a positive integer m), we set $\alpha \geq \beta$ if $m\alpha \geq m\beta$.

The proof of (5.5) gives a computation of γ_f. First note that $\gamma_f = -\infty$ if and only if f is linear (we employ the obvious conventions with $-\infty$). Suppose f is not linear; then there exists a largest m less than n with deg $S > [k_m : k_v]$ $(\Gamma_m : \Gamma_v)$. Let us define

$$\gamma_f = [k_{m+1} : k_m](\Gamma_{m+1} : \Gamma_m)\, q_m.$$

Then one can show that γ_f satisfies the conditions of the proposition. (The

method of proof of (3.5) shows that $z(f) > \gamma_f$ implies $\langle \theta_i, q_i \rangle_{i<m}$ is associated with z. Now use Lemma B of §4.)

We will use w and γ_f to describe certain "extensions" of f to an irreducible polynomial over F. The simplest case is treated in the next proposition, which also gives an alternate definition of γ_f. The lemma quantifies the well-known result that a polynomial sufficiently close to f (in the sense that respective coefficients are sufficiently close in the valuation topology on F) is irreducible.

(5.6) **Proposition.** *γ_f is the least element of $\Gamma_v^{\text{div}} \cup \{-\infty\}$ such that any monic polynomial g in $F[x]$ is irreducible if it has the same degree as f and $w(f-g) > \gamma_f$.*

Note $w(f-g) = w(g)$. (5.6) is a special case of (5.10) below.

One of the many equivalent forms of Hensel's lemma says that the canonical image in $k_v[x]$ of a monic irreducible polynomial whose coefficients are in A_v is an integral power of an irreducible polynomial in $k_v[x]$. The following proposition generalizes this fact.

(5.7) **Proposition.** *Suppose $f = \Sigma a_i x^i$. Then*

(A) $v(a_i)/(n-i) \geq v(a_0)/n \neq \infty$ $(i < n)$.

(B) *If e is the smallest positive integer with $e(v(a_0)/n) \in \Gamma_v$, say with $v(s) = (e/n)v(a_0)$ for $s \in F$, then*

$$y^{n/e} + \sum_{i<n/e} (s^{n/e-i} a_{ie} + \wp_v) y^i \tag{17}$$

is an integral power of an irreducible polynomial over k_v.

Notice that (A) ensures that formula (17) makes sense. Condition (A) is well known; it says that the Newton polygon of f is a straight line segment [16, p. 500], [21, p. 54].

To prove (5.7), write $f = g_1^m + h$ where $\deg f = m \deg g_1$. Then the coefficients of h have sufficiently large value that the above conditions on the coefficients of f can be proven by establishing the analogous conditions on the coefficients of g_1^m (induct on m).

The above proposition offers formal motivation for the next definition.

(5.8) **Definition.** A polynomial $g \in F[x]$ is an *extension* of f if and only if its expansion in powers of f has the form

$$f^n + \sum_{i<n} r_i f^i \qquad (\deg r_i < \deg f)$$

where

(i) $w(r_i)/(n-i) \geq w(r_0)/n > \gamma_f$ $(0 \leq i < n)$;

(ii) if e is the smallest positive integer with $e(w(r_0)/n) \in \Gamma_w$, say with

$w(s) = -(e/n)w(r_0)$ for $s \in F[x]$, then

$$y^{n/e} + \sum_{i<n/e} (s^{n/e-i} r_{ie} + \mathfrak{p}_w) y^i$$

is irreducible over k_w.

Again, (i) above guarantees that (ii) makes sense. Notice that this definition could easily have been phrased in terms of the valuation u: $F[\theta] \to \Gamma_w \cup \{\infty\}$ of (15).

(5.9) **Examples.** (A) Let $g = \Sigma a_i x^i$ be a monic polynomial with coefficients a_i in the valuation ring of v. If the image of g in $k_v[x]$ is irreducible, then g is an extension of x.

(B) *Eisenstein polynomials* are extensions of x, i.e., if $g = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ $(a_i \in F)$ has each $a_i \in \mathfrak{p}_v$ and has $v(a_0)$ the smallest positive element of Γ_v, then g is an extension of x. More generally, g is an extension of x if $v(a_i)/(n-i) > v(a_0)/n$ for $0 < i < n$, and the least positive integer s with $s(v(a_0)/n) \in \Gamma_v$ is $s = n$.

(C) Suppose g satisfies all the hypotheses of Proposition (5.6). Then g is an extension of f. In particular any polynomial of the form $x + a$ is an extension of any other such polynomial.

(D) If $\langle g_i \rangle_{i \le n}$ is the generating sequence of w, then g_{i+1} is an extension of g_i for all $i < n$.

(5.10) **Theorem.** *Let $g \in F[x]$. Then g is a monic nonconstant irreducible polynomial if and only if there exists a finite sequence of polynomials in $F[x]$*

(18) $$g_0, g_1, \cdots, g_m = g$$

such that $\deg g_0$ *equals* 1, *and for each* $i < m$, g_{i+1} *is an extension of* g_i.

Proof (sketch). It suffices to show that f admits such a sequence (18), and that any extension of f is irreducible. Let $\langle g_i \rangle_{i \le n}$ be the generating sequence of w. If $n < \infty$, we are done (cf. (5.9D)). Otherwise take the sequence (18) to be $g_0, g_1, \cdots, g_s, f$ where $s < n$ has $\deg g_s = \deg f$. Now let g be an extension of f. Let s be as large as possible with $\deg g_s < \deg g$. One can then extend $\langle \theta_i, q_i \rangle_{i<s}$ to a signature of which g is the generator (use Lemma G of §8).

(5.10) can also be proven by using (5.5) to apply [17, Theorem 1].

Note. We may require the polynomials in (18) to have strictly increasing degree. Suppose this is done. Then the sequence (18) is still not unique. However, the value groups and residue class fields of the extensions of v to $F[x]/(g_i)$ are invariants of g. For more in this direction, see [3, p. 32].

The sequence (18) can be used to compute inductively γ_g and the unique extension z of v to $F[x]$ with $z(g) = \infty$. Suppose g is an extension of f. Then

$\gamma_g = \gamma_f$ if $\deg g = \deg f$, and $\gamma_g = w(g)$ otherwise. Further, for any $h \in F[x]$,

$$z(h) = \min_i w(t_i) + (i \deg f/\deg g)\, w(g)$$

where

$$\sum t_i f^i \qquad (\deg t_i < \deg f)$$

is the remainder upon dividing h by g.

Let us now suppose that h is a separable monic nonconstant irreducible polynomial over F, say associated with the signature S'. It is well known that if h and f are sufficiently close (i.e. their respective coefficients are sufficiently close in the valuation topology of F), then $F[x]/(h)$ and $F[x]/(f)$ are isomorphic over F [20, Chapter F]. We can give a quantitative statement of this result for finite dimensional tamely ramified (abbreviated, *tame*) extensions of F. Notice that $F[x]/(f)$ is a tame extension of F if and only if k_S/k_v is separable and the characteristic of k_v does not divide $(\Gamma_S : \Gamma_v)$.

Recall $S = \langle \theta_i, q_i \rangle_{i<n}$. Let red S denote the signature obtained from S by deleting all terms (θ_i, q_i) with $\theta_i \in k_i$ and $q_i \in \Gamma_i$. Formally,

$$\text{red } S = \langle \theta_{\sigma(i)}, q_{\sigma(i)} \rangle_{i<\sigma(n)}$$

where $\sigma(n)$ is the number of terms (θ_i, q_i) with $\theta_i \notin k_i$ or $q_i \notin \Gamma_i$, and, for each $i < \sigma(n)$, $(\theta_{\sigma(i)}, q_{\sigma(i)})$ is the $(i+1)$th such term.

(5.11) **Proposition.** *Suppose $F[x]/(f)$ is tamely ramified over F. Then $F[x]/(f)$ is isomorphic to $F[x]/(h)$ over F if* red S = red S'.

Proof. Use Lemma E of §8 to apply the proposition and first theorem of [6].

The possibility of generalizing (5.11) is suggested by the following corollaries to Krasner's lemma [20, p. 190]. The first is the well-known "p-power theorem".

(5.12) **Remark.** Let p be a prime number. Let $a, a' \in F$.

(A) Suppose char $F \neq p$. Then $x^p - a$ and $x^p - a'$ give isomorphic extensions of F (by adjoining a root to F) if for some $b \in F$

$$v((ab^p/a') - 1) > pv(p)/(p-1). \tag{19}$$

(B) Suppose char $F = p$. Then $x^p - x - a$ and $x^p - x - a'$ give isomorphic extensions of F if $v(a - a') > 0$.

These results can also be proved directly but tediously from (5.10). (One uses (5.10) to show that (19) implies $x^p - a'$ is not irreducible in $F[a^{1/p}]$, cf. [3, pp. 46–48]. (B) is similar, but easier.)

The task of giving necessary and sufficient conditions for the isomorphism of $F[x]/(f)$ and $F[x]/(h)$ in terms of S and S' seems prohibitively difficult (with (5.1), this would characterize all simple algebraic extensions of F in terms

of signatures!). It is possible to give such conditions for a family of signatures whose associated generators yield all tame extensions of F. The resulting computation of tame extensions of F shows the set of F-isomorphism classes of tame extensions of F with specified residue class field k and value group Γ is bijective with the set of equivalence classes of elements in $k^\times \otimes \Gamma/\Gamma_v$ (tensor product as abelian groups), where two elements of $k^\times \otimes \Gamma/\Gamma_v$ are equivalent if one is carried into the other by an automorphism of $k^\times \otimes \Gamma/\Gamma_v$ induced by an automorphism of k leaving k_v fixed. (See [4].)

(5.13) **Remark.** In this final remark we drop the hypothesis that F is complete. All of our results about irreducible polynomials (namely (5.6) through (5.10)) remain valid if we replace everywhere the word "irreducible" by "irreducible over the completion of F" or even "irreducible over the Henselization of F". In particular, these results hold without modification when F is Henselian.

We mention a possible application. In 1898, Stieltjes conjectured that the Legendre polynomials were irreducible over Q except for obvious factors. Theorem (5.10) seems a natural tool for continuing the study of the conjecture. Indeed much of the work on the conjecture has consisted of proving that particular Legendre polynomials were irreducible over appropriate completions of Q. (See McCoart [13] for a summary of results.)

6. Valuations and primes on polynomial rings and rational function fields.

Throughout this section F will denote a field all of whose nontrivial valuations are discrete rank one, e.g. an algebraic number field, or more generally, a global field. We will assume that for each nontrivial valuation v of F we have fixed as usual a system of representatives for Γ_v and a system of representatives for $F^\times/(1 + \mathfrak{p}_v)$; associated signatures are assumed to be defined with respect to these choices.

Most of the results of this section can be generalized by rephrasing them in terms of extending a given discrete rank one valuation on an arbitrary field K to $K[x]$ or $K(x)$.

For a valuation v on a commutative ring R, let $\mathfrak{E}(v)$ denote the set of equivalence classes of extensions of v to a valuation on $R[x]$. $\mathfrak{E}(v)$ was computed in §4 for the case R a complete field. The next lemma will enable us to apply §4 to the noncomplete case.

(6.1) **Lemma.** *Let $\tilde{F}$, with valuation $\tilde{v}$, be the completion of F at a nontrivial valuation v. Restricting valuations from $\tilde{F}[x]$ to $F[x]$ induces a well-defined map*

$$\text{Res: } \mathfrak{E}(\tilde{v}) \to \mathfrak{E}(v).$$

Res *is surjective and preserves residue class rings. Also,* Res *maps the set of prime valuations in* $\mathfrak{E}(\tilde{v})$ *bijectively onto the set of prime valuations in* $\mathfrak{E}(v)$, *and the set of valuations in* $\mathfrak{E}(\tilde{v})$ *with trivial infinity ideal bijectively onto the set of valuations in* $\mathfrak{E}(v)$ *with trivial infinity ideal.*

One can also show that Res maps the "valuations in the sense of Manis" [19] in $\mathfrak{E}(\tilde{v})$ onto the corresponding subset of $\mathfrak{E}(v)$.

Before proving Lemma (6.1) at the end of this section, we make a number of easy applications. These are based on the next definition.

(6.2) **Definition.** Let w be a valuation on $F[x]$ which restricts to a nontrival valuation, call it v, on F. By *the signature associated with* w we mean the signature S over (k_v, Γ_v) of largest possible length n such that $n \leq \infty$ and S is associated (cf. (3.3)) with w.

While there may be many signatures associated with w in the sense of Definition (3.3), *the* signature associated with w is unique. For let $\tilde{w} \in \mathfrak{E}(\tilde{v})$ have Res $(\tilde{w}) = w$ (notation as in (6.1) above). Notice that our systems of representatives for Γ_v and $F^\times/(1 + \mathfrak{p}_v)$ may also be regarded as systems of representatives for $\Gamma_{\tilde{v}}$ and $\tilde{F}^\times/(1 + \mathfrak{p}_{\tilde{v}})$. Let $\langle \theta_i, q_i \rangle_{i<m}$ be the augmented signature associated with $\tilde{w}$, defined with respect to these systems of representatives. Let us set

$$\begin{aligned} t &= \infty && \text{if } m \geq \infty, \\ &= m-1 && \text{if } q_{m-1} = \infty,\ m < \infty, \\ &= m && \text{if } q_{m-1} \neq \infty,\ m < \infty. \end{aligned}$$

Then by inspection of Definition (3.3), $\langle \theta_i, q_i \rangle_{i<t}$ is seen to be *the* signature associated with w.

(6.3) **Corollary.** *Let* v *be a nontrivial valuation on* F. *Assigning to each extension of* v *to* $F(x)$ *the signature associated with its restriction to* $F[x]$ *induces a bijection between the set of equivalence classes of extensions of* v *to* $F(x)$ *and the set of signatures over* (k_v, Γ_v) *either of length* ∞, *or of finite length and infinite degree.*

Proof. Use Lemma (6.1) to apply (4.3). Notice that every signature of infinite length and finite degree extends uniquely to a signature of infinite degree.

For any finite prime P of a commutative ring R, let us denote by v_P, Γ_P and k_P the unique (up to equivalence) valuation associated with P, its value monoid, and its residue class field, respectively (cf. Harrison [10, p. 18]; v_P is determined up to equivalence by the conditions that Γ_P be a group and $P = \mathfrak{p}_{v_P}$).

(6.4) **Corollary (the primes of** $F[x]$). *Assign to each finite prime* P *of* $F[x]$

the signature associated with v_P (*cf.* (6.2)). *This gives a bijection between the finite primes of* $F[x]$ *and the set of pairs* (S, T) *where* T *is a finite prime of* F *and* S *is a signature over* (k_T, Γ_T) *with* Γ_S *a group and* k_S *a field.*

(The above conditions on S are equivalent to every element of Γ_S being commensurable with Γ_T, and every element of k_S being algebraic over k_T.)

Proof. The valuations w on $F[x]$ associated with finite primes are those with Γ_w a group and k_w a locally finite field. Use (6.1) to apply (4.1) and (4.2) to the family of such valuations.

We remark that if (S, T) and P correspond as in (6.4), then $P \cap F = T$, and we have natural isomorphisms $k_S \cong k_P$ and $\Gamma_S \cong \Gamma_P$. The theorem of §2 follows from the above Corollary (also use (4.2) to show that the p-signature associated with a prime valuation w in §2 is the signature associated with w in the sense of (6.2)).

An argument similar to that establishing (6.4) gives

(6.5) **Corollary (the primes of** $F(x)$**).** *Assign to each finite prime* P *of* $F(x)$ *the signature associated with the restriction of* v_P *to* $F[x]$. *This gives a bijection from the finite primes of* $F(x)$ *onto the set of pairs* (S, T) *where* T *is a finite prime of* F *and* S *is a signature over* (k_T, Γ_T) *such that* k_S *is a field and* S *has either length* ∞, *or finite length and infinite degree.*

Combining (6.4) and (6.5) we obtain a result which is well known for finite fields F ([8], [10]).

(6.6) **Corollary.** *Every finite prime of* $F[x]$ *is contained in one, and only one, prime of* $F(x)$.

One can show that if P is a finite prime of $F(x)$, then $P \cap F[x]$ is a prime of $F[x]$ if and only if the rank and rational rank [2, pp. 114 and 163] of Γ_P are the same.

(6.7) **Remark.** Let us suppose in this remark that F is a global field and that R is a ring whose field of fractions is F. We use (6.4) to study the finite primes of $R[x]$.

First, the primes of $R[x]$ which are ideals (i.e. "ideal primes") all have the form $\mathfrak{p} \cdot R[x] + f \cdot R[x]$ where $\mathfrak{p}$ is an ideal prime of R and $f \in R[x]$ is irreducible and nonconstant modulo $\mathfrak{p}$. Hence the ideal primes of $R[x]$ correspond bijectively to the signatures over $(R/\mathfrak{p}, \{0\})$ of finite degree, where $\{0\}$ denotes the trivial ordered group and $\mathfrak{p}$ ranges over the ideal primes of R.

Now let P be a finite prime of $R[x]$ which is not an ideal. Then there is a unique prime T of $F[x]$ containing P, and v_T is the unique extension of v_P to a valuation on $F[x]$ (use here that Γ_T has rational rank one). Hence we have a

bijection between the finite nonideal primes of $R[x]$ and the signatures of primes T of $F[x]$ such that v_T restricts to a prime valuation of $R[x]$.

Things now become simpler if we assume that F is an algebraic number field (otherwise $F[x]$ can admit finite primes with trivial intersection with $R[x]$!). Then every finite prime of $F[x]$ intersects down to a prime of $R[x]$ (use the fact that every prime of $F[x]$ contains a nonzero prime number). Hence the nonideal finite primes of $R[x]$ correspond bijectively with signatures S over (k_P, Γ_P) where P ranges over the finite primes of F, Γ_S is a group, k_S is a field, and either R is not contained in the valuation ring of v_P, or else $q_0 < 0$ (here, (θ_0, q_0) denotes the "first term" of S).

A concrete example. The primes of $Z[x]$ which are ideals correspond to signatures over $(Z_p, \{0\})$ of finite degree, p ranging over all prime numbers. The finite primes of $Z[x]$ which are not ideals correspond to signatures $\langle \theta_i, q_i \rangle_{i<n}$ over (Z_p, Z) where p is any prime number, $n \leq \infty$, each q_i is commensurable with Z, each θ_i is algebraic over Z_p, and $q_0 < 0$ if $0 < n$.

(6.8) **Remark.** Let P be a finite prime of $F[x]$, say with associated signature S. Let $\tilde{F}$ with valuation $\tilde{v}$ be the completion of F at the restriction of v_P to F; by (6.1) there is a unique prime $\tilde{P}$ of $\tilde{F}[x]$ with $\tilde{P} \supseteq P \cup \mathfrak{p}_{\tilde{v}}$. P and $\tilde{P}$ have the same residue class field and value group, and we can get a pretty good idea of the internal structure of the primed ring $(F[x], P)$ from the picture that Supplement (4.2) provides of $(\tilde{F}[x], \tilde{P})$ (notice that aug S is the augmented signature associated with $v_{\tilde{P}}$). Incidentally, one can give a formula for v_P without referring explicitly to $\tilde{F}$ by a limiting process similar to that in formula (14) at the end of §4; see [3, p. 20] or [15, p. 372] for details.

Associated signatures also give an *external* picture of sets of finite primes. For example, if we give the set of finite primes of $F(x)$ the topology in which a typical basic open set is the collection of finite primes containing a given finite subset of F, then the bijection of (6.5) carries this topology into a *transparent* topology on the set of signatures associated with primes of $F(x)$ [5, §10]. In [5], an approximation theorem is proven for compact subsets of the space of finite primes of a field which generalizes (among other things) the classical approximation theorem for inequivalent valuations.

Let notation be as in (6.1). In our next and final remark we describe how much is lost when a valuation in $\mathfrak{E}(\tilde{v})$ is restricted to $F[x]$. In particular, when do inequivalent valuations in $\mathfrak{E}(\tilde{v})$ restrict to equivalent valuations on $F[x]$, and what happens to value monoids under the mapping Res (recall that Res preserved residue class fields)? Notice that answering the first question gives a computation of $\mathfrak{E}(v)$ (since Res is surjective and $\mathfrak{E}(\tilde{v})$ is computed in §4).

(6.9) **Remark.** Notation is as in (6.1). Let $w \in \mathfrak{E}(\tilde{v})$.

First suppose the associated signature of w (i.e. signature of maximal length $\leq \infty$ which is associated with w, cf. (6.2)) is not a signature of length ∞ and finite degree. Then w is the unique extension of $\mathrm{Res}(w)$ in $\mathfrak{E}(\tilde{v})$, w and $\mathrm{Res}(w)$ have the same value group, and the infinity ideal of w is generated as an ideal of $\tilde{F}[x]$ by the infinity ideal of $\mathrm{Res}(w)$.

Next suppose that the associated signature S of w has finite degree and length ∞. Let $g_\infty \in \tilde{F}[x]$ be its generator. We have two cases.

Case I. g_∞ divides (in $\tilde{F}[x]$) no nonzero polynomial whose coefficients are in F (equivalently, one of the coefficients of g_∞ is transcendental over F). Then $\mathrm{Res}(w)$ has exactly two extensions to an element of $\mathfrak{E}(\tilde{v})$ (corresponding to the two augmented signatures extending S), the infinity ideal of $\mathrm{Res}(w)$ is trivial, $k_S = k_w$, and $\Gamma_S = \Gamma_w$.

Case II. g_∞ divides some monic irreducible $f \in F[x]$. Then w is the unique extension of $\mathrm{Res}(w)$ to an element of $\mathfrak{E}(\tilde{v})$, $k_{\mathrm{Res}(w)} = k_w$, and the following six conditions are equivalent: (1) $w(f) = \infty$. (2) Γ_w is a group. (3) $\Gamma_w = \Gamma_S$. (4) Aug S is the augmented signature of w. (5) The infinity ideal of $\mathrm{Res}(w)$ is nontrivial. (6) The infinity ideal of $\mathrm{Res}(w)$ is (f). When none of the above conditions hold, then $\Gamma_{\mathrm{Res}(w)}$ is generated by Γ_S and $w(f)$, and $w(f)$ is finite and larger than every element of Γ_S.

We prove (6.1) and (6.9) together. For related results about extensions of valuations, see [3, p. 68].

Let $w \in \mathfrak{E}(v)$. w induces a valuation u on the field of fractions E of $F[x]/w^{-1}(\infty)$. There exists an algebraically closed maximal field (E', u') containing (E, u) (that is, $E' \supseteq E$ and u' extends u). By a simple transfinite construction there exists a maximal extension (E'', u'') of $(\tilde{F}, \tilde{v})$ with the same value group and residue class field as u'. By Kaplansky [12, Theorem 7], there exists a value preserving isomorphism leaving F elementwise fixed,

$$\Theta\colon (E', u') \to (E'', u'').$$

Now define $\tilde{w} \in \mathfrak{E}(\tilde{v})$ by

$$\tilde{w}\colon \sum a_i x^i \mapsto u''\Big(\sum a_i \Theta(x^i + w^{-1}(\infty))\Big) \qquad (a_i \in F).$$

Clearly $\mathrm{Res}(\tilde{w}) = w$.

This proves that the map Res is surjective. One now can check (6.9) directly using §4. The rest of (6.1) follows from (6.9).

7. **Linearly compact fields.** In this section we sketch a generalization of the results of §§3, 4 and 5 on fields complete at a discrete rank one valuation to fields which are linearly compact at a valuation of arbitrary rank. A valued field is *linearly compact* (alias, *maximal*, *ultracomplete*) when its additive group

is complete at every (not necessarily Hausdorff) topology admitting a family of fractional ideals as a neighborhood system of zero. (See [2], [9], [20], [21].)

Our notion of a sequence must be generalized. For any ordinal number λ, the expression $\langle a_\nu \rangle_{\nu<\lambda}$ denotes the function defined on the set of ordinal numbers less than λ whose value at ν is a_ν; we call it a *sequence of length* λ. The reader may find it convenient to regard each ordinal number as the set of ordinal numbers less than it, but we use no special properties of this "representation" of the ordinal numbers. For any ordinal number λ, we denote by $\lambda + 1$ its successor. 0 denotes the first ordinal number.

Now let F with valuation v be a linearly compact field. Let A be a system of representatives in $F^\times$ for Γ_v. Instead of picking a system of representatives for $F^\times/(1 + \mathfrak{p}_v)$, we pick a "display" Φ for v in the sense of the following proposition.

(7.1) **Proposition and Definition.** *Let $W(v)$ denote the set of all well ordered subsets of $F^\times/(1 + \mathfrak{p}_v)$, where we write $a(1 + \mathfrak{p}_v) < b(1 + \mathfrak{p}_v)$ if and only if $v(a) < v(b)$. Then there exists a bijection Φ: $F \to W(v)$ such that for any $a \in F^\times$ and $b \in F$ we have*

(i) *$a(1 + \mathfrak{p}_v)$ is the least element of $\Phi(a)$,*

(ii) *if every element of $\Phi(b)$ is less than every element of $\Phi(a)$, then $\Phi(a + b) = \Phi(a) \cup \Phi(b)$.*

We call such a map Φ a display of v.

(7.2) **Remark.** (A) Suppose $F = Q_p$ (the p-adic numbers). Then

$$\sum a_i p^i \mapsto \{a_i p^i(1 + \mathfrak{p}_v) \mid i \text{ an integer with } a_i \neq 0\};$$

is a display of v (here $0 \leq a_i < p$ for all i). The situation for power series fields is even simpler.

(B) Suppose v is discrete rank one. Then the set of displays of v is bijective with the set of systems of coset representatives in $F^\times$ for $F^\times/(1 + \mathfrak{p}_v)$ (correspond to each display the set of elements of $F^\times$ whose images under the display are singletons).

(C) $W(v)$ can naturally be given the structure of a valued field [3, p. 22]; it is then isomorphic to ΛF (cf. [6]) which is (not naturally) isomorphic to the generalized power series field $S(k_v, \Gamma_v, f)$ [21, p. 23]. Here f is any factor set whose cohomology class in $\mathrm{Ext}(\Gamma_v, k_v^\times)$ corresponds to the exact sequence

$$1 \to k_v^\times \to F^\times/(1 + \mathfrak{p}_v) \to \Gamma_v \to 0.$$

(D) When F is not necessarily linearly compact, there exists an injection Φ: $F \to W(v)$ satisfying (i) and (ii) of (7.1) and such that $\Phi(F)$ is closed under

the taking of initial and terminal segments. Such a "generalized display" is surjective if and only if F is linearly compact (this fact is essentially due to Carruth [7]).

The construction of Φ is a long but basically routine exercise in transfinite induction, much like Krull's proof of the existence of maximal immediate extensions [21, pp. 37–38]. We refer the reader to [3, §5] for details and a fuller discussion of the remarks above.

Our choice of Φ serves two purposes. It gives us a system of representatives for $F^{\times}/(1 + \mathfrak{p}_v)$ (namely the elements of F which Φ maps to singletons) and it allows us to assign a specific pseudolimit to each psuedoconvergent sequence [21, p. 39] in F (essentially, the unique pseudolimit whose image in $W(v)$ has minimal order type).

We now define "signatures over (k_v, Γ_v)" by strict analogy with Definition (3.1) (but allowing our sequences to be indexed over ordinal numbers). That is, a *presignature* over (k_v, Γ_v) is a sequence of ordered pairs $S = \langle \theta_\nu, q_\nu \rangle_{\nu < \lambda}$ where the θ_ν lie in some field containing k_v and the q_ν lie in some ordered group containing Γ_v. Given such a presignature S, we let $k_\mu = k_v[\{\theta_\nu | \ \nu < \mu\}]$ and let Γ_μ be the semigroup generated by Γ_v and $\{q_\nu | \ \nu < \mu\}$, for any $\mu \leq \lambda$. Set $k_S = k_\lambda$ and $\Gamma_S = \Gamma_\lambda$. Presignatures S and S' over (k_v, Γ_v) are *equivalent* if there are isomorphisms of k_S and Γ_S onto $k_{S'}$ and $\Gamma_{S'}$ leaving k_v and Γ_v fixed, which map each θ_ν to θ'_ν and q_ν to q'_ν.

(7.3) **Definition.** A *signature* over (k_v, Γ_v) is an equivalence class of presignatures S with (notation as above):

(i) if $\nu < \lambda$, then $[k_\nu : k_v](\Gamma_\nu : \Gamma_v) < \infty$, and the sequence $\langle q_\nu / [k_\nu : k_v](\Gamma_\nu : \Gamma_v) \rangle_{\nu < \lambda}$ is strictly increasing;

(ii) if $\nu < \lambda$, then θ_ν is nonzero if and only if q_ν is commensurable with Γ_v.

The sequence of (i) above of course lies in Γ_S^{div} (cf. (3.2)).

If one considers ∞ as the first infinite ordinal number and $\infty + 1$ as its successor, then the signatures of Definition (3.1) are signatures in the above sense, and if Γ_v is discrete rank one, then every signature in the above sense is a signature in the sense of (3.1).

(7.4) **Notation.** Let $S = \langle \theta_\nu, q_\nu \rangle_{\nu < \lambda}$ be a signature over (k_v, Γ_v). We define $\deg S$, $\operatorname{aug} S$, $k_{\operatorname{aug} S}$, and $\Gamma_{\operatorname{aug} S}$ by strict analogy with Definition (3.3) (i.e., just as (7.3) was obtained from (3.1) by allowing i and n to be ordinal numbers). Given a sequence of polynomials $g = \langle g_\nu \rangle_{\nu < \lambda}$, we define (by analogy with the notation of Lemma B, §4) $D(S, g)$ to be the set of all products $\prod_{\nu < \lambda} g_\nu^{r_\nu}$ where all but a finite number of the r_ν are zero and

$$0 \leq r_\nu < [k_{\nu+1} : k_\nu](\Gamma_{\nu+1} : \Gamma_\nu) \quad (\nu < \lambda). \tag{20}$$

If $\lambda = 0$, we also set $D(S, g) = \{1\}$. When there is no danger of ambiguity, we write

$$D(\mu) = D(\langle \theta_\nu, q_\nu \rangle_{\nu<\mu}, \langle g_\nu \rangle_{\nu<\mu}) \qquad (\mu \leq \lambda). \tag{21}$$

Finally, if S is an augmented signature, we still define $D(\mu)$ as in (21) for μ less than the length of S.

(7.5) **Definition.** Let $w \in \mathfrak{E}(v)$ (cf. §6). A (possibly augmented) signature $S = \langle \theta_\nu, q_\nu \rangle_{\nu<\lambda}$ over (k_v, Γ_v) is *associated with* w if and only if there exists a sequence $\langle g_\nu \rangle_{\nu<\lambda}$ in $F[x]$ (called a *generating sequence for* w *and* S) such that

(i) if $0 < \lambda$, then $g_0 = x$;

(ii) if $\mu + 1 < \lambda$, then we can write

$$g_{\mu+1} = g_\mu^{[k_{\mu+1} : k_\mu](\Gamma_{\mu+1} : \Gamma_\mu)} + \sum_{f \in D(\mu+1)} b_{\mu,f} f \tag{22}$$

where each nonzero term on the right-hand side of (22) has the same value, and for each nonzero coefficient $b_{\mu,f}$, $\Phi(b_{\mu,f})$ is a singleton;

(iii) if $\mu < \lambda$, then we can write

$$g_\mu = g_{\mu^*} + \sum_{f \in D(\mu)} d_{\mu,f} f \tag{23}$$

where μ^* is least with $\deg g_\mu = \deg g_{\mu^*}$ and for each $f \in D(\mu)$

$$\Phi(d_{\mu,f}) = \bigcup_{\mu^* \leq \nu < \mu} \Phi(b_{\nu,f}); \tag{24}$$

(iv) if $\mu \prec \lambda$, then $q_\mu = w(g_\mu)$;

(v) if $\mu < \lambda$ and q_μ is finite and commensurable with Γ_v, then

$$\theta_\mu = \left(a \prod_{\nu \leq \mu} g_\nu^{r_\nu} \right) g_\mu + \wp_w$$

where $a \in A$ and $0 \leq r_\nu < (\Gamma_{\nu+1} : \Gamma_v)$ for all $\nu \leq \mu$.

As in §3, a sequence g of monic polynomials in $F[x]$ is called a *generating sequence for* w when there exists a (possibly augmented) signature S such that g is a generating sequence for w and S.

Let $\mu < \lambda$. $D(\mu)$ is an F-module basis for the set of polynomials in $F[x]$ of degree less than $\deg g_\mu$. This is because the degree of g_ν is clearly $[k_\nu : k_\nu](\Gamma_\nu : \Gamma_\nu)$ for each $\nu < \lambda$. Hence the coefficients $b_{\mu,f}$ and $d_{\mu,f}$ of (22) and (23) above are uniquely determined, so that (24) is unambiguous.

It is not hard to show that this definition generalizes (3.4); for this we assume, of course, that Φ has been chosen so that $\Phi(b)$ is a singleton for each $b \in B$ (cf. (7.2B)). The real point is that the ∞-term of a generating sequence in the sense of (3.4), if there is one, is obtained by the limiting process of (iii) above.

We now make a blanket assertion. *With the above definitions, all the results*

of §§3, 4 and 5 about a field complete at a discrete rank one valuation hold for any linearly compact field. Specifically, we have generalizations of the following.

1. The Fundamental Lemma (3.5) (of course one allows the indices i and n in (3.5) to be ordinal numbers).

2. The Main Theorem, its Supplement, and Corollary (in §4).

3. Theorem (5.1) on irreducible polynomials.

4. Corollaries (5.2), (5.3), and (5.4) on algebraic extensions. Again, the condition that (16) hold for arbitrary field extensions E/F is necessary and sufficient for F to be linearly compact.

5. Propositions (5.5), (5.6) and (5.7), Definition (5.8), the Examples (5.9), and Theorem (5.10). Of course we do *not* replace i and n here by ordinal numbers (except in (5.9D)).

6. Remarks (5.11) and (5.12) hold, as well as the bijection mentioned after (5.12) from the F-isomorphism classes of tame extensions of F with residue class field k and value group Γ onto the equivalence classes in the tensor product $\Gamma/\Gamma_v \otimes k^\times$.

We will prove the generalized Fundamental Lemma in §8. The other results require only a routine generalization of the arguments given above in the discrete rank one case. A minor exception is Corollary (5.3), which uses the criterion for linear compactness mentioned in (7.2D). Details can be found in [3].

We were able in §6 to apply our results on complete fields to noncomplete fields. No such generalization seems possible in general. Similarly no analogue to Remark (5.13) seems available. One can show that if $\tilde{F}$ with valuation $\tilde{v}$ is a maximal immediate extension of a not necessarily linearly compact field F (with valuation v), then the obvious map Res: $\mathfrak{E}(\tilde{v}) \to \mathfrak{E}(v)$ is surjective. One can get a fair insight into the possible extensions of v to $F[x]$ and $F(x)$ by using this surjection to apply our computation of $\mathfrak{E}(\tilde{v})$ (e.g. one can read off an inductive proof of Proposition (2.46) of [1]).

8. **Proof of the Fundamental Lemma.** Let w be a valuation on a commutative ring R. Following Mac Lane [15], we will call elements a and b of R *equivalent* in w when either $w(a-b) > w(a)$ or $w(a) = w(b) = \infty$. For $a \in R$ we denote by $[a]_w$ the set of elements of R equivalent in w to a. Multiplication preserves equivalence and we have a monoid with cancellation

$$C_w = \{[a]_w \mid a \in R,\ w(a) \neq \infty\}.$$

Note that if $w(a) = 0$, then $[a]_w = a + \mathfrak{p}_w$, so $k_w^\times \subseteq C_w$ ($k_w^\times$ denotes the multiplicative monoid of nonzero elements of k_w). Let w operate on C_w by $w([a]_w) = w(a)$; we then have an exact sequence of monoids

$$1 \to k_w^\times \to C_w \to \Gamma_w \to 0.$$

Clearly, C_w is a group if and only if Γ_w is a group and k_w is a field. If R is a field, then $C_w = R^{\times}/(1 + \mathfrak{p}_w)$.

Equivalence plays an essential role in the proof of the Fundamental Lemma. Its role in our earlier exposition has been important, if only implicit, e.g. the key condition (III) in §2 says g_{m+1} can be written in a certain way as a difference of equivalent polynomials.

We now prove the Fundamental Lemma, generalized to linearly compact fields. So let F, v, Φ, and A be as in §7. Let $\langle \theta_\nu, q_\nu \rangle_{\nu<\rho}$ be a signature of finite degree. By induction on ρ, we may suppose we have a sequence $\langle g_\nu \rangle_{\nu<\rho}$ of monic nonconstant polynomials in $F[x]$ such that for any $\lambda < \rho$ and $w \in \mathfrak{E}(v)$, the following are equivalent:

(I) $\langle \theta_\nu, q_\nu \rangle_{\nu<\lambda}$ is associated with w;

(II) $\langle g_\nu \rangle_{\nu\le\lambda}$ is the unique generating sequence for w of length $\lambda + 1$;

(III) $w(g_\lambda) > [k_\nu : k_v](\Gamma_\nu : \Gamma_v)q_\nu$ for all $\nu < \lambda$.

It suffices to construct a monic nonconstant $g_\rho \in F[x]$ such that for any $w \in \mathfrak{E}(v)$, the above three conditions are equivalent with $\lambda = \rho$.

Let $\lambda \le \rho$. In the next five lemmas we let $w \in \mathfrak{E}(v)$ denote any valuation with which $S = \langle \theta_\nu, q_\nu \rangle_{\nu<\lambda}$ is associated. The existence of such w is guaranteed when $\lambda < \rho$ by our induction hypothesis (consider any $w \in \mathfrak{E}(v)$ with $w(g_\lambda) = \infty$). We let F_λ denote the set of polynomials in $F[x]$ of degree less than $\deg g_\lambda$, and set

$$C_w(\lambda) = \{[a]_w \mid 0 \ne a \in F_\lambda\}.$$

The structure of $C_w(\lambda)$ is computed in Lemma E below.

By our induction hypothesis $D(\lambda)$ is a basis for F_λ considered as an F-module (cf. (7.4)). For each $f = \Pi_{\nu<\lambda} g_\nu^{r_\nu}$ in $D(\lambda)$, we set $v_\lambda(f) = \Sigma\, r_\nu q_\nu$ (just as in (4.2B); we of course assume the r_ν satisfy (20)). The next lemma says that w is completely determined on F_λ by S.

Lemma C. *For any* $a_f \in F$ $(f \in D(\lambda))$,

$$w\Big(\sum a_f f\Big) = \min(v(a_f) + v_\lambda(f)).$$

Proof. By our induction hypothesis, $\langle g_\nu \rangle_{\nu<\lambda}$ is a generating sequence for w. Now proceed as in the proof of Lemma B of §4. Done.

Let $B(\lambda)$ denote the set of polynomials $\Sigma\, a_f f$ in F_λ such that each nonzero coefficient a_f has $\Phi(a_f)$ a singleton, and each nonzero term $a_f f$ has the same value. By the preceding lemma, $B(\lambda)$ depends only on S (i.e. is independent of the choice of w) and is a system of representatives in F_λ for $C_w(\lambda)$.

For each $\mu < \rho$, let $e_\mu = (\Gamma_{\mu+1} : \Gamma_\mu)$ and $f_\mu = [k_{\mu+1} : k_\mu]$. Let $A(\mu)$ denote the set of polynomials

$$a \prod_{\nu<\mu} g_\nu^{r_\nu} \tag{25}$$

where $a \in A$ and $0 \leq r_\nu < e_\nu$ for $\nu < \mu$. There exists a unique $a_\mu \in A(\mu)$ which when written as in (25) has $v(a) + \Sigma\, r_\nu q_\nu + e_\mu q_\mu = 0$. Notice that $\theta_\mu = a_\mu g_\mu^{e_\mu} + \wp_w$ if $\mu < \lambda$, and w maps $A(\lambda)$ bijectively to Γ_λ.

Lemma D. *$C_w(\lambda)$ is a subgroup of C_w. Also, $w(C_w(\lambda)) = \Gamma_\lambda$ and $k_w^\times \cap C_w(\lambda) = k_\lambda^\times$.*

Proof. Induct on λ. Lemma C implies $w(C_w(\lambda)) = \Gamma_\lambda$. Lemma A (§4) generalizes to our situation (same proof), so clearly $k_w^\times \cap C_w(\lambda) \subseteq k_\lambda^\times$. F_λ is closed under addition, so the reverse implication follows if any $\theta = (b + \wp_w)\theta_\mu^i$ ($\mu < \lambda$, $i < f_\mu$, $b \in F_\mu$ and $w(b) = 0$) is in $C_w(\lambda)$. $C_w(\mu)$ is a group by induction, so $[f]_w = [ba_\mu^i]_w$ for some $f \in F_\mu$. Since $fg_\mu^{ie_\mu} \in F_\lambda$, $\theta = fg_\mu^{ie_\mu} + \wp_w \in C_w(\lambda)$. That $C_w(\lambda)$ is a group now follows from the exactness of the sequence of monoids

$$1 \to k_\lambda^\times \to C_w(\lambda) \to \Gamma_\lambda \to 0. \tag{26}$$

The lemma is proved.

For each $\alpha \in \Gamma_\nu$, let a_α be the unique element of A with $v(a_\alpha) = \alpha$. More generally, for $\alpha \in \Gamma_\lambda$, let a_α be the unique element of $A(\lambda)$ of the form (25) with $v(a) + \Sigma\, r_\nu q_\nu = \alpha$.

We now define a map

$$\varphi_\lambda : \Gamma_\lambda \times \Gamma_\lambda \to k_\lambda^\times$$

by induction on λ. If $\lambda = 0$, we define φ_λ by

$$\varphi_0(\alpha, \beta) = a_\alpha a_\beta a_{\alpha+\beta}^{-1} + \wp_w \qquad (\alpha, \beta \in \Gamma_\nu).$$

Suppose $\lambda = \mu + 1$. Let $\alpha, \beta \in \Gamma_\mu$ and let r and s be nonnegative integers less than e_μ. We then define $\varphi_\lambda(\alpha + rq_\mu, \beta + sq_\mu)$ to be $\varphi_\mu(\alpha, \beta)$ if $r + s < e_\mu$ and to be $\varphi_\mu(\alpha, \beta)\theta_\mu / \varphi_\mu(-e_\mu q_\mu, \alpha + \beta + e_\mu q_\mu)$ otherwise. Finally, if λ is a limit ordinal, let φ_λ be the union of all the maps φ_μ, $\mu < \lambda$.

φ_λ induces a (not necessarily associative) multiplication on the direct product $C_\lambda = k_\lambda^\times \times \Gamma_\lambda$, namely

$$(\theta, q) \cdot (\theta', q') = (\varphi_\lambda(q, q')\theta\theta', q + q').$$

The sequence

$$1 \to k_\lambda^\times \to C_\lambda \to \Gamma_\lambda \to 0 \tag{27}$$

preserves multiplication and is exact (i.e. "image = kernel" everywhere).

Lemma E. *C_λ is a group, and the map*

$$\alpha \mapsto (\alpha \cdot [a_{w(\alpha)}]_w^{-1},\ w(\alpha)) \qquad (\alpha \in C_w(\lambda))$$

is an isomorphism from $C_w(\lambda)$ to C_λ.

Proof. The above map is a bijection (use Lemma D), so it suffices to show it preserves multiplication. The set of $[a_\alpha]_w$ $(\alpha \in \Gamma_\lambda)$ is a system of representatives in $C_w(\lambda)$ for Γ_λ. A straightforward (inductive) computation shows that the corresponding factor set for the group extension (26) is exactly φ_λ, proving the lemma. (For factor sets and group extensions, see Mac Lane [18, p. 111].)

Lemma F. *Suppose $w' \in \mathfrak{W}(v)$ is associated with S. We identify k_λ with its canonical images in k_w and $k_{w'}$ (thus we identify $a_\mu g_\mu^{e_\mu} + \mathfrak{p}_w$ with $a_\mu g_\mu^{e_\mu} + \mathfrak{p}_{w'}$ for all $\mu < \lambda$). Then the correspondence $[a]_w \leftrightarrow [a]_{w'}$ $(a \in F_\lambda,\ a \neq 0)$ is a group isomorphism between $C_w(\lambda)$ and $C_{w'}(\lambda)$ which is the identity on $k_\lambda^\times$.*

Proof. We also identify Γ_λ with its canonical image in Γ_w and $\Gamma_{w'}$. By Lemma C, we then have $w(b) = w'(b)$ for all $b \in F_\lambda$. Let us inductively suppose the lemma true for all $\mu < \lambda$. It suffices to show that

$$[b]_w [a_{w(b)}]_w^{-1} = [b]_{w'} [a_{w(b)}]_{w'}^{-1} \tag{28}$$

for any $0 \neq b \in F_\lambda$, since we may then apply Lemma E to w and w'. It suffices to consider b of the form $c g_\mu^{ne_\mu + m}$ where $c \in F_\mu$, $m < e_\mu$ and $n < f_\mu$. Then $a_{w(b)} = a' g_\mu^m$, $a' \in A(\mu)$. The left-hand side of (28) is $[c]_w [a']_w^{-1} [a_\mu]_w^{-n} \theta_\mu^n$, which by hypothesis is independent of w, and hence equal to the right-hand side of (28). Done.

Lemma G. *Suppose $\lambda + 1 = \rho$ and that $\langle \theta_\nu, q_\nu \rangle_{\nu < \rho}$ is associated with w. Then a polynomial of the form*

$$g_\lambda^{e_\lambda f_\lambda} + \sum_{i < f_\lambda} b_i g_\lambda^{i e_\lambda} \tag{29}$$

(where for each $i < f_\lambda$, if $b_i \neq 0$ then $b_i \in B(\lambda)$ and $w(b_i) = (f_\lambda - i) e_\lambda q_\lambda$) is the ρth term of a generating sequence for w if and only if

$$y^{f_\lambda} + \sum_{i < f_\lambda} (a_\lambda^{f_\lambda - i} b_i + \mathfrak{p}_w) y^i \tag{30}$$

is the monic irreducible polynomial over k_λ with θ_λ as a zero. If this is indeed the case, then $b_0 \neq 0$.

Proof. The last sentence follows from the fact that the constant term of the irreducible polynomial of θ_λ over k_λ is nonzero.

Let g_ρ be as in (29). If it is in the generating sequence for w, then

$$0 = a_\lambda^{f_\lambda} g_\rho + \wp_w = \theta_\lambda^{f_\lambda} + \sum (a_\lambda^{f_\lambda - i} b_i + \wp_w)\theta_\lambda^i$$

so (30) is indeed the irreducible polynomial of θ_λ over k_λ. Conversely, if (30) is this irreducible polynomial, then $w(g_\rho) > -w(a_\lambda^{f_\lambda}) = e_\lambda f_\lambda q_\lambda$, so the lemma follows by inspection of Definition (7.5).

We now construct g_ρ. For each $\mu + 1 < \rho$, we have unique $b_{\mu,f}$ ($f \in D(\mu + 1)$) with $g_{\mu+1} = g_\mu^{e_\mu f_\mu} + \sum b_{\mu,f} f$ (cf. (22)). If ρ is a limit ordinal, let $\lambda < \rho$ be smallest with $\Gamma_\lambda = \Gamma_\rho$ and $k_\lambda = k_\rho$. Define $d_{\rho,f} \in F$ for each $f \in D(\lambda)$ by

$$\Phi(d_{\rho,f}) = \bigcup_{\lambda \le \nu < \rho} \Phi(b_{\nu,f}).$$

We then set $g_\rho = g_\lambda + \sum d_{\rho,f} f$. If ρ is not a limit ordinal, say $\rho = \lambda + 1$, we can pick $b_i \in B(\lambda) \cup \{0\}$ such that, for any $w \in \mathfrak{S}(v)$ with which $\langle \theta_\nu, q_\nu \rangle_{\nu < \lambda}$ is associated,

$$y^{f_\lambda} + \sum_{i < f_\lambda} (a_\lambda^{f_\lambda - i} b_i + \wp_w) y^i$$

is the irreducible polynomial of θ_λ over k_λ, and the value of b_i is $(f_\lambda - i)e_\lambda q_\lambda$ whenever $b_i \neq 0$. The existence and uniqueness of the b_i follow from Lemmas D and F. We set

$$g_\rho = g_\lambda^{e_\lambda f_\lambda} + \sum_{i < f_\lambda} b_i g_\lambda^{ie_\lambda}$$

which can be uniquely written in the form

$$g_\lambda^{e_\lambda f_\lambda} + \sum_{f \in D(\rho)} b_{\lambda,f} f.$$

Now let $w \in \mathfrak{S}(v)$. We prove our three conditions are equivalent with $\lambda = \rho$.

(I) *implies* (II). By induction, $\langle g_\nu \rangle_{\nu < \rho}$ is the unique generating sequence of w of length ρ. First suppose w is a limit ordinal. Then one checks (II) using Definition (7.5) (the key fact is that $w(g_\rho) > q_\nu$ for all sufficiently large $\nu < \rho$). Next, suppose $\rho = \lambda + 1$. (II) then follows by Lemma G and our construction of g_ρ.

(II) *implies* (III). (III) follows by induction if ρ is a limit ordinal. If $\rho = \lambda + 1$, then $\langle \theta_\nu, q_\nu \rangle_{\nu < \lambda}$ is associated with w. Let f be the remainder obtained when dividing g_ρ by g_λ. By the last sentence of Lemma G (applied to *whatever* signature w has), we have $w(g_\rho) > w(f) = e_\lambda f_\lambda q_\lambda$, which proves (III).

(III) *implies* (I). First suppose $w(g_\nu) = q_\nu$ for all $\nu < \rho$. We are then done by induction if ρ is a limit ordinal, so suppose $\rho = \lambda + 1$. Then $\langle \theta_\nu, q_\nu \rangle_{\nu < \lambda}$ is associated with w, so it suffices to show that $a_\lambda g_\lambda^{e_\lambda} + \wp_w$ satisfies the same irreducible polynomial over k_λ as θ_λ does (cf. (3.1)). But since $w(g_\rho) > e_\lambda f_\lambda q_\lambda$, this follows by our construction of g_ρ.

Now suppose that for some least $t < \rho$, $w(g_t) \neq q_t$. We are done if we obtain a contradiction. Let $0 = \lambda_0 < \lambda_1 < \cdots < \lambda_n < \lambda_{n+1} = \rho$ be a finite sequence of ordinals containing $\{\nu < \rho \mid e_\nu f_\nu \neq 1\} \cup \{t\}$. For the remainder of this section we will identify the nonnegative integer i with the ordinal number λ_i; we regard $i+1$ as denoting λ_{i+1} and not $\lambda_i + 1$. For each $0 \leq i \leq n$ we have unique $c_{i,f}$ ($f \in D(i+1)$) with $g_{i+1} = g_i^{e_i f_i} + \sum c_{i,f} f$. Evidently, for each $f \in D(i+1)$,

$$\Phi(c_{i,f}) = \bigcup \Phi(b_{\nu,f}) \quad \text{(union over } i \leq \nu < i+1)$$

and, by the last sentence of Lemma G, for some $h = \prod g_\nu^{s_\nu} \in D(i)$,

$$v(c_{i,h}) + \sum_{\nu < i} s_\nu q_\nu = e_i f_i q_i. \tag{31}$$

Claim 1. $w(g_t) > q_t$, so $\langle \theta_\nu, q_\nu \rangle_{\nu < t}$ is associated with w.

Proof. Suppose not. Then $w(g_t) < q_t$, so $w(g_i) < q_i$ for $t \leq i \leq n$ (use the induction hypothesis on g_i). We claim $w(g_{j+1}) = e_j f_j w(g_j)$ for $t \leq j \leq n$. Suppose inductively that this is true for all $i < j$, where $t \leq j \leq n$. For each $f = \prod_{\nu \leq j} g_\nu^{r_\nu}$ $\in D(j+1)$,

$$w(c_{j,f} f) \geq e_j f_j q_j + w(f) - \sum_{0 \leq i \leq j} r_i q_i \geq e_j f_j q_j + \sum_{0 \leq i \leq j} (e_i f_i - 1)(w(g_i) - q_i)$$

$$\geq e_j f_j w(g_j) + q_t - w(g_t) + \sum_{t \leq i \leq j} q_{i+1} - e_i f_i q_i > e_j f_j w(g_j) = w(g_j^{e_j f_j})$$

which implies $w(g_{j+1}) = e_j f_j w(g_j)$. Now set $j = n$ to get $w(g_{n+1}) = e_n f_n w(g_n)$. Hence $w(g_n) > q_n$. Since $w(g_t) < q_t$, we cannot have $n > t$; hence $n = t$ and the claim is proved.

Claim 2. $n > t$ and $w(g_{t+1}) = e_t f_t q_t$.

The first assertion follows from the second by (III). Using (31) and Claim 1 we have $w(\sum_{f \in D(t)} c_{t,f} f) = e_t f_t q_t$. Writing

$$g_{t+1} = \left(\sum_{f \in D(t)} c_{t,f} f \right) + \left(g_t^{e_t f_t} + \sum_{f \notin D(t)} c_{t,f} f \right) \tag{32}$$

we see $w(g_{t+1}) = e_t f_t q_t$. (Use that the second term of (32) has value greater than $e_t f_t q_t$ by Claim 1.)

Claim 3. $w(g_{j+1}) = e_j f_j w(g_j)$ for all $t < j \leq n$.

Proof. Suppose the claim holds for all $i < j$. For each $f \in B(j+1)$ we have $w(c_{j,f} f) > e_j f_j w(g_j)$ (a straightforward computation along the lines of that in Claim 1). The claim follows immediately.

If in Claim 3 we take $j = n$, then $w(g_{n+1}) = e_n f_n w(g_n)$. By Claim 2, $n > t$, so $w(g_n) < q_n$. Hence $w(g_{n+1}) < e_n f_n q_n$, contradicting (III).

The Fundamental Lemma is proved.

The Lemmas C, D, E and F can be proven in much greater generality [3, p. 78].

It is easy to apply them to compute C_w for any extension w of v to $F[x]$ or $F(x)$.

9. **Polynomials in several variables.** Let F be a global field. In this brief section we sketch a computation of the finite primes of $F[x, y]$ which have discrete rank one value group (abbreviated, *discrete primes*). This allows us to illustrate how the methods of §6 can be applied to commutative rings, and also gives an application of our remarks on equivalence in §8. As in §6, we assume we have chosen systems of representatives for the value group Γ_v and "equivalence class group" C_v of each nontrivial valuation v of F. For more on valuations on rings of polynomials in several variables see Mac Lane [17, §6] and Inoue [11].

First note that a discrete prime of $F[x, y]$ restricts to a discrete prime of $F[x]$. The discrete primes of $F[x]$ are computed in §6; hence it suffices to calculate the extensions of such a prime P to a discrete prime of $F[x, y]$. Now for any valuation v on a commutative ring R, $\mathfrak{E}(v)$ is naturally bijective with $\mathfrak{E}(v^*)$, where v^* is the valuation induced by v on the field of fractions of $R/v^{-1}(\infty)$. Thus it suffices to compute the extensions of u to a prime discrete rank one valuation on $E[y]$, where u is the valuation induced by v_P on the field of fractions E of $F[x]/v_P^{-1}(\infty)$. By our remarks in §8, the chosen systems of representatives for the value group and equivalence class group of the restriction of v_P to F extend canonically to systems of representatives for Γ_P and C_{v_P} (recall "$A(\lambda)$ and $B(\lambda)$"), thence giving systems of representatives in $E^\times$ for Γ_u and C_u. We can then compute the discrete rank one prime valuations in $\mathfrak{E}(u)$ by defining associated signatures (cf. (6.2)) with respect to these systems of representatives.

Putting all this together, we obtain a bijection between the discrete primes of $F[x, y]$ and the set of triples (P, S, T) where P is a finite prime of F, S is a signature over (k_P, Γ_P) with $(\Gamma_S : \Gamma_P) < \infty$ and k_S a field, and T is a signature over (k_S, Γ_S) with $(\Gamma_T : \Gamma_S) < \infty$ and k_T a field. This bijection is natural modulo the choice of systems of representatives in $F^\times$ for the value groups and equivalence class groups of valuations on F. The bijection can be iterated in the obvious way to any number of variables.

10. **Mac Lane's inductive and limit values.** We now give the connections between the concepts and results above and those in Mac Lane ([15], [16], [17]). We delayed until now the detailed acknowledgement of Mac Lane's work because of the rather technical nature of these connections.

Assume v is a discrete rank one valuation on a field F, and that we have chosen systems of representatives A and B in $F^\times$ for Γ_v and C_v with $1 \in A \cap B$. We shall regard Γ_v as contained in the ordered additive group of real numbers $\mathbf{R}$. We also regard all rank one valuations as taking values in $\mathbf{R} \cup \{\infty\}$.

We review the construction in [15] of extensions of v to $F[x]$, using slightly

different notation. For any $\mu \in \mathbf{R} \cup \{\infty\}$, we let $[v; (x, \mu)]$ denote the valuation on $F[x]$,

$$\sum r_i x^i \mapsto \min_i (v(r_i) + i\mu) \qquad (r_i \in F).$$

Next (the induction step), let w be any rank one valuation on $F[x]$ extending v. Suppose $\phi \in F[x]$ and $\mu \in \mathbf{R} \cup \{\infty\}$ satisfy

(i) ϕ has minimal degree in its equivalence class $[\phi]_w$;

(ii) $[\phi]_w$ is irreducible in the semigroup C_w;

(iii) $\mu > w(\phi)$.

We understand (ii) to exclude the possibility that $[\phi]_w$ is a unit in C_w. We then let $[w; (\phi, \mu)]$ denote the valuation on $F[x]$ which maps a polynomial (expanded in powers of ϕ) $\Sigma\, r_i \phi^i$ ($\deg r_i < \deg \phi$) to $\min_i (w(r_i) + i\mu)$. $[w; (\phi, \mu)]$ is called an *augmentation* of w (cf. [15, Theorem (4.2)]). ϕ is called a *key polynomial* for w.

We now define, for appropriate sequences $\langle \mu_i \rangle_{i<n}$ in $\mathbf{R} \cup \{\infty\}$ and $\langle \phi_i \rangle_{i<n}$ in $F[x]$, where $1 \leq n \leq \infty$, a valuation denoted by

$$[v; \langle \phi_i, \mu_i \rangle_{i<n}]. \tag{33}$$

For finite n, (33) is defined inductively by the formula

$$[v; \langle \phi_i, \mu_i \rangle_{i<m+1}] = [[v; \langle \phi_i, \mu_i \rangle_{i<m}]; (\phi_m, \mu_m)] \tag{34}$$

where we let $[v; \langle \phi_i, \mu_i \rangle_{i<0}] = v$. Such valuations Mac Lane calls *inductive values*. If $n = \infty$, we define (33) to be the limit of the $[v; \langle \phi_i, \mu_i \rangle_{i<m}]$ as $m \to \infty$. That is, any $f \in F[x]$ is assigned the value $\lim_{m\to\infty} [v; \langle \phi_i, \mu_i \rangle_{i<m}](f)$. These valuations Mac Lane calls *limit values*. The conditions that must be placed on the ϕ_i and μ_i are simply those ensuring that (34) always be defined (i.e. see (i), (ii), (iii) above).

One says that the sequence $\langle \phi_i, \mu_i \rangle_{i<n}$ gives a *homogeneous representation* of the valuation $[v; \langle \phi_i, \mu_i \rangle_{i<n}]$ if the ϕ_i are distinct polynomials of nondecreasing degree and, for $0 < m < n$, ϕ_m is monic and $[v; \langle \phi_i, \mu_i \rangle_{i<m}]$-homogeneous in $\langle \phi_i \rangle_{i<m}$ (cf. §3). Then [15, Theorems (16.2) and (16.3)] *every extension of v to a rank one valuation on $F[x]$ has a unique homogeneous representation.* (Strictly speaking, Mac Lane only considers "finite" values in [15], i.e. valuations with trivial infinity ideals, but the above result follows immediately from his methods. Some caution is indicated when allowing nonfinite values, e.g. his [15, Corollary (16.4)] is false in this case.)

The following two propositions allow one to translate the language of generators and signatures into that of inductive and limit values. Let w be an extension of v to a rank one valuation on $F[x]$, say with homogeneous representation

$[v; \langle \phi_i, \mu_i \rangle_{i<m}]$. Let $\langle \theta_i, q_i \rangle_{i<n}$ be the signature associated with w (cf. (6.2)) and let $\langle g_i \rangle_{i<n}$ be the corresponding generating sequence.

Proposition A. *The sequences* $\langle \phi_i, \mu_i \rangle_{i<m}$ *and* $\langle g_i, q_i \rangle_{i<n}$ *are identical.*

Proposition B. w *admits an augmentation if and only if* C_w *is not a group, and hence if and only if, for some* $s < n$, $[k_{s+1} : k_s](\Gamma_{s+1} : \Gamma_s) = \infty$ *(necessarily then,* $s + 1 = n$*). The key polynomials over* w *are exactly the polynomials* ϕ *which are either equivalent in* w *to* g_s*, or equivalent in* w *to the generator of a signature identical with* $\langle \theta_i, q_i \rangle_{i<n}$ *except for* θ_s*. Of course, equivalent key polynomials give the same augmentations.*

(The second case, i.e. ϕ not equivalent in w to g_s, arises only if θ_s is transcendental over k_s and is the only case in which ϕ is a key polynomial for an inductive value in the sense of [15, Theorem (9.4)].)

Let notation be as above. For each $m < n$, ϕ_m is the unique monic $f \in F[x]$ of least degree which is w-homogeneous in $\langle \phi_i \rangle_{i<m}$ and has

$$w(f) > [v; \langle \phi_i, \mu_i \rangle_{i<m}](f). \tag{35}$$

Using (4.2) (and (6.1) of course) and assuming inductively that, for some $m < n$, $\langle \phi_i, \mu_i \rangle_{i<m} = \langle g_i, q_i \rangle_{i<m}$, one checks that $f = g_m$ satisfies (35), so $g_m = \phi_m$. Hence $q_m = w(g_m) = w(\phi_m) = \mu_m$. This proves Proposition A. The first sentence of B follows from (4.2) and (6.1). The second sentence is a corollary of Proposition A (consider the homogeneous representation of w and its augmentation). With a little more work one can prove the existence and uniqueness of homogeneous representations, and hence the above two propositions, using only the results of this paper.

With the above two propositions, all the theorems of [15] with the exception of the interesting but peripheral [15, Theorem (6.5)] can be proved as corollaries to the results of this paper. (A second exception must be also made for fundamental elementary results like [15, Theorem (2.1)] which we have treated as common property.) With somewhat more effort, our Theorems (4.1) and (4.2) can be proved using the methods of [15]; the argument centers around the careful inductive application of [15, Theorems (12.1) and (13.1)]. The rank two valuations do not fit nicely into the framework of [15] and must be handled on an ad hoc basis. For example, [15, Theorem (16.1)] is false if one allows nonfinite and rank two valuations. (For F complete, [15, Theorem (16.1)] is true but [15, Theorem (16.2)] fails.) The trouble comes from valuations with generating sequences of length $\infty + 1$, where the polynomial g_∞ can take on either a finite value or value ∞. Homogeneous representations do not distinguish between these possibilities. This was the reason of course for considering sequences of length

$\infty + 1$. Part of the fundamental lemma can also be proven with the methods of [15], but the crucial assertion (that (iii) of (3.5) implies (i)) seems to require the elementary but complicated counting argument of §8.

In discussing irreducibility, Mac Lane starts from the observation that the key polynomials over an extension of v to $F[x]$ are irreducible. This fairly obvious fact includes a large number of "polygonal irreducibility criteria" (cf. [17, §5])—the strength of the fact lies in our knowledge of the extensions themselves. When F is locally compact, Mac Lane obtains a method for testing in a finite number of steps the irreducibility of a polynomial in $F[x]$. Of course this is only implicit in his papers since he never (except in [15, Theorem (7.1)]) mentions locally compact or even complete fields. The irreducibility criterion we give can of course be proven from Mac Lane's if one assumes the Fundamental Lemma (or, more precisely, (5.5) together with the computation of γ_f).

REFERENCES

1. S. Abhyankar, *Ramification theoretic methods in algebraic geometry*, Ann. of Math. Studies, no. 43, Princeton Univ. Press, Princeton, N. J., 1959. MR 21 #4158.
2. N. Bourbaki, *Éléments de mathématique*. Fasc. XXX. *Algèbre commutative*. Chap. 6: *Valuations*, Actualités Sci. Indust., no. 1308, Hermann, Paris, 1964. MR 33 #2660.
3. Ron Brown, *Irreducibility over complete rings*, Thesis, University of Oregon, Eugene, Ore., 1968.
4. ———, *Tame extensions of linearly compact fields* (in preparation).
5. ———, *An approximation theorem for extended absolute values*, Canad. J. Math. 24 (1972), 167–184.
6. Ron Brown and D. K. Harrison, *Tamely ramified extensions of linearly compact fields*, J. Algebra 15 (1970), 371–375.
7. P. W. Carruth, *Generalized power series fields*, Trans. Amer. Math. Soc. 63 (1948), 548–559. MR 9, 561.
8. J. W. S. Cassels and A. Frölich, *Algebraic number theory*, Proc. Instructional Conf. Organized by the London Math. Soc. (A NATO Advanced Study Institute), supported by the Internat. Math. Union, Academic Press, London; Thompson, Washington, D. C., 1967. MR 35 #6500.
9. I. Fleischer, *Completeness in valued spaces and algebras*, Quart. J. Math. Oxford Ser. (2) 15 (1964), 345–348. MR 31 #2241.
10. D. K. Harrison, *Finite and infinite primes for rings and fields*, Mem. Amer. Math. Soc. No. 68 (1966).
11. H. Inoue, *On valuations of polynomial rings of many variables*. I, J. Fac. Sci. Hokkaido Univ. Ser. I 21 (1970), 46–74. MR 41 #8410.
12. I. Kaplansky, *Maximal fields with valuations*, Duke Math. J. 9 (1942), 303–321. MR 3, 264.
13. R. F. MacCoart, *Irreducibility of certain classes of Legendre polynomials*, Duke Math. J. 28 (1961), 239–246.
14. R. E. MacKenzie and G. Whaples, *Artin-Schreier equations in characteristic zero*, Amer. J. Math. 78 (1956), 473–485. MR 19, 834.
15. S. Mac Lane, *A construction for absolute values on polynomial rings*, Trans. Amer. Math. Soc. 40 (1936), 363–395.
16. ———, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. J. 2 (1936), 492–510.

17. S. Mac Lane, *The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals*, Trans. Amer. Math. Soc. 43 (1938), 226–239.

18. ———, *Homology*, Die Grundlehren der math. Wissenschaften, Band 114, Academic Press, New York; Springer-Verlag, Berlin, 1963. MR 28 #122.

19. M. E. Manis, *Valuations on a commutative ring*, Proc. Amer. Math. Soc. 20 (1969), 193–198. MR 38 #2134.

20. P. Ribenboim, *Théorie des valuations*, 2ième éd., Séminaire de Mathématiques Supérieures, no. 9 (Été, 1964), Les Presses de l'Université de Montréal, Montréal, Que., 1968. MR 40 #2670.

21. O. F. G. Schilling, *The theory of valuations*, Math. Surveys, no. 4, Amer. Math. Soc., Providence, R. I., 1950. MR 13, 315.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OREGON, EUGENE, OREGON 97403

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, B. C., CANADA

Current address: Department of Mathematics, University of Hawaii, Honolulu, Hawaii 96822