THE SCHÖNEMANN-EISENSTEIN IRREDUCIBILITY CRITERIA IN TERMS OF PRIME IDEALS*

BY

SAUNDERS MacLANE

1. **Introduction.** The Eisenstein criterion† for the irreducibility of a polynomial has been repeatedly generalized, in many cases by the use of Newton polygons. All of these irreducibility criteria for polynomials can be systematically viewed in terms of non-archimedean absolute values—so that we can state a general theorem which includes all these theorems as special cases and which also establishes the irreducibility of new classes of polynomials. Our general theorem asserts, in effect, that a polynomial $G(x)$ with no multiple roots and with rational coefficients is irreducible if there is a rational prime p which has just one prime ideal factor in the ring $R[x]/G(x)$, which is obtained by reducing modulo $G(x)$ the ring of all polynomials with rational coefficients. This criterion can be constructively applied by using a previously developed method for actually exhibiting the prime decomposition of any p.‡

The known irreducibility criteria are simply conditions which imply that the first few stages of the prime ideal construction will show that p has but one prime ideal factor. The Schönemann criterion asserts the irreducibility of polynomials of the form

$$f(x) = \phi(x)^e + pM(x), \tag{1}$$

where $\phi(x)$ is an irreducible polynomial modulo p and where $M(x)$ is a polynomial relatively prime to ϕ, mod p, and of degree less than the degree of f. Alternatively, these conditions show that in the ring $R[x]/f(x)$, p has just one prime ideal factor $P=(p, \phi(x))$, and that this factor may be found by the "second stage" of the construction of the factors of p. Because there is but one prime factor,§ and because the degree of P times the exponent to which P divides p is the degree of $f(x)$, $f(x)$ must be irreducible.

* Presented to the Society, January 2, 1936; received by the editors February 23, 1937.

† For a simple statement see B. L. van der Waerden, *Moderne Algebra*, §22.

‡ S. MacLane, *A construction for absolute values in polynomial rings*, these Transactions, vol. 40 (1936), pp. 363–395; S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal, vol. 2 (1936), pp. 492–510. We refer to these two papers as Const I and Const II, respectively. They contain the definition of absolute values, etc., used subsequently.

§ The connection between the Eisenstein irreducibility criterion and the prime ideal factorization of a rational prime was observed by M. Bauer, *Zur allgemeinen Theorie der algebraischen Grössen*, Journal für die Mathematik, vol. 132 (1907), pp. 21–32, especially §IV; also by O. Perron, *Idealtheorie und Irreduzibilität von Gleichungen*, Mathematische Annalen, vol. 60 (1905), pp. 448–458.

Our new irreducibility criterion may be stated with reference to a rational prime p or, alternatively, in terms of the corresponding "p-adic" absolute value. This simple form of the theorem is stated in §2 for a polynomial with coefficients in any field K. It involves certain absolute values of the polynomial ring $K[x]$. We include also a more general theorem giving all possible degrees for the factors of a reducible polynomial.* Next, in §3, we indicate how our result includes both old and new cases. To establish the prime ideal interpretation, we first develop briefly in §4 the properties of prime ideals in a ring $K[x]/G(x)$, where K is an algebraic number field. These properties give the irreducibility theorem in the prime ideal form. Finally in §5 we show how the successive "approximant" values used in our irreducibility criteria do, in fact, give a construction for the prime ideals in the corresponding ring $K[x]/G(x)$. Hence the general irreducibility theorem, stated in terms of absolute values, implies the form of the irreducibility theorem already stated in terms of prime ideals.

The fundamental irreducibility theorem of §2 can also be applied to polynomials in several variables. In the last section we give several specific examples of the new irreducibility criteria which result.

2. **Irreducibility criteria with approximants.** An *absolute value* of a ring is a function $V(a)$ defined for all a in the ring and with the properties

$$V(ab) = V(a) + V(b). \qquad V(a+b) \geqq \min(Va, Vb).$$

An element a of the ring is *equivalence-divisible* in V by an element b if there is an element c with $V(a-bc) > V(a) = V(bc)$.

Consider now polynomials with coefficients in any field K. A polynomial $f(x)$ is a *key polynomial* over a value V of $K[x]$ if $f(x)$ has the first coefficient 1, if any polynomial equivalence-divisible by $f(x)$ in V has a degree at least as great as the degree of $f(x)$, and if any product equivalence-divisible by $f(x)$ in V has a factor equivalence-divisible by $f(x)$ in V.† The first form of our general irreducibility criterion for polynomials is

THEOREM 1. *If K is any field and if $G(x)$ is a key polynomial over a value V of the polynomial ring $K[x]$, then $G(x)$ is irreducible.*

Proof. Suppose that $G(x)$ could be factored as $G(x) = f(x)h(x)$. Then this product is equivalence-divisible by G in V. As G is equivalence-irreducible, by the definition of a key, one of the factors f or h must be equivalence-

* Simple theorems of this type have been stated by Dumas and Ore (cf. §3 below) and by O. Perron, loc. cit., and E. Netto, *Ueber die Irreductibilität ganzzahliger ganzer Funktionen*, Mathematische Annalen, vol. 48 (1896), pp. 82–88.

† MacLane, Const I, Definition 4.1.

divisible by G. But G is also minimal, so that this factor has a degree at least that of G. Therefore the assumed decomposition is trivial, so G is irreducible.

The relevance of this Theorem derives from the possibility of explicitly constructing all possible values of $K[x]$ for many fields K and from an explicit criterion* which determines when $G(x)$ is a key polynomial over such values. Any value V in $K[x]$ determines a value $V_0a = Va$ in the coefficient field K. The simplest values of $K[x]$ are the "inductive values"† V_k characterized by the properties: (i) V_k agrees in the field K with a given value V_0; (ii) V_k gives certain polynomials $\phi_1(x) = x, \phi_2(x), \cdots, \phi_k(x)$ specific assigned values $V_k\phi_i(x) = \mu_i$; (iii) V_k assigns to every polynomial in the ring $K[x]$ the smallest possible value consistent with the conditions (i) and (ii). Such an inductive value is denoted by

$$V_k = [V_0, V_1x = \mu_1, V_2\phi_2(x) = \mu_2, \cdots, V_k\phi_k(x) = \mu_k]. \tag{2}$$

These values may be obtained by an inductive definition of the values V_i of $K[x]$ determined by the first i polynomials $\phi_i(x)$. In (2), each μ_i is a number, while each polynomial $\phi_i(x)$, with $i>1$, must be a key polynomial over the previous inductive value V_{i-1}, and must satisfy two other minor conditions (Const I, Definition 6.1). The set of all numbers $\nu = V_kf(x) - V_kg(x)$ which are values of rational functions $f(x)/g(x)$ in V_k is a group, the *value-group* Γ_k. For a given $\phi_k(x)$ there is for each polynomial $G(x)$ a unique "expansion" in powers of ϕ_k, of the form

$$G(x) = g_m(x)\phi_k^m + g_{m-1}(x)\phi_k^{m-1} + \cdots + g_0(x), \tag{3}$$

where the coefficients $g_i(x)$ in the expansion are 0 or of degree less than the degree of ϕ_k. The value V_kG is the minimum of the values of the terms in this expansion.

The hypothesis in Theorem 1 that G is a key polynomial is most easily fulfilled by making a suitable multiple of G have a residue class modulo V (Const I, part II) which is a linear polynomial.

THEOREM 2. *If V_k is an inductive value with a last key polynomial ϕ_k, and if a polynomial $G(x)$ has an expansion* (3) *in terms of ϕ_k such that* (i) $g_m(x) = 1$, (ii) $V_kG = V_k\phi_k^m = V_kg_0$; (iii) *if $n<m$ is a positive integer, then $n\mu_k$ is not in the value-group Γ_{k-1}; then $G(x)$ is a key polynomial over V_k and hence irreducible.*

---

* The method of Const I, Theorem 9.4 and §13 applies whenever V is an inductive value and K an algebraic field.

† For the explicit definition, see MacLane, Const I, §4, (3) or Const II, §2, (4).

Proof. Conditions (i) and (ii) will make $G(x)$ a key, by Const I, Theorem 9.4, provided we also show $G(x)$ equivalence-irreducible in V_k. But any G has by Const II, Theorem 4.2 a representation as a product of key polynomials $\psi(x)$. Each one must have the form of an expansion

$$\psi(x) = \phi_k^e + h_{e-1}(x)\phi_k^{e-1} + \cdots + h_0(x), \qquad e > 0$$

in which the first and last terms again have the same value in V_k. By the minimal property (iii) of m this is possible only if e is a multiple of m. Hence the representation of G has just one factor ψ. This factor has the same degree and the same equivalence-divisors as G, so that G, like ψ, is equivalence-irreducible and therefore a key polynomial.* These theorems include and generalize all the classical irreducibility criteria of the Newton polygon type.

To obtain information about the degree of possible factors of a reducible polynomial, we use "approximants." If V_k is a finite and homogeneous† kth stage value of $K[x]$, and if $G(x)$ is any polynomial expanded as in (3), consider the exponents j in (3) with the property that $V_kG = V_k(g_j(x)\phi_k^j)$, and denote by α the largest and by β the smallest of these exponents. Then the *projection* of G on V_k is taken to be

$$\text{proj}\,(V_k, G) = \alpha - \beta. \tag{4}$$

The homogeneous value V_k, considered as an extension of the value V_0 of K, is an *approximant* of G over V_0 if and only if proj $(V_k, G) > 0$. For any polynomial $G(x)$ with coefficients in an algebraic number field, the set of all kth approximants can be found by Newton polygons with the procedure used in Const II for an irreducible polynomial $G(x)$.

A homogeneous inductive value V_s is non-finite if $V_s\phi_s = \mu_s = \infty$. We call such a V_s an *improper kth approximant* to $G(x)$, for any $k \geqq s$, if ϕ_s is a factor of $G(x)$. We define proj (V_s, G) as the exponent to which ϕ_s divides G. Henceforth the phrase "kth approximants" refers both to proper and improper kth approximants.

To interpret (4), note that the integer β can be uniquely characterized by the properties

(4a) ϕ_k^β is an equivalence-divisor of $G(x)$ in V_k,
$\phi_k^{\beta+1}$ is not an equivalence-divisor of $G(x)$ in V_k.

* This could also have been proven by the method of Const I, by finding an $R(x)$ so that $R \cdot G$ has value 0, showing (Theorem 12.1) that $R \cdot G$ has a residue-class which is a linear polynomial and thus proving G equivalence-irreducible by Lemma 11.2.

† Homogeneity is required because every inductive value with a discrete V_0 is equal to one and only one homogeneous value (cf. Const I, p. 393).

For all terms to the right of $g_\beta(x)\phi_k^\beta$ in the expansion (3) certainly have larger values than this term, hence the first half of (4a). If in addition the second half of (4a) were false, there would be an $h(x)$ with $f(x) \sim h(x)\phi_k^{\beta+1}$ in V_k; that is, with

$$V_k[f(x) - h(x)\phi_k^{\beta+1}] > V_k f(x) = V_k[h(x)\phi_k^{\beta+1}].$$

By inserting in $f = h\phi_k^{\beta+1} + [f - h\phi_k^{\beta+1}]$ the expansions in powers of ϕ_k for $h(x)$ and for the term in brackets we get an expansion for $f(x)$ in which the last term with the minimal value has the exponent $\beta+1$ or greater, counter to the definition of β. Therefore (4a) characterizes* β.

For a product $G = f'(x)f''(x)$, each factor f', or f'', has exponents α' and β', or α'' and β'', as in (4). By (4a), β' is the power to which ϕ_k is an equivalence-divisor of f', and similarly for β''. Therefore, by the uniqueness of the equivalence decomposition, $\beta = \beta' + \beta''$ (see Const II, §4). Furthermore α is the "effective degree" of $G(x)$ and has the property $\alpha = \alpha' + \alpha''$ (see Const II, §4, (1)). Combining these, we have

$$\text{proj}\,(V_k, f'(x)f''(x)) = \text{proj}\,(V_k, f'(x)) + \text{proj}\,(V_k, f''(x)). \tag{5}$$

This also holds for improper approximants. We obtain at once

LEMMA 1. *The kth approximants of a product $G(x)H(x)$ over V_0 consist of all the kth approximants of $G(x)$ and of all the kth approximants of $H(x)$ over V_0.*

THEOREM 3. The degree-of-factors theorem. *If for a value V_0 of the field K all the kth stage homogeneous approximants to the polynomial $G(x)$ over V_0 are denoted by $V_k^{(i)}$, $i = 1, \cdots, t_k$, then any factor $f(x)$ of $G(x)$ has a degree*†

$$\deg f(x) = \sum_{i=1}^{t_k} c_i \deg \phi(V_k^{(i)}) \tag{6}$$

where each c_i is any number satisfying

$$0 \leqq c_i \leqq \text{proj}\,(V_k^{(i)}, G), \qquad (i = 1, 2, \cdots, t_k).$$

Proof. This will follow at once by (5) combined with the equation

$$\deg G(x) = \sum_{i=1}^{t_k} \text{proj}\,(V_k^{(i)}, G) \cdot \deg \phi(V_k^{(i)}) \tag{7}$$

for any polynomial $G(x)$. To establish (7), decompose $G(x)$ into its irreducible

* A longer proof of this fact is also given in Const II, Theorem 5.1.

† Here $\deg \phi(V_k^{(i)})$ represents the degree of the last key polynomial of $V_k^{(i)}$. It is equal to the degree of the residue-class field of V_k multiplied by the exponent of V_{k-1}. See Const II, §9, (1).

factors, apply Const II, Theorems 5.2 and 5.3* to obtain equations similar to (7) for each such irreducible factor, and combine these equations by using the relation (5).

If $G(x)$ has no multiple factors and V_0 is "discrete," then k can be taken so large that every kth approximant has† the projection 1. A consequence is:

THEOREM 4. *If for a value V_0 of K and an integer k there is only one kth stage approximant V_k to $G(x)$, and if* proj $(V_k, G) = 1$, *then $G(x)$ is irreducible.*

If V_k be replaced by V_{k+1}, this is essentially a restatement of Theorem 1 with the additional advantage that the value V introduced arbitrarily there is now characterized as an approximant of $G(x)$.

Irreducibility can also be established by several applications of the degree-of-factors theorem.

THEOREM 5. *If V_0 and W_0 are two given values of a field K, if $G(x)$ is of degree $n = n_1 \cdot n_2$, where $(n_1, n_2) = 1$, and if there is an integer k such that every kth approximant V_k to $G(x)$ over V_0 has* deg $\phi(V_k) \equiv 0 \pmod{n_2}$, *while every kth approximant W_k to $G(x)$ over W_0 has* deg $\phi(W_k) \equiv 0 \pmod{n_1}$, *then $G(x)$ is irreducible.*

Proof. By the condition on V_0 and Theorem 3 each factor $f(x)$ has a degree which is a sum of multiples of deg $\phi(V_k)$ and which is therefore a multiple of n_2. By the same argument for W_0 the degree of $f(x)$ is a multiple of n_1, and so this degree must be n, the degree of $G(x)$.

This theorem can be generalized to apply to s different values with $n = n_1 n_2 \cdots n_s$. The conditions on the approximants over V_0 can be fulfilled, for example, by making the first approximant have the exponent n_2, for then deg $\phi(V_2)$ must be a multiple of n_2.

3. **Examples.** The theorem of Schönemann, as stated in §1, (1), follows from our results, for the condition on $\phi(x)$ is sufficient to make ϕ a key polynomial for a value

$$V_2 = [V_0 p = 1, V_1 x = 0, V_2 \phi(x) = 1/e],$$

while the condition on $M(x)$ makes the last term in the expansion of $f(x)$ in powers of ϕ have the value 1. Hence $f(x)$ is irreducible by Theorem 2.

In a similar fashion, the various generalizations of the Eisenstein irreducibility theorem for polynomials with rational coefficients can all be shown

* It may be observed that the assumption that V_0 was discrete was made in §5 only to insure that the approximants and limit values give all possible values of $K[x]$, so that this discreteness assumption is not needed here.

† By Const II, Theorem 8.1, which applies whenever G has a non-vanishing discriminant. The b_i in this theorem are then all 0 or 1.

to depend on the use of absolute values which are the extension of p-adic values. This is illustrated in the following list of known theorems which are special cases of our theorem applied to particular first and second stage values. Unless otherwise indicated the author stated our Theorem 2 for the field of rational numbers and for the special value indicated, in most cases not explicitly in terms of absolute values but in some equivalent form.*

Eisenstein: $[V_0 p = m,\ V_1 x = 1]$.

Schönemann: $[V_0 p = m,\ V_1 x = 0,\ V_2 \phi = 1]$.

Königsberger: $[V_0 p = n,\ V_1 x = r]$, $r > 0$. Also Theorem 5 for two such first stage values.

Bauer: $[V_0 p = n,\ V_1 x = 0,\ V_2 \phi = \alpha]$.

Dumas: $[V_0 p = n,\ V_1 x = r]$, Newton polygons, Theorem 3.
$[V_0 p = n,\ V_1 x = r,\ V_2 g = s]$, with restrictions.

Kürschák: $[V_0 p = 1,\ V_1 x = \mu,\ V_2 f = \nu]$, Newton polygons, $V_1 f = 0$.

Rella: As in Kürschák, for K a domain of integrity.

Ore: $[V_0 p = n,\ V_1 x = 0,\ V_2 \phi = r]$, Newton polygons, Theorem 3.

Ore: $[V_0 p = n,\ V_1 x = r]$, Theorem† 1.

Ore:‡ $[V_0 p = n,\ V_1 x = 0,\ V_2 \phi_2 = r,\ V_3 \phi_3]$. The degree-of-factors Theorem 3.

Irreducibility criteria have also been systematized by Blumberg§ in terms of a notion of "rank." This "rank" is closely related to our "absolute value." It applies also to differential expressions, but does not include the higher stage values.

Our methods for constructing inductive values allow the construction of

* The papers cited here are, in order: G. Eisenstein, *Ueber die Irreduzibilität und einige andere Eigenschaften der Gleichungen*, etc., Journal für die Mathematik, vol. 39 (1850), p. 166; Th. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, Journal für die Mathematik, vol. 32 (1846), pp. 93–105, §61; L. Königsberger, *Ueber den Eisensteinschen Satz von der Irreduzibilität algebraischer Gleichungen*, Journal für die Mathematik, vol. 115 (1895), pp. 53–78, especially (67) on p. 69; M. Bauer, *Verallgemeinerung eines Satzes von Schönemann*, Journal für die Mathematik, vol. 128 (1905), pp. 87–89; G. Dumas, *Sur quelques cas d'irreductibilité des polynomes à coefficients rationnels*, Journal de Mathematique, (6), vol. 2 (1906), pp. 191–258; J. Kürschák, *Irreduzible Formen*, Journal für die Mathematik, vol. 152 (1923), pp. 180–191; T. Rella, *Ordnungsbestimmungen in Integritätsbereichen und Newtonsche Polygone*, Journal für die Mathematik, vol. 158 (1927), pp. 33–48; O. Ore, *Zur Theorie der Irreduzibilitätskriterien*, Mathematische Zeitschrift, vol. 18 (1923), pp. 278–288; O. Ore, *Zur Theorie der Eisensteinschen Gleichungen*, Mathematische Zeitschrift, vol. 20 (1924), pp. 267–279.

† This is the first treatment of a non-linear criterion.

‡ O. Ore, *Zur Theorie der algebraischen Körper*, Acta Mathematica, vol. 44 (1924), pp. 219–314. Theorem 4 on page 230 is stated for an algebraic number field as coefficient field, while Theorem 9 on page 240 gives the degree of any factor in terms of the first two stages, plus the key polynomials only on the third stage. Hence this theorem differs in form from our statement.

§ H. Blumberg, *On the factorization of expressions of various types*, these Transactions, vol. 17 (1916), pp. 517–544.

examples of polynomials which are irreducible in virtue of arbitrary complicated inductive values not falling under the above cases. For example, the value

$$[V_0 p = 4,\ V_1 x = 0,\ V_2(x^2+1) = 2,\ V_3((x^2+1)^2+p) = 5] \qquad (p = 3)$$

of the ring of polynomials with rational coefficients proves

$$f(x) = [(x^2+1)^2+p]^2 + p^2(x^2+1) = x^8 + 4x^6 + 12x^4 + 25x^2 + 25$$

irreducible by Theorem 2, although the second stage approximant V_2 does not show it irreducible. The use of non-homogeneous key polynomials (or of constant degree inductive values) is illustrated by

$$[V_0 p = 2,\ V_1 x = 0,\ V_2(x^2+1) = 2,\ V_3(x^2+1+p) = 3] \qquad (p = 7),$$

which, by Theorem 2, proves the irreducibility of

$$(x^2+1+p)^2 + p^3 = x^4 + 16x^2 + 407.$$

A case of Theorem 1 not included in the linear Theorem 2 is

$$V_2 = [V_0 p = 1,\ V_1 x = 0,\ V_2(x^2+x+1) = 1] \qquad (p = 5),$$
$$f(x) = (x^2+x+1)^2 - p(x^2+x+1) + 3p^2x + 3p^3$$
$$= x^4 + 2x^3 - 2x^2 + 72x + 371.$$

The residue-class ring of $K[x]$ for this V_2 is by Const I, Theorem 12.1 just the ring $F[\theta, y]$, where F is the field of integers, modulo 5, and θ is the residue-class of x and so is the root of x^2+x+1 over F, while y is a symbol representing the residue-class* of $(x^2+x+1)/p$. To test this $f(x)$ for equivalence-irreducibility we first multiply it by p^{-2} to make it have the value 0. Then

$$p^{-2}f(x) = [(x^2+x+1)/p]^2 - [(x^2+x+1)/p] + 3x + 3p,$$

so that the residue-class polynomial is

$$H_2[p^{-2}f] = y^2 - y + 3\theta$$

which, although not linear, is irreducible over the Galois field $F(\theta)$. Hence $F(x)$ is equivalence-irreducible† and therefore irreducible by Theorem 1.

4. **Prime decomposition in algebraic rings.** To interpret our irreducibility criteria for $G(x)$ we first summarize some arithmetic properties of the corresponding residue-class ring

$$A = K[x]/(G(x)). \tag{8}$$

* See Const I, §12, (6).

† Const I, Lemma 11.2, where $R = p^{-2}$.

Here, and throughout §§4 and 5, K denotes an algebraic number field, $G(x)$ is a polynomial in $K[x]$, and $\mathfrak{O}$ the ring of all integers of the commutative algebra A.

THEOREM 6. *In $\mathfrak{O}$, every ideal B which is not a divisor of zero* has a decomposition, unique except for the order of factors, as a product of prime ideals from $\mathfrak{O}$. For ideals B and C, B not a divisor of zero, the inclusion $B \subset C$ implies the existence of an ideal D with† $B = CD$. Let*

$$G(x) = g_1(x)^{e_1} g_2(x)^{e_2} \cdots g_t(x)^{e_t} \tag{9}$$

be the decomposition of $G(x)$ into distinct irreducible factors $g_i(x)$, and denote by K_i the algebraic field $K[x]/(g_i(x))$, and by $\mathfrak{O}_i$ the ring of all the integers of K_i. For each prime ideal $P_i \neq \mathfrak{O}_i$ of the ring $\mathfrak{O}_i$ there is a corresponding prime ideal P' of $\mathfrak{O}$, and the residue-class rings $\mathfrak{O}/P'$ and $\mathfrak{O}_i/P_i$ are isomorphic. These ideals P' are all distinct and include all the prime ideals of $\mathfrak{O}$, except for $\mathfrak{O}$ itself. If $\mathfrak{p}$ is a prime ideal of the ring of integers of the base field K, the decomposition of $\mathfrak{p}$ in $\mathfrak{O}$ may be found by decomposing $\mathfrak{p}$ in each $\mathfrak{O}_i$, replacing each prime factor P_i in these decompositions by the corresponding P' and multiplying the resulting decompositions.

The proof is omitted, since the results are implicit in the more general arithmetic of non-commutative algebras.‡ The theorem can easily be obtained directly by the usual consideration of A as the direct sum of the fields K_i.

The degree of a prime ideal P' in the ring of integers $\mathfrak{O}$ of Theorem 6 is defined to be the degree of its residue-class ring $\mathfrak{O}/P'$ over the residue-class ring of $\mathfrak{p}$, where $\mathfrak{p}$ is the prime ideal of K such that $\mathfrak{p} \cdot \mathfrak{O} \subset P'$. This is, by the theorem, the same as the degree of the corresponding prime ideal P_i of K_i over $\mathfrak{p}$. The relation between the degree of an algebraic number field and the degree and exponents of prime ideals yields then the following analogue to our irreducibility theorem.

THEOREM 7. The degree-of-factors theorem. *If $G(x)$ has no multiple factors and if, in the ring of integers of the algebraic number field K, $\mathfrak{p}$ is any prime ideal with the decomposition*

---

* An ideal B in $\mathfrak{O}$ is a divisor of zero if every element of B is a divisor of zero.

† This second property, "every divisor is a factor," is closely associated with the decomposition into prime ideals (van der Waerden, *Moderne Algebra*, vol. 2, §100). When it holds for all ideals, including divisors of zero, the ring is called a multiplication-ring. See Krull, *Idealtheorie*, Ergebnisse der Mathematik, vol. 5, p. 26.

‡ M. Deuring, *Algebren*, Ergebnisse der Mathematik, vol. 4, p. 108. E. Artin, *Zur Arithmetik hyperkomplexer Zahlen*, Abhandlungen des Mathematischen Seminars, Hamburg, vol. 5 (1928), pp. 261–289.

$$\mathfrak{O}\cdot\mathfrak{p} = P_1^{b_1}P_2^{b_2}\cdots P_s^{b_s} \qquad (b_i = \exp P_i) \tag{10}$$

into prime ideals in $\mathfrak{O}$, then any factor $f(x)$ of $G(x)$ has a degree of the form

$$\deg f(x) = \sum{}'b_i\cdot\deg P_i = \sum{}'(\exp P_i)(\deg P_i), \tag{11}$$

where the sum is to be taken over any subset of the given set of prime ideal factors P_i.

THEOREM 8. The irreducibility criterion. *If $\mathfrak{p}$ is a prime ideal from the algebraic number field K and if $\mathfrak{p}$ has but one prime ideal factor in $\mathfrak{O}$, then the polynomial $G(x)$ is a power of an irreducible polynomial.*

Proof. The decomposition of $\mathfrak{p}$ in $\mathfrak{O}$ is obtained, as in Theorem 6, by combining decompositions from all the direct summand fields K_i. If the final decomposition of $\mathfrak{p}$ is to have but one factor, there can be only one such direct summand and hence only one irreducible factor $g_i(x)$ in (9).

THEOREM 9. *If K is an algebraic number field, δ an integer in K, and $G(x)$ a polynomial such that the principal ideal (δ) becomes the nth power of an ideal in $\mathfrak{O}$, then any factor of $G(x)$ in $K[x]$ has a degree r such that $(\delta)^r$ is the nth power of some ideal in the ring of integers of K.*

One case of this theorem, in which the decomposition $(\delta)=B^n$ was insured by specifying the form of $G(x)$ and taking $n=\deg G(x)$, was first stated by Sopman.* The general Theorem 9 can be established by Sopman's methods, applied to the fields K_i, or by the direct use of Theorem 8.

5. **Approximants and prime ideals in algebraic rings.** Our two forms of the irreducibility criterion are essentially the same, because the approximants to any polynomial $G(x)$ can be used to construct the prime ideals in the corresponding $K[x]/(G(x))=A$. For a prime ideal $\mathfrak{p}$ from the algebraic number field K let V_0 be the $\mathfrak{p}$-adic absolute value of K. Without essential loss of generality, we assume throughout this section that $G(x)$ has first coefficient 1 and its other coefficients V_0-integers. If in (9) we make all factors $g_i(x)$ have the first coefficient 1, they will also have V_0-integers as coefficients.

THEOREM 10. *Given a $G(x)$ and a $\mathfrak{p}$-adic value V_0 of K, there is for k sufficiently large a one-to-one correspondence between the kth approximants V_k to G over V_0, and the prime ideal factors P' of $\mathfrak{p}$ in $\mathfrak{O}$. If ϕ_k is the last key polynomial of V_k, and P' is the corresponding prime ideal, then*

$$\deg \phi_k = (\deg P')(\exp P'). \tag{12}$$

---

* M. Sopman, *Ein Kriterium für Irreduzibilität ganzer Funktionen in einem beliebigen algebraischen Körper*, Mathematische Annalen, vol. 91 (1924), pp. 60–61.

Proof. If for G as in (9) we set $G^*(x) = g_1(x)g_2(x) \cdots g_t(x)$, then, by Lemma 1, G and G^* have the same kth approximants. The "finiteness" Theorem 8.1 of Const II applies to G^*, and gives a k' so large that, for $k \geqq k'$, every kth approximant V_k to G^* has the projection 1. Each V_k is then, by (5), an approximant to just one factor $g_i(x)$ of G^*. But each approximant to the irreducible $g_i(x)$ constructs an extension W of the value V_0 to the field K_i (Const II, Theorem 10.2). Each such W corresponds to just one prime ideal factor P_i of $\mathfrak{p}$ in $\mathfrak{O}_i$, while, by Theorem 6, P_i corresponds to just one prime ideal factor P' of $\mathfrak{p}$ in $\mathfrak{O}$. Combining these successive correspondences we find that approximants V_k do correspond to prime ideals P', as asserted. The relation (12) follows by Const II, Theorem 9.3.

With this connection between the approximants and prime ideals, the two forms of the two irreducibility criteria become essentially identical. For if $G(x)$ has no multiple roots, then in the presence of Theorem 10, the irreducibility criterion of Theorem 8 in terms of prime ideals is immediately equivalent to the irreducibility criterion of Theorem 4 in terms of approximants. Similarly results hold for the degree-of-factors theorem, if k is large, for then (12) reduces (6) to (11). Hence the generalizations of the Eisenstein criterion are merely statements about prime ideal decompositions.

6. **Irreducibility of polynomials in several variables.** A number of theorems concerning such polynomials with coefficients in any field F will now be derived from the general results of §2.

THEOREM 11. *If $\phi(x)$ is irreducible over the field F, if $g(x, y)$ is a polynomial in $F[x, y]$ of degree in y less then n, and if $a(x) \not\equiv 0 \pmod{\phi}$ and $g(x, 0) \not\equiv 0 \pmod{\phi}$, then*

$$f(x, y) = a(x)y^n + g(x, y)\phi(x)$$

is irreducible in $F[x, y]$, except perhaps for a factor involving only x.

Proof. By the irreducibility of $\phi(x)$

$$V_0 = [V_0F = 0, V_0x = 0, V_0\phi(x) = 1]$$

is a value of the coefficient field $F(x)$, where we have indicated by $V_0F = 0$ that $V_0a = 0$ for all constants $a \neq 0$ in F. The inductive values $V_1 = [V_0, V_1y = 1/n]$ is an approximant to $f(x, y)$, and the irreducibility then follows by Theorem 2 applied to this V_1. By altering the value V_1y to m_n/n we obtain a more general theorem of this sort:

THEOREM 12. *If $\phi = \phi(x)$ is irreducible over F, if*

$$f(x, y) = a_0(x)y^n + a_1(x)\phi^{m_1}y^{n-1} + a_2(x)\phi^{m_2}y^{n-2} + \cdots + a_n(x)\phi^{m_n},$$

where the $a_i(x)$ are polynomials in $F[x]$ with $a_0(x) \not\equiv 0 \pmod{\phi}$, $a_n(x) \not\equiv 0 \pmod{\phi}$, and if the positive integers m_i are such that m_n is prime to n and $n \cdot m_i \geqq i \cdot m_n$ for $i = 1, \cdots, n$, then $f(x, y)$ is irreducible in $F[x, y]$, except perhaps for a factor involving only x.

A special case of this theorem, for $\phi(x) = x - \alpha$, was first stated by Königsberger.* If F is the field of all complex numbers the conditions of this theorem imply that the sheets of the Riemann surface hang together in a single cycle at $x = \alpha$, so that $f(x, y)$ is necessarily irreducible. In the theorem above, this single cycle is obtained by the first approximant; that is, by the first step of the Puiseux expansion. Similar theorems involving further steps of the expansion can be stated, but they are all consequences of our general criteria. The theorem corresponding to the point at infinity on the Riemann surface runs as follows:

THEOREM 13. *If $a_i(x)$ for $i = 0, 1, \cdots, n$ are polynomials in $F[x]$ with no common factors except constants, if*

$$f(x, y) = a_0(x)y^n + a_1(x)y^{n-1} + \cdots + a_n(x),$$

if $\deg a_i(x) = \gamma_i$ *satisfies the conditions*

$$(13) \qquad n(\gamma_i - \gamma_0) < i(\gamma_n - \gamma_0), \qquad \gamma_n - \gamma_0 \neq 0, \qquad (i = 0, 1, \cdots, n-1),$$

and if $\gamma_n - \gamma_0$ is prime to m, then $f(x, y)$ is irreducible in $F[x, y]$.

A related theorem stated by Perron† replaces (13) by the condition that there is an integer j such that

$$\gamma_j > \gamma_i, \qquad j\gamma_i < i\gamma_j \qquad \text{(for } i = 1, \cdots, n, \text{ but } i \neq j)$$

holds, while $a_0(x) = 1$, and γ_j is prime to j. This theorem is apparently more general, but it can be deduced from Theorem 13 by simply interchanging x and y. The effect of the change can be visualized by constructing the Newton polygon for V_0.

Still other types of theorems are possible in case the coefficient field is not algebraically closed.

THEOREM 14. *If $\phi(x)$ is irreducible over F, if*

$$\psi(x, y) = y^m + a_1(x)y^{m-1} + \cdots + a_m(x), \qquad a_i(x) \text{ in } F[x],$$

is irreducible‡ $\pmod{\phi(x)}$ *in $F[x, y]$, if*

* Königsberger, loc. cit., p. 63.

† O. Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, Journal für die Mathematik, vol. 132 (1907), p. 304. See also Blumberg, loc. cit., p. 543.

‡ In other words if $\psi(\theta, y)$ is irreducible in $F(\theta)[y]$, where θ is a root of $\phi(x) = 0$.

$$f(x, y) = \psi(x, y)^e + g(x, y)\phi(x)\psi(x, y) + r(x, y)\phi(x),$$

where the degrees of g *and* r *in* y *satisfy* $\deg_y r(x, y) < m$; $\deg_y g(x, y) < m(e-1)$, *and if* $r(x, y) \not\equiv 0 \pmod{\phi}$, *then* $f(x, y)$ *is irreducible in* $F[x, y]$.

Proof. If we omit the case where $m=1$ and $a_m(x) \equiv 0 \pmod{\phi}$, the conditions on $\psi(x, y)$ suffice to make ψ a key polynomial over the value

$$V_1 = [V_0 F = 0, V_0 x = 0, V_0\phi(x) = 1, V_1 y = 0]$$

of $F[x, y]$. The only second stage approximant to f over V_0 is $V_2 = [V_1, V_2\psi(x, y) = 1/e]$. The given form of $f(x, y)$ shows that the expansion of f will satisfy the conditions of Theorem 2 for irreducibility. In the omitted case where $m=1$ and $a_m(x) \equiv 0 \pmod{\phi}$, the theorem is a direct consequence of Theorem 11.

Other theorems may be obtained by using the non-trivial values of the coefficient field F.

THEOREM 15. *If* R *is the field of rational numbers, if* p *is a prime, if* $\phi(x)$ *is a polynomial irreducible* (mod p), *if*

$$f(x, y) = y^n + g(x, y)\phi(x) + h(x, y)p,$$

where the polynomials g *and* h *have integral coefficients and degrees in* y *less than* n, *and if either* $g(x, 0) \not\equiv 0$ (modd $p, \phi(x)$) *or* $h(x, 0) \not\equiv 0$ (modd $p, \phi(x)$) *holds, then* $f(x, y)$ *is irreducible in* $R[x, y]$.

This theorem follows from Theorem 2 applied to the value

$$V_1 = [V_0 p = 1, V_0 x = 0, V_0\phi(x) = 1, V_1 y = 1/n].$$

If $h=0$, Theorem 15 is a special case of Theorem 11. Other simple cases of Theorem 15 arise for $\phi(x) = x$. Under the same conditions on ϕ, g, and h, it is also possible to assert the irreducibility of

$$y^n + g(x, y)\phi(x)^e + h(x, y)p^f,$$

provided $(e, n) = 1 = (f, n)$.

Theorems on polynomials in several variables may also be stated. For example, the following theorem can be proven for any number of variables.

THEOREM 16. *If* F *is any field, if*

$$f(x, y, z) = a(y, z)x^k + b(x, z)y^m + c(x, y)z^n$$

where $a(y, z)$, $b(x, z)$, *and* $c(x, y)$ *are polynomials with coefficients in* F, *each with degrees less than* k, m, *and* n *in* x, y, *and* z *respectively, while* $a(0, 0) \neq 0$, $b(0, 0) \neq 0$, *and* $c(0, 0) \neq 0$, *and if* $(k, m) = 1$, $(k, n) = 1$, $(m, n) = 1$, *then* $f(x, y, z)$ *is irreducible in* $F[x, y, z]$.

Shanok* has also stated irreducibility criteria for polynomials in several variables in terms of convex polyhedra. Corresponding to each term $x^\alpha y^\beta p^\gamma$ in the polynomial there is a point with the coordinates (α, β, γ). Each side of the convex polyhedron on these points corresponds to a suitable absolute value $V=[Vp=\lambda, Vx=\mu, Vy=\nu]$, chosen so that three distinct terms in the original polynomial have the same minimum value. Thus, although Shanok's theorems are not special cases of ours, they could be stated in terms of absolute values.

---

* C. Shanok, *Convex polyhedra and criteria for irreducibility*, Duke Mathematical Journal, vol. 2 (1936), pp. 103–111.

CORNELL UNIVERSITY,
ITHACA, N. Y.