A CONSTRUCTION FOR ABSOLUTE VALUES IN POLYNOMIAL RINGS

BY

SAUNDERS MacLANE

1. Introduction. An absolute value of a ring is a function $\|b\|$ which has some of the formal properties of the ordinary absolute value. More explicitly, for any b in the ring, $\|b\|$ must be a real number with the properties

$$\|bc\| = \|b\| \cdot \|c\|, \qquad \|b + c\| \le \|b\| + \|c\|.$$

If the second inequality holds also in the stronger sense

$$\|b + c\| \le \max(\|b\|, \|c\|)$$

then the value $\|b\|$ is called non-archimedean. The thus delimited non-archimedean values are of considerable arithmetic interest. They are useful in questions of divisibility and irreducibility and in fact often correspond exactly to the prime ideals of the given ring. This paper is devoted to the explicit construction of non-archimedean values. More specifically, given all such values for the field R of rational numbers, we construct all possible values of the ring $R[x]$ of all polynomials in x with coefficients in R.

In treating a non-archimedean value it is convenient to replace $\|a\|$ by a related "exponential" value

$$V(a) = -\log \|A\|,$$

with corresponding forms (§2) of the formal properties of V. The possible non-archimedean values of the field of rational numbers were determined by Ostrowski (1917): For every prime p there is a p-adic exponential value V_0 in which the value of any rational number is obtained by writing the number as $p^\alpha(u/v)$, where u and v are prime to p, and setting

$$V_0\big(p^\alpha(u/v)\big) = k\alpha, \tag{1}$$

where k is any fixed positive constant. This value we denote by the symbol $[V_0(p) = k]$. The only other value V is a trivial one, in which $V(a)$ is zero for $a \ne 0$.

On this basis we can determine all possible values in the ring of polynomials with rational coefficients. Any such value W gives a p-adic or trivial value $V_0(a) = W(a)$ for the rational numbers and a value $\mu = W(x)$ for the variable x. These facts alone give a first approximation V_1 to the value W, as follows:

$$\begin{aligned} &V_1\big(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0\big) \\ &\qquad = \min\big\{ V_0(a_n) + n\mu,\ V_0(a_{n-1}) + (n-1)\mu,\ \ldots,\ V_0(a_0) \big\}. \end{aligned} \tag{2}$$

This V_1 is actually a value and is never larger than W. If V_1 is not equal to W, we choose a $\phi(x)$ of smallest possible degree for which $W\big(\phi(x)\big) > V_1\big(\phi(x)\big)$. We than define a second approximation $V_0\big(f(x)\big)$ by using* the true value for $\phi(x)$. In this manner we construct successive approximations V_1, V_2, V_3, … which in the limit will give the arbitrary value W (§8).

The succession of values V_1, V_2, … is defined in Part I for polynomials with coefficients in any field K. This requires a general method (§§4 and 5) of constructing a value V_k from a previously obtained value V_{k-1}. The value given by the limit of such a sequence needs a special study (§7). Here, as in §§8 and 16, we assume that every value of the field K is "discrete"; that is, that the real numbers used as values form an isolated point set, as in the case of p-adic values.

Part II investigates the structure of the values which have been constructed. The central problem is the construction of the "residue-class field" which arises when polynomials which differ by a polynomial of positive value are put into the same residue-class. For the absolute values constructed in Part I this field is determined by an inductive construction of the homomorphism of polynomials to residue-classes (§§10–14). This homomorphism also yields a more specific description of how our values can be built up (§§9, 13). Since a given value W can be represented in many ways by a sequence of approximations V_1, V_2, V_3, …, we treat in §§15 and 16 the questions as to when two such sequences can give the same ultimate value W, and how such a sequence can be put in a normal form.

Among the applications of this construction of absolute values we mention the classification of irreducibility criteria of the Newton Polygon type. The theorem of Eisenstein states that a polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$$

with integral coefficients a_i is irreducible if each coefficient a_i is divisible by some fixed prime p, while the last term a_0 is not divisible by p^2. In terms of the value V_1 of (2) with $\mu = 1/n$ these hypotheses on $f(x)$ become

$$V_1\big(f(x)\big) = V_1(x^n) = V_1(a_0) < V_1(a_i x^i) \qquad (i = 1, \ldots, n-1).$$

In this form a simple proof of the theorem can be given. The theorems of Königsberger (1895), Dumas (1906), and Ore (1928) are likewise related to the values V_1. The second stage values V_2 can be similarly applied to interpret the irreducibility theorems of Schöneman (1846), Bauer (1905), Kürschák (1923), and Ore (1923). By using the general value V_k one can obtain a still more extensive irreducibility criterion which includes all these previous theorems (MacLane

*Similar "second-stage" values V_2 appear implicitly in the irreducibility investigations of Ore (1923), Kürschák (1923), and Rella (1927).

(1935)), and which asserts that certain polynomials $f(x)$ with irreducible homomorphic images of sufficiently high degree are themselves irreducible. Our construction for absolute values can also be applied to give a new and complete treatment of the problem of constructing the prime ideal factors of a given rational prime in a given algebraic field.

I. The construction of non-archimedean values

2. Elementary properties of values in rings. A ring* S is said to have a *non-archimedean value* (for short, a value) V if to every element $a \neq 0$ in S there is assigned a unique real number $V(a)$ with the properties

$$V(ab) = V(a) + V(b), \qquad V(a+b) \geq \min\big(V(a), V(b)\big).$$

These we call the *product* and *triangle* laws respectively. We assume also that 0 is assigned the value $+\infty$, with the following conventions for any finite number γ:

$$\gamma < \infty, \qquad \infty + \gamma = \gamma + \infty = \infty + \infty = \infty.$$

Two simple consequences of the product law are

(1) $$V(1) = V(-1) = 0, \qquad V(-a) = V(a).$$

More important is the strengthened form of the triangle law:

(2) $$V(a) \neq V(b) \text{ implies } V(a+b) = \min\big(V(a), V(b)\big).$$

For suppose instead that $V(a) > V(b)$ and $V(a+b) > \min\big(V(a), V(b)\big)$. Then

$$V(b) = V(a+b-a) \geq \min\big(V(a+b), V(a)\big) > V(b),$$

a contradiction.

Since we are using a value analogous to the negative logarithm of the ordinary absolute value, a "small" absolute value will correspond to a "large" value V. Hence we say that two ring elements a and b are of the same order of magnitude or *equivalent in* V — denoted $a \approx_V b$ — if and only if

$$V(a-b) > V(a).$$

The product and strong triangle laws show that equivalent elements have the same value and that equivalence is a reflexive, symmetric, and transitive relation, provided the supplementary assumption† that $0 \approx_V 0$ be made.

*Here and in the sequel "ring" means "commutative ring with unit element".

†Here and subsequently the element 0 plays an exceptional role.

Two equivalences $a \approx_V b$ and $c \approx_V d$ can be multiplied to give

(3) $$ac \approx_V bd.$$

An element b is *equivalence-divisible* in V by a — denoted $a \parallel_V b$ — if and only if there exists a c in S such that

$$b \approx_V ca.$$

If this is true, it remains true when a or b is replaced by an equivalent element.

The product law implies that a ring S with a value V must be an integral domain. The value V may be extended to the quotient field of S by defining, in accord with the product law,

(4) $$V\Big(\frac{a}{b}\Big) = V(a) - V(b)$$

for any elements a and $b \neq 0$ in S. One then obtains the

Theorem 2.1. *Let S be an integral domain with quotient field K. If V is a value of S, then the function defined by* (4) *is a value of K. Conversely, every value of K can be obtained in this way from one and only one value of S.*

When $S = K$ is a field, the set of all real numbers $V(a)$ for $a \neq 0$ is an additive group Γ, called the *value-group* of V. If the positive numbers of Γ have a positive minimum $\delta > 0$, then the value V is said to be *discrete*. In this case the group Γ is cyclic and consists of all multiples of δ. If all elements not 0 have the value 0, then V is called *trivial*. Every ring has a trivial value, while the p-adic values for the field of rational numbers are examples of discrete values. Values of arithmetic interest are generally discrete.

3. The first stage values. Our problem is this: Given all values of a field K; to construct all values for the ring $K[x]$ of all polynomials* in x with coefficients in K. By Theorem 2.1, this is equivalent to determining all values in the field $K(x)$ of rational functions of x with coefficients in K. No gain in generality would result were a ring S used instead of the field K.

As indicated in the introduction, the values for $K[x]$ will be constructed in stages. For the first step, take any value V_0 for the field K and any real number μ, and then define a corresponding *first stage value* V_1 for any polynomial by the equation (2) of §1. In particular, this gives

$$V_1(x) = \mu, \qquad V_1(a) = V_0(a) \qquad (\text{any } a \in K).$$

Hence we use the symbol $[V_0, V_1(x) = \mu]$ for the value V_1.

*Henceforth all polynomials considered are to have coefficients in K, unless otherwise noted.

Theorem 3.1. *If V_0 is a value of K and μ a real number, the function $[V_0, V_1(x) = \mu]$ defined above is a value of $K[x]$.*

A particularly simple V_1 arises when $\mu = 0$. On the other hand, if V_0 is trivial and $\mu < 0$, then

$$V_1\big(a(x)\big) = \mu \deg a(x).$$

The symbol $\deg a(x)$ here and in the sequel denotes the *degree in x* of the polynomial $a(x)$.

4. Augmented values. Our construction now proceeds to build a second stage value on the basis of a first stage one; or, more generally, a kth stage value from one at the stage $k-1$. The process involved can be formulated once for all: Given a value W for $K[x]$; to construct an "augmented" value V by assigning larger values to a certain "key" polynomial $\phi(x)$ and to its equivalence-multiples. The *key polynomial* $\phi(x)$ must be suitably chosen.

Definition 4.1. A key polynomial $\phi(x) \neq 0$ over a value W of $K[x]$ is one which satisfies the following conditions:

- (i) Irreducibility. If a product is equivalence-divisible in W by $\phi(x)$, then one of the factors is equivalence-divisible by $\phi(x)$.
- (ii) Minimal degree. Any non-zero polynomial equivalence-divisible in W by $\phi(x)$ has a degree in x not less than the degree of $\phi(x)$.
- (iii) The leading coefficient* of $\phi(x)$ is 1.

This key polynomial is to be assigned a new value

$$V\big(\phi(x)\big) = \mu > W\big(\phi(x)\big). \tag{1}$$

To find the new values of other polynomials, we use *expansions in ϕ*; that is, expressions in powers of $\phi(x)$ of the form†

$$f(x) = f_m(x)\,\phi^m + f_{m-1}(x)\,\phi^{m-1} + \cdots + f_0(x), \tag{2}$$

in which each coefficient polynomial $f_i(x)$ is either zero or of degree less than the degree of $\phi(x)$. Any polynomial has one and only one such expansion, which may be found by successive division by powers of ϕ. The new value $V\big(f(x)\big)$ is computed from the expansion thus:

$$V\big(f_m(x)\,\phi^m + f_{m-1}(x)\,\phi^{m-1} + \cdots + f_0(x)\big) = \min{}_i\big(\,W\big(f_i(x)\big) + i\mu\,\big). \tag{3}$$

Here "min" with subscript i means the smallest quantity of the form $W\big(f_i(x)\big) + i\mu$, for $i = 0, 1, \ldots, m$.

*This assumption, although unnecessary, will simplify the subsequent work.

†We use ϕ as an abbreviation for $\phi(x)$, and similarly for other polynomials.

Theorem 4.2. *If W is a value of $K[x]$, $\phi(x)$ is a key polynomial over W and μ is a real number satisfying* (1)*, then the function V defined in* (3) *is also a value of $K[x]$. V is called an augmented value, and is denoted by*

$$V = [\,W,\, V(\phi) = \mu\,].$$

Proof. The product and triangle laws for V must be verified. We first prove the triangle law for a sum $f(x) + g(x)$. Let f and g have the expansions (2) and

$$g(x) = g_n(x)\,\phi^n + g_{n-1}(x)\,\phi^{n-1} + \cdots + g_0(x) \tag{4}$$

respectively. By adjoining zero coefficients we can make $m = n$. Hence $f + g$ has the expansion

$$f(x) + g(x) = \sum_{i=0}^{n} [f_i(x) + g_i(x)]\,\phi^i.$$

By the definition of V and the triangle law for W,

$$\begin{aligned}
V(f+g) &= \min{}_i\big(\,W(f_i + g_i) + i\mu\,\big)\\
&\geq \min{}_i\big(\min\big(W(f_i),\, W(g_i)\big) + i\mu\,\big)\\
&\geq \min{}_i\big(\,W(f_i) + i\mu,\, W(g_i) + i\mu\,\big)\\
&= \min\big(\min{}_i\big(W(f_i) + i\mu\big),\, \min{}_i\big(W(g_i) + i\mu\big)\,\big),\\
V(f+g) &\geq \min\big(V(f),\, V(g)\big).
\end{aligned}$$

To prove the product law we will use the *quotient-remainder* expression for a polynomial $f(x)$,

$$f(x) = q(x)\,\phi + r(x), \tag{5}$$

where $r(x)$ is zero or of degree less than that of $\phi(x)$.

Lemma 4.3. *If ϕ is a key polynomial over a value W of $K[x]$, and if $f(x) \neq 0$ has the quotient-remainder expression* (5)*, then*

$$W\big(r(x)\big) \geq W\big(f(x)\big), \tag{6}$$

$$W\big(q(x)\phi\big) \geq W\big(f(x)\big). \tag{7}$$

The inequality in (6) *holds if and only if $\phi \parallel_W f$.*

Proof of Lemma. Were the first conclusion (6) false, then $W\big(f(x)\big) > W\big(r(x)\big)$ in (5) and the definition of equivalence would give

$$r(x) \approx_W -q(x)\,\phi.$$

Hence $\phi \parallel_W r$ and $r(x) \neq 0$, a contradiction to the minimal property of ϕ and the restricted degree of $r(x)$. The second conclusion (7) now follows from (6) by the triangle law.

The third conclusion gives a test for equivalence-divisibility in terms of ordinary division. When $W\big(r(x)\big) > W\big(f(x)\big)$, then (5) shows $\phi \parallel_W f$. Conversely, if $\phi \parallel_W f$ then there exist polynomials $h(x)$ and $s(x)$ so that

$$f(x) = h(x)\,\phi + s(x), \qquad W\big(s(x)\big) > W\big(f(x)\big).$$

If now the equality sign in (6) should hold, we would have

$$r(x) = f(x) - q(x)\,\phi = \big(h(x) - q(x)\big)\,\phi + s(x),$$

with

$$W\big(s(x)\big) > W\big(f(x)\big) = W\big(r(x)\big),$$

so that $\phi \parallel_W r$, again a contradiction. □

Return to Theorem 4.2 and consider the product law first for a product of two monomial expansions $a(x)\,\phi^t$ and $b(x)\,\phi^u$. Because of the limited degrees of $a(x)$ and $b(x)$, the product $a(x)b(x)$ has an expansion with not more than two terms,

$$a(x)\,b(x) = c(x)\,\phi + d(x). \tag{8}$$

Were it the case that $\phi \parallel_W ab$ then the equivalence-irreducibility of ϕ (Definition 4.1) would require that either $\phi \parallel_W a$ or $\phi \parallel_W b$, contrary to the minimal property. Hence $\phi \nparallel_W ab$. Lemma 4.3 and the triangle axiom then yield

$$W\big(c(x)\,\phi\big) \geq W\big(a(x)\,b(x)\big) = W\big(d(x)\big).$$

Since the new value of ϕ exceeds the old value,

$$W\big(c(x)\big) + \mu > W\big(a(x)\,b(x)\big) = W\big(d(x)\big). \tag{9}$$

The product under consideration has by (8) the expansion

$$\big(a(x)\,\phi^t\big)\big(b(x)\,\phi^u\big) = c(x)\,\phi^{t+u+1} + d(x)\,\phi^{t+u};$$

hence the definition of V and the conclusion (9) give

$$\begin{aligned} V\big[\big(a(x)\,\phi^t\big)\big(b(x)\,\phi^u\big)\big] &= \min\big\{\,W\big(c(x)\big) + \mu + (t+u)\mu,\ W\big(d(x)\big) + (t+u)\mu\,\big\} \\ &= W\big(d(x)\big) + (t+u)\mu \\ &= W\big(a(x)\big) + t\mu + W\big(b(x)\big) + u\mu \\ &= V\big(a(x)\,\phi^t\big) + V\big(b(x)\,\phi^u\big). \end{aligned}$$

This is the product law for monomial expansions.

The product law for polynomials $f(x)$ and $g(x)$ with arbitrary expansions (2) and (4) respectively is an immediate consequence. The product $f(x)\,g(x)$ has an expansion obtained by adding expansions of monomial products; hence

$$V\big(f(x)\,g(x)\big) \geq V\big(f(x)\big) + V\big(g(x)\big). \tag{10}$$

To show that the equality holds, choose t and u as the largest integers with

$$V\big(f_t(x)\,\phi^t\big) = V\big(f(x)\big), \qquad V\big(g_u(x)\,\phi^u\big) = V\big(g(x)\big)$$

respectively. The monomial case then shows[‡] that the expansion of $f(x)\,g(x)$ has a term $r(x)\,\phi^{t+u}$ with the value $V\big(f\big) + V\big(g\big)$. The equality holds in (10), and Theorem 4.2 is established. □

5. Properties of augmented values. An augmented value V is never less than the original value W. This characteristic property will now be established. As a consequence the method used to compute V can be extended (Theorem 5.2) in a way subsequently useful in §12.

Theorem 5.1 (*Monotonicity*)**.** *The augmented value* $V = [\,W,\ V(\phi) = \mu\,]$ *makes*

$$V\big(f(x)\big) \geq W\big(f(x)\big)$$

for all polynomials $f(x) \neq 0$*. The inequality sign holds if and only if* $\phi \parallel_W f$*. In particular, the equality sign holds whenever the degree of* $\phi(x)$ *exceeds that of* $f(x)$*.*

Proof. The proof is by induction on the degree m of the expansion of $f(x)$ in ϕ (see §4, (2)). If $m = 0$, the definition of V shows $V\big(f(x)\big)$ and $W\big(f(x)\big)$ equal. If $m > 0$, the quotient-remainder expression

$$f(x) = q(x)\,\phi + r(x) \tag{1}$$

indicates that $q(x)$ has an expansion of degree $m-1$ in ϕ; hence the induction assumption will be

$$V\big(q(x)\big) \geq W\big(q(x)\big).$$

The value of the first term on the right of (1), by §4, (1), and the quotient-remainder Lemma 4.3, is

$$V\big(q(x)\,\phi\big) \geq W\big(q(x)\big) + V(\phi) > W\big(q(x)\,\phi\big) \geq W\big(f(x)\big).$$

[‡]The details here omitted are given in Rella's proof.

For the second term, the case $m = 0$ and Lemma 4.3 imply

$$V\big(r(x)\big) = W\big(r(x)\big) \geq W\big(f(x)\big),$$

where the inequality holds if and only if $\phi \parallel_W f$. The strong triangle law for V applied to (1) now gives the result (see §2, (2)). □

Theorem 5.2. *If in the expression*

$$a(x) = a_n(x)\,\phi^n + a_{n-1}(x)\,\phi^{n-1} + \cdots + a_0(x)$$

the degrees of the $a_i(x)$ are not limited, but $\phi \nparallel_W a_i$ for $i = 0, \ldots, n$ and $a_i \neq 0$, then the augmented value $V = [\,W,\, V(\phi) = \mu\,]$ is

$$V\big(a(x)\big) = \min_i \big[\,W(a_i) + i\mu\,\big] \qquad (i = 0, \ldots, n).$$

Proof. A quotient-remainder expression for each coefficient polynomial gives

$$a_i(x) = q_i(x)\,\phi + r_i(x) \qquad (i = 0, \ldots, n),$$

$$a(x) = \textstyle\sum_{i=0}^{n} q_i(x)\,\phi^{i+1} + \sum_{i=0}^{n} r_i(x)\,\phi^i.$$

Lemma 4.3 shows that the second summation has a value

$$V\big(\textstyle\sum_i r_i\,\phi^i\big) = \min_i \big[\,W(r_i) + i\mu\,\big] = \min_i \big[\,W(a_i) + i\mu\,\big]$$

and that the first summation has a larger value

$$V\big(\textstyle\sum_i q_i\,\phi^{i+1}\big) \geq \min_i \big[\,V(q_i) + V(\phi) + i\mu\,\big] > \min_i \big[\,W(q_i) + W(\phi) + i\mu\,\big],$$

because of the monotonicity. The strong triangle law for the sum of these two summations yields the desired conclusion. □

6. Inductive and limit-values.

This section classifies the values and value-groups obtained by successive augmented values.

Definition 6.1. A kth stage inductive value V_k is any value of $K[x]$ obtained by a sequence of values $V_1, V_2, \ldots, V_k$, where $V_1 = [\,V_0,\, V_1(x) = \mu_1\,]$ is a first stage value (§3) and where each V_i is obtained by augmenting V_{i-1}:

$$V_i = [\,V_{i-1},\, V_i(\phi_i) = \mu_i\,] \qquad (i = 2, 3, \ldots, k).$$

Furthermore, for $i = 2, \ldots, k$, the key polynomials $\phi_i(x)$ must satisfy: *

(1) $$\deg \phi_i(x) \geq \deg \phi_{i-1}(x);$$

(2) $$\phi_i(x) \not\approx_{V_{i-1}} \phi_{i-1}(x).$$

Here the first key polynomial is understood to be $\phi_1(x) = x$.

*These conditions involve no loss of generality, but simplify subsequent proofs (see Theorem 6.7 and the end of §9).

The value V_k may be conveniently symbolized thus:

(3) $$V_k = [\,V_0,\, V_1(\phi_1) = \mu_1,\, V_2(\phi_2) = \mu_2,\, V_3(\phi_3) = \mu_3,\, \ldots,\, V_k(\phi_k) = \mu_k\,].$$

Given an infinite sequence $V_1, V_2, \ldots, V_k, \ldots$ of such values, we set

(4) $$V_\infty\big(f(x)\big) = \lim_{k\to\infty} V_k\big(f(x)\big).$$

The monotonic character of V_k indicates that this limit, if not finite, is $+\infty$. V_∞ satisfies the product law for values, as can be shown by taking limits in the product law for V_k. As for the sum $f(x) + g(x)$, note that the triangle law in V_k indicates that one of the inequalities

$$V_k\big(f(x) + g(x)\big) \geq V_k\big(f(x)\big), \qquad V_k\big(f(x) + g(x)\big) \geq V_k\big(g(x)\big)$$

holds for infintely many k. One of the conclusions

$$V_\infty\big(f(x) + g(x)\big) \geq V_\infty\big(f(x)\big), \qquad V_\infty\big(f(x) + g(x)\big) \geq V_\infty\big(g(x)\big)$$

then results, and thence follows the triangle law for V_∞. We have

Theorem 6.2. *Let $\{\phi_k(x)\}$ and $\{\mu_k\}$ be fixed infinite sequences such that all the functions V_k indicated in (3) are inductive values. Then the function $V_\infty\big(f(x)\big)$ defined in (4) is a value of $K[x]$, provided some polynomials not zero be allowed to have the value $+\infty$.*

This function V_∞ will be called a *limit-value*. The case when several successive key polynomials have the same degree will often require separate treatment, based on

Lemma 6.3. *If in the inductive value V_k in (3) the key polynomials $\phi_{t+1}(x)$, $\phi_{t+2}(x), \ldots, \phi_k(x)$ all have the same degree, for t with $0 \leq t \leq k-1$, then*

(i) $V_t(\phi_{j+1} - \phi_j) = \mu_j \qquad (j = t+1, t+2, \ldots, k-1),$

(ii) $\mu_k > \mu_{k-1} > \cdots > \mu_{t+1},$

(iii) $V_t(\phi_k) = V_t(\phi_{k-1}) = \cdots = V_t(\phi_{t+1}) \qquad$ (*if* $t > 0$).

Proof. Let j range from $t+1$ to $k-1$, and set

(5) $$s_j(x) = \phi_{j+1}(x) - \phi_j(x).$$

Since both ϕ's have the first coefficient 1, the degree of $s_j(x)$ is less than that of $\phi_j(x)$. Therefore, by Theorem 5.1,

$$V_t\big(s_j(x)\big) = V_{t+1}\big(s_j(x)\big) = \cdots = V_k\big(s_j(x)\big).$$

If the first conclusion were false for some j, we would have

$$V_t\big(s_j(x)\big) = V_j(\phi_{j+1} - \phi_j) > \mu_j = V_j(\phi_j),$$

for the other inequality is impossible by Lemma 4.3. This would give

$$\phi_{j+1} \approx_{V_j} \phi_j,$$

a contradiction of assumption (2). The conclusion (i) is thus established. Coupled with the monotonicity and the triangle axiom for (5), it gives the second conclusion, for

$$\mu_{j+1} = V_{j+1}\big(\phi_{j+1}\big) > V_j\big(\phi_{j+1}\big) \geq \min\big\{\, V_j(\phi_j),\, V_t(s_j)\,\big\} = \mu_j.$$

For similar reasons, assuming now that $t > 0$,

$$V_t\big(s_j(x)\big) = \mu_j = V_j(\phi_j) > V_{j-1}(\phi_j) \geq V_t(\phi_j).$$

The strong triangle axiom for V_t in (5) then yields conclusion (iii),

$$V_t(\phi_{j+1}) = \min\big\{\, V_t\big(s_j(x)\big),\, V_t(\phi_j)\,\big\} = V_t(\phi_j). \qquad \square$$

An interesting consequence of this lemma is the invariance of the values assigned to the key polynomials.

Theorem 6.4. *If the ith stage of the inductive value V_k in* (3) *uses a key polynomial ϕ_i with an assigned value μ_i, then*

$$V_k\big(\phi_i(x)\big) = V_i\big(\phi_i(x)\big) = \mu_i.$$

For this conclusion follows directly from Theorem 5.1 if the degree of $\phi_{i+1}(x)$, and hence that of every subsequent key polynomial, exceeds the degree of $\phi_i(x)$. The only case remaining is that of Lemma 6.3, with $t = i - 1$. But, by (5),

$$\phi_i = \phi_k - s_{k-1}(x) - s_{k-2}(x) - \cdots - s_i(x).$$

The terms on the right have by the preceding lemma the V_k values μ_k, $\mu_{k-1}, \ldots, \mu_i$ respectively, so that the conclusion follows by the strong triangle law. Both this theorem and Lemma 6.3 hold equally well for limit-values.

The monotonic property of inductive values can be sharpened thus:

Theorem 6.5. *Let a limit or inductive value be built up by the inductive values $V_1, V_2, \ldots$. Then, for any fixed polynomial $f(x) \neq 0$, either*

$$V_{k+1}\big(f(x)\big) > V_k\big(f(x)\big) \qquad (k = 1, 2, \ldots),$$

or else there is an $i \geq 1$ such that

$$V_1\big(f(x)\big) < V_2\big(f(x)\big) < \cdots < V_{i-1}\big(f(x)\big) = V_i\big(f(x)\big) = V_{i+1}\big(f(x)\big) = V_{i+2}\big(f(x)\big) = \cdots.$$

In the latter case there is an $r(x)$ of degree less than that of ϕ_{i+1} with

$$f(x) \approx_{V_k} r(x) \qquad (k = i+1,\, i+2,\, \ldots).$$

Suppose, contrary to the first alternative, that for some i

$$V_{i+1}\big(f(x)\big) = V_i\big(f(x)\big).$$

Then the quotient-remainder expression

$$f(x) = q(x)\,\phi_{i+1} + r(x)$$

must by Theorem 5.1 and Lemma 4.3 have $V_i(r) = V_i(f)$. Hence, for any $k \geq i+1$,

$$V_k(f - r) \geq V_{i+1}(f - r) = V_{i+1}(q\phi_{i+1}) > V_i(q\phi_{i+1}) \geq V_i(f) = V_i(r) = V_k(r).$$

Therefore $f(x) \approx_{V_k} r(x)$ and

$$V_k(f) = V_k(r) = V_i(r) = V_i(f),$$

so that $V_i\big(f(x)\big)$ is constant for $k \geq i$, which is the second alternative.

An inductive value V_k of $K[x]$ gives by Theorem 2.1 a value for the field $K(x)$ of rational functions. This value has by §2 a value-group Γ_k, which we call the *value-group associated with* V_k. It may be determined in the following way:

Theorem 6.6. *The value V_k in* (3) *has a value-group Γ_k consisting of all real numbers of the form*

$$\nu + m_1\mu_1 + m_2\mu_2 + \cdots + m_k\mu_k,$$

where the m_i are integers and ν is an element of the value-group of the original value V_0.

That every number of Γ_k must be of this form follows by induction from the definition of the augmented value V_k. Conversely, any number of this form is by Theorem 6.4 the value in V_k of the rational function

$$b\, x^{m_1}\, \phi_2^{m_2} \cdots \phi_k^{m_k},$$

where b is a constant in K with the value ν.

For a more precise description, designate a real number μ as *commensurable* with an additive group of numbers whenever some integral multiple of μ lies in the group. Then

Theorem 6.7. *In an inductive value V_k from* (3) *every assigned value μ_i, except perhaps μ_k, is commensurable with the value-group Γ_{i-1} of the preceding value* (*the case $i = 1$ included*).

Proof. Consider the expansion in ϕ_i of the next key,

$$\phi_{i+1}(x) = f_m(x)\,\phi_i^m + f_{m-1}(x)\,\phi_i^{m-1} + \cdots + f_0(x).$$

If μ_i is not commensurable with Γ_{i-1}, no two terms here can have the same value in V_i. Only one term, say the jth, has the minimum value, and

$$\phi_{i+1}(x) \approx_{V_i} f_j(x)\,\phi_i^j.$$

By the irreducibility of ϕ_{i+1} at least one of the conditions

(6) $$\phi_{i+1} \parallel_{V_i} f_j(x),$$

(7) $$\phi_{i+1} \parallel_{V_i} \phi_i,$$

must hold. Because of the minimal property of ϕ_{i+1} the first possibility (6) contradicts the assumption (1) of Definition 6.1. For the same reasons the second possibility (7) implies that ϕ_{i+1} and ϕ_i have the same degree, while

$$s(x) = \phi_{i+1}(x) - \phi_i(x)$$

has a smaller degree. Because of (7), Lemma 4.3 applied to V_i and the key polynomial ϕ_{i+1} shows $V_i\big(s(x)\big) > V_i\big(\phi_{i+1}(x)\big)$. Hence

$$\phi_i(x) \approx_{V_i} \phi_{i+1}(x),$$

a contradiction of assumption (2). There can be no next key ϕ_{i+1}. □

7. Constant degree limit-values. A limit-value V_∞ for polynomials does not give a value for all rational functions if some of the polynomials have the value $+\infty$. Hence the problem: When is V_∞ *finite*; that is, when is $V_\infty\big(f(x)\big)$ finite for all $f(x) \neq 0$? We obtain an answer in the discrete case.

If the key polynomials $\phi_k(x)$ increase indefinitely in degree, then $V_k\big(f(x)\big)$ is by Theorem 5.1 ultimately constant for fixed $f(x)$ and V_∞ is finite. A different situation arises if the degrees of $\phi_k(x)$ are then all equal to some M for k sufficiently large. For an example of such a *constant degree limit-value*, start with the p-adic value $[\,V_0(3) = 1\,]$ for the rational field (see §1, (1)) and set

$$V_1 = [\,V_0,\, V_1(x) = 1\,],$$
$$V_k = [\,V_{k-1},\, V_k(x + 2p + p^2 + p^3 + \cdots + p^{k-1}) = k\,] \qquad (k = 2, 3, \ldots).$$

This gives a limit-value of constant degree 1. Since

$$\frac{p}{2} = 2p + p^2 + p^3 + \cdots + p^{k-1} - \frac{p^k}{2} \qquad (k > 1,\ p = 3)$$

holds by the usual methods for p-adic numbers, we find

$$V_\infty\Big(x + \frac{p}{2}\Big) = \lim_{k\to\infty} V_k\Big((x + 2p + p^2 + p^3 + \cdots + p^{k-1}) - \frac{p^k}{2}\Big) = \lim_{k\to\infty} k = \infty.$$

Hence this V_∞ is not finite.

This use of p-adic numbers suggests the general notion of a perfect ring. In any ring S with a value V, a sequence $\{a_n\}$ is a *Cauchy sequence* if $V(a_n - a_m)$ approaches ∞ with n and m. If every Cauchy sequence has a V-limit b such that $V(a_n - b)$ approaches ∞ with n, the ring S is said to be *perfect.* Any ring can be embedded in a perfect ring by the usual procedure of adjoining limits of Cauchy sequences.

Theorem 7.1 (*Finiteness criterion*)**.** *Let V_∞ be a limit-value with key polynomials $\phi_k(x)$ of constant degree M for $k > t > 0$. Extend the ring $K[x]$ with the value V_t to be a perfect ring S^*. Assume that all values of K are discrete. Then $\{\phi_k\}$ is a Cauchy sequence in V_i and has a limit ϕ in S^*. Furthermore V_∞ is finite if and only if there is no $g(x) \neq 0$ in $K[x]$ divisible in S^* by the limit ϕ.*

For V_∞ the symbolism of Theorem 6.2 may be used. Since ϕ_{t+1}, ϕ_{t+2}, … all have the same degree M, the conclusions of Lemma 6.3 on constant degree values are applicable. Each number μ_i is by Theorem 6.7 commensurable with the value-group Γ_{i-1} of V_{i-1}. Our assumption shows the original value-group Γ_0 of V_0 to be discrete, hence, by Theorem 6.6 and by induction, the group Γ_t is discrete. But Lemma 6.3 gives

(1) $$\mu_i = V_i(\phi_{i+1} - \phi_i) \in \Gamma_i \qquad (i > t);$$

hence $\Gamma_i = \Gamma_t$ for $i > t$. This lemma also shows the sequence $\{\mu_i\}$ to be monotone increasing for $i > t$; it lies in the discrete set Γ_t, hence

(2) $$\lim_{i\to\infty} \mu_i = \infty.$$

The strong triangle law combined with (1) then proves

$$V_t(\phi_{i+j} - \phi_i) = V_t\big(\textstyle\sum_{k=i}^{i+j-1}(\phi_{k+1} - \phi_k)\big) = \min_k\{\mu_k\} = \mu_i.$$

Therefore, by (2), $\{\phi_i\}$ is a Cauchy sequence with a limit ϕ in S^*. This ϕ need not be a polynomial, but, by conclusion (iii) of Lemma 6.3, $\phi \neq 0$.

Now consider the necessary condition for finiteness. If $g(x) \neq 0$ is divisible by ϕ in S^*, then

$$g(x) = h\,\phi,$$

where h is the V_i-limit of a Cauchy sequence $\{h_i(x)\}$ from $K[x]$. The usual argument for the convergence of a product shows

$$\text{(3)} \qquad \lim_{i\to\infty} V_t\big(g(x) - h_i(x)\,\phi_i(x)\big) = \infty.$$

By the triangle axiom and the monotonic property for $i > t$,

$$\text{(4)} \quad V_i(g) \geq \min\big\{\, V_i(h_i\phi_i),\, V_i(g - h_i\phi_i) \,\big\} \geq \min\big\{\, V_t(h_i) + \mu_i,\, V_t(g - h_i\phi_i) \,\big\}.$$

But $\{h_i(x)\}$ is a convergent sequence in V_i with a limit not zero, so that, as is well known, $V_t(h_i)$ is ultimately constant. Consequently (2), (3), and (4) prove

$$\text{(5)} \qquad V_\infty\big(g(x)\big) = \lim_{i\to\infty} V_i\big(g(x)\big) = \infty,$$

so that V_∞ is not a finite limit-value.

Conversely, suppose that V_∞ is not finite. Then (5) holds for some $g(x) \neq 0$. If $g(x)$ has the quotient-remainder expressions $q_i(x)\phi_i + r_i(x)$, then, by Theorem 5.1 and by Lemma 4.3,

$$V_i(g - q_i\phi_i) = V_i(r_i) = V_{i-1}(r_i) \geq V_{i-1}\big(g(x)\big) \to \infty \qquad (i > t).$$

Thus the sequence $\{q_i\phi_i\}$ converges in V_i to the limit $g(x) \neq 0$. Since $\{\phi_i\}$ already converges to the limit $\phi \neq 0$, the standard argument for the limit of a quotient $(q_i\phi_i)/\phi_i$ shows that $\{q_i\}$ must converge in V_i to some limit q in S^*, such that

$$f(x) = q\phi.$$

Hence ϕ is a factor of $f(x)$ in S^*, as asserted.

8. Completeness. We have the following theorem.

Theorem 8.1. *If every value of the field K is discrete, then every non-archimedean value W of the ring $K[x]$ can be represented either as an inductive or as a limit-value.*

Given W, we shall construct by stages a corresponding inductive value V_k with the following three properties (notation as in §6, (3)):

$$\text{(1)} \qquad W\big(f(x)\big) \geq V_k\big(f(x)\big) \qquad \text{(for all } f(x)\text{)},$$

$$\text{(2)} \qquad \deg f(x) < \deg \phi_k \text{ implies } W\big(f(x)\big) = V_k\big(f(x)\big),$$

$$\text{(3)} \qquad W\big(\phi_i(x)\big) = V_k\big(\phi_i(x)\big) = \mu_i \qquad (i = 1,\, 2,\, \ldots,\, k).$$

The initial value V_1 is defined by

$$\mu_1 = W(x), \qquad V_0(a) = W(a) \qquad \text{(any } a \in K\text{)};$$

the triangle axiom for W and the definition of V_1 in §1, (2), then show that conditions (1), (2), and (3) hold for $k = 1$.

Suppose now that an inductive value V_k with these three properties has already been constructed, and that the equality in (1) does not always hold. As a prospective key polynomial, choose a $\psi(x)$ of smallest possible degree with the property

$$\text{(4)} \qquad W\big(\psi(x)\big) > V_k\big(\psi(x)\big).$$

Multiplication with some constant gives $\psi(x)$ the first coefficient 1. Furthermore the two statements

$$\text{(5)} \qquad W\big(f(x)\big) > V_k\big(f(x)\big),$$

$$\text{(6)} \qquad \psi(x) \parallel_{V_k} f(x),$$

are logically equivalent. For if (5) is given, and if $f(x)$ has the quotient-remainder expression $q(x)\psi + r(x)$, then

$$V_k(q\psi - f) = W(q\psi - f) \geq \min\big\{\, W(q\psi),\, W(f) \,\big\} > \min\big\{\, V_k(q\psi),\, V_k(f) \,\big\},$$

because of (2), the minimum degree choice of ψ and the induction assumption (1) for $q(x)$. Hence the strong triangle law shows $f \approx_{V_k} q\psi$, which is the conclusion (6). Conversely, if (6) holds there exist polynomials $h(x)$ and $s(x)$ with

$$f(x) = h(x)\psi + s(x), \qquad V_k\big(s(x)\big) > V_k\big(f(x)\big) = V_k\big(h(x)\psi\big).$$

Then, because of the induction assumption (1),

$$\begin{aligned} W(f) &\geq \min\big\{\, W(h\psi),\, W(s) \,\big\} \\ &\geq \min\big\{\, V_k(h) + W(\psi),\, V_k(s) \,\big\} > V_k(h) + V_k(\psi) = V_k(f), \end{aligned}$$

which gives conclusion (5). The equivalence of (5) and (6) is established.

From the equivalence one readily shows that $\psi(x)$ satisfies the Definition 4.1 of a key polynomial over the value V_k. Finally we can assign $\psi(x) = \phi_{k+1}$ the new value

$$\text{(7)} \qquad \mu_{k+1} = W(\psi) > V_k(\psi),$$

satisfying the proper inequality, and then construct the augmented value $V_{k+1} = [\,V_k,\, V_{k+1}(\phi_{k+1}) = \mu_{k+1}\,]$. This will be an inductive value if only conditions (1) and (2) of Definition 6.1 hold. By the choice of $\phi_{k+1} = \psi$ and the induction assumption (2), $\phi_k(x)$ cannot exceed $\phi_{k+1}(x)$ in degree, therefore condition (1) of §6 is true. Condition (2) of §6 could only be false if $\phi_{k+1} \approx_{V_k} \phi_k$; in other words, only if

$$V_k(\phi_k - \phi_{k+1}) > V_k(\phi_k) = V_k(\phi_{k+1}).$$

By (2), (3), and the choice of ψ in (4) this would entail

$$\begin{aligned} W(\phi_k) \geq \min\left\{ W(\phi_{k+1}),\, W(\phi_k - \phi_{k+1}) \right\} \\ > \min\left\{ V_k(\phi_{k+1}),\, V_k(\phi_k) \right\} = V_k(\phi_k) = W(\phi_k), \end{aligned}$$

a contradiction which establishes the desired condition.

The inductive value V_{k+1} thus constructed satisfies the analogues of the desired conditions (1), (2), and (3). The latter two are consequences of the definitions in (4) and (7), while (1) follows from the definition (see §4, (3)) of the augmented value V_{k+1} by the triangle axiom for W:

$$W\big(\textstyle\sum_{i=0}^m f_i(x)\psi^i\big) \geq \min_i\big(W\big(f_i(x)\big) + i\mu_{k+1}\big) = V_{k+1}\big(\textstyle\sum_{i=0}^m f_i(x)\psi^i\big).$$

The inductive construction of the value V_k associated with W is complete.

This process either will ultimately yield an inductive value V_k equal to W or will give an infinite sequence of inductive values with a limit-value V_∞ such that

$$W\big(f(x)\big) \geq V_\infty\big(f(x)\big) = \lim_{k\to\infty} V_k\big(f(x)\big) \qquad \text{(for all } f(x)\text{)}.$$

In the discrete case the first inequality sign never occurs. For suppose instead that it did hold for some $f(x)$; then since $\{V_k(f)\}$ is monotone non-decreasing,

$$W\big(f(x)\big) > V_k\big(f(x)\big) \qquad (k = 1, 2, \ldots).$$

The equivalence of (5) and (6) then implies that $\phi_{k+1}(x) \parallel_{V_k} f(x)$. Hence the monotonicity Theorem 5.1 shows

$$V_{k+1}\big(f(x)\big) > V_k\big(f(x)\big) \qquad (k = 1, 2, \ldots).$$

This cannot hold if the degrees of the key polynomials $\phi_k(x)$ increase indefinitely, so that we have the case where $\phi_k(x)$ has the fixed degree M for $k > t$, as in Theorem 7.1. The monotonic increasing sequence $\{V_k\big(f(x)\big)\}$ consists of numbers all from the discrete group Γ_t, with the result

$$W\big(f(x)\big) \geq V_\infty\big(f(x)\big) = \lim_{k\to\infty} V_k\big(f(x)\big) = \infty.$$

This can occur only for $f(x) = 0$, a trivial case. Accordingly, $W = V_\infty$, and the completeness theorem is established.

9. Properties of key polynomials. To apply the preceding construction of values to any particular case it is necessary to know what polynomials can be used as key polynomials. This question is not constructively answered by the definition in §4. Part of this question will be answered at once (Theorem 9.4); the rest after the structure of the inductive values V_k has been more explicitly formulated. We first show that certain polynomials act like "equivalence-units":

Lemma 9.1. *If V_k is an inductive value with $k > 1$, then for every polynomial $b(x)$ with $V_k\big(b(x)\big) = V_{k-1}\big(b(x)\big)$ there is a polynomial $b'(x)$ with*

(1) $$b'(x)\, b(x) \approx_{V_k} 1, \qquad V_k\big(b'(x)\big) = V_{k-1}\big(b'(x)\big).$$

The hypothesis on $b(x)$ implies that $b(x)$ is not divisible by the last key polynomial $\phi_k(x)$. Since ϕ_k is certainly irreducible in the ordinary sense, there are polynomials $b'(x)$ and $c(x)$ with

$$b'(x)\, b(x) + c(x)\, \phi_k(x) = 1, \qquad \deg b'(x) < \deg \phi_k(x).$$

By Theorem 5.1, $V_k(b') = V_{k-1}(b')$. The transition from V_{k-1} to V_k increases the value of $c\phi_k$, but leaves unchanged the values of $b'\,b$ and 1 in this equation. Hence $b'\,b \approx_{V_k} 1$, as in (1).

Lemma 9.2. *In any inductive V_k, the last key polynomial ϕ_k is equivalence-irreducible in V_k; a polynomial $g(x)$ with $\phi_k \nparallel_{V_k} g(x)$ has a value $V_k(g)$ in Γ_{k-1}.*

Proof. If a polynomial $f(x)$ has the expansion

(2) $$f(x) = f_n(x)\, \phi_k^n + f_{n-1}(x)\, \phi_k^{n-1} + \cdots + f_0(x), \qquad \deg f_i(x) < \deg \phi_k(x),$$

then $\phi_k \parallel_{V_k} f(x)$ if and only if $V_k(f_0) > V_k(f)$. For if $V_k(f_0) > V_k(f)$, then $f - f_0$ is a polynomial equivalent to f with a factor ϕ_k. Conversely, if $f \approx_{V_k} h(x)\phi_k$, then the last term f_0 of the expansion for f is obtained from $f - h\phi_k$, where $V_k(f - h\phi_k) > V(f)$, so that $V_k(f_0) > V_k(f)$. In particular, if $\phi_k \nparallel_{V_k} f$ then $V_k(f) = V_k(f_0) = V_{k-1}(f_0) \in \Gamma_{k-1}$, as asserted.

This criterion shows ϕ_k equivalence-irreducible in V_k. For suppose instead that $\phi_k \parallel_{V_k} fg$, although neither factor is so divisible. Then the criterion gives $V_k(f_0) = V_k(f)$, $V_k(g_0) = V_k(g)$, where $g_0(x)$ is the last term in the expansion for g. The last term in the expansion for fg is the remainder $r_0(x)$ obtained by dividing $f_0 g_0$ by ϕ_k; but since $\phi_k \nparallel_{V_{k-1}} f_0 g_0$, Lemma 4.3 shows

$$V_k(r_0) = V_{k-1}(r_0) = V_{k-1}(f_0 g_0) = V_k(f_0) + V_k(g_0) = V_k(fg).$$

This means that $\phi_k \nparallel_{V_k} fg$, a contradiction proving the lemma. □

An inductive value V_k will be called *commensurable* if the value μ_k assigned the last key polynomial is commensurable with the previous value-group Γ_{k-1} (cf. Theorem 6.7). There is then a smallest positive integer τ_k such that $\tau_k\mu_k$ is in Γ_{k-1}. For each $t \le k$ there is a similar τ_t:

(3) τ_t is the smallest integer such that $\tau_t\mu_t \in \Gamma_{t-1}$.

We will subsequently need polynomials with any given values:

Lemma 9.3. *If V_k is a commensurable inductive value, then for any real number λ in the value-group Γ_k of V_k there is a polynomial $R_\lambda = R_\lambda(x)$ with value λ in V_k and in every value V_{k+1} obtained by augmenting V_k.*

Proof. As in Theorem 6.6, λ has the form

$$\lambda = \nu + m_1\mu_1 + m_2\mu_2 + \cdots + m_k\mu_k, \qquad \nu \in \Gamma_0.$$

Each integer m_k may be made non-negative by adding to $m_i\mu_i$ and subtracting from ν a sufficiently large term $q\mu_i$, so chosen that $q\mu_i \in \Gamma_0$ (e.g., choose $q \equiv 0$ (mod $\tau_1, \tau_2, \ldots, \tau_i$)). If then a is a constant of value ν,

$$R_\lambda = R_\lambda(x) = a\,x^{m_1}\,\phi_2^{m_2}\,\phi_3^{m_3}\cdots\phi_k^{m_k}, \qquad V_k(R_\lambda) = \lambda, \qquad m_k \ge 0,$$

is the required polynomial. In any augmented value V_{k+1}, R_λ has value λ by Theorem 6.4. □

Theorem 9.4. *A polynomial $f(x)$ is a key polynomial for an inductive value over V_k if and only if the following conditions hold:*

(i) *the expansion* (2) *has a last term with $V_k(f) = V_k(f_0)$;*

(ii) *the expansion has a first term $f_n(x)\phi_k^n$ with $f_n(x) = 1$, $V_k(\phi_k^n) = V_k(f)$, and $n \equiv 0$ (mod τ_k);*

(iii) *$f(x)$ is equivalence-irreducible in V_k.*

Proof. Condition (i) means, as in the proof of Lemma 9.2, that $\phi_k(x) \nmid\!\!\mid_{V_k} f(x)$. Assume first that $f(x)$ is a key. Condition (iii) is necessary by definition. Were (i) false, then $V_k(f) < V_k(f_0)$, so that $f \approx_{V_k} (f - f_0)$, while (2) shows $f - f_0 = q(x)\phi_k$ for a $q(x)$ of degree less than $f(x)$. Thus $f \approx_{V_k} q\phi_k$. Since f is a key, this leads to a contradiction much as in the proof of Theorem 6.7. The assumption $V_k(f_0) \ne V_k(f)$ is false.

Since $f(x)$ is minimal (Definition 4.1) it has no equivalence-multiples of degree less than itself. Hence $f_n(x)$ is a constant in K, for otherwise $k > 1$, and Lemma 9.1 supplies a $b'(x)$ with $b'(x)f_n(x) \approx_{V_k} 1$. The product $b'(x)f(x)$ formed from (2) and modified by replacing the first coefficient by 1 and by reducing the other coefficients modulo ϕ_k is then an equivalence-multiple of $f(x)$. Its degree is $n \deg \phi_k$, and is less than that of $f(x)$ unless $f_n(x) \in K$. As the leading coefficient of f must be 1, $f_n(x) = 1$ follows, as in (ii). Certainly $V_k(\phi_k^n) = V_k(f)$ is necessary, for otherwise $f - \phi_k^n$ is an equivalent polynomial of smaller degree. Thus

$$V_k(\phi_k^n) = V_k(f) = V_k(f_0) = V_{k-1}(f_0) \in \Gamma_{k-1},$$

so that $n \equiv 0$ (mod τ_k) by (3). This establishes the necessity of (ii).

Conversely, if $f(x)$ satisfies (i), (ii), and (iii), it has first coefficient 1 and is minimal, because any equivalence-multiple of $f(x)$ must be of degree at least n in ϕ_k (cf. the proof of Theorem 4.2). The remaining restrictions of Definition 6.1 are readily verified, so that $f(x)$ is in fact a key polynomial. □

10. Residue-class fields. The structure of a ring S with a value V involves the corresponding *value-ring* S^+, which consists of all elements a of S with $V(a) \ge 0$ (these elements are the so-called "integers" of S). A *congruence* for integers can be defined thus

(1) $a \equiv b \pmod V$ if and only if $V(a - b) > 0$.

All elements of S^+ congruent to a given b form a *residue-class*; these classes together yield as usual the *residue-class ring* of V in S. This ring can also be considered as the residue-class ring S^+/P, where P, the set of all elements of S^+ with positive value, is a prime ideal in S^+. If S is a field, then S^+/P is also a field, the *residue-class field* of V in S. The structure of V depends essentially on this residue-class field. For the p-adic value V_0 of the rational numbers (see §1, (1)) this field is simply the field of integers modulo p. Our problem is the determination of the residue-class field for any discrete inductive value.

If the residue-class of each integer a be denoted by $[\![a]\!]$, then $H : a \mapsto [\![a]\!]$ is a homomorphism of S^+ to the residue-class ring $\Delta = S^+/P$, so that H has the following properties:

I. H is a many-one correspondence between S^+ and Δ;

II. H leaves sums and products unchanged; i.e., for $V(a) \ge 0$ and $V(b) \ge 0$:

(2) $[\![a + b]\!] = [\![a]\!] + [\![b]\!]; \qquad [\![ab]\!] = [\![a]\!][\![b]\!].$

III. If $V(a) \ge 0$, then $[\![a]\!] = [\![0]\!]$ if and only if $V(a) > 0$.

By II, the last condition means that H carries congruent elements and only congruent elements into the same residue-class.

For an inductive value V_k we denote the residue-class rings thus, for $t = 1, 2, \ldots, k$:

(3) Λ_t is the residue-class field of V_t in $K(x)$;

(4) H_t is the homomorphism from $K(x)^+$ to Λ_t;

(5) Δ_t is the residue-class ring of V_t in $K[x]$.

But $f(x)$ and $g(x)$ are congruent as polynomials (mod V_t) if and only if they are congruent as rational functions (mod V_t). Hence each residue-class of Δ_t is contained in a residue-class of Λ_t, and no two residue-classes of Δ_t are contained in the same class of Λ_t. Addition and multiplication of classes are defined as addition and multiplication on elements in the classes, and hence are the same in Δ_t as in Λ_t. Therefore Δ_t is isomorphic to a subring of Λ_t. Since isomorphism does not alter the structure of a ring, we will *replace Δ_t henceforth by the isomorphic subring of Λ_t*. Then the H_t of (4) is also the homomorphism from $K[x]^+$ to Δ_t.

The correspondence H_t for rational functions is usually determined by the H_t for polynomials. For if $f(x)/g(x) \neq 0$ is a rational function with non-negative value and if V_t is commensurable, there is by Lemma 9.3 a polynomial $g^{\flat_t}(x)$ with $V_t(g^{\flat_t}) = -V_t(g)$, and by (2)

$$(6) \qquad \left[\!\!\left[\frac{f(x)}{g(x)} \right]\!\!\right]_t = \left[\!\!\left[\frac{g^{\flat_t} f}{g^{\flat_t} g} \right]\!\!\right]_t = \frac{[\![g^{\flat_t} f]\!]_t}{[\![g^{\flat_t} g]\!]_t}.$$

Both $[\![g^{\flat_t} f]\!]_t$ and $[\![g^{\flat_t} g]\!]_t$ are residue-classes of polynomials, while $[\![g^{\flat_t} g]\!]_t \neq [\![0]\!]_t$ by Property III. We have proved

Lemma 10.1. *For a commensurable V_k, the residue-class field Λ_k of $K(x)$ is the quotient-field of the residue-class ring Δ_k of $K[x]$.*

Theorem 10.2. *For a commensurable first stage inductive value*

$$V_1 = [\, V_0,\, V_1(x) = \mu_1 \,],$$

the residue-class ring Δ_1 is isomorphic to the ring $F_0[y]$ of all polynomials in a variable y with coefficients in F_0, the residue-class field of the value V_0 for K.

Proof. There is given a homomorphism H_0 from the ring K^+ of all V_0-integers b in K to the residue-class field F_0. Each residue-class $[\![b]\!]_1$ of Δ_1 contains the residue-class $[\![b]\!]_0$ of F_0, and this correspondence $[\![b]\!]_1 \longleftrightarrow [\![b]\!]_0$ is an isomorphism between F_0 and the set of those classes of Δ_1 containing elements of K. We will identify F_0 with this isomorphic subfield of Δ_1; then Δ_1 is an extension of F_0 and $[\![b]\!]_1 = [\![b]\!]_0$ for all b in K^+.

Any monomial bx^n of value zero has $V_0(b) = -nV_1(x) = -n\mu_1$, so that the exponent n is a multiple of the integer τ_1, defined in §9, (3). Any $f(x)$ with $V_1(f) \geq 0$ thus has the form

$$f(x) \equiv b_m x^{m\tau_1} + b_{m-1} x^{(m-1)\tau_1} + \cdots + b_1 x^{\tau_1} + b_0 \pmod{V_1}$$

after terms of positive value are omitted. If e is a constant in K of value $V_0(e) = \tau_1\mu_1$, each term $b_j x^{j\tau_1}$ may be rewritten as a product $(b_j e^j)(e^{-j} x^{j\tau_1})$ of two factors of value 0. The application of the homomorphism H_1 then yields

$$(7) \qquad [\![f(x)]\!]_1 = \sum_{j=0}^{m} [\![b_j e^j]\!]_0\, y^j; \qquad y = [\![e^{-1} x^{\tau_1}]\!]_1.$$

With y so defined, any $[\![f]\!]_1$ in Δ_1 becomes a polynomial in y with coefficients $[\![b_j e^j]\!]_0$ in F_0, so that the residue-class ring Δ_1 is contained in $F_0[y]$. Since $y \in \Delta_1$ and Δ_1 is a ring, $\Delta_1 = F_0[y]$. The element y is transcendental (i.e., a variable) over F_0, for otherwise it would satisfy an algebraic relationship $\alpha(y) = [\![0]\!]_1$, where

$$\alpha(y) = \alpha_m\, y^m + \alpha_{m-1}\, y^{m-1} + \cdots + \alpha_0; \qquad \alpha_m \neq [\![0]\!]_1, \qquad \alpha_j \in F_0.$$

Then the residue-class $\alpha(y)$ contains the polynomial

$$f(x) = a_m\, e^{-m}\, x^{m\tau_1} + a_{m-1}\, e^{-m+1}\, x^{(m-1)\tau_1} + \cdots + a_0,$$

where each a_j is a constant with $[\![a_j]\!]_0 = \alpha_j$. Then $V_1(f) \geq 0$ and $[\![f]\!]_1 = \alpha(y) = [\![0]\!]_1$, so that, by Property III of H_1, $V_1(f) > 0$. But $\alpha_m \neq [\![0]\!]_1$, so that $V_0(a_m) = 0$ and $V_1(a_m e^{-m} x^{m\tau_1}) = V_1(f) = 0$, a contradiction. The theorem is established. We note also that (7) enables us to calculate the residue-class of any given $f(x)$. □

11. Conditions for equivalence-irreducibility. If ϕ_{k+1} is a key polynomial over a value V_k then $\phi_k \nparallel_{V_k} \phi_{k+1}$ (Theorem 9.4, condition (i)). For any $f(x)$ with this property, questions of equivalence-divisibility can be handled as follows:

Lemma 11.1. *In a commensurable V_k let $f(x)$ be a polynomial with $\phi_k \nparallel_{V_k} f$, and choose a polynomial $f^{\flat_k}(x)$ so that $V_{k-1}(f^{\flat_k}) = V_k(f^{\flat_k}) = -V_k(f)$. Then a polynomial $g(x)$ with $V_k(g) = 0$ satisfies $f \parallel_{V_k} g$ if and only if $[\![g]\!]_k$ is divisible by $[\![f^{\flat_k} f]\!]_k$ in the residue-class ring Δ_k.*

By Lemma 9.2, $V_k(f)$ is in Γ_{k-1}, so Lemma 9.3 yields the $f^{\flat_k}$ desired, and $[\![f^{\flat_k} f]\!]_k \neq [\![0]\!]_k$. Suppose first that $[\![g]\!]_k$ (which is not $[\![0]\!]_k$ by Property III of H_k) is divisible by $[\![f^{\flat_k} f]\!]_k$. Then $[\![g]\!]_k = \alpha [\![f^{\flat_k} f]\!]_k$ for some residue-class $\alpha = [\![h(x)]\!]_k \neq [\![0]\!]_k$ in Δ_k, and

$$[\![g]\!]_k = \alpha\, [\![f^{\flat_k} f]\!]_k = [\![h]\!]_k\, [\![f^{\flat_k} f]\!]_k = [\![h f^{\flat_k} f]\!]_k.$$

Thus g and $hf^{\flat_k}f$ have the same residue-class, $V_k(g - hf^{\flat_k}f) > 0 = V_k(g)$, so $g \approx_{V_k} hf^{\flat_k}f$ and $f \parallel_{V_k} g$, as asserted.

Conversely, if $f \parallel_{V_k} g$, then $g \approx_{V_k} hf \approx_{V_k} hf^{\sharp_k}f^{\flat_k}f$, where $f^{\sharp_k}(x)$ is a polynomial chosen as in Lemma 9.1 so that $f^{\flat_k}f^{\sharp_k} \approx_{V_k} 1$. But $f^{\flat_k}f$, g, and hence $hf^{\sharp_k}$ have value 0, so that

$$g \approx_{V_k} hf^{\sharp_k}f^{\flat_k}f; \qquad [\![g]\!]_k = [\![hf^{\sharp_k}]\!]_k \, [\![f^{\flat_k}f]\!]_k,$$

which shows $[\![g]\!]_k$ divisible by $[\![f^{\flat_k}f]\!]_k$.

Lemma 11.2. *For f and $f^{\flat_k}$ as in Lemma 11.1, $f(x)$ is equivalence-irreducible in V_k if and only if every product in Δ_k divisible by $[\![f^{\flat_k}f]\!]_k$ has* a factor divisible by $[\![f^{\flat_k}f]\!]_k$ in Δ_k.*

Proof. Suppose first that f is equivalence-irreducible and that $[\![g]\!]_k [\![h]\!]_k = [\![gh]\!]_k$ is a multiple of $[\![f^{\flat_k}f]\!]_k$. As we can assume $V_k(g) = V_k(h) = 0$, the previous lemma shows the product gh equivalence-divisible by the equivalence-irreducible f, so that one of the factors is so divisible. By Lemma 11.1 this means that $[\![g]\!]_k$ or $[\![h]\!]_k$ is a multiple of $[\![f^{\flat_k}f]\!]_k$, as asserted in the lemma.

Conversely, suppose that every product $[\![g]\!]_k \, [\![h]\!]_k$ divisible by $[\![f^{\flat_k}f]\!]_k$ has a factor so divisible, and consider a product $a(x)\, b(x)$ with $f \parallel_{V_k} ab$, so that $ab \approx_{V_k} c(x) f$ for some c. Write $a(x) \approx_{V_k} g(x)\, \phi_k^d$ and $b(x) \approx_{V_k} h(x)\, \phi_k^e$, where the powers d and e are chosen so large that $\phi_k \nparallel_{V_k} g$ and $\phi_k \nparallel_{V_k} h$. Then $V_k(g)$ and $V_k(h)$ are by Lemma 9.2 in Γ_{k-1}, so that there are polynomials $g^{\flat_k}(x)$ and $h^{\flat_k}(x)$ with $V_k(g^{\flat_k}g) = V_k(h^{\flat_k}h) = 0$. Then

$$g^{\flat_k}\, h^{\flat_k}\, a\, b \approx_{V_k} (g^{\flat_k}\, g)\, (h^{\flat_k}\, h)\, \phi_k^{d+e} \approx_{V_k} g^{\flat_k}\, h^{\flat_k}\, c\, f.$$

But $\phi_k \nparallel_{V_k} f$, while ϕ_k is equivalence-irreducible (Lemma 9.2), so

$$\phi_k^{d+e} \parallel_{V_k} g^{\flat_k}\, h^{\flat_k}\, c.$$

Removal of the factor ϕ_k^{d+e} gives $f \parallel_{V_k} (g^{\flat_k}\, g)\, (h^{\flat_k}\, h)$, so that as in the previous lemma $[\![g^{\flat_k}g]\!]_k [\![h^{\flat_k}h]\!]_k$ is divisible by $[\![f^{\flat_k}f]\!]_k$. One of the factors, say $[\![g^{\flat_k}g]\!]_k$, is then divisible by $[\![f^{\flat_k}f]\!]_k$, and (Lemma 11.1) $f \parallel_{V_k} g^{\flat_k}\, g$. But $a \approx_{V_k} g^{\sharp_k}\, (g^{\flat_k}\, g)\, \phi_k^d$, where $g^{\sharp_k}$ is chosen so that $g^{\sharp_k}\, g^{\flat_k} \approx_{V_k} 1$. Hence $f \parallel_{V_k} a(x)$, and f is equivalence-irreducible. □

*That is, the principal ideal $([\![f^{\flat_k}f]\!]_k)$ is a prime ideal in Δ_k.

12. Residue-class rings for commensurable values.

We have

Theorem 12.1. *If V_k is a commensurable inductive value of $K[x]$, given as in §6, (3), and if the original value V_0 of K has a residue-class field F_0, then there is a sequence of fields $F_1 = F_0, F_2, F_3, \ldots, F_k$, each an algebraic extension of the preceding, such that for any $t = 1, \ldots, k$ the V_t-residue-class ring of $K[x]$ is (isomorphic to) the ring $F_t[y]$ of polynomials in a variable y with coefficients in F_t. For $t > 1$ the degree m_t of F_t is determined by* (cf. §9, (3))

$$m_t \tau_{t-1} \deg \phi_{t-1} = \deg \phi_t; \qquad m_t = \deg[\, F_t : F_{t-1} \,].$$

By Lemma 10.1 we can then conclude at once

Corollary 12.2. *$F_t(y)$ is the V_t-residue-class field of $K(x)$.*

Proof of Theorem. The case $t = 1$ of this theorem is known (Theorem 10.2); hence we use induction, and assume the theorem true for V_t. It is convenient to omit the subscript $t+1$ (but not the subscript t) and to write V, ϕ, H, τ, etc., for V_{t+1}, ϕ_{t+1}, H_{t+1}, τ_{t+1}, etc. By the monotonic character of V (Theorem 5.1) polynomials $f(x)$ and $g(x)$ with $V_t(f) \geq 0$ and $V_t(g) \geq 0$ are congruent mod V_t only if they are congruent mod V. Each residue-class mod V_t is thus contained in a residue-class mod V, and this gives a homomorphism between $\Delta_t = F_t[y]$ and a subring F of the residue-class ring Δ (cf. §10, (5)), where $F = F_{t+1}$ *is composed of all residue-classes* mod V *containing an $f(x)$ with $V_t(f) \geq 0$*. Polynomials f and g incongruent mod V_t become congruent mod V if and only if $\phi_{t+1} \parallel_{V_t} f - g$ (Theorem 5.1). This means that $[\![f]\!]_t - [\![g]\!]_t$ is divisible by the polynomial

(1) $$\psi_{t+1}(y) = \psi(y) = [\![\phi^{\flat_t}\phi]\!]_t;$$
$$\big(V_{t-1}(\phi^{\flat_t}) = V_t(\phi^{\flat_t}) = -V_t(\phi),\, \phi^{\flat_t} = \phi_{t+1}^{\flat_t}(x)\big),$$

constructed as in Lemma 11.1. Since not all polynomials are equivalence-divisible by ϕ in V_t, $\psi(y)$ is not a constant in F_t, while Lemma 11.2 shows $\psi(y)$ an irreducible polynomial in $F_t[y]$. In the above homomorphism between $F_t[y]$ and F the mutiples of $\psi(y)$ in $F_t[y]$ are the elements corresponding to $[\![0]\!]$, so that F is isomorphic to the ring of polynomials $F_t[y]$ modulo $\psi(y)$, or, alternatively, to the field obtained by adjoining to F_t a root θ of $\psi(y)$. We identify F with this isomorphic field:

(2) $$F = F_{t+1} = F_t(\theta); \qquad \psi(\theta) = 0 \qquad (\theta = \theta_{t+1}).$$

Then the residue-class $[\![f]\!]_t$, when reduced modulo $\psi(y)$, will be identical to the residue-class $[\![f]\!]$; that is,

(3) $$V_t\big(f(x)\big) \geq 0 \text{ implies } [\![f]\!] = [\![f]\!]_t\big|_{y=\theta}.$$

A monomial expansion $a(x)\phi^n$ of value 0 must have n a multiple of τ (cf. §9, (3)). Hence any $f(x)$ with $V(f) \geq 0$ has the form

$$(4)\quad f(x) \equiv f_m(x)\phi^{m\tau} + f_{m-1}(x)\phi^{(m-1)\tau} + \cdots + f_0(x) \pmod V, \qquad \deg f_i < \deg \phi.$$

Since $V(\phi^\tau) \in \Gamma_t$, there are by Lemmas 9.1 and 9.3 polynomials $\phi^{\tau\sharp}(x)$ and $\phi^{\tau\flat}(x)$ such that

$$(5)\quad V_t(\phi^{\tau\sharp}) = V(\phi^{\tau\sharp}) = V(\phi^\tau), \quad \phi^{\tau\sharp}\phi^{\tau\flat} \equiv 1 \pmod V, \qquad V_t(\phi^{\tau\flat}) = V(\phi^{\tau\flat}) = -V(\phi^\tau).$$

The terms $f_i\phi^{i\tau}$ in (4) can be rewritten as products $(f_j\,\phi^{\tau\sharp j})(\phi^{j\tau}(\phi^{\tau\sharp})^{-j})$, where $V_t(f_j\,\phi^{\tau\sharp j}) \geq 0$ and $V(\phi^{j\tau}(\phi^{\tau\sharp})^{-j}) = 0$, the former because $V(f) \geq 0$. The application of H, with (3), then proves

$$(6)\quad [\![f(x)]\!] = \sum_{j=0}^{m} [\![f_j(x)\,\phi^{\tau\sharp j}]\!]_t\big|_{y=\theta}\, y_1^j; \qquad y_1 = [\![\phi^\tau(\phi^{\tau\sharp})^{-1}]\!].$$

This shows that every $[\![f]\!]$ in the residue-class ring Δ is also in $F[y_1]$, while by (5), $y_1 = [\![\phi^\tau(\phi^{\tau\sharp})^{-1}]\!] = [\![\phi^\tau\phi^{\tau\flat}]\!]$ is a residue-class of a polynomial, hence is in Δ. Consequently, $F[y_1] = \Delta$, as asserted in the theorem.

The element y_1 is transcendental over F; for suppose instead that y_1 satisfied an algebraic relation $\alpha(y_1) = [\![0]\!]$, with

$$\alpha(y_1) = \alpha_m\, y_1^m + \alpha_{m-1}\, y_1^{m-1} + \cdots + \alpha_0; \qquad \alpha_m \neq [\![0]\!], \qquad \alpha_j \in F.$$

By the original (italicized) definition of F each residue-class α_j of F contains a polynomial $b_j(x)$ with $V_t(b_j) \geq 0$, so that $[\![b_j]\!] = \alpha_j$. Then

$$f(x) = \sum_{j=0}^{m} b_j(x)\,\phi^{\tau\flat j}\phi^{j\tau} \equiv \sum_{j=0}^{m} b_j(x)\,(\phi^{\tau\sharp})^{-j}\phi^{j\tau} \qquad (\text{in } V)$$

is a polynomial of non-negative value which has $[\![f]\!] = \alpha(y_1) = [\![0]\!]$. By Property III of H, $V(f) > 0$. On the other hand $V(f)$ must equal 0, for $[\![b_m]\!] = \alpha_m \neq [\![0]\!]$ gives $V(b_m) = 0$ and $V(f) \leq V(b_m(\phi^{\tau\sharp})^{-m}\phi^{m\tau}) = 0$, by Theorem 5.2. This contradiction shows y_1 a variable over F.

The formula (6) enables us to calculate $[\![f(x)]\!]$ effectively for any $f(x)$ given in (4), provided only that $V_t(f_j\,\phi^{\tau\sharp j}) \geq 0$ for all j.

It remains to determine the degree of the field F over F_t, which by (2) is the degree of $\psi(y)$. The key ϕ has by Theorem 9.4 an expansion of the form

$$(7)\quad \phi = \phi_t^{m\tau_t} + \sum_{i=0}^{m\tau_t - 1} a_i(x)\phi_t^i, \qquad V_t(\phi) = V_t(\phi_t^{m\tau_t}) = V_t(a_0).$$

If $t > 1$, $\psi = [\![\phi^{\flat_t}\phi]\!]_t$ can be computed by the analog of (6) for the preceding stage (with t in (6) replaced by $t-1$), for the coefficients $\phi^{\flat_t}a_i$ must by the choice of $\phi^{\flat_t}$ have $V_{t-1}(\phi^{\flat_t}a_i) \geq 0$. This calculation shows $\psi(y)$ to be a polynomial in y with a first term $[\![\phi^{\flat_t}\phi_t^{\tau_t\sharp_t m}]\!]_t\, y^m$ arising from the first term of (7). But

$$V_t(\phi^{\flat_t}\phi_t^{\tau_t\sharp_t m}) = V_t(\phi^{\flat_t}) + V_t(\phi_t^{\tau_t\sharp_t m}) = -V_t(\phi) + V_t(\phi_t^{m\tau_t}) = 0,$$

so that the coefficient of y^m is not $[\![0]\!]$. The polynomial ψ has degree m, and by (7)

$$m\tau_t \deg\phi_t = \deg\phi, \qquad m = \deg\psi = \deg[\,F : F_t\,],$$

as asserted* in Theorem 12.1. This theorem has now been demonstrated. □

13. Conditions for key polynomials. In the criterion of Theorem 9.4 for a key polynomial the condition (iii) of equivalence-irreducibility can now be replaced by the condition of Lemma 11.2,

(iiia), $\quad [\![f^{\flat_k}f]\!]_k$ is an irreducible polynomial in $F_k[y]$.

This yields a final explicit description of key polynomials. A partial converse is possible:

Theorem 13.1. *In a given V_k, let $\psi(y) \neq y$ be a polynomial† of degree $m > 0$, irreducible in $F_k[y]$ and with first coefficient* 1. *Then there is one and, except for equivalent polynomials in V_k, only one $\phi(x)$ which is a key polynomial and which has $[\![\phi_k^{\tau_k\flat_k m}\phi]\!]_k = \psi(y)$.*

Proof. There is a polynomial $f(x)$ with the residue-class ψ, so that $[\![f]\!]_k = \psi$ and $V_k(f) = 0$. If we multiply f by $\phi_k^{\tau_k\sharp_k m}$ (chosen as in §12, (5)) and in the expansion of the resulting product drop all terms not of minimum value and then replace the leading coefficient of ϕ_k by 1, we obtain a polynomial $\phi(x)$ with the value $V_k(\phi_k^{\tau_k\sharp_k m})$. Then

$$[\![\phi_k^{\tau_k\flat_k m}\phi]\!]_k = [\![\phi_k^{\tau_k\flat_k m}\phi_k^{\tau_k\sharp_k m}f]\!]_k = [\![f]\!]_k = \psi(y).$$

Furthermore ϕ can be shown to satisfy the remaining conditions (i) and (ii) of Theorem 9.4, hence ϕ is a key polynomial. The uniqueness is readily established. □

*The proof given holds for $t > 1$, but may be simplified for the case $t = 1$.

†The assumption $\psi(y) \neq y$ is needed, for the condition $V_k(f) = V_k(f_0)$ in Theorem 9.4 implies $[\![f^{\flat_k}f]\!]_k \neq y$.

Since $[\![f^{\flat_k} f]\!]_k$ can be effectively constructed by §12, (6), the problem of testing whether a given $f(x)$ is a key polynomial is reduced to that of testing the image $[\![f^{\flat_k} f]\!]_k$ of $f(x)$ for irreducibility in $F_k[y]$. If K is the field of rationals, then F_k is a finite field and the latter problem is completely solvable. This result can be used to construct examples for inductive values of any stage and for limit-values of both constant degree[‡] and increasing degree types. The construction of constant degree values may be simplified by deducing from Theorem 9.4 the following partial converse of Lemma 6.3:

Corollary 13.2. *In V_k let $s(x)$ be a polynomial of degree less than that of $\phi_k(x)$ and with $V_k\big(s(x)\big) = V_k(\phi_k)$. Then $\phi_k(x) + s(x)$ is a key polynomial for an inductive value over V_k.*

14. Special cases of homomorphism.

The residue-class fields can be similarly found for finite discrete limit-values and for inductive values where the value for K is trivial (§2) or where the last assigned value μ_k is incommensurable (§6).

Theorem 14.1. *Let V_∞ be a limit-value constructed as in Theorem 6.1 from a sequence of values $V_0, V_1, V_2, \ldots,$ and satisfying one of the conditions:*

(a) *the degrees of the keys ϕ_k are not bounded as $k \to \infty$;*

(b) *V_∞ is finite and discrete, and $\deg \phi_k = M$ for all $k > t$.*

The fields F_k of Theorem 12.1 yield a (possibly infinite) extension field $F_\infty = F_0 + F_1 + F_2 + \cdots$ which is isomorphic to the V_∞ residue-class field both for $K[x]$ and for $K(x)$. In case (b), $F_\infty = F_{t+1}$.

Let H_k be the homomorphism of $K[x]$ to the V_k residue-class ring $F_k[y]$ and H_∞ the homomorphism of $K[x]$ to the V_∞ residue-class ring Δ_∞. Then

$$(1) \qquad V_{k-1}\big(f(x)\big) \geq 0 \text{ implies that } [\![f]\!]_{k+j} = [\![f]\!]_k \in F_k \qquad (j = 1, 2, \ldots).$$

For, according to §12, (3),

$$[\![f]\!]_k = [\![f]\!]_{k-1}\big|_{y=\theta_k}, \qquad [\![f]\!]_{k+1} = [\![f]\!]_k\big|_{y=\theta_{k+1}},$$

which indicates that $[\![f]\!]_k$ is a constant free of y in F_k, and that $[\![f]\!]_{k+1}$ must equal $[\![f]\!]_k$, and so on.

In case (a) there is for every $f(x)$ a k so large that $\deg \phi_k > \deg f$, so that $V_\infty(f) = V_{k-1}(f)$, as in Theorem 5.1. If $V_\infty(f) \geq 0$, then, by (1), $[\![f]\!]_{k+j} = [\![f]\!]_k$ is a constant in F_k independent of j.

[‡] By using a transcendental p-adic number the finiteness condition of §7 can be satisfied.

The correspondence

$$(2) \qquad [\![f]\!]_\infty \longleftrightarrow [\![f]\!]_k, \quad \text{for } k \text{ with } [\![f]\!]_k = [\![f]\!]_{k+1} = [\![f]\!]_{k+2} = \cdots,$$

carries each element of Δ_∞ into an element of F_∞. Every element α of F_∞ is used, for, by the definition of F_∞, α is in some F_k so that α has the form $[\![f]\!]_k$, and $[\![f]\!]_{k+j} = [\![f]\!]_k$ as in (1), whence α corresponds in (2) to $[\![f]\!]_k$. The correspondence (2) is one-to-one, for elements are congruent mod V_∞ if and only if they are congruent modulo some V_k. Finally, (2) is an isomorphism, making $F_\infty \cong \Delta_\infty$, as asserted. The residue-class field of $K(x)$ is, by the argument of Lemmas 9.3 and 10.1, just the quotient field of F_∞, and must then be F_∞ itself.

In the case (b), the degrees of the extensions $F_{k+1} : F_k$ as determined in Theorem 12.1 are all 1 for $k > t$. Hence $F_k = F_{t+1}$. Because V_∞ is finite (§7) and discrete, Theorem 6.5 yields for any $f(x)$ with $V_\infty(f) \geq 0$ an $i \geq t$ so large that $V_\infty(f) = V_i(f) \geq 0$. Then $[\![f]\!]_k$ is again ultimately constant, and (2) gives the isomorphism as before.

Theorem 14.2. *For an incommensurable inductive value V_k of $K(x)$ the field F_k determined from F_{k-1} and ϕ_k exactly as in §12 is the V_k residue-class field of both $K[x]$ and $K(x)$.*

Proof. Since no non-zero multiple of $\mu_k = V_k(\phi_k)$ lies in Γ_{k-1}, no two terms in a ϕ_k-expansion can have the same value in V_k. Hence any polynomial is equivalent to a monomial expansion, and every rational function has by Lemma 9.1 the form

$$f(x)/g(x) \approx_{V_k} c(x)\phi_k^m, \qquad V_k(c) = V_{k-1}(c).$$

If f/g has value 0, then $m = 0$, $V_{k-1}(c) \geq 0$, and $[\![f/g]\!]_k = [\![c]\!]_k$. But F_k is defined in §12, italics (or, for $k = 1$, in §10) as all residue-classes $[\![h]\!]_k$ with $V_{k-1}(h) \geq 0$. In this case every residue-class has this form, so that F_k is as asserted the whole residue-class field, either for $K[x]$ or for $K(x)$. □

In particular, over the trivial value V_0 (§2) of K the only non-trivial inductive values are

$$V_1 = [\, V_0,\, V_1(x) = \mu_1 \,], \qquad \mu_1 \neq 0;$$

$$V_2 = [\, V_0,\, V_1(x) = 0,\, V_2(\phi) = \mu_2 \,], \qquad \mu_2 > 0, \;\; \phi(x) \text{ irreducible.}$$

Both are incommensurable (no multiple of μ_2 lies in the group Γ_0, which contains only 0). Furthermore, the residue-class field of K for the trivial V_0 is K itself. Hence the residue-class field for V_1 is K and for V_2 is $K(\theta)$, where θ is a root of $\phi(x)$.

15. Equality conditions for values. An inductive value is essentially a representation; the same value of $K[x]$ could easily have several such representations. This section and the next one will formulate necessary and sufficient conditions for the equality of two inductive or limit-values. In this connection two values V and W of a ring S will be called equal if an only if

$$V(a) = W(a) \qquad \text{(all } a \in S). \tag{1}$$

In this section we consider the case when each key polynomial ϕ_k exceeds the preceding ϕ_{k-1} in degree — a case which can often be made to apply by omitting any ϕ_{k-1} without the above property.

Lemma 15.1. *If an inductive value*

$$V_k = [\,V_{k-2},\, V_{k-1}(\phi_{k-1}) = \mu_{k-1},\, V_k(\phi_k) = \mu_k\,] \qquad (k \geq 2)$$

has two key polynomials $\phi_{k-1}(x)$ and $\phi_k(x)$ of the same degree, then

$$W = [\,V_{k-2},\, W(\phi_k) = \mu_k\,]$$

is an inductive value equal to V_k.

We first prove W an inductive value. Since ϕ_k exceeds $\phi_k - \phi_{k-1}$ in degree, the constant-degree Lemma 6.3 shows that

$$V_{k-2}(\phi_k - \phi_{k-1}) = V_{k-1}(\phi_k - \phi_{k-1}) = \mu_{k-1}, \quad \mu_k > \mu_{k-1} > V_{k-2}(\phi_{k-1}). \tag{2}$$

A combination of these two results proves

$$\phi_k \approx_{V_{k-2}} \phi_{k-1}. \tag{3}$$

Thus ϕ_k and ϕ_{k-1} have the same equivalence-divisibility properties in V_{k-2}, and so ϕ_k, like ϕ_{k-1}, is a key polynomial over V_{k-2}. By (2) and (3) the value $\mu_k > V_{k-2}(\phi_k)$ assigned to ϕ_k is sufficiently large. Therefore W is inductive, for conditions (1) and (2) of Definition 6.1 hold trivially. The definition of augmented values applied to the usual expansion (e.g., §9, (2)) of any $f(x)$ in powers of ϕ_k gives

$$V_k\big(f(x)\big) = \min_i \{\, V_{k-1}\big(f_i(x)\big) + i\mu_k \,\}, \;\; W\big(f(x)\big) = \min_i \{\, V_{k-2}\big(f_i(x)\big) + i\mu_k \,\}.$$

The corresponding terms $V_{k-1}(f_i)$ and $V_{k-2}(f_i)$ are equal by Theorem 5.1, for each $V_i(x)$ has a degree less than that of ϕ_k or of ϕ_{k-1}. Therefore $V_k = W$. Successive applications of this lemma give

Theorem 15.2. *Any inductive value is equal to an inductive value in which $\{\deg \phi_k\}$ is a monotone increasing sequence. A similar representation holds for any limit-value not of constant-degree type.*

For values in this particular form we can obtain necessary and sufficient conditions for equality.

Theorem 15.3. *If the two inductive values*

$$V_s = [\,V_0, \;\; V_1(x) = \mu_1, \;\; V_2(\phi_2) = \mu_2, \;\ldots,\; V_s(\phi_s) = \mu_s\,] \tag{4}$$

$$W_t = [\,W_0, W_1(x) = \nu_1, \; W_2(\psi_2) = \nu_2, \;\ldots, W_s(\psi_t) = \nu_t\,] \tag{5}$$

both have a monotone character such that

$$1 < \deg \phi_2 < \cdots < \deg \phi_s, \qquad 1 < \deg \psi_2 < \cdots < \deg \psi_t,$$

then $V_s = W_t$ holds if and only if

(i) $V_0 = W_0, \quad s = t;$

(ii) $\deg \phi_k(x) = \deg \psi_k(x) \qquad (k = 1, \ldots, t);$

(iii) $V_{k-1}(\psi_k - \phi_k) \geq \mu_k = \nu_k \qquad (k = 1, \ldots, t).$

The theorem is still true if either s or t is $+\infty$.

First prove the sufficiency of these conditions. Since (i) and (iii) make V_1 and W_1 identical, we can proceed by induction, assuming that $V_{k-1} = W_{k-1}$ is already established. Now compute the V_k value of ψ_k. Because key polynomials have the leading coefficient unity, (ii) shows that the degree of ϕ_k exceeds that of $\psi_k - \phi_k$, so that ψ_k has the expansion

$$\psi_k = \phi_k + (\psi_k - \phi_k) \tag{6}$$

in powers of ϕ_k. The definition of V_k and (iii) prove

$$V_k(\psi_i) = \min \{\, \mu_k,\, V_{k-1}(\psi_k - \phi_k)\,\} = \mu_k = \nu_k.$$

The V_k value of any polynomial $f(x)$ can now be estimated from the expansion of $f(x)$ in ψ_k, for the triangle axiom for V_k gives

$$\begin{aligned} V_k\big(\textstyle\sum_{j=0}^n f_j \psi_k^j\big) &\geq \min_j \{\, V_{k-1}(f_j) + jV_k(\psi_k)\,\} \\ &= \min_j \{\, V_{k-1}(f_j) + j\nu_k \,\} = W_k(f), \end{aligned}$$

because of the definition of W_k. Thus $V_k(f) \geq W_k(f)$, while the inverse inequality is similarly proved. Hence $V_k = W_k$, and the induction is complete.

The necessity of the conditions depends chiefly on the invariance of the values assigned the key polynomials (Theorem 6.4). The assumption $V_s = W_t$ shows that $V_0 = W_0$ and $\mu_1 = \nu_1$. Hence (ii) and (iii) hold for $k = 1$. We prove them by induction on k. If they hold through $k-1$, then the sufficiency proof shows $V_{k-1} = W_{k-1}$. By Theorem 5.1, $\deg \phi_k$ can be characterized as the smallest degree of any polynomial $a(x)$ with the property that $V_s(a) > V_{k-1}(a)$. Since V_s and W_t are equal, $\deg \psi_k$ can be characterized by the same statement, so that

$$\deg \phi_k(x) = \deg \psi_k(x). \tag{7}$$

The monotonic assumption on $\{\deg \phi_k\}$ then shows $V_s(\psi_k) = V_k(\psi_k)$. Hence, because of the invariance in W of the value assigned to ψ_k,

$$\nu_k = W_t(\psi_k) = V_s(\psi_k) = V_k\big(\phi_k + (\psi_k - \phi_k)\big).$$

As before, (6) is an expansion in powers of ϕ_k, so that this equation becomes

$$\nu_k = \min\{\, \mu_k,\, V_{k-1}(\psi_k - \phi_k)\,\}.$$

Combining this with the symmetric conclusion (using $V_{k-1} = W_{k-1}$)

$$\mu_k = \min\{\, \nu_k,\, V_{k-1}(\psi_k - \phi_k)\,\}.$$

we obtain (iii) for index k. With (7) this completes the induction. The condition $s = t$ results, even in the case $s = t = \infty$.

16. Normal forms for values. The results of the previous section do not apply to constant degree limit values, nor do they yield unique normal forms. Both these goals can be reached in the discrete case by using key polynomials from which all unnecessary high-valued terms have been dropped.

In the expansion of any $f(x)$ in a value V_k, the coefficient $f_i(x)$ of any power of ϕ_k can itself be expanded in powers of ϕ_{k-1}. Since the degree of $f_i(x)$ is limited, the highest power of ϕ_{k-1} occurring is less than n_k/n_{k-1}, where n_i has the meaning

$$n_i = \deg \phi_i(x) \qquad (i = 1, \ldots, k). \tag{1}$$

By an inductive process of this sort one can prove

Theorem 16.1. *In any V_k every polynomial $f(x)$ can be expanded as a polynomial in the key polynomials with constant coefficients,*

$$f(x) = \sum\nolimits_j a_j \phi_1^{m_{1j}} \phi_2^{m_{2j}} \cdots \phi_k^{m_{kj}}, \qquad (a_j \in K), \tag{2}$$

where the exponents m_{ij} are limited as follows

$$m_{ij} < n_{i+1}/n_i \qquad (\text{all } j;\ i = 1, 2, \ldots, k-1). \tag{3}$$

The value of $f(x)$, when computed from the definition, is

$$V_k\big(f(x)\big) = \min\nolimits_j \{\, V_k\big(a_j\, \phi_1^{m_{1j}} \cdots \phi_k^{m_{kj}}\big)\,\}. \tag{4}$$

For a p-adic value, every number is equivalent to one of the numbers cp^m, $c = 0, 1, \ldots, p-1$. For any value V_0 of a field K we can similarly (axiom of choice) pick from each class of equivalent elements a single representative element; in particular, we can make 1 one of the representatives. Given fixed representatives of this sort for each V_0, we say that a polynomial $f(x)$ is *homogeneous* in a value V_k derived from V_0 if in the expansion (2) of $f(x)$ all the coefficients a_j are representatives in V_0 and all the terms have the same minimum value $V_k\big(f(x)\big)$.

Lemma 16.2. *If $f(x)$ is a polynomial then $f(x) \approx_{V_k} h(x)$ for a unique homogeneous polynomial $h(x)$. This $h(x)$ is called the "homogeneous part" of $f(x)$.*

Proof. Given $f(x)$, we find $h(x)$ by altering coefficients and dropping out terms in the expansion (2) for f. Were $f(x)$ also equivalent to a homogeneous $g(x)$, then all terms in the expansions of both $h(x)$ and $g(x)$ would have the same value $V_k(h)$, while $h - g$ would have a larger value. Thus corresponding coefficients are equivalent and therefore equal. □

An inductive or limit value $V_k = [\,V_0,\, V_i(\phi_i) = \mu_i\,]$ may be called *homogeneous* if every key polynomial $\phi_i(x)$ is homogeneous in V_{i-1} $(i = 2, \ldots, k)$. We will prove

Theorem 16.3. *Any inductive or limit-value constructed from a discrete value V_0 of K is equal to a homogeneous inductive or limit-value.*

We have to prove that, if $U = [\,V_k,\, U(\phi) = \mu\,]$ is an augmented value over a homogeneous value V_k, then U itself is equal to a homogeneous inductive value. This is done by introducing successive homogeneous parts of ϕ as new keys. First use $\psi_1(x)$, the homogeneous part of ϕ in V_k. By Lemma 16.2

$$\psi_1(x) \approx_{V_k} \phi(x), \qquad \deg \psi_1(x) = \deg \phi(x). \tag{5}$$

It follows that $\psi_1(x)$ is a key polynomial over V_k. Setting

$$\nu_1 = V_k\big(\phi(x) - \psi_1(x)\big) > V_k\big(\psi_1(x)\big),$$

we can construct a homogeneous value $W_1 = [\,V_k,\, W_1(\psi_1) = \nu_1\,]$. If $\mu \le \nu_1$, then the sufficiency proof of Theorem 15.3 shows $U = W_1$. Otherwise $\mu > \nu_1$, and Corollary 13.2 proves $W' = [\,W_1,\, W'(\phi) = \mu\,]$ an inductive value, which by Lemma 15.1 is equal to U. We repeat the above argument, constructing a W_2 from $\psi_2(x)$, the principal part of ϕ in W_1. This gives a sequence of homogeneous inductive values,

$$W_1 = [\,V_k,\, W_1(\psi_1) = \nu_1,\, W_2(\psi_2) = \nu_2,\, \ldots,\, W_t(\psi_t) = \nu_t\,] \qquad (i = 1, 2, \ldots).$$

The degrees of the $\psi(x)$ are all identical by (5), so that Lemma 6.3 proves that

$$\nu_1 < \nu_2 < \nu_3 < \cdots \tag{6}$$

and that each ν_i is in the value-group Γ_k of V_k. By hypothesis and Theorem 6.7, this Γ_k is discrete. Hence there is a smallest t with $\nu_t \geq \mu$ in (6), and U is equal to the homogeneous value W_t. The advantage of so representing every value in a homogeneous form lies in the following uniqueness theorem:

Theorem 16.4. *Two homogeneous inductive or limit-values which are equal must be identical.*

Proof. If the equal values are V_s and W_t as in §15, (4) and (5), then the asserted identity means simply that

$$V_0 = W_0, \qquad s = t, \tag{7}$$

$$\phi_k = \psi_k, \qquad \mu_k = \nu_k \qquad (k = 1,\, 2,\, \ldots,\, s). \tag{8}$$

The hypotheses readily give $V_0 = W_0$ and (8) for $k = 1$.

Suppose (8) true up to $k-1$ inclusive. Then $V_{k-1} = W_{k-1}$. We can assume $s > k-1$, whence also $t > k-1$. Then ϕ_k has the following invariant properties which refer only to $V_{k-1} = W_{k-1}$ and $V_s = W_t$: ϕ_k is totally homogeneous in V_{k-1}, it has the first coefficient 1 and it has the minimum degree consistent with the property $V_s(\phi_k) > V_{k-1}(\phi_k)$. Furthermore ψ_k has the same properties. But these properties uniquely determine ϕ_k, for, since the difference $\phi_k - \psi_k$ is of degree less than ϕ_k, its value is

$$\begin{aligned} V_{k-1}(\phi_k - \psi_k) &= V_s(\phi_k - \psi_k) \\ &\geq \min\{\, V_s(\phi_k),\, V_s(\psi_k)\,\} > \min\{\, V_{k-1}(\phi_k),\, V_{k-1}(\psi_k)\,\}. \end{aligned}$$

Hence by the triangle law $\phi_k \approx_{V_{k-1}} \psi_k$, so that by Lemma 16.2, $\phi_k = \psi_k$. By Theorem 6.4, $\mu_k = \nu_k$, as in (8). The induction ends when k reaches $s = t$, and the identity $V_s \equiv W_t$ is proved. □

A simple consequence is

Corollary 16.5. *If every value of K is discrete, then no inductive value can ever equal a limit-value, and no limit-value of constant degree type* (§7) *can equal a limit-value not of this type.*

Bibliography

Papers on irreducibility:

(1846) Th. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, Journal für die Mathematik **32** 93–105, §61.

(1850) G. Eisenstein, *Über die Irreduztibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, Journal für die Mathematik **39** 166.

(1895) L. Königsberger, *Über den Eisensteinschen Satz von der Irreduzibilität algebraischer Gleichungen*, Journal für die Mathematik **115** 53–78; especially (67) on p 69.

(1905) M. Bauer, *Verallgemeinerung eines Satzes von Schönemann*, Journal für die Mathematik **128** 87–89.

(1906) G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, Journal de Mathématiques Pures et Appliquées (6) **2** 191–258.

(1907) O. Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, Journal für die Mathematik **132** 304.

(1916) H. Blumberg, *On the factorization of expressions of various types*, Transactions of the American Mathematical Society **17** 517–544.

(1923) J. Kürschák, *Irreduzible Formen*, Journal für die Mathematik **152** 180–191.

(1923) Ø. Ore, *Zur Theorie der Irreduzibilitätskriterien*, Mathematische Zeitschrift **18** 278–288.

(1924) Ø. Ore, *Zur Theorie der Eisensteinischen Gleichungen*, Mathematische Zeitschrift **20** 267–279.

(1927) T. Rella, *Ordnungsbestimmungen in Integritätsbereichen und Newtonische Polygone*, Journal für die Mathematik **158** 33–48.

Papers on absolute values:

(1912) J. Kürschák, *Limesbildung und allgemeine Körpertheorie*, Journal für die Mathematik **142** 211–253.

(1917) A. Ostrowski, *Über einige Lösingen der Funktionalgleichung $\phi(x)\cdot\phi(y) = \phi(xy)$*, Acta Mathematica **41** 217–284.

(1930) W. Krull, *Idealtheorie in unendlichen algebraischen Zahlkörpern* II, Mathematische Zeitschrift **31** 527–557.

(1932) W. Krull, *Allgemeine Bewertungstheorie*, Journal für die Mathematik **167** 161–196.

(1933) H. Hasse and F. K. Schmidt, *Die Struktur diskret bewerter Körper*, Journal für die Mathematik **170** 4–63.

(1934) A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper*, Mathematische Zeitschrift **39** 269–404.

(1935) S. MacLane, *Abstract absolute values which give new irreducibility criteria*, Proceedings of the National Academy of Sciences **21** 272–274.

(1936) S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society **40**(3) 363–395.

(1936) S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2** 492–510.