A CONSTRUCTION FOR PRIME IDEALS AS ABSOLUTE VALUES OF AN ALGEBRAIC FIELD

By Saunders MacLane

1. Introduction. The difficulties of actually constructing the prime ideal factors of a rational prime p in an algebraic field have had a considerable influence upon the development of ideal theory. One of the most practical of the methods for this construction consists of three successive "approximations" to the prime factors of p in terms of certain Newton Polygons, similar to the polygons used in the expansion of algebraic functions. This method, due to Ore,[1] is directly applicable in all but certain exceptional cases. The present paper extends the method to all cases by making not three but any number of successive approximations. To formulate this extension simply, it is necessary to replace the prime ideals by certain corresponding "absolute values", which succinctly express the essential properties of the Newton polygons. In terms of these values, the successive approximations are a natural application of a method of finding possible "absolute values" for polynomials.

To introduce these absolute values, consider the ring $\mathfrak{o}$ of all algebraic integers of an algebraic number field, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{o}$. Since every integer α of the field can be written in the form $(\alpha) = \mathfrak{p}^m \cdot \mathfrak{b}$, where $\mathfrak{b}$ is an ideal prime to $\mathfrak{p}$, we can write the exact exponent m to which $\mathfrak{p}$ divides α as a function $W(\alpha) = m$. Because of the unique decomposition theorem,

$$(1) \qquad W(\alpha\cdot\beta) = W(\alpha) + W(\beta), \quad W(\alpha+\beta) \geq \min\big(W(\alpha),\, W(\beta)\big).$$

Any function $V(\alpha)$ which has these two properties is called a non-archimedean value or a "Bewertung"[2] of the ring $\mathfrak{o}$, while the particular function W obtained from $\mathfrak{p}$ may be called a $\mathfrak{p}$-adic value. Every value V of $\mathfrak{o}$ is a constant multiple[3] of some $\mathfrak{p}$-adic value W. Hence absolute values can replace prime ideals.

In the same way every non-archimedean value V_0 of the rational integers is a "p-adic" value for some rational prime p; that is, for any integer a, $V_0(a)$ is $m\delta$, where m is the highest power of p dividing a and δ is a constant > 0. If $\mathfrak{p}$ is a prime ideal factor of p in an algebraic field, every $\mathfrak{p}$-adic value W, considered only as a value of the rational integers, coincides with one of the p-adic values V_0. Thus W is an "extension" of V_0.

The equivalence of prime ideals to values enables us to state the problem of constructing the prime ideal factors of a rational prime in the following generalized form (with a notation to be used throughout the paper): *Given a field K and a separable extension $K(\theta)$ generated by a root θ of the irreducible polynomial $G(x)$; given also a "discrete" (see §2) value V_0 of K, to construct all extensions W of V_0 in $K(\theta)$.*

This problem will first be reduced in §2 to that of constructing for the ring of polynomials with coefficients in K those values V which are extensions of V_0 and which assign the defining equation $G(x)$ the value $+\infty$. All values of this polynomial ring can be constructed[4] by successive approximations, which consist essentially in determining first the values of the polynomials of lowest degree (in x and in p). The salient features of this method are summarized in §2. Those approximations which can ultimately give G the desired value $+\infty$ we call "approximants" to G (see §3). Each such approximant is itself a value V_k of the polynomial ring and can be constructed from a previous approximant V_{k-1} by using a unique "equivalence" decomposition of $G(x)$ (see §4) and a "Newton polygon" of $G(x)$ with respect to V_{k-1} (see §5). After a finite number of steps (§8) we obtain a set of approximants corresponding to the desired values or prime ideals of $K(\theta)$. The proof of this fact uses the integers of K (§7) and the exponents of prime ideals (§6). The computation of the degrees of prime ideals in §9 yields a constructive proof of the usual relation betwen degrees and exponents. Finally, the theorems of §10 summarize the results. A comparison with previous methods is also made. We note that some of the concepts resemble those used by Ostrowski[5] and by Deuring and Krull[6] in the (non-constructive) theory of Galois fields with absolute values.

2. Non-finite values of polynomial rings. A non-archimedean exponential *absolute value* of a ring S is a function V, such that, for a in S, $V(a)$ is a uniquely defined real number or $+\infty$, with the properties

$$(1) \qquad V(ab) = V(a) + V(b), \quad V(a+b) \geq \min\big(V(a),\, V(b)\big)$$

[1] Ø. Ore, *Zur Theorie der algebraischen Körper*, Acta Math, **44** (1924) 219–314; Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math Annalen, **99** (1928) 84–117. These papers will be cited as Ore I and Ore II, respectively.

[2] W. Krull, *Idealtheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd 4, Heft 3. This text, cited henceforth as Krull I, contains further references on absolute values.

[3] E. Artin, *Ueber die Bewertungen algebraischer Zahlkörper*, Jour für Math **167** (1932) 157–159. The theorem may be proved thus: Given V, first show that any rational integer $n = 1 + 1 + \cdots + 1$ has a non-negative value and then from (1) that every algebraic integer has a non-negative value. If the value of an ideal $\mathfrak{b}$ be defined as the minimum of $V(\alpha)$ for $\alpha \in \mathfrak{b}$, then one and only one prime ideal $\mathfrak{p}$ can have a positive value, and V must be $\mathfrak{p}$-adic. A similar theorem holds when $\mathfrak{o}$ is an abstract ring in which the usual prime-ideal decomposition holds. (B. L. van der Waerden, *Moderne Algebra* **2**, §100.)

[4] S. MacLane, *A construction for absolute values in polynomial rings*, to appear in the Trans Amer Math Soc. Cited henceforth as M. All theorems from M required in the sequel will be explicitly stated, so that we refer to M only for certain proofs.

[5] A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper* (Die Theorie der Teilbarkeit in allgemeinen Körpern), Math Zeit **39** (1934) 269–404.

[6] M. Deuring, *Verzweigungstheorie bewerteter Körper*, Math Ann **105** (1931) 277–307.
W. Krull, *Galoissche Theorie bewerteter Körper*, S B München Akad Wiss (1930) 225–238.

for all a and b in S. These properties are called the "product" and "triangle" laws respectively. If we exclude the trivial cases when $V(a) = 0$ for all a or $V(a) = \infty$ for all a, the laws (1) imply that $V(1) = V(-1) = 0$, that the equality in the triangle law of (1) must hold whenever $V(a) \neq V(b)$, and that $V(0) = +\infty$. Contrary to previous usage, our definition allows elements not 0 to have the value $+\infty$. However, if $V(a) \neq \infty$ for all $a \neq 0$, we shall call V a *finite* value. Since $V(a^{-1}) = -V(a)$, every value V of a field must be finite. A value V is *discrete* if every $V(a)$ is an integral multiple of some fixed $\delta > 0$. The original value V_0 of K is discrete by assumption.

Two elements a and b of S are *equivalent* in V if and only if either $V(a-b) > V(a) = V(b)$ or $V(a) = V(b) = \infty$. We write $a \approx_V b$ for this equivalence. It is a reflexive, symmetric and transitive relation. An element a is *equivalence-divisible* by b in V if and only if there is a c in S such that $a \approx_V cb$. For this divisibility we write $b \parallel_V a$.

A value V of a ring S is an *extension* of a value V_0 of a subring of S if $V(a)$ and $V_0(a)$ are identical for all a in the subring. Our original problem can now be reduced to one concerning the polynomial ring $K[x]$, which consists of all polynomials in x with coefficients in K.

Theorem 2.1. *There is a one-to-one correspondence between the values W of $K(\theta)$ and those values V of $K[x]$ for which $V\big(G(x)\big) = \infty$. Corresponding values V and W are extensions of identical values of K.*

The proof depends on the homomorphism of $K[x]$ to $K(\theta)$. If the value V with $V\big(G(x)\big) = \infty$ is given, two polynomials congruent mod $G(x)$ must have the same value, so that the value W for any $f(\theta)$ can be defined by $W\big(f(\theta)\big) = V\big(f(x)\big)$. The same equation serves to define V when W is given.

The method of the paper M for constructing finite values of $K[x]$ applies without essential change for non-finite values. It consists fundamentally in the formation of a sequence of simple values

$$V_1,\, V_2,\, V_3,\, \ldots,\, V_{k-1},\, V_k,\, \ldots. \tag{2}$$

To obtain any V_k in (2) from the preceding V_{k-1}, we assign a new value μ_k to a suitable polynomial $\phi_k = \phi_k(x)$. The following conditions[7] must hold:

2.21 ϕ_k is *equivalence-irreducible* in V_{k-1}; that is, $\phi_k \parallel_{V_{k-1}} f(x)\, g(x)$ always implies $\phi_k \parallel_{V_{k-1}} f(x)$ or $\phi_k \parallel_{V_{k-1}} g(x)$;

2.22 ϕ_k is *minimal* in V_{k-1}; that is, $\phi_k \parallel_{V_{k-1}} g(x)$ always implies that $\deg \phi_k \leq \deg g(x)$;

2.23 ϕ_k has the leading coefficient 1 and $\deg \phi_k > 0$;

2.24 $\mu_k > V_{k-1}(\phi_k)$.

When these are true, we call ϕ_k a *key polynomial* and μ_k a *key value* of ϕ_k over V_{k-1}. Given such "key" quantities the new value V_k of any polynomial $f(x)$ is determined from V_{k-1} by first finding the *expansion* of $f(x)$

$$f(x) = f_m(x)\phi_k^m + f_{m-1}(x)\phi_k^{m-1} + \cdots + f_0(x), \quad \deg f_i(x) < \deg \phi_k \tag{3}$$

in powers of $\phi_k(x)$ with coefficients of degree less than that of ϕ_k, then setting

$$V_k\big(f(x)\big) = \min\big[V_{k-1}(f_m) + m\mu_k,\, V_{k-1}(f_{m-1}) + (m-1)\mu_k,\, \ldots,\, V_{k-1}(f_0)\big]. \tag{4}$$

The so-defined function V_k is always a value of $K[x]$. We say that V_k is obtained by *augmenting* V_{k-1}, and write

$$V_k = \big[V_{k-1},\, V_k(\phi_k) = \mu_k\,\big]. \tag{5}$$

To apply the condition 2.22 it is convenient to note (M, Theorem 9.3):

2.3 The polynomial $f(x)$ with the expansion (3) is minimal in V_k if and only if $f_m(x)$ is a constant from K and $V_k\big(f(x)\big) = V_k\big(f_m(x)\phi_k^m\big)$. In particular, the product of two minimal polynomials is itself minimal.

The construction of any value V of $K[x]$ starts with a "first stage" value V_1 which is defined as in equation (4), except that the first key polynomial ϕ_1 is now taken to be x itself and μ_1 is arbitrary; while the value V_{k-1} used for the coefficients f_i, which are now constants, is simply the originally given value V_0 for K. Given such a V_1, new values can now be defined by repeatedly augmenting V_1. A sequence (2) in which each V_i arises by augmenting V_{i-1} with a pair of keys ϕ_i and μ_i from V_{i-1} is called an *augmented sequence*. Each V_k of such a sequence is an *inductive value*, and may be symbolized as

$$V_k = \big[\,V_0,\, V_1(x) = \mu_1,\, V_2(\phi_2) = \mu_2,\, \ldots,\, V_k(\phi_k) = \mu_k\,\big]. \tag{6}$$

We assume in addition the conditions (M, Definition 6.1)

2.41 $\deg \phi_i \geq \deg \phi_{i-1}$ $\qquad (i = 2,\, 3,\, \ldots);$

2.42 $\phi_i \not\approx_{V_{i-1}} \phi_{k-1}$ $\qquad (i = 2,\, 3,\, \ldots).$

[7] Functions $f(x)$, $g(x)$ or simply f and g, etc., will always represent polynomials in $K[x]$, while $\deg f(x)$ stands for the degree of $f(x)$. If $f = 0$, $\deg f$ is meaningless, and statements about $\deg f$ are taken to be vacuously true.

The last key value μ_k may be $+\infty$, but then there is no key over V_k satisfying these conditions, so that no further augmented value is possible. An infinite augmented sequence (2) also gives a limit value, defined by

$$V_\infty\big(f(x)\big) = \lim_{k\to\infty} V_k\big(f(x)\big) \qquad \text{(for all } f(x)\text{)}. \tag{7}$$

We will consider only those inductive or limit values which are extensions of the originally given V_0.

To put the values of $K[x]$ in a normal form, we first choose in K a complete set of "representatives" with respect to V_0, such that each element of K is equivalent in V_0 to one and only one representative. If next the coefficients of the expansion (3) are expanded repeatedly with respect to $\phi_{k-1}, \phi_{k-2}, \ldots$, then $f(x)$ is expressed uniquely in the form

$$f(x) = \sum\nolimits_j a_j\, \phi_1^{m_{1j}} \phi_2^{m_{2j}} \cdots \phi_k^{m_{kj}} \qquad (a_j \in K). \tag{8}$$

The exponent m_{ij} is always less than $(\deg\phi_{i+1})/(\deg\phi_i)$, for $i = 1, \ldots, k-1$ (see M, §16). If all terms in (8) have the same value in V_k, and if each a_j is one of the previously specified representatives, then $f(x)$ is in a sense *homogeneous* in V_k. Any polynomial is equivalent in V_k to a homogeneous polynomial. Henceforth we require in any inductive or limit value (6) that each ϕ_i be homogeneous in the previously constructed V_{i-1}. Then, since the given V_0 is discrete, *every extension of V_0 to $K[x]$ can be uniquely represented as an inductive or limit value* (M, §8, §16).

3. Approximants to non-finite values. Our program requires the construction of values V of $K[x]$ for which $V\big(G(x)\big) = \infty$. Any such V can be obtained from a sequence of suitable inductive values V_k. A V_k which might be so used to construct a V with $V(G) = \infty$ will be called an "approximant", in an explicit sense now to be given. This involves the way in which $V_i(G)$ increases in a sequence of inductive values V_i, $i = 1, \ldots, k$. This increase is described by M, Theorems 5.1, 6.4, and 6.5, for any $f(x)$ and any $i \neq k$:

3.11 $V_k(f) \geq V_i(f)$;

3.12 $V_k(f) > V_i(f)$ if and only if $\phi_{i+1} \parallel_{V_i} f$;

3.13 $V_k(\phi_i) = V_i(\phi_i)$, and $V_k(f) = V_i(f)$ whenever $\deg f < \deg\phi_{i+1}$.

Further analysis uses the expansion of $G(x)$ in ϕ_k:

$$G(x) = g_m(x)\,\phi_k^m + g_{m-1}(x)\,\phi_k^{m-1} + \cdots + g_0(x). \tag{1}$$

Among the exponents j for which $V_k(G) = V_k(g_j\phi_k^j)$, let α be the largest and β the smallest. The difference $\alpha - \beta$, which depends on both V_k and G, will be called the *projection* of V_k (symbol: $\operatorname{proj}_G V_k$). One application is

Lemma 3.2. *If $\operatorname{proj}_G V_k = 0$, then no V with $V(G) > V_k(G)$ can be obtained by augmenting V_k.*

Proof. The value of each term in (1) is by 3.13 the same in any V as in V_k. By hypothesis there is but one term of minimum value, so that the triangle law (§2, (1)) proves $V(G) = V(g_\alpha\phi_k^\alpha) = V_k(G)$. □

Since we want only those values V_k leading to $V(G) = \infty$, we are led to

Definition 3.3. *A k-th approximant to $G(x)$ over V_0 is a k-th stage homogeneous finite inductive value of $K[x]$ which is an extension of V_0 and which has a positive projection.*

Lemma 3.4. *If V_k, given as in §2, (6), is a k-th approximant to $G(x)$, then so is V_i for $i = 1, \ldots, k-1$. Furthermore $\phi_k \parallel_{V_{k-1}} G(x)$ and*

$$V_k\big(G(x)\big) > V_{k-1}\big(G(x)\big) > \cdots > V_1\big(G(x)\big).$$

First note that in the expansion (1) of $G(x)$

$$V_{k-1}(G) = \min\big[\,V_{k-1}(g_m\phi_k^m),\ V_{k-1}(g_{m-1}\phi_k^{m-1}),\ \ldots,\ V_{k-1}(g_0)\,\big], \tag{2}$$

much as in the definition of V_k. For were $V_{k-1}(G)$ to exceed the indicated minimum, then by the triangle law $V_{k-1}(g_i\phi_k^i)$ would equal this minimum for at least two i's. Were γ the largest such i, then

$$-g_\gamma\phi_k^\gamma \approx_{V_{k-1}} g_{\gamma-1}\phi_k^{\gamma-1} + \cdots + g_0.$$

Then ϕ_k^γ would be an equivalence-divisor of the polynomial on the right, which is of smaller degree than ϕ_k^γ, a contradiction because ϕ_k and hence ϕ_k^γ is minimal (see §2, 2.3).

By hypothesis $\operatorname{proj}_G V_k > 0$, so that there is an $\alpha > 0$ with $V_k(G) = V_k(g_\alpha\phi_k^\alpha)$. As $V_{k-1}(\phi_k) < V_k(\phi_k)$, we have by (2) and 3.13

$$V_{k-1}(G) \leq V_{k-1}(g_\alpha\phi_k^\alpha) < V_k(g_\alpha\phi_k^\alpha) = V_k(G).$$

Hence by 3.12 $\phi_k \parallel_{V_{k-1}} G$, and the remaining conclusions follow by Lemma 3.2. Another useful fact is

Lemma 3.5. *Let $a(x)$ be a minimal polynomial in V_k, and $r(x)$ the remainder of the division of a polynomial $f(x)$ by $a(x)$. Then $V_k(r) > V_k(f)$ if and only if $a(x) \parallel_{V_k} f(x)$.*

The proof is exactly like that of M, Lemma 4.3.

4. Unique equivalence-decomposition. The construction of an approximant V_{k+1} from a given approximant V_k must by Lemma 3.4 use a key polynomial ϕ_{k+1} which is an equivalence factor of $G(x)$. These factors can be found from the unique equivalence-decomposition of $G(x)$, the existence of which will now be established by a modified euclidean algorithm.[8] We first introduce for any V_k an "effective degree" thus: if $f(x)$ is any polynomial, expanded in powers of ϕ_k as in §2, (3), the largest exponent i for which $V_k(f) = V_k(f_i\phi_k^i)$ is the *effective degree* of f in ϕ_k and is denoted $D_{\phi_k}(f)$. Equivalent polynomials have the same effective degree. The proof of the product law (§2, (1)) for any inductive V_k (see M, §4, end) shows that

$$D_{\phi_k}(fg) = D_{\phi_k}(f) + D_{\phi_k}(g). \tag{1}$$

If we call a polynomial of effective degree zero an *equivalence-unit*, then $e(x)$ is an equivalence unit if and only if there is an "equivalence-reciprocal" $h(x)$ such that $e(x)h(x) \approx_{V_k} 1$. For if $e(x)$ has such a reciprocal, then (1) proves that $D_{\phi_k}(e) = 0$. Conversely, if $D_{\phi_k}(e) = 0$, then, by definition of D_{ϕ_k}, $e(x)$ is equivalent to the last term $e_0(x)$ in the expansion of e in powers of ϕ_k. As $\deg e_0 < \deg \phi_k$, e_0 is prime to ϕ_k, so that there are polynomials $g(x)$ and $h(x)$ with $g(x)\phi_k + h(x)e_0(x) = 1$. Using the minimal property of ϕ_k, we then conclude that $h(x)e(x) \approx_{V_k} 1$.

Lemma 4.1. *Any polynomial $f(x)$ can be represented as $f(x) \approx_{V_k} e(x)a(x)$, where $e(x)$ is a unit and $a(x)$ is minimal and has the first coefficient* 1. *In addition, $f(x)$ and $a(x)$ have the same equivalence-divisors.*

Proof. Expand $f(x)$ as in §2, (3), pick out the first term $f_\alpha(x)\phi_k^\alpha$ of minimum value, and find the equivalence-reciprocal $h(x)$ for the equivalence-unit $f_\alpha(x)$. Then expand the polynomial $h(x)\cdot f(x)$ and drop out all terms not of minimum value. There remains an equivalent polynomial $a(x)$, with an expansion beginning with ϕ_k^α. This $a(x)$ is minimal, and we have $f(x) \approx_{V_k} f_\alpha(x)\cdot a(x)$, as required. □

To carry out the euclidean algorithm for two polynomials $f(x)$ and $g(x)$ with $D_{\phi_k}(f) \geq D_{\phi_k}(g)$, write $g(x) \approx_{V_k} e_1(x)a_1(x)$ in accordance with Lemma 4.1 and divide $f(x)$ by $a_1(x)$, getting

$$f(x) = q(x)\cdot a_1(x) + r_2(x) \qquad D_{\phi_k}(r_2) < D_{\phi_k}(a_1). \tag{2}$$

If $V_k(r_2) > V_k(f)$, a_1 and hence g is an equivalence-divisor of f. Otherwise, since a_1 is minimal, $V_k(r_2) = V_k(f)$ and all three terms in (2) have the same value. Repeat this process with $a_1(x)$ and $r_2(x) \approx_{V_k} e_2(x)a_2(x)$, etc., until a remainder exceeding the dividend in value is obtained. The preceding remainder $d(x)$ is the greatest common equivalence-divisor of $f(x)$ and $g(x)$. As usual,

$$d(x) \approx_{V_k} s(x)f(x) + t(x)g(x) \tag{3}$$

for suitable $s(x)$ and $t(x)$. To establish (3), it is convenient to note that, unless $g(x) \parallel_{V_k} f(x)$, all the terms in (3) must be of the same value in V_k.

The properties of equivalence-irreducible polynomials are now obtained as usual from (3). A decomposition of any $f(x)$ into such irreducible factors must exist (because of D_{ϕ_k}). If we factor out a suitable unit, these irreducible factors can as in Lemma 4.1 be made minimal and hence key polynomials (§2, Conditions 2.21–2.23).

Theorem 4.2. *In an inductive value V_k every polynomial $f(x)$ has a decomposition*

$$f(x) \approx_{V_k} e(x)\,\psi_1(x)\,\psi_2(x)\cdots\psi_t(x) \tag{4}$$

where $e(x)$ is a unit and each $\psi_i(x)$ is a key polynomial. This decomposition is unique, except for the order of the factors and except that $e(x)$ may be replaced by any equivalent unit and $\psi_i(x)$ by any equivalent key.

If we require the factors $\psi_i(x)$ to be homogeneous in V_k (see §2, (8)), they are then unique. Note also that ϕ_k itself may occur as a factor, by

Lemma 4.3. *In an inductive V_k, ϕ_k is a key polynomial.*

Proof. Since ϕ_k is a key in V_{k-1}, it has the first coefficient 1. Furthermore $D_{\phi_k}(\phi_k) = 1$, hence in any factorization of ϕ_k one factor is a unit, so that ϕ_k is equivalence-irreducible. Finally, ϕ_k is minimal in V_k. □

In many cases the construction of the unique equivalence-decomposition (4) for a given polynomial $f(x)$ in a given V_k can be carried out in a finite number of steps.

Theorem 4.4. *The decomposition* (4) *is constructive when K is the field of rationals.*

The original value V_0 is then associated with a rational prime p, so that every rational number is equivalent in V_0 to one of the numbers $c\cdot p^m$, $c = 0, 1, \ldots, p-1$; $V_0(p) = 1$. Hence the complete set of representatives for V_0 (see §2, end) includes but a finite number of representatives of each possible value[9] m.

[8] A similar algorithm has been used by A. Fraenkel, *Ueber einfache Erweiterungen zerlegbarer Ringe*, Jour für Math **151** (1920) 120–166. Compare Ore I, Theorem 6.

[9] Theorem 4.4 is true for any K and V_0 with this property.

There are but a finite number of minimal homogeneous polynomials $b(x)$ of a given degree d and with first coefficient 1. For any such $b(x)$ may be expanded in powers of x, ϕ_2, …, ϕ_k as in §2, (8) with a highest coefficient 1 of value 0. Because of the homogeneity, this determines the value of every other non-zero coefficient in the expansion. Since these coefficients are representatives, there is but a finite number of possibilities for each coefficient, and hence but a finite number of polynomials $b(x)$.

If $f(x)$ is to be decomposed, write $f(x) \approx_{V_k} e(x)a(x)$ by Lemma 4.2, find all minimal homogeneous polynomials $b(x)$ of degree less than that of $a(x)$ as above and by trial find which products, if any, are equivalent to $a(x)$.

The decomposition (4) can often be constructed by first decomposing the residue-class of $f(x)$ (cf. §9 and M, part II). We can assume that all factors ϕ_k, if any, have already been removed from f. Then $V_k\bigl(f(x)\bigr)$ will be in the previous value-group Γ_{k-1} (M, Lemma 9.2), so that there is a unit polynomial $f^\flat_{V_k}(x)$ such that $V_k(f^\flat_{V_k} f) = 0$. In the value V_k the residue-class of any polynomial $g(x)$ is denoted by $[\![g]\!]_{V_k}$ and is itself a polynomial in a new variable y (M, Theorem 12.1). In particular, $[\![f^\flat_{V_k} f]\!]_{V_k}$ is a polynomial with a decomposition

$$[\![f^\flat_{V_k} f]\!]_{V_k} = \alpha_1(y)\,\alpha_2(y) \cdots \alpha_t(y) \tag{5}$$

into irreducible polynomials $\alpha_i(y)$. But there is essentially just one key polynomial $\psi_i(x)$ in V_k with the residue-class $[\![\psi'_i \psi_i]\!]_{V_k} = \alpha_i$, for a suitable unit ψ'_i (M, Theorem 13.1). Since the residue-class of a product is the product of the residue-classes

$$[\![f^\flat_{V_k} f]\!]_{V_k} = [\![\psi'_1 \psi_1 \psi'_2 \psi_2 \cdots \psi'_t \psi_t]\!]_{V_k},$$

and since polynomials in the same residue-class are congruent,

$$f^\flat_{V_k} f \equiv \psi'_1 \psi'_2 \cdots \psi'_t\, \psi_1\, \psi_2 \cdots \psi_t \pmod{V_k}.$$

If we multiply by an equivalence-reciprocal of $f^\flat_{V_k}$, we get the decomposition (4). Consequently, (4) can be constructed in this way whenever (5) can be found; that is, whenever polynomials can be constructively factored in the residue-class field of V_0 in K (see §9). In particular, this method applies when K is the field of rationals.

5. The construction of approximants. If

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

the key μ_1 of any first approximant $V_1 = [\,V_0,\, V_1(x) = \mu_1\,]$ must by Definition 3.3 be so chosen that, for suitable $\alpha > \beta$,

$$\alpha\mu_1 + V_0(a_\alpha) = \beta\mu_1 + V_0(a_\beta) \le i\mu_i + V_0(a_i) \qquad (i = 0, \ldots, n), \tag{2}$$

where the inequality holds for $i > \alpha$ or $\beta > i$. To interpret this, plot the points $P_i = \bigl(n - i, V_0(a_i)\bigr)$ in a cartesian plane. Then (2) states that the line $P_\alpha P_\beta$ has slope μ_1 and that all the points P_i are either above this line or on the line between P_α and P_β. The line segments $P_\alpha P_\beta$ with this property for some μ_1 form a convex broken line stretching from P_n to P_0. This broken line segment is called the *Newton polygon* of the points P_i, while none of the points lie below the polygon. We have shown that each first approximant V_1 corresponds to a side of this polygon of slope $\mu_1 = V_1(x)$ and of horizontal projection equal to the "projection" of V_1. Hence

$$\sum \operatorname{proj}_G V_1 = \deg G, \tag{3}$$

the sum being taken over all first approximants V_1.

Next, given any $(k-1)$-th approximant V_{k-1} we wish to construct all k-th approximants V_k which can be obtained by augmenting V_{k-1}. Consider first the "terminating case" when $G(x)$ is a homogeneous key polynomial[10] over V_{k-1}. Then by Lemma 3.4 the key polynomial ϕ_k must be an equivalence-divisor of the equivalence-irreducible $G(x)$, whence $\phi_k = G$. We obtain no finite approximants, but only the non-finite value $V_k = \bigl[\,V_{k-1},\, V_k\bigl(G(x)\bigr) = \infty\,\bigr]$, which by Theorem 2.1 corresponds to a value of $K(\theta)$.

Suppose instead that $G(x)$ is not a homogeneous key polynomial over V_{k-1}. Then by Theorem 4.2 and Lemma 4.3

$$G(x) \approx_{V_{k-1}} e(x)\,\phi_{k-1}(x)^{n_0}\,\psi_1(x)^{n_1} \cdots \psi_t(x)^{n_t}, \tag{4}$$

where the $\psi_i(x)$ are homogeneous keys over V_{k-1}, all different and different from $G(x)$ and ϕ_{k-1}, while the exponents n_i are all positive, except perhaps for n_0. An augmented V_k must have a key ϕ_k with $\phi_k \parallel_{V_{k-1}} G(x)$ (Lemma 3.4) and $\phi_k \neq \phi_{k-1}$ (§2, Condition 2.42). Hence ϕ_k is one of ψ_1, …, ψ_t.

If one of these factors ψ_i has been selected as ϕ_k, then $G(x)$ has as in §3, (1) an expansion with coefficients $g_i(x)$. To determine the new value $\mu_k = V_k(\phi_k)$ to be assigned to ϕ_k, we again use a point $Q_i = \bigl(m - i, V_{k-1}\bigl(g_i(x)\bigr)\bigr)$ for each term in the expansion and construct the Newton polygon for these points. The requirement that $\operatorname{proj}_G V_k > 0$ again means that μ_k must be the slope of some side of this polygon. An inductive value requires also that $\mu_k > V_{k-1}(\phi_k)$, so that we use only the *principal part*[11] of the polygon, composed of those sides of slope $\mu > V_{k-1}(\phi_k)$.

[10] For convenience, we assume henceforth that the first coefficient in (1) is $a_n = 1$.

[11] In special cases, this has been called a "Haputpolygon" by Ore (Ore I, p 229; Ore II, p 88) and a "verkürztes Polygon" by Rella, *Ordnungsbestimmungen in Integritätsbereichen und Newtonsche Polygone*, Jour für Math **158** (1927) 33–48.

Theorem 5.1. *If V_{k-1} is a $(k-1)$-th approximant in which $G(x)$ is not a homogeneous key, then the k-th approximants which can be derived by augmenting V_{k-1} are all values $V_k = [\, V_{k-1},\, V_k(\phi_k) = \mu_k \,]$ in which $\phi_k \neq \phi_{k-1}$ is any one of the keys in the decomposition* (4) *of $G(x)$, while, for given ϕ_k, μ_k is the slope of any side of the principal Newton polygon of $G(x)$ with respect to ϕ_k and V_{k-1}. Furthermore*

$$(5) \qquad \sum \big(\operatorname{proj}_G V_k\big) \cdot \big(\deg \phi(V_k)\big) = \big(\operatorname{proj}_G V_{k-1}\big) \cdot \big(\deg \phi(V_{k-1})\big),$$

where the sum is taken over all such augmented V_k, and where $\phi(V)$ represents the last key of V. Hence there is at least one approximant V_k from V_{k-1}.

It remains to prove (5). On the left side of (5) suppose first that ϕ_k is the factor ψ_1 in (4), and consider the power $n = n_1$ to which ϕ_k divides G. Since ϕ_k and hence ϕ_k^n is minimal in V_{k-1}, the remainder

$$r(x) = g_{n-1}\, \phi_k^{n-1} + g_{n-2}\, \phi_k^{n-2} + \cdots + g_0$$

obtained on dividing G by ϕ_k^n must by Lemma 3.5 have $V_{k-1}(r) = V_{k-1}(G)$. Calculation of $V_{k-1}(r)$ as in §3, (2) gives

$$(6) \qquad \min\big[\, V_{k-1}(g_{n-1}\phi_k^{n-1}),\, \ldots,\, V_{k-1}(g_0) \,\big] > V_{k-1}(g_n \phi_k^n) = V_{k-1}(G),$$

with the equality because n is the largest exponent with $\phi_k^n \parallel_{V_{k-1}} G$. If we set $\nu = V_{k-1}(\phi_k)$ and use §3, (2), this becomes

$$\begin{aligned} V_{k-1}(g_n) + n\nu &\leq V_{k-1}(g_j) + j\nu && (j = n+1,\, \ldots,\, m) \\ &< V_{k-1}(g_i) + i\nu && (i = 0,\, \ldots,\, n-1). \end{aligned}$$

Geometrically, this means that the line L of slope ν through the point Q_n lies above none of the points Q_j and lies below $Q_{n-1}, \ldots, Q_0$. The convex Newton polygon is hence above or on L, so that the principal polygon, containing those sides of slope exceeding ν, consists of the sides joining Q_n to Q_0. The horizontal projection of the principal polygon for $\phi_k = \psi_1$ is therefore $n = n_1$.

However, $\operatorname{proj}_G V_k$ is by definition (§3) the projection of the corresponding side of the principal polygon. Hence a sum taken over those V_k with ψ_1 as the last key gives $\sum \operatorname{proj}_G V_k = n_1$. Similar equations for all ψ_i yield

$$(7) \qquad \sum (\operatorname{proj}_G V_k) \cdot (\deg \phi_k) = n_1 \deg \psi_1 + \cdots + n_t \deg \psi_t = \deg(\psi_1^{n_1} \cdots \psi_t^{n_t}).$$

But $\psi_1^{n_1} \cdots \psi_t^{n_t}$ is minimal, so that its effective and actual degrees in $\phi = \phi_{k-1}$ must agree. Thus

$$(8) \qquad \deg(\psi_1^{n_1} \cdots \psi_t^{n_t}) = D_{\phi_{k-1}}(\psi_1^{n_1} \cdots \psi_t^{n_t}) \cdot (\deg \phi_{k-1}).$$

Because of (4) the effective degree is

$$(9) \qquad D_{\phi_{k-1}}(\psi_1^{n_1} \cdots \psi_t^{n_t}) = D_{\phi_{k-1}}(G) - D_{\phi_{k-1}}(\phi_{k-1}^{n_0}) = D_{\phi_{k-1}}(G) - n_0.$$

If the expansion of $G(x)$ is $\sum h_i(x)\phi_{k-1}^i$, then $D_{\phi_{k-1}}(G)$ is by definition the exponent of the first term of minimum value, while n_0, the highest power with $\phi_{k-1}^{n_0} \parallel_{V_{k-1}} G$, is by the argument used in (6) simply the exponent of the last term of minimum value in the expansion of $G(x)$. By the definition of the projection,

$$(10) \qquad D_{\phi_{k-1}}(G) - n_0 = \operatorname{proj}_G V_{k-1}.$$

The last four equations combine to give the result (5). By induction on k we obtain from (3) and (5) the following result.

Theorem 5.2. *If the "terminating" case does not occur by the k-th stage, there is a finite number of k-th approximants, such that*[12]

$$(11) \qquad \sum \big(\operatorname{proj}_G V_k\big) \cdot \big(\deg \phi(V_k)\big) = \deg G,$$

the sum being taken over all k-th approximants V_k.

Theorem 5.3 (Terminating case)**.** *If there is a non-finite homogeneous inductive value V_k with $V_k(G) = \infty$, then for $i < k$ the value V_i from which V_k is obtained is the only i-th approximant.*

Proof. By Lemma 3.2, V_{k-1}, and hence by Lemma 3.4 each V_i, is an approximant. Since $V_k(G) = \infty$ and G is irreducible, G must be the last key of V_k, whence G is minimal in V_{k-1} (see §2, 2.3):

$$G(x) = \phi_{k-1}^m + g_{m-1}(x)\phi_{k-1}^{m-1} + \cdots + g_0(x).$$

Since G is minimal and (§2, 2.42) $\phi_{k-1} \nparallel_{V_{k-1}} G$, the first and last terms here take on the minimum value $V_{k-1}(G)$, so that $\operatorname{proj}_G V_{k-1} = m$. Thus

$$\deg G = m \deg \phi_{k-1} = (\operatorname{proj}_G V_{k-1}) \cdot (\deg \phi_{k-1}),$$

and by (11) V_{k-1} is the only $(k-1)$-th approximant. Hence each V_i is the only i-th approximant. ☐

6. Exponents for values.

To estimate the growth of μ_k we need "value-groups". If in an algebraic number field the prime ideal $\mathfrak{p}$ is a factor of the rational prime p, and if the corresponding $\mathfrak{p}$-adic value W is an extension of the p-adic value V_0, then the highest power e to which $\mathfrak{p}$ divides p is characterized

[12] An invariant interpretation of (11) will be given in §9.

by $V_0(p) = eW(\mathfrak{p})$. Hence the group of all numbers used as p-adic values is a subgroup of index e in the group of $\mathfrak{p}$-adic values. For any value V of a ring S, the additive group Γ which contains all real numbers $V(b) - V(c)$ for b and c in S is called the *value group* of V. This group is cyclic if and only if the value V is discrete (§2). If V is an extension of V_0 to $K[x]$ or to $K(\theta)$, the value group Γ_0 of V_0 must be a subgroup of the value group Γ of V. The order of the factor group Γ/Γ_0 is called the *exponent*,[13] $\exp(V)$.

Now compute this exponent for an inductive value V_k with a value-group Γ_k. The definition of §2, (4) indicates that every number in Γ_k has the form $\gamma + n\cdot\mu_k$, where n is an integer and γ is in Γ_{k-1}. If we consider only the case when μ_k is commensurable with Γ_{k-1} (by M, Theorem 6.7, this is true whenever V_k can be augmented to some V_{k+1}), there is a unique smallest positive integer τ_k with the property that $\tau_k\mu_k \in \Gamma_{k-1}$. By group theory

(1) $$\operatorname{order}(\Gamma_k/\Gamma_{k-1}) = \tau_k,$$

(2) $$\exp(V_k) = \tau_1\cdot\tau_2\cdots\tau_k,$$

where τ_i for $i = 1, \ldots, k$ is similarly defined. The assumption that μ_k is commensurable also proves Γ_k is discrete. If $\mu_k = \infty$, the formulas still hold if we take $\tau_k = 1$.

In the course of §8 we shall need an estimate for $\exp(V_k)$. Since each key polynomial ϕ_{i+1} is homogeneous (§2) in V_i, any two terms in the expansion of ϕ_{i+1} in powers of ϕ_i must be of equal value, so that this expansion appears as a polynomial in $\phi_i^{r_i}$ (M, §11). Consequently $\deg\phi_{i+1} \geq \tau_i \deg\phi_i$. Combining these inequalities for all i, we find

(3) $$\deg\phi_k \geq \tau_1\tau_2\cdots\tau_k = \exp(V_{k-1}).$$

7. Integral key polynomials. It is often convenient to use keys with "integral" coefficients. Here an *integer*[14] with respect to V_0 is an element $a \in K$ with $V_0(a) \geq 0$. All such integers form a ring, and every element of K is a quotient of two such integers. After the usual transformations we can *assume that $G(x)$ has V_0-integers as coefficients and the first coefficient* 1. The Newton polygon of the first stage then must give a $\mu_1 \geq 0$, so that $V_k(x) \geq 0$ for every approximant.

Theorem 7.1. *In a homogeneous V_{k+1} with $V_{k+1}(x) \geq 0$, we have*

(1) $$0 \leq \mu_1 < \mu_2 < \cdots < \mu_k < \mu_{k+1},$$

and the keys ϕ_i are all polynomials in x with V_0-integers as coefficients.

[13] Similarly defined in Deuring, *op cit*, p 281 and Ostrowski, *op cit*, p 322.
[14] Cf. Ostrowski, *op cit*, p 288, or the "Bewertungsring" in Krull, *Idealtheorie*, p 101.

The last key ϕ_{k+1} is minimal (2.3), so has a leading term $\phi_k^{u_k}$ and a homogeneous expansion as in §2, (8):

(2) $$\phi_{k+1} = \phi_k^{u_k} + \sum\nolimits_j a_j\,\phi_1^{m_{1j}}\phi_2^{m_{2j}}\cdots\phi_k^{m_{kj}} \qquad (a_j \in K,\ m_{kj} < u_k),$$

where, if n_i stands for $\deg\phi_i$, the degrees m_{ij} are limited by

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

Since ϕ_{k+1} is homogeneous, all terms in (2) have the same value. Hence

(4) $$\mu_{k+1} > V_k(\phi_{k+1}) = u_k\mu_k = (n_{k+1}\mu_k)/n_k.$$

Since $\mu_1 \geq 0$, (4) for every k gives (1). We next estimate the terms of (2).

Lemma 7.2. *In any V_k with $V_k(x) \geq 0$, a term*

$$T = \phi_1^{m_1}\phi_2^{m_2}\cdots\phi_{k-1}^{m_{k-1}}, \qquad (m_i < n_{i+1}/n_i \textit{ for all } i)$$

has a value $V_k(T) \leq V_k(\phi_k)$.

This inequality can also be written as

$$m_1\mu_1 + \cdots + m_{k-1}\mu_{k-1} \leq \mu_k.$$

It is true for $k = 1$ or 2, by hypothesis and (4). If we assume it for $k-1$, then, since n_k/n_{k-1} is integral,

$$\sum_{i=1}^{k-1} m_i\mu_i = m_{k-1}\mu_{k-1} + \sum_{i=1}^{k-2} m_i\mu_i \leq (m_{k-1}+1)\mu_{k-1} \leq \frac{n_k}{n_{k-1}}\mu_{k-1} < \mu_k.$$

Theorem 7.1 now follows by induction. It is true for $k = 1$. If all the keys of V_k have V_0-integral coefficients, all terms in the expansion (2) of ϕ_{k+1} have the same value. But $\phi_1^{m_{1j}}\cdots\phi_k^{m_{kj}} = T\cdot\phi_k^{m_{kj}}$ has by the lemma a value not exceeding $V_k(\phi_k^{m_{kj}+1}) = V_k(\phi_k^{u_k})$. Hence the coefficient a_j has a non-negative value, and a_j is V_0-integral.

Note. If K is the field of rational numbers, $G(x)$ with leading coefficient 1 can be so chosen that all its coefficients are ordinary integers (with non-negative value in every V_0). The same proof then shows that all ϕ_k have ordinary integers as coefficients, provided only that the representatives (§2) for each p-adic value V_0 are chosen as the numbers $c\cdot p^m$, $c = 0, \ldots, p-1$. Similar results hold when K is an algebraic number field.

8. The finiteness theorem. Each k-th approximant may give rise to one or more $(k+1)$-th approximants, so that the number of k-th approximants can increase with k. Ultimately, the number of approximants stops increasing, but for a finite construction we must be able to tell how soon this is the case:

Theorem 8.1. *One can find an integer k' so large that each k'-th approximant has the projection 1. As a result, only one $(k+1)$-th approximant can be obtained by augmenting any given k-th approximant, for any $k \geq k'$.*

The second conclusion follows from the first, because in §5, (5), $\deg \phi_k$ cannot decrease (§2, Condition 2.41). To establish the first conclusion, we will show that a projection not 1 gives G a multiple factor "mod μ_k", in the sense in which $h(x)$ is a common factor "mod ν" in

Lemma 8.2. *If, in any homogeneous V_k with $V_k(x) \geq 0$, $f(x)$ and $g(x)$ are polynomials with V_0-integral coefficients and a resultant $R(f,g)$, if there are polynomials $h(x)$, $a(x)$, and $b(x)$ with*

$$V_k(f - ha) \geq \nu, \quad V_k(g - hb) \geq \nu, \qquad (\nu \text{ real}),$$

and if $h(x)$ is not a unit in V_k, then $V_k\big(R(f,g)\big) \geq \nu$.

Proof. Since $R(f,g) = 0$ would imply $V_k(R) = \infty$, we can assume $R(f,g) \neq 0$, so that there exist $c(x)$ and $d(x)$, with V_0-integral coefficients, such that

$$c(x)f(x) + d(x)g(x) = R(f,g)$$

(van der Waerden, *Moderne Algebra* **2**, page 4). Hence

$$R(f,g) = (ca + db)h + c(f - ha) + d(g - hb).$$

Since $V_k(x) \geq 0$ and therefore $V_k(c) \geq 0$ and $V_k(d) \geq 0$, the last two terms here have values not less than ν. Were $V_k(R) < \nu$, we should have

$$R(f,g) \approx_{V_k} (ca + db)h.$$

Since R is a constant, this makes h a unit (see §4), contrary to hypothesis. □

To apply this lemma when R is a discriminant, use

Lemma 8.3. *In any homogeneous V_k with $V_k(x) \geq 0$ and $V_k(\phi_k) = \mu_k$ the derivative $f'(x)$ of any polynomial $f(x)$ has a value $V_k\big(f'(x)\big) \geq V_k\big(f(x)\big) - \mu_k$.*

For $k = 1$ the result follows readily, since the value of a natural integer $1 + \cdots + 1$ is never negative. If the lemma is true for V_{k-1}, and if $f(x)$ has the expansion $\sum f_j(x)\phi_k^j$ as in §2, (3), then

$$f'(x) = \sum f_j'(x)\phi_k^j + \sum j f_j(x)\phi_k^{j-1}\phi_k'(x).$$

The value of the first sum exceeds $V_k(f) - \mu_k$ because of the induction assumption and because $\mu_k > \mu_{k-1}$. The value of the second sum is $\geq V_k(f) - \mu_k$, since $V_k(j) \geq 0$ and $V_k(\phi_k') \geq 0$, the latter because ϕ_k has V_0-integral coefficients by Theorem 7.1.

To establish Theorem 8.1, consider a V_k with a projection $\alpha - \beta > 1$. The expansion of §3, (1), used to define this projection gives

(1) $$V_{k-1}(g_\alpha) + \alpha\mu_k \leq V_{k-1}(g_i) + i\mu_k \qquad (i = 0, \ldots, m).$$

Division of $G(x)$ by ϕ_k^α yields, in terms of this expansion,

(2) $$G(x) = q(x)\phi_k^\alpha + r(x), \quad r(x) = \sum_{i=0}^{\alpha-1} g_i(x)\phi_k^i.$$

For this remainder $r(x)$ the triangle law (§2, (1)) and (1) show

$$\begin{aligned} V_{k-1}(r) &\geq \min_i \big[\, V_{k-1}(g_i) + i \cdot V_{k-1}(\phi_k)\,\big] \\ &\geq \min_i \big[\, V_{k-1}(g_\alpha) + (\alpha - i)\mu_k + i \cdot V_{k-1}(\phi_k)\,\big], \end{aligned}$$

where i ranges from 0 to $\alpha - 1$. Since $\mu_k > V_{k-1}(\phi_k)$, the minimum is at $i = \alpha - 1$:

(3) $$V_{k-1}(r) \geq V_{k-1}(g_\alpha) + \mu_k + (\alpha - 1)V_k(\phi_k). \qquad [\,V_{k-1}(\phi_k)?\,]$$

As the divisor ϕ_k^α has V_0-integral coefficients and first coefficient 1, the quotient and $g_\alpha(x)$ likewise have integral coefficients, whence $V_{k-1}(g_\alpha) \geq 0$, since $V_{k-1}(x) \geq 0$. Further, (4) of §7 proves $V_{k-1}(\phi_k) \geq \mu_{k-1}$, while $\alpha \geq \operatorname{proj}_G V_k$ was assumed to exceed 1, so that (3) becomes

(4) $$V_{k-1}(r) \geq \mu_k + \mu_{k-1}.$$

Differentiation of (2), with Lemma 8.3, now proves

$$V_{k-1}\big(G' - (\alpha q\phi_k' + q'\phi_k)\phi_k^{\alpha-1}\big) \geq \mu_k; \qquad V_k\big(G - q\phi_k^\alpha\big) \geq \mu_k.$$

Thus G and G' have a "common factor" $\phi_k^{\alpha-1}$, with $\alpha - 1 > 0$. This factor is not a unit because ϕ_k is minimal in V_{k-1}. Thus Lemma 8.2 with §3, (1) gives

(5) $$V_{k-1}\big(R(G, G')\big) \geq \mu_k \geq \mu_{k-1} \qquad (k > 1).$$

For large k this is impossible. For if Γ_{k-1}, the cyclic value group of V_{k-1}, has the generator $\delta_{k-1} > 0$, while the group Γ_0 for V_0 is generated by $\delta_0 > 0$, then, because of §6, (3), and §5, (2),

(6) $$\delta_0/\delta_{k-1} = \exp V_{k-1} \leq \deg \phi_k \leq (\deg G)/(\operatorname{proj}_G V_k).$$

Hence δ_{k-1} is bounded below by $\delta_0/\deg G$. But the sequence μ_i for $i \le k-1$ lies in Γ_{k-1} and is increasing (§7, (1)), so that it increases by steps of at least δ_{k-1}. Therefore $\mu_{k-1} \to \infty$ with k. But the field $K(\theta)$ was assumed separable, so that G has no multiple roots, whence $R(G, G') \ne 0$ and $V_{k-1}(R) = V_0(R)$ is finite. Thus the inequality (5) is impossible for large k, and the assumption $\mathrm{proj}_G V_k > 1$ is untenable for large k.

This proof can be used to estimate how soon $\mathrm{proj}_G V_k$ becomes 1.

If one combines (5) and (6) as indicated above, then

$$V_{k-1}\big(R(G, G')\big) \ge \big((k-2)\delta_0 \cdot \mathrm{proj}_G V_k\big)/(\deg G).$$

This gives an upper bound for any k with $\mathrm{proj}_G V_k > 1$. If we use the worst value, $\mathrm{proj}_G V_k = 2$, in this bound and compute k' as the next larger integer, we find that *the integer k' of Theorem* 8.1 *may be taken as*

$$k' = \left[\frac{\rho n}{2}\right] + 3, \tag{7}$$

where n is the degree of $G(x)$ and ρ the integer determined by $V_0\big(R(G, G')\big) = \rho\delta_0$.

Several improvements in this estimate are possible: (i), the term $\mu_k - \mu_{k-1}$, neglected in (5), can be estimated as not less than δ_0/n; (ii), if n is odd and $\mathrm{proj}_G V_k = 2$, the last inequality of (6) can be improved, while the remaining cases of $\mathrm{proj}_G V_k \ge 3$ or n even, $\mathrm{proj}_G V_k = 2$ can be treated by the original method. If this is carried out, one finds

$$k' = \rho\left[\frac{n}{2}\right] + 2. \tag{8}$$

The whole argument can now be repeated with $\mathrm{proj}_G V_k$ replaced by the projection of the principal polygon for ϕ_k. This shows that once ϕ_k is chosen for $k \ge k'$, the principal polygon has only one side, so that μ_k is completely determined. In other words, only the first half of the k'-th stage is needed for Theorem 8.1.

In the algebraic number case, ρ is the power to which the prime p under consideration divides the discriminant of G. If $\rho = 0$, then two stages suffice. This is essentially a part of the result of Dedekind, that under these conditions the prime ideal factors of p correspond to the irreducible factors $\phi_2(x)$ of $G(x)$ modulo[15] p. Presumably the estimate (8) could be improved by introducing the index (involving the non-essential discriminant divisors) of the original equation.

9. The degree of a value.

To interpret the relation (11) of §5 we need the notion of the "degree" of an absolute value. In an algebraic number field, the "inertial" degree of a prime ideal factor $\mathfrak{p}$ of a rational prime p is just the degree of the residue-class field of $\mathfrak{p}$ over the field of the integers mod p. To generalize to any value V of a ring S, use the ring of all "integers" $a \in S$ with $V(a) \ge 0$, and call two integers a and b *congruent* mod V if $V(a-b) > 0$. The set of residue-classes of the integers with respect to this congruence forms as usual a ring, the *residue-class ring* S/V. If S is a field, so is S/V. If W is any extension of our original value V_0 to $K(\theta)$, the usual arguments show that the residue-class field $K(\theta)/W$ contains a subfield F_0 isomorphic to K/V_0 and that $K(\theta)/W$ is algebraic over this F_0. The *degree of* W is defined to be the degree, $\deg W$, of $K(\theta)/W$ over F_0.

To compute the degree, we use the results of M, part II, which show that for a sequence of discrete inductive values $V_1, V_2, \ldots, V_k$ the residue-class ring of each V_i has the form of a polynomial ring $F_i[y]$, where F_i is an algebraic extension of $F_0 = K/V_0$. Furthermore (M, Theorem 12.1) $F_1 = F_0$, while, for $i \ne 0$, F_{i+1} is an algebraic extension of F_i of a degree which is exactly the degree of ϕ_{i+1} considered as a polynomial in $\phi_i^{\tau_i}$. In other words (M, Theorem 12.1),

$$\mathrm{degree}(F_{i+1} : F_i) = \deg\phi_{i+1}/(\tau_i \cdot \deg\phi_i) \qquad (i = 1, \ldots, k-1).$$

These formulas, combined with the interpretation of τ_i in §6, (2), give

$$\mathrm{degree}(F_{i+1} : F_i) = \frac{\deg\phi_k}{\tau_1\tau_2\cdots\tau_{k-1}} = \frac{\deg\phi_k}{\exp(V_{k-1})}. \tag{1}$$

These results can be extended to non-finite inductive values thus[16]:

Theorem 9.1. *For a non-finite value $V_k = [\,V_{k-1}, V_k(\phi_k) = \infty\,]$ the residue-class ring $K[x]/V_k$ is isomorphic to a field F_k, which is an algebraic extension of F_{k-1} of a degree determined as in* (1)*, where $F_{k-1}[y]$ is the residue-class field of V_{k-1}.*

Proof. Exactly as in the proof M, Theorem 12.1, F_k is defined as the set of all residue-classes modulo V_k which contain a polynomial $f(x)$ with $V_{k-1}(f) \ge 0$. But if a polynomial $f(x)$ in any residue-class is divided by ϕ_k, giving

$$g(x) = q(x)\phi_k + r(x),$$

then the term $q\phi_k$ has value ∞, so that g and r belong to the same residue-class, while $V_{k-1}(r) = V_k(r) \ge 0$. Hence F_k includes all residue-classes and is the residue-class ring. Its degree is found as in M, Theorem 12.1. □

Theorem 9.2. *If W, an extension of V_0 to $K(\theta)$, corresponds as in Theorem* 2.1 *to an inductive value V_k with $V_k\big(G(x)\big) = \infty$, then*

$$(\exp W)\cdot(\deg W) = \deg\phi_k. \tag{2}$$

[15] R. Dedekind, *Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Gesammelte Werke **I** 202–233.

[16] Theorem 9.1, as well as the last paragraph of §4, was revised July 15, 1936.

The correspondence of W to V_k yields an isomorphism between the residue-class rings $K(\theta)/W$ and $K[x]/V_k$. Hence by (1) and the definition of the degree of W,

$$\deg W = \text{degree}(F_k : F_0) = (\deg \phi_k)/\exp V_{k-1}.$$

But since any $V_k(f)$ is either $+\infty$ or some value from V_{k-1}, the value-groups of V_k and V_{k-1} are identical, and V_{k-1}, V_k, and W have the same exponent. Therefore (2) results.

A similar interpretation holds for a limit-value $V_\infty = \lim V_k$. We first prove as in M, Theorem 14.1, that, as soon as $\deg \phi_k = \deg \phi_{k+1} = \cdots$, we have $F_k = F_{k+1} = \cdots$, and that this constant F_k is the residue-class ring $K[x]/V_\infty$. As before, this F_k is then also the residue-class field of the corresponding value W of $K(\theta)$. Consequently, using (1) again, we get

Theorem 9.3. *If W is an extension of V_0 to $K(\theta)$ which corresponds as in Theorem 2.1 to a limit-value $V_\infty = \lim V_k$ with $V_\infty\big(G(x)\big) = \infty$, then*

$$(\exp W)\cdot(\deg W) = \lim_{k\to\infty} \deg \phi_k, \tag{3}$$

and the limit on the right is actually attained for large k.

10. The totality of values. The existence theorem is

Theorem 10.1. *There are only a finite number of extensions W', W'', …, $W^{(s)}$ of a given discrete value V_0 of K to the separable field $K(\theta)$, where θ is a root of $G(x) = 0$. Furthermore,*

$$(\exp W')\cdot(\deg W') + \cdots + (\exp W^{(s)})\cdot(\deg W^{(s)}) = \deg G(x). \tag{1}$$

The relation (1) is a generalization of a well-known property of prime ideals. We first show that all W come from approximants. Every value W of $K(\theta)$ corresponds by Theorem 2.1 to a value of $K[x]$, which must be either an inductive value V_k or a limit-value V_∞. In the latter case, V_∞ is the limit of a sequence V_1, V_2, …, in which each V_k is by Lemma 3.2 an approximant. In the former case, $V_k\big(G(x)\big) = \infty$ and V_{k-1} is by §2 and Lemma 3.2 a finite approximant. Since V_k is not finite, $V_k(\phi_k) = \mu_k = \infty$. Then only the multiples of ϕ_k have non-finite values, so that the last key ϕ_k must be $G(x)$ itself. This is the "terminating case" of Theorem 5.3. In this case there is only one sequence of approximants and hence only one value W of $K(\theta)$. The equation (2) of §9 thus gives the relation (1) above.

In the non-terminating case, we can construct one or more sequences of approximants V_1, V_2, V_3, …. We must show that each such sequence gives a value W of $K(\theta)$. By Lemma 3.4

$$V_1\big(G(x)\big) < V_2\big(G(x)\big) < V_3\big(G(x)\big) < \cdots, \tag{2}$$

while ultimately $\text{proj}_G V_k = 1$ and $\deg \phi_k$ is constant (Theorem 8.1 and §5, (5)). The index τ_k of each value-group Γ_{k-1} in the succeeding Γ_k is thus eventually unity (§6, (1) and (3)). Therefore all the values in (2) lie in some one discrete group $\Gamma_{k'}$, so that $V_k(G)$ must approach ∞. The limit-value V_∞ then has $V_\infty(G) = \infty$, so that V_∞ corresponds to a value W of $K(\theta)$. The relation (1) for all these values follows from Theorems 5.2 and 9.3 because $\text{proj}_G V_k = 1$.

The complete limit-value V_∞ cannot be written down, but its essential properties can be calculated.

Theorem 10.2. *Each value $W^{(i)}$ of Theorem 10.1 is uniquely determined by an "approximant" inductive value $V_k^{(i)}$ of $K[x]$, for some $k = k'$. If it is possible to construct the irreducible factors of polynomials with coefficients in the residue-class field K/V_0, the approximants $V_k^{(i)}$ can be computed in a finite number of steps by finding certain slopes $\mu_j^{(i)}$ of the Newton polygons of $G(x)$ and certain key polynomials $\phi_j^{(i)}$ as the irreducible factors of $G(x)$ in various equivalence-decompositions. In this case one finds, in a finite number of steps,* (i) *the number s of extensions of V_0 to $K(\theta)$;* (ii) *the exponent and degree of each such $W^{(i)}$;* (iii) *the values $W^{(i)}(\alpha)$ for any previously given α in $K(\theta)$.*

This is a restatement of previous results, except for the last assertion, which gives a construction of the "prime ideal" decomposition of any α. If $\alpha = g(\theta) \neq 0$, then we need only compute $V_\infty\big(g(x)\big)$ for each limit value V_∞ involved. If for every k, $V_k(g) > V_{k-1}(g)$, the argument following (2) proves $V_\infty(g) = \infty$ and $\alpha = 0$. Otherwise $V_k(g) = V_{k-1}(g)$ for some k, so that V_k is not an approximant to $g(x)$ in the sense of Definition 3.3 and $V_\infty(g) = V_k(g)$ as in Lemma 3.2. Hence W_α can be computed in k stages.

In the algebraic number case ($K =$ the field of rationals) the construction of a prime ideal with inductive values can be extended to give a representation of the prime ideal as the greatest common divisor of integers. It can then also be proved that the "terminating case" of the construction arises whenever the prime p in question has only one prime ideal factor. The proof depends on the fact that every rational integer can be expressed as a sum of a finite number of terms cp^m, with $c = 0, 1, \ldots, p-1$. Thence it can be argued that any approximant V_k with $\deg \phi_k = \deg G$ must ultimately lead to the terminating case.

It remains to connect our results with previous investigations on this topic. Ore[17] developed (Ore I) a construction for prime ideals in algebraic fields which for this special case is equivalent to the first $2\frac{1}{2}$ stages of our method, which involve the approximants V_2 and the key polynomials ϕ_3. This part of the construction does

[17] Ore uses $\mu_1 = 0$, which is possible because θ is assumed integral.

not suffice[18] for all equations $G(x)$. In a subsequent paper (Ore II, especially Kap 2, §5) Ore made an extension equivalent to one more stage of our method, coupled with successive transformations of the defining equation $G(x)$, which have the effect of reducing several stages of our method to one stage. This method is constructive and applies in all cases, but is justified only by appeal to another, more elaborate construction[19] of prime ideals in terms of congruences mod p^α. Berwick has developed[20] approximations equivalent to $2\frac{1}{2}$ stages of our method, and mentions the possibility of a third stage. The investigations of Wilson,[21] although they are formulated in terms of group-bases for ideals, are closely related to the first two stages of our method. However, if the method of successive approximations is to be universally applicable, it must be formulated in terms of an arbitrary number of steps; for, given an integer k and a prime p, an irreducible polynomial $G(x)$ can always be constructed so that the decomposition of p in the field defined by $G(x)$ will require more than k stages.

Our construction can also be employed to give a simple form to a number of irreducibility criteria,[22] to prove one of the fundamental theorems relating Hensel's p-adic numbers to prime ideals and to constructively establish the unique decomposition theorem in terms of the "Hauptordnungen" of Krull.[23] I plan to discuss some of these topics in a later paper.

Harvard University.

[18]Ø. Ore, *Weitere Untersuchungen zur Theorie der algebraischen Körper*, Acta Math **45** (1925) 145–160. Here it is proved that for every p and every algebraic field there "exists" a regular defining equation for which the second stage is sufficient. However, the existence proof is not constructive.

[19]Ø, Ore, *Ueber den Zusammenhang swischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*, Math Ann **96** (1926) 313–351; **97** (1927) 569–598.

[20]W. E. H. Berwick, *Integral Bases*, Cambridge Tracts in Mathematics and Mathematical Physics, No 22.

[21]N. R. Wilson, *On finding ideals*, Annals of Math **30** (1928–29) 411-428.

[22]S. MacLane, *Abstract absolute values which give new irreducibility criteria*, Proc Nat Acad Sci **21** (1935) 472–474; *The ideal-decomposition of rational primes in terms of absolute values*, Proc Nat Acad Sci **21** (1935) 663–667.

[23]W. Krull, *Idealtheorie*, p 104.