NEW TYPES OF IRREDUCIBILITY CRITERIA

GRACE MURRAY MOTHER

PLEASE SIGN THE SIGNATURE SHEET IN FRONT OF THE VOLUME.

THANK YOU VERY MUCH,
YALE UNIVERSITY
INTERLIBRARY LOANS
NEW TYPES OF IRREDUCIBILITY CRITERIA

Grace Murray Hopper

A.B. Vassar College 1923
M.A. Yale University 1930

A Dissertation
presented to the faculty
of the Graduate School of Yale University
in Candidacy for the Degree of
Doctor of Philosophy
1934
The author wishes to acknowledge her indebtedness to Professor Oystein Ore for his suggestions and criticisms and to express her appreciation of the assistance which he has offered throughout this investigation.
The Newtonian polygon occupies an important position among the criteria used to determine the reducibility of a polynomial $f(x)$. It is proposed to extend the use of this polygon in order to develop certain criteria dependent upon the absolute values as well as the divisibility properties of the coefficients.

In the first part will be given a historical outline of those theorems and generalizations which have been shown to depend on the above mentioned polygons. A brief review of other types of criteria will also be given.

The Newtonian polygon as defined by Dumas is then extended to one of closed convex form, the upper sides of which are dependent upon the absolute values of the coefficients. The study of these polygons leads to an approximate multiplication theorem. The converse, the decomposition of these polygons, leads to certain criteria of irreducibility. While these are algebraic in nature they will, in general, be stated in geometric form, with algebraic formulation for certain specific cases.
# TABLE OF CONTENTS

Acknowledgment ....................................................................................... i
Preface ........................................................................................................ ii

I. Historical Introduction
   1. Earliest Theorems on Irreducibility ................................................. 1
      Schönenmann, Eisenstein
   2. Generalizations of the Theorem of Eisenstein ............................. 3
      Königberger, Netto, Bauer, Ore
   3. Generalizations of the Theorem of Schönenmann ....................... 7
      Kahan, Bauer, Ore
   4. The Newtonian Polygon .............................................................. 9
      Dumas, Furtwangler, Kürschak, Ore
   5. Criteria Dependent upon Values for Integral Arguments ........... 12
      Schur, Westlund, Flügel, Stäckel, Polyá, Brauer, Brauer and Hopf, Ille,
      Wegner, Dorwart and Ore
   6. Other Types of Criteria ............................................................... 19
      Schur, Perron

II. The Closed Convex Polygon
   1. The Polygon of $f(xy)$ .................................................................. 22
   2. The Polygon of $f(x)$ .................................................................. 26

III. On the Product of Two Polynomials ................................................. 30

IV. Irreducibility Criteria
   1. The Application of the Convex Polygon ..................................... 39
   2. Irreducible Polygons ............................................................... 40
   3. Polygons of Type I ................................................................. 42
   4. Polygons of Type II ............................................................... 51
   5. Numerical Cases ...................................................................... 55

V. Bibliography ....................................................................................... 57

Addenda
   Abstract and Report ................................................................. 63
CHAPTER I
HISTORICAL INTRODUCTION

1. Earliest Theorems on Irreducibility

Given a polynomial
\[ f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_r x + a_n, \]
where the coefficients \( a_0, a_1, \ldots, a_r \) are rational integers. It is frequently necessary to decide whether or not there exists a decomposition,
\[ f(x) = f_1(x) f_2(x) \cdots f_r(x) \]
where \( f_i(x) = b_{i0} x^{n_i} + b_{i1} x^{n_i-1} + \cdots + b_{ir_i} x + b_{ir_i} \), \( i = 1, 2, \ldots, r \),
the coefficients \( b_{ij} \) are rational integers and \( \sum_{i=0}^{r} n_i = n \).

Among the methods of deciding this question which may be completed in a finite number of steps are those of

---

Kronecker, Runge, and Mandl. Since these calculations are exceedingly long and tedious to manipulate, it is natural that criteria dependent upon the coefficients should be sought.

The earliest of this type was that of Schönemann;

Theorem: Given
\[ f(x) = \phi^t(x) + pM(x). \]
Then \( f(x) \) is irreducible if
\[ M(x) \neq 0 \pmod{p \phi(x)}, \]
\( \phi(x) \) is a prime function of degree \( s \), and \( M(x) \)
is of degree less than \( st \).

Schönemann's theorem was followed in 1850 by

that of Eisenstein.

Theorem: Given
\[ f(x) = x^n + a_1 x^{n-1} + \ldots + a_n, \]

---


"Von denjenigen Moduln, welche Potenzen von Primzahlen sind." Journal für Mathematik. XXXII (1846), 93-100.

where the coefficients $a_i$ are rational integers, 

$$a_n \neq 0.$$ 

If $a_i = 0 \pmod{p}, \quad (i = 1, 2, \ldots, n),$ 

and $a_n \neq 0 \pmod{p^r}$; then $f(x)$ is irreducible.

That the theorem of Eisenstein is a special case of Schönemann's theorem is apparent when 

$$\phi(x) = x^k, \quad M(x) = b_n x^n + \ldots + b_1.$$ 

2. Generalizations of the Theorem of Eisenstein.

Not until much later did any further theorems appear. Königsberger in his first paper gives little but results, but his second contains proofs for two theorems.

**Theorem:** Given 

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$ 

If $a_i = b_i \cdot p^{\frac{c_i}{n}} \neq 0, \quad (i = 1, 2, \ldots, n-1),$ 

$$a_n = b_n \cdot p^r, \quad b_n \neq 0 \pmod{p}, \quad a_n \neq 0 \pmod{p},$$ 

and $(r, n) = 1$; then $f(x)$ is irreducible.

**Theorem:** Given 

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0.$$ 

If $a_n \neq 0 \pmod{p} \neq 0 \pmod{q},$ 

$$a_{n-r} = p^r q^r b_n, \quad b_n \neq 0 \pmod{p} \neq 0 \pmod{q},$$ 

where $n - \frac{1}{\mu}, \quad (\frac{\mu}{q}) = 1$, $p$ and $q$ are two different rational primes, and the symbol $\left( \frac{p}{q} \right)$ indicates one or

7. Schönemann, "Über einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze irreducible Congruenzen betreffend." *Journal für Mathematik.* XL (1850), 188.


zero according as \( r \) is or is not divisible by \( s \); then \( f(x) \) is irreducible.

Königsberger proves these statements by analogy to certain theorems in algebraic functions. He sets up an equation whose roots are powers of those of \( f(x) \). This equation is reducible simultaneously with \( f(x) \) and the irreducibility of the new equation can be shown by the theorem of Eisenstein.

Netto gives several theorems concerning the number and degrees of possible factors of certain types of polynomials.

**Theorem:** Given
\[
f(x) = x^n + a_1x^{n-1} + \ldots + a_n.
\]
If \( a_i = pb_i \), \( (i = 1, 2, \ldots, \alpha - 1) \), then \( f(x) \) has no factors of degree less than \( \alpha + 1 \).

**Corollary I:** If \( n = 2\alpha + 2 \); then \( f(x) \) can have only two irreducible factors both of degree \( \alpha + 1 \).

**Corollary II:** If \( n = 2\alpha + 1 \); then \( f(x) \) is irreducible.

**Theorem:** Given
\[
f(x) = x^n + a_1x^{n-1} + \ldots + a_n.
\]
If \( a_i = pb_i \), \( (i = 0, 1, \ldots, n - 2\alpha - 2) \), then \( f(x) \) has no factors of degree less than \( \alpha + 1 \).

**Corollary I:** If \( n = 2\alpha + 2 \); then \( f(x) \) can have only two irreducible factors both of degree \( \alpha + 1 \).

**Corollary II:** If \( n = 2\alpha + 1 \); then \( f(x) \) is irreducible.

---

then \( f(x) \) can at most have two factors, the degree of one being not less than \( 2^s + 2 \) and that of the other not less than \( s + 1 \).

Theorems giving criteria for polynomials which are either irreducible or have irreducible factors of degree \( n-1 \) or \( n-2 \) are also included in this paper.

11

In 1900 Königsberger gives a more general criterion.

Theorem: Given

\[
f(x) = x^n + p \delta_{\alpha_2} a_{\alpha_2} x^{n-\alpha} + \ldots + p \delta_{\alpha_s} a_{\alpha_s} x^{n-s} + q \mu \beta \ v \ a_{\mu} x^{n-\mu} + \ldots + q \mu \beta \ v \ a_{\mu} x^{n-\mu} + \ldots + p \delta_{\alpha_2} q \mu \beta \ v \ a_{\alpha_2} x + p \delta_{\alpha_2} q \mu \beta \ v \ a_{\alpha_2},
\]

where \( p \) and \( q \) are two different rational primes.

If

\[
\delta_{\alpha_i} = \left\lceil \frac{(\mu_i - \alpha_i)}{\mu_i + \rho_i} \right\rceil \quad \text{or} \quad \left\lceil \frac{(\mu_i - \alpha_i)}{\mu_i + \rho_i} \right\rceil + 1
\]

\[
\delta_{\beta_i} = \left\lceil \frac{(\mu_i - \beta_i)}{\mu_i + \rho_i} \right\rceil \quad \text{or} \quad \left\lceil \frac{(\mu_i - \beta_i)}{\mu_i + \rho_i} \right\rceil + 1
\]

\[
\epsilon_{\alpha_i} = \left\lceil \frac{v - \alpha_i}{\mu_i} \right\rceil \quad \text{or} \quad \left\lceil \frac{v - \alpha_i}{\mu_i} \right\rceil + 1
\]

according as \( e \) is or is not an integer,

\[
\mu_i + \rho_i > \frac{v}{\mu_i}, \quad \frac{\rho_i}{\mu_i}, \quad \frac{\rho_i}{\mu_i}, \quad \frac{v}{\mu_i}
\]

the fractions \( \frac{\rho_i}{\mu_i}, \frac{\rho_i}{\mu_i}, \frac{v}{\mu_i} \) are irreducible,

\[
a_o \neq 0 \, (\text{mod } p) \neq 0 \, (\text{mod } q)
\]

\[
a_{\mu_i} \neq 0 \, (\text{mod } p), \quad a_{\nu} \neq 0 \, (\text{mod } q);
\]

then \( f(x) \) is irreducible.

12

Bauer's extension of this theorem made it applicable

---


for any number of primes. His proof depends upon ideal theory.

Theorem: Given

\[ f(x) = x^n + a_1 x^{n-1} + \ldots + a_n. \]

If 1) \( n = \prod_{i=1}^{r} n_i \), where the \( n_i \) are all relatively prime,
2) \( a_i = \prod_{s=1}^{\ell} p_i^{\ell - \alpha_i} C_i \), where the \( \alpha_i \) are positive integers such that \( (\alpha_i, n_i) = 1 \). (The symbol \( \lceil \frac{\alpha}{n} \rceil \) denotes the largest rational integer less than or equal to \( \frac{\alpha}{n} \).)

3) \( (C_n, \prod_{s=1}^{\ell} p_i) = 1 \), \( p_i, p_2, \ldots, p_r \) are different rational primes; then \( f(x) \) is irreducible.

All of the previous theorems are included in one given by Perron who makes use of two auxiliary theorems from ideal theory.

1. A rational prime can have at most \( n \) prime ideal factors in a field of degree \( n \).

2. A rational prime can only be the \( n \)th power of a prime ideal if the degree of the field containing the prime is divisible by \( n \).

Theorem: Given

\[ f(x) = x^n + a_1 x^{n-1} + \ldots + a_n. \]

If \( a_i = \prod_{s=1}^{\ell} p_i^{\ell - \alpha_i} C_i \), \( (i=1, 2, \ldots, n-1) \),
\( a_n = \prod_{s=1}^{\ell} p_i^{\ell - \alpha_n} C_n \), \( (C_n, \prod_{s=1}^{\ell} p_i) = 1 \),
and the \( r+1 \) numbers \( n, \alpha_1, \alpha_2, \ldots, \alpha_n \), have no common divisor; then \( f(x) \) is irreducible.

Perron extended this method to certain other theorems on the number and the degrees of possible factors, including a proof of Netto's first theorem.

---

Ore further extended these theorems to reducibility in an arbitrary algebraic field, using the prime ideals \( \mathfrak{p} \) in place of the primes \( p \).

**Theorem:** Given

\[
f(x) = x^n + a_1 x^{n-1} + \ldots + a_n,
\]

where the \( a_i \) are integers in an algebraic field \( K(\mathfrak{p}) \).

If \( a_i = \prod_{\mathfrak{p}} \frac{b_i}{\mathfrak{p}} \), \((i=1, 2, \ldots, n)\),

\[
(b_n, \prod_{\mathfrak{p}} \frac{b_i}{\mathfrak{p}}) = 1, \quad \mathfrak{p}, \mathfrak{p}_2, \ldots, \mathfrak{p}_r \text{ are prime ideals. Here } \frac{a}{b} \text{ indicates the rational integer next greater than } \frac{a}{b} \text{ if } \frac{a}{b} \text{ is not integral and } \frac{a}{b} \text{ if it is integral.}
\]

If \( n, \alpha, \alpha_2, \ldots, \alpha_r \) have no common factor \( f(x) \) is irreducible. If \( \gamma \) is the greatest common factor of \( n, \alpha, \alpha_2, \ldots, \alpha_r \) and \( \gamma \) is one of the numbers \( 1, 2, \ldots, e \); then \( f(x) \) can only have factors of degree \( m = \frac{Y_k}{e} \).

In the rational field this reduces to a theorem similar to that of Perron but imposing more stringent conditions. In this same paper Ore adds the theorem:

**Theorem:** Given

\[
f(x) = x^n + a_1 px^{n-1} + \ldots + a_npx + a_n p.
\]

If \( a_1 \neq 0 \text{(mod } p) \); then \( f(x) \) will be irreducible in all algebraic fields \( K(\mathfrak{p}) \) in which \( p \) does not divide the discriminant of \( \mathfrak{p} \).

3. **Generalizations of the Theorem of Schonemann.**

The first such theorems are given by

---

Theorem: Given the polynomial
\[ f(x) = x^n + c_{n-1}x^{n-1} + p(c_{n-2}x^{n-2} + \ldots + c_1x + c_0, x \pm 1). \]
If \( c_{n-1} \neq 0 \pmod{p} \neq \pm 1 \pmod{p} \); then \( f(x) \) is irreducible.

Theorem: Given the polynomial
\[ f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + p(c_1x + c_0, x \pm 1), \]
where \( c_{n-1} \neq 0 \pmod{p} \neq \pm 1 \pmod{p} \). If no root of this polynomial is equal to \( \pm 1 \); the polynomial is irreducible.

The next theorem, a more direct generalization, was proved by Bauer in 1905. The proof is completed by means of ideal theory.

Theorem: Given \( \Phi(x) = \frac{\varphi(x)}{\varphi(x)} + \frac{\varphi(x)}{\varphi(x)} \).

If 1) \( \Phi(x) \) is a prime function \( \pmod{p} \) of degree \( m \),
2) \( (t, \omega) = 1 \),
3) the degree of \( \Phi(x) \) is less than \( mt \), and
4) \( \Phi(x) \neq 0 \pmod{p} \), \( \Phi(x) \); then \( f(x) \) is irreducible.

This theorem was included in a more general one by Ore.

Theorem: Given
\[ f(x) = \frac{n}{\sum_{i=1}^{n} f_i(x)^{c_i} + p^\omega \Phi(x), f(x) \text{ of degree } n. \]

If 1) \( f_i(x) \) is a prime function of degree \( n \),
2) \( (e_1, \alpha) \equiv b_i \),
3) the degree of \( M(x) \) is less than \( n \), and
4) \( M(x) \not\equiv 0 \pmod{p, f_i(x)} \); then \( f(x) \) can only have factors of degree

\[ r_i = \sum_{j=1}^{s} k_i \frac{c_i}{b_i} n_i, \]

where \( k_i \) is one of the numbers 1, 2, \ldots, \( b \).

For \( s = 1 \) and \( (e, \alpha) = 1 \), this is the theorem of Bauer.
Ore also indicates that this theorem may be generalized to the case where \( f(x) = \sum_{j=1}^{r} f_j(x)^{e_i} + kM(x), \) \( k = \frac{r}{\sum_{j=1}^{r} p_j} \), and states this theorem for the case of \( s = 1 \).

**Theorem:** Given \( \phi(x) = \sum_{j=1}^{r} \frac{c_j}{p_j} M(x) \)

If 1) \( \phi(x) \) is a prime function of degree \( m \),
2) \( (e_1, \alpha_1, \alpha_2, \ldots, \alpha_r) = b \),
3) the degree of \( M(x) \) is less than \( \alpha m \), and
4) \( M(x) \not\equiv 0 \pmod{p, \phi(x)} \); then \( f(x) \)
can only have factors of degree \( r = \frac{k}{b} m \) where \( k \) is one of the numbers 1, 2, \ldots, \( b \).

4. **The Newtonian Polygon.**

The Newtonian polygon of a polynomial is defined as the least convex polygon lying on or below the points \( P_i \) defined as follows:

Given \( f(x) = x^{n_r} a_r x^{n_{r-1}} \ldots + a_1 \).

If \( a_i = p^{\alpha} b_i \), \( b_i \not\equiv 0 \pmod{p} \);
then \( P_i = (n-1, \alpha_i) \).

In 1906 Dumas proved that the polygon of a polynomial coincides

---

with the product of the polygons of the factors. Here
the product of two polygons is defined as the polygon
formed by laying off the sides of the factor polygons in
order of increasing inclination. Hence if the polygon
of a polynomial is a straight line crossing no lattice
points, the polynomial is irreducible.

If a polynomial satisfies the theorem of
Eisenstein evidently the polygon will be the straight
line \((n,0),(0,1)\) which contains no lattice points.

If the conditions of Königsberger's theorem are satisfied, the polygon will likewise be a straight line
\((n,0),(0,r)\) containing no lattice points since \((n,r)=1\).

Suppose the Newtonian polygon of \(f(x)\) has the
sides \(S_1, S_2, \ldots, S_m\) whose projections on the \(x\) and \(y\)
axes are respectively \(l_1, l_2, \ldots, l_m\), \(k_1, k_2, \ldots, k_m\).
The slopes of the sides can then be indicated by
\[\tan \theta_i = \frac{k_i}{l_i}\]
If \((k_i, l_i) = e_i\) then \(k_i = e_i \rho_i, l_i = e_i \lambda_i\) and
\[\tan \theta_i = \frac{\rho_i}{\lambda_i} \quad (\rho_i, \lambda_i) = 1.
Dumas' product theorem then gives the theorem:

**Theorem:** \(f(x)\) can have factors of degree \(r\) only
when \(r\) is of the form
\[r = \sum_{i=1}^{m} \mu_i \lambda_i\]
where \(\mu_i\) is one of the numbers \(0,1,2, \ldots, e_i\).

19. Förtwangler states a similar theorem in the

---

19. Förtwangler, "Über Kriterien für irreducible und für
primitive Gleichungen." *Mathematische Annalen.*
LXXXV (1922), 34-40.
form:

Theorem: Given the polynomial
\[ f(x) = e_0 x^n + p e_1 a_1 x^{n-1} + \ldots + p^{e_n} a_n x + p^{e_n} a_n \]
where \( a_i \neq 0 \pmod{p} \).

1) If the positive fraction \( \frac{\epsilon_i}{\epsilon} \leq \frac{e_n-k}{k} \) (i = 1, 2, ..., n); then \( f(x) \) is either irreducible or if reducible can have factors only of degree \( \lambda \frac{n-k}{t} + \mu \), \( t = (e_{n-k}, n-k) \), \( \lambda \) and \( \mu \) are integers \( \lambda > 0, 0 < \mu < k \).

2) If \( (e_{n-k}, n-k) = 1 \) then \( f(x) \) is reducible has one factor whose degree is at least \( k \).

3) If \( k = n \); then \( f(x) \) if reducible can have factors only of degrees which are multiples of \( \lambda \frac{n}{t} \) where \( t = (n, e_n) \).

4) If \( k = n \) and \( (n, e_n) = 1 \); \( f(x) \) is irreducible.

20 Kürschak’s paper published in 1923 defines a more general type of polygon giving a generalized Dumas-Eisenstein theorem.

However in the same year, Ore extended the definition of the Newtonian polygon to completely generalize the Schönemann-Eisenstein theorems.

Given the polynomial,
\[ f(x) = x^n + A_1 x^{n-1} + \ldots + A_n x + A_n \]
Choose \( p \) a rational prime and \( \phi(x) \) a prime function (mod \( p \)) whose degree \( m \) is a divisor of \( n \). \( f(x) \) can then


be written in the form:

\[ f(x) = \sum_{i=0}^{\infty} a_i \phi_i(x) \alpha_i \phi_i'(x), \]

where \( a_i \neq 0 \) (mod \( p \)), and \( \phi_i(x) \) is at most of degree \( m-1 \).

If the points \( P_i = (s-i, \alpha_i) \) are plotted, a Newtonian polygon can be constructed. From this polygon Ore derived the general theorem.

**Theorem:** Given

\[ f(x) = a_0 \phi^n(x) + a_1 \phi^{n-1}(x) \ldots + a_n \phi(x). \]

If 1) \( \phi(x) \) is a prime function (mod \( p \)) of degree \( m \),

2) \( \alpha_i = \alpha_{i+1} \frac{\phi'_{i+1}}{\phi_i', \ldots, \alpha_n = \alpha_{n-1} \phi'(x).} \)

\( a_0 \neq 0 \) (mod \( p \)), \( \alpha_n \neq 0 \) (mod \( p \)),

3) the degree of \( \phi_i(x) \) is at most \( m-1 \), and

4) \( \phi_n(x) \neq 0 \) (mod \( p \))

then \( f(x) \) can only have factors of degree

\[ t = m \frac{n-1}{r}, \]

where \( e = (n,r) \) and \( \tau \) is one of the numbers 1, 2, \ldots, \( e \).

5. **Criteria Dependent Upon Values for Integral Arguments.**

In 1908 Schur proposed the problem:

When are the polynomials

\[ f(x) = (x-a_1)(x-a_2) \ldots (x-a_n)+1 \]

\[ f'(x) = (x-a_1)(x-a_2) \ldots (x-a_n)-1 \]

reducible or irreducible in the rational field?

Westlund showed that \( f'(x) \) is always irreducible.

---


and that $f(x)$ is reducible only if it is a perfect square.

24

Flügel in solving the problem set by Schur gave the more complete solution that $f'(x)$ is always irreducible and $f_2(x)$ is reducible only in the two cases

$$(x-a)(x-a+2)+1 = [(x-a+1)]^2$$

$$(x-a)(x-a+1)(x-a+2)(x-a+3) = [(x-a)(x-a+3)+1]^2.$$  

In the same year Schur set a second problem:

Show that $f_1(x) = (x-a)(x-a+1)\ldots(x-a_n)+1$

$\ell(x) = (x-a)(x-a+1)\ldots(x-a_n)+1$

are irreducible in the rational field.

25

A few years later Stäckel considered rational integral functions taking prime values for integral arguments. He made use of several auxiliary theorems.

There is no rational integral function which for integral arguments represents only prime numbers. If a function represents an infinite number of primes it is irreducible. A reducible function of degree $n$ can at most represent $2n$ primes when integers are substituted for $x$. Therefore when $k$ exceeds some arbitrary limit $f(k)$ will represent only composite numbers.

Finally, every rational integral function $f(x)$ defines a related positive integer $S$ such that $f(x)$

is irreducible in the rational field if for \( k > S \), \( f(k) \) represents a prime.

**Theorem:** If \( A \) is the upper bound of the coefficients; i.e., \( A > |a_i| \), of a polynomial \( f(x) \) of degree \( n \geq 4 \), and if for \( k > S \),

\[
S = 2^\frac{1}{2} \frac{n!(n-1)}{1!2!3!... (n-1)!}
\]

\( f(k) \) is a prime; then \( f(x) \) is irreducible.

Polya in order to prove three criteria makes use of the auxiliary theorem:

If a polynomial \( f(x) \) of \( n \)th degree is such that for \( n+1 \) values \( \gamma_i \) of \( x \),

\[
|f(\gamma_i)| < \frac{n!}{2^n}
\]

then \( f(x) \) is not integral.

**Theorem:** If the polynomial \( f(x) \) of \( n \)th degree is such that for \( n \) values \( \gamma_i \) of \( x \), no \( f(\gamma_i) = 0 \) and

\[
|f(\gamma_i)| < \frac{(n-\lfloor \frac{n}{2} \rfloor)!}{2^{n-\lfloor \frac{n}{2} \rfloor}}
\]

then \( f(x) \) is irreducible.

**Theorem:** If there exist \( n \) integers \( \gamma_1, \gamma_2, ..., \gamma_n \) such that the difference between any two of them \( \gamma_i - \gamma_j \geq d \), \( i \neq j \), and such that when they are substituted for \( x \) in the polynomial \( f(x) \), \( f(\gamma_i) \neq 0 \) and

\[
|f(\gamma_i)| < \left( \frac{d}{2} \right)^{n-\lfloor \frac{n}{2} \rfloor} (n-\lfloor \frac{n}{2} \rfloor)!
\]

then \( f(x) \) is irreducible.

**Theorem:** If \( f(x) \) of degree \( n \geq 17 \), takes on the value \( p \) for \( n \) different integral values of \( x \) where

---

p is a rational prime; then f(x) is either irreducible or the product of two factors of the same degree.

The theorems proved by Brauer, Brauer and Hopf included a solution of Schur's second problem. Where

\[ P(x) = (x-a_1)(x-a_2) \ldots (x-a_n) \]

the three authors showed that:

**Theorem:** If \( G(x) = z^2 + 1 \); then \( G \left[ P(x) \right] \) is irreducible.

**Theorem:** If \( G(x) = cz^2 + 1 \) where \( c \) is a positive integer is irreducible; then \( G \left[ P(x) \right] \) is irreducible.

**Theorem:** If \( G(x) = z^3 + 1 \); then \( G \left[ P(x) \right] \) is irreducible.

**Theorem:** If \( G(x) = c \cdot z^2 + c_2 z^2 + c_3 z^3 + c_4 z^4 + 1 \) is an irreducible integral polynomial; then there are only a finite number of different polynomials \( P(x) \) for which \( G \left[ P(x) \right] \) will be reducible.

\( G \left[ P(x) \right] \) decomposes in factors of unequal degrees only when

\[ P(x) = x(x-1)(x+1) \]

and \( G(x) \) is one of the polynomials:

\[
\begin{align*}
z^6 - z^3 + 1 & \quad 8z^5 - 4z^3 + 1 \\
z^6 + 2z^3 + 3z + 1 & \quad 8z^5 + 3z^3 - z^2 - 3z + 1 \\
z^6 + 2z^3 - 3z + 1 & \quad 8z^5 - 3z^3 - z^2 + 3z + 1 \\
27z^6 - 9z^3 + 1
\end{align*}
\]

In the same year Ille used an auxiliary theorem similar to that of Polya. If a positively definite polynomial of degree \( n = 2k \) is such that for at least \( k \) integral values \( \xi_i \) of \( x \), \( f(\xi_i) \neq 0 \),

\[
|f(\xi_i)| < \frac{k}{2^{2k-1}}
\]

then \( f(x) \) is irreducible in the rational field. Ille used this theorem to prove that:

Theorem: \( P(x) = a(x-a_1)(x-a_2)^2 \cdots (x-a_n)^2 + 1 \) where \( a \) is a positive integer not a perfect square and \( k \geq 8 \), is irreducible.

Theorem: If \( G(x) = az^n + bz^{n-1}cz + dz + 1 \) is an irreducible polynomial, \( P(x) = (x-a_1)(x-a_2) \cdots (x-a_n) \) where the \( a_i \) are all different; then \( G[P(x)] \) can have no factors of degree less than \( k \).

30 Wegner in 1931 extended the first of Brauer, Brauer and Hopf's theorems to the case where the last term of \( G(z) \) may be different from one.

Theorem: If \( P(x) = (x-a_1)(x-a_2) \cdots (x-a_n) \), \( n > 5 \), \( d \) a rational integer not a perfect square and \( d \equiv 3(\text{mod } 4) \); then

\[
[P(x)]^d + d \text{ is irreducible.}
\]

29 Ille, "Einige Bermerkung zur einem von O. Polya herrührenden Irreduzibilitätskriterium." Jahresberichte der Deutsche Mathematiker Vereinigung. XXXIV (1926), 204-205.

The paper by Dorwart and Ore besides showing that the previous criteria may be derived from a common source, generalizes the previous criteria, adds several new theorems and extends to quadratic imaginary fields. Three theorems are derived by use of the auxiliary theorems:

A polynomial \( f(x) \) taking the value \( +1 \) \((-1) \), \( m>3 \) times cannot take the value \(-1 \) \((+1) \).

A polynomial \( f(x) \) of \( n \)th degree taking the values \(+1\) at \( m \) points \( a_1, a_2, \ldots, a_m \), where \( 4 \leq m \leq n \) can have factors only of the form

\[
g(x) = (x-a_1)(x-a_2) \ldots (x-a_m)h(x) + 1.
\]

The degree of a factor is therefore never less than \( m \), and when \( m > \frac{2n}{2} \), \( f(x) \) is irreducible.

These lead to the theorems:

**Theorem:** The polynomials

\[
f(x) = a(x-a_1)(x-a_2) \ldots (x-a_m) + 1
\]

are always irreducible except when \( f(x) \) is equivalent to one of the following polynomials,

\[
x(x-1)(x-2)(x-3) + 1 = [x(x-3) + 1]^2
\]

\[
x(x-2) + 1 = (x-1)^2
\]

\[
4(x-1)x + 1 = (2x-1)^2.
\]

This is the complete generalization of the case examined by Schur, Westlund and Flügel.

**Theorem:** The polynomials

\[
F[P(x)] = b_3P(x)^2 + b_2P(x) + 1
\]

where \( F(x) = b, x^2 + b, x + 1 \) is irreducible and
\[ P(x) = (x-a_1)(x-a_2)\ldots(x-a_n) \]
are always irreducible when \( n \geq 5 \).
The possible exceptional cases for \( n \leq 4 \) are also listed.

**Theorem:** The polynomials
\[ f(x) = c(x-a_1)^r (x-a_2)^r \ldots (x-a_n)^r + 1 \]
are always irreducible if \( c \neq b^2 \) except when \( f(x) \) is equivalent to
\[ -8(x-1)^r x^2(x-1)^2 + 1 = (2x-1)(-4x^2+6x^2-1). \]
This included Schur’s second problem and generalized the theorem of Ille.

These theorems are then extended in general form to the question of reducibility in quadratic imaginary fields.

Theorems are enunciated upon the number of times a function may take the values \(+p\) or \(-p\) which lead to the theorems:

**Theorem:** A polynomial of the form
\[ f(x) = (x-a_1)(x-a_2)\ldots(x-a_n)f_1(x) \pm p \]
where \( m > 10 \) can have factors only of degrees \( \frac{m}{2} \).

Or where \( m = n \) the degree of \( f(x) \):

**Theorem:** A polynomial of the form
\[ f(x) = a(x-a_1)(x-a_2)\ldots(x-a_n) \pm p \]
where \( n > 10 \), is irreducible if \( n \) is odd and when \( n \) is even it may have only two factors of degree \( \frac{n}{2} \).

For \( n = 10 \) it is found that this theorem holds except when \( n = 3 \) where \( f(x) \) is reducible only for the two polynomials
\[ (x-1)(x+1)(x+p) + p = x(x^2 px - 1) \]
\[ 4x(x-1)(2x+p-1) + p = (2x-1)(4x^2 px - 4x-p) \]
Theorem: A polynomial taking the values $\pm 1$ or $\pm p$ at altogether $m > 10$ points cannot have any factors of degree less than $\frac{m}{2}$.

It is also indicated that these methods may be extended to polynomials taking the value $\pm d$, and generalized to quadratic imaginary fields.

6. Other Types of Criteria.

Schur in 1929 added criteria for several special types of polynomials. Four similar types are defined.

Theorem: Every polynomial of the form

$$f(x) = 1 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + \ldots + a_n \frac{x^n}{n!} \pm \frac{x^n}{n!},$$

where the $a_i$ are rational integers, is irreducible.

Theorem: Every polynomial of the form

$$f(x) = 1 + a_1 \frac{x}{u_1} + a_2 \frac{x^2}{u_2} + \ldots + a_n \frac{x^n}{u_n} \pm \frac{x^n}{u_n},$$

where the $a_i$ are rational integers,

$$u_n = 1, 2, 3, \ldots, (2^n-1),$$

is irreducible.

Theorem: In general every polynomial of the form

$$f(x) = 1 + a_1 \frac{x}{u_1} + a_2 \frac{x^2}{u_2} + \ldots + a_n \frac{x^n}{u_n} \pm \frac{x^n}{u_n},$$

is irreducible. The exception is the case where $2n$ is of the form $3^n - 1$ ($r \geq 2$). In this case $f(x)$ may have a factor of the form $x^2 \pm 3$.

Theorem: A polynomial of the form

$$f(x) = 1 + a_1 \frac{x}{2!} + a_2 \frac{x^2}{3!} + \ldots + a_n \frac{x^n}{n!} \pm \frac{x^n}{(n+1)!},$$

will in general be irreducible. If however $n$ is of the form $2^n - 1$ ($r \geq 2$), then $f(x)$ may have factors...
of the form $x^2$. If $n=8$ then $f(x)$ may have two irreducible factors one of degree 2 and the other of degree 6.

In 1907 Perron introduced a new type of criterion dependent upon relations between the magnitudes of the absolute values of the coefficients. These are based on a simple principle. Given $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0$, where the $a_i$ are rational integers, $a_n \neq 0$; if the absolute value of $n-1$ of the roots are less than one, then $f(x)$ is irreducible. Perron first proves that if $f(x)$ has a root $\alpha$ such that

$$|\alpha + 1| > n + \sum_{i=2}^{n} |a_i|$$

where $A = |a_1| + |a_2| + \ldots + |a_n|$; then $|\alpha| > 1$ and the absolute values of the other $n-1$ roots are less than one. This leads to the theorems:

**Theorem:** If the coefficients of $f(x)$ satisfy the relation $|a_1| > 1 + |a_2| + |a_3| + \ldots + |a_n|$; then $f(x)$ is irreducible.

**Theorem:** If the coefficients of $f(x)$ satisfy either of the relations

$$f\left(\frac{A+1}{2}\right) < 0 \quad \text{or} \quad (-1)^n f\left(-\frac{A+1}{2}\right) < 0$$

where $A = |a_1| + |a_2| + \ldots + |a_n|$; then $f(x)$ is irreducible.

A second principle used by Perron is that if the equation $f(x) = 0$ has a pair of conjugate complex

---

roots, and the remaining $n-2$ roots are in absolute value less than one, then $f(x)$ is irreducible. From this is derived the theorem:

**Theorem:** If

$$\sqrt{\sum a_i^2} \geq 4^n \left( |a_1| + |a_2| + \ldots + |a_n| \right)$$

then $f(x)$ is irreducible.

If $f(x)$ is of degree $\geq 5$ it is irreducible if

$$\sqrt{\sum a_i^2} \geq \left( \frac{1}{2} \right)^{n-1} \left( |a_1| + |a_2| + \ldots + |a_n| \right).$$

Of interest in connection with the auxiliary theorems used by Perron is a paper by Mayer. Using a problem in probability and its difference equation Mayer showed that:

**Theorem:** Given $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$

where the $a_i$ are real or imaginary. If

$$|a_1| + |a_2| + \ldots + |a_n| + \ldots + |a_k| > 1$$

then $f(x)$ has $n-k$ roots $\alpha_i$ such that $|\alpha_i| > 1$ and $k$ roots $\alpha_j$ such that $|\alpha_j| < 1$.

In 1921 Tajima showed that if

$$|a_k| = |a_1| + |a_2| + \ldots + |a_k| + \ldots + |a_n|$$

and at least two of the quantities

$$\frac{a_1}{a_2}, \frac{a_2}{a_3}, \ldots, \frac{a_{n-1}}{a_n}$$

are not equal;

then $n-k$ of the roots are such that $|\alpha_i| < 1$ and $k$ roots such that $|\alpha_i| > 1$.

---


1. **The Polygon of** $f(xy)$.

In the rapid tracing of algebraic curves in two variables a form of Newton's polygon is used to determine approximating curves. This polygon is closed and convex in form and is defined by the powers of $x$ and $y$ appearing in the terms of the polynomial. We consider a polynomial

$$f(xy) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j.$$  

For all terms having a non-vanishing coefficient $a_{ij}$, we plot the points

$$P = (i, j)$$

in a Cartesian co-ordinate system and construct the least convex polygon including all of this set of points. For example, $f(xy) = x^2 y^2 - 5x^3 y + 3x^2 y^3 - 2x^3 y^2 + x^2 y^3 + 10x^2 y^2 + 13x^2 y - 62xy^2 - 2xy + 13y^2$.

The starting point of such a polygon may be defined as

the lowest point on the y-axis. The sides may then be assigned directions by proceeding in a counter-clockwise direction from the starting point and considering the sides as vectors. (A polygon which reduces to a straight line is considered as having two directions.)

The product of two such polygons is defined as the polygon constructed by laying off the sides of the factor polygons in order of increasing inclination. (If the inclinations of two sides are equal, their order is immaterial.) The starting point for such a construction may be defined as that point on the y-axis whose ordinate is the sum of the ordinates of the starting points of the factor polygons.

37. It must be noted here that this type of polygon has been mentioned by Shanok, Convex Polyhedra and Criteria for Irreducibility. (Dissertation 1933, Yale University.) Also that Dines in his paper "A theorem on the factorization of polynomials of certain types." (American Mathematical Society Bulletin. XXIX (1923), 440) has indicated the converse of a similar theorem for polynomials of the form

\[ P = y^n + P_{n-1}(x)y^{n-1} + \ldots + P_1(x)y + P_0(x) \]

where the coefficients \( P_i(x) \) are power series convergent in a sufficiently restricted neighborhood of the origin and vanishing with \( x \).
Consider
\[ f(xy) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j \]
where at least one \( a_{ij} \neq 0 \) and one \( a_{ij} \neq 0; \]
\[ g(xy) = \sum_{k=0}^{p} \sum_{l=0}^{q} a'_{kl} x^k y^l \]
where at least one \( a'_{kl} \neq 0 \) and one \( a'_{kl} \neq 0. \]

Then \( h(xy) = f(xy)g(xy) \)
\[ = \sum_{k=0}^{p} \sum_{l=0}^{q} c_{kl} x^k y^l \]
where \( c_{kl} = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} a'_{kl} x^i y^j \).

We see that the construction of the product of two polygons could also be defined as follows:

To every point \((i, j)\) of \( P_i \) and \((k, l)\) of \( P_j \) is drawn a vector from the origin.

By the laws of vector combini-
By definition the polygon $P_{\delta}$ of $h(xy)$ is the least convex polygon containing the points $(u,v); i.e., 
(i+k, j+l)$. Hence the points defining the polygons $P_{\delta}$ and $P_{\delta'}$ coincide provided that $c_{uv} \neq 0$.

In order that $c_{uv} = 0$, it is necessary that the summation defining $c_{uv}$ shall contain more than one term and that for these terms

$$i_1+k = i'_1+k' = i''_1+k'' = \ldots = u$$
$$j_1+l = j'_1+l' = j''_1+l'' = \ldots = v$$
or

$$c_{uv} = a_{i_1}a_{k_1} + a_{i'_1}a'_{k'_1} + a_{i''_1}a''_{k''_1} + \ldots$$

Consider any two of these terms

$$a_{i_1}a_{k_1} x^{i+k} y^{j+l} \text{ and } a_{i'_1}a'_{k'_1} x^{i'+k'} y^{j'+l'}$$

These are derived from the terms

$$a_{i_1} x^{i_1} y, a_{k_1} x^{k_1} y \text{ and } a_{i'_1} x^{i'_1} y, a_{k'_1} x^{k'_1} y$$

respectively. We then consider the second pair of terms defined by the opposite combination of these terms

$$a_{i_1}a_{k_1} x^{i+k} y^{j-l}, a_{i'_1}a'_{k'_1} x^{i'+k'} y^{j'-l'}$$

These terms define the points

$$(i+k', j-l') (i'+k, j'+l')$$

The midpoint of the line joining these points is

$$\left(\frac{i+k+i'+k', j+l+j'+l'}{2}, \frac{i+k+i'+k', j+l+j'+l'}{2}\right)$$

or since $i+k = i'+k' = u$, $j+l = j'+l' = v$,

this midpoint is the missing point $(u,v)$ of $P_{\delta}$.

That is, if a point $P$ of $P_{\delta}$ corresponding to a point of $P_{\delta} + P_{\delta}$ is missing through the vanishing of $c_{uv}$, it can be shown that terms on either side of this term so operate as to define points which when
plotted will so define the polygon $P_3^2$ as to include the point $P$.

We note that the two sets of points consisting one of the maximum and the other of the minimum point on each ordinate include all corner points and points on the sides of the polygon of a polynomial. That is, of the set of terms

$$a_i x^i + a_j y^j + \cdots + a_m x^m y^m$$

the first and last of these for which $a_i j \neq 0$ are those actively involved in the definition of the polygon. Thus we see that to each polynomial there corresponds but one polygon, but that there exist more than one polynomial corresponding to each polygon.

The converse of our product theorem is that if a polynomial is factorable the polygon of the polynomial is reducible to the polygons of the factors. And we may state the theorem that if the polygon of a polynomial is irreducible so also is the polynomial.

2. The Polygon of $f(x)$

Returning then to the consideration of

$$f(x) = x^n + A_1 x^{n-1} + \cdots + A_n$$

it is possible to write $f(x)$ in the form

$$f(x) = \sum_{i,j} r_{i,j} x^{i-j} p^j$$

where $p$ is a rational prime and the coefficients $r_{i,j}$ are all less than $p$.

Then the plotting of the points $(n-i,j)$ again defines a closed convex polygon. Recalling that the sign of a coefficient has no effect upon the poly-
gon, we need only consider the absolute values of the coefficients of $x$. Recalling also that the maximum and minimum points on any ordinate are the active points defining the polygon, we see that the minimum point on any ordinate $x = n-1$ corresponds to the highest power of $p$ dividing $A_i$ and the maximum point on the ordinate is $(n-1, \alpha_i)$ where
\[ p^{\alpha_i} \leq |A_i| < p^{\alpha_i + 1}. \]
That is, the lower sides of this polygon of $f(x)$ coincide with the Dumas polygon while the upper sides depend upon the magnitudes of the absolute values of the coefficients, or the logarithms of the coefficients to a base $p$.

Evidently we need not plot all of the points $(1, j)$ for our purpose, hence we shall define the polygon of $f(x)$ thus:

Given $f(x) = x^n + A_1x^{n-1} + \ldots + A_n$,
\[ A_i \neq 0, A_i \equiv 0 \pmod{p^{\alpha_i}} \neq 0 \pmod{p^{\alpha_i + 1}} \]
\[ p^{\alpha_i} \leq |A_i| < p^{\alpha_i + 1}. \]

The points $(n-1, a_i)$ $(n-1, \alpha_i)$ are plotted in a Cartesian co-ordinate system (if $A_i \neq 0$ no point is plotted on the ordinate $x = n-1$) and the least closed convex polygon including these points is constructed. For example: $f(x) = x^5 - 14x^4 + 30x^3 - 30x^2 - 60x + 26$.
\[ a_i = 1, a_i = 1, a_i = 1, a_i = 2, a_i = 2, a_i = 3, a_i = 4, a_i = 4, a_i = 5, a_i = 4. \]
We see that if a product theorem holds we shall be able to derive three forms of irreducibility criteria from these polygons.

I. The lower or Dumas polygon is irreducible, which gives rise to theorems dependent upon the divisibility properties of the coefficients.

II. The upper polygon is irreducible, which gives rise to theorems dependent upon the absolute values of the coefficients similar to those given by Perron (1907).

III. The upper and lower polygons are in themselves reducible but do not combine to form closed polygons, which gives rise to theorems dependent upon the combined properties of the coefficients.

We find when we attempt to state a product theorem that while the lower sides of $P_h + P_j$ and $P_{ij}$ coincide by Dumas' theorem, the correspondence between the upper sides is no longer exact. Consider

$$f(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} r_{ij} x^i p^j$$
$$g(x) = \sum_{k=0}^{m} \sum_{l=0}^{n} r_{kl} x^k p^l$$
$$h(x) = f(x)g(x) = \sum_{u=0}^{m+n} \sum_{v=0}^{m+n} r_{uv} x^u p^v$$

The points defining the upper sides of $P_i$ and $P_j$ are respectively

$$(n-i, \alpha_i) \quad (m-k, \beta_k)$$

These points define the points

$$(n+m-i-k, \alpha_i + \beta_k) \text{ of } P_i + P_j.$$
Consider the terms defining a corresponding point in $h(x)$; i.e., $u = i + k$. It consists of all the terms for which $i + k = u$,

$$
\sum_{j=0}^{\beta_k} \sum_{k=0}^{\infty} r_{i-j} r_{i+k} x^{i-j-k} p^{i+1}
$$

In this expansion the coefficient containing the maximum power of $p$ is

$$
F_{i\alpha_i} r_{i+j} p^{\alpha_i + \beta_k}
$$

In $f(xy)$ the coefficient $r_{i\alpha_i} r_{i+j} p^{\beta_k}$ could not affect the powers of $y$, it may now however affect the powers of $p$. If

$$
F_{i\alpha_i} r_{i+j} p_{\beta_k, \gamma_k} > p
$$

we have a term containing $p$ to the power $\alpha_i + \beta_k + 1$, and the point defining $P_{i\beta}$ lies above the corresponding point defining $P_{i\gamma} + P_{j\alpha}$. Correspondingly if in the coefficient

$$
F_{i\alpha_i - 1} r_{i+j} p^{\alpha_i + \beta_k - 1}
$$

we may have a second term containing $p$ to the power $\alpha_i + \beta_k$. If these two terms differ in sign they may cancel each other and the point defining $P_{ij}$ may fall below the point defining $P_{i\gamma} + P_{j\alpha}$. We then consider terms either side of such a variant term and see whether or not we may state that they so operate as to include the lost point or that the point lies within a certain distance of the line joining points on either side. That the latter statement is correct and the limits within which the point must lie are shown in the next chapter.
CHAPTER III.

ON THE PRODUCT OF TWO POLYNOMIALS

1. We shall consider an arbitrary polynomial
\[ f(x) = x^n + a_n x^{n-1} + \ldots + a_1 \]
with complex coefficients. For all non-vanishing coefficients \(a_i\) we plot the points
\[ P_i = (i, \log |a_i|) \quad (i = 1, 2, \ldots, n) \]
in a Cartesian coordinate system and construct the lowest convex polygon lying above all points. We shall denote the sides of this polygon by
\[ S_1, S_2, \ldots, S_r \]
The projections of these sides on the \(X\)-axis are
\[ l_1, l_2, \ldots, l_r, \]
and these numbers are all positive integers, while the projections
\[ h_1, h_2, \ldots, h_r \]
of the sides on the \(Y\)-axis are real numbers, which may be positive or negative according to the slope of the corresponding sides. The slopes themselves are then
\[ (1.) \quad k_i = \tan \phi_i = \frac{h_i}{l_i} = \log R_i (i = 1, 2, \ldots, r). \]
The first and last point of the $i$-th side are respectively
\[ (\lambda_i + \ldots + \lambda_{i-1}, \log |a_{\lambda_i,\ldots,\lambda_{i-1}}|), \quad (\lambda_i + \ldots + \lambda_i, \log |a_{\lambda_i,\ldots,\lambda_i}|) \]
and hence one finds for the slope
\[ k_i = \tan \varphi_i = \frac{1}{\lambda_i} (\log |a_{\lambda_i,\ldots,\lambda_i}| - \log |a_{\lambda_i,\ldots,\lambda_{i-1}}|) \]
or
\[ \log |a_{\lambda_i,\ldots,\lambda_i}| = \log |a_{\lambda_i,\ldots,\lambda_{i-1}}| + \lambda_i k_i \]
or also according to (1)
\[ \mathcal{R}_i = \left| \frac{a_{\lambda_i,\ldots,\lambda_i}}{a_{\lambda_i,\ldots,\lambda_{i-1}}} \right|^{\lambda_i} \]

Now let
\[ \lambda_i = \lambda_i + \ldots + \lambda_i \]
denote the abscissa of the end-point of the $i$-th side $S_i$.
We shall then compare the size of the coefficients of $f(x)$ to $|a_{\lambda_i}|$.

Let us first consider points $P_{\lambda_i+j}$ lying to the right of $P_{\lambda_i}$. Since all such points are lying on or below the $(i+1)$-st side $S_{i+1}$, we have
\[ \log |a_{\lambda_{i+j}}| \leq \log |a_{\lambda_i}| + jk_{i}, \quad \log |a_{\lambda_i}| + j \log \mathcal{R}_{i+j}, \]
or
(3)
\[ |a_{\lambda_{i+j}}| \leq |a_{\lambda_i}| \mathcal{R}^j_{i+j}. \]
In the same way one finds for the points to the left of $P_{\lambda_i}$
\[ \log |a_{\lambda_{i-j}}| \leq \log |a_{\lambda_i}| - jk_{i}, \quad \log |a_{\lambda_i}| - j \log \mathcal{R}_{i} \]
or
(4)
\[ |a_{\lambda_{i-j}}| \leq |a_{\lambda_i}| \mathcal{R}^{-j}_{i}. \]
These two inequalities (3) and (4) are fundamental in the following considerations.

2. Next let
\[ g(x) = x^n + b_1 x^{n-1} + \ldots + b_n \]
be another polynomial and let us construct the corresponding polygon with the sides

\[ S'_1, S'_2, \ldots, S'_s \]

and the slopes

\[ k'_i = \log \xi'_i \quad (i = 1, 2, \ldots, s). \]

When then \( \mu_i \) denotes the abscissa of the end-point of the \( i \)-th side \( S'_i \) we obtain the inequalities corresponding to (3) and (4):

\[
|b_{\mu_i} \cdot j| \leq |b_{\mu_i} \cdot \xi'_i|, \quad |b_{\mu_i} \cdot j| \leq |b_{\mu_i} \cdot \xi'_i|.
\]

We shall now form the product

\[ h(x) = f(x)g(x) = x^{n+m} + c_n x^{n+m-1} + \ldots + c_1 x + c_0 \]

of the two polynomials. Our main problem in the following is to determine the relation between the polygons of \( f(x), g(x) \) and \( h(x) \). We shall denote these polygons by \( P_f, P_g, \) and \( P_{h} \) respectively.

By \( P_f + P_g \) we understand the convex polygon obtained from \( P_f \) and \( P_g \) by arranging the totality of sides \( S_i \) and \( S'_j \) of these polygons according to decreasing slopes.

Our principal result is that the two polygons \( P_f + P_g \) and \( P_{h} \) are approximately equal.

We suppose first \( a_n \neq 0, b_m \neq 0 \). Since

\[ c_{n+m} = a_n b_m, \]

we find

\[ \log |c_{n+m}| = \log |a_n| + \log |b_m| \]

and this shows that the two polygons \( P_f + P_g \) and \( P_{h} \) have the same first point \((0, 0)\) and the same end-point

\[ (n + m, \log |a_n| + \log |b_m|). \]

3. We shall first determine how much greater an
ordinate \( y_{k,3} \) of \( P_k \) may be than the corresponding ordinate \( y_{k,3} \) of \( P_k + P_3 \). The coefficients in the product have the form

\[
c_i = a_i + b_i + \ldots + b_i + a_i + b_i
\]

and hence

(6) \[ |c_i| \leq |a_i| + |b_i| + \ldots + |b_i| + |a_i| + |b_i| \]

The number \( t_i \) of terms on the right-hand side of (6) is, when we suppose \( m = n, N = m + n \)

\[
\begin{cases}
  t_i = i + 1 & \text{for } i \leq m \\
  t_i = m + 1 & \text{for } n \geq i \geq m \\
  t_i = n + m + 1 - i & \text{for } i \geq n
\end{cases}
\]

In every case we have

(8) \[ t_i \leq m + 1 \leq \frac{N}{2} + 1 \]

The point \( \{i, \log |c_i| \} \) lies on or below the polygon \( P_{\xi, \gamma} \). From the construction of the sum polygon \( P_{\xi, \gamma} + P_3 \) it follows that no expression \( \log |a_i||b_i| \) can exceed the ordinate \( y_{\xi,\gamma} \) of \( P_{\xi} + P_j \) at this point. Hence we obtain from (6)

(9) \[ \log |c_i| \leq y_i + \log t_i \]

for all \( i \) and hence we obtain

(10) \[ y_{\xi,\gamma} - y_{\xi,\gamma} \leq \log t_i \leq \log (m + 1) \leq \log \left( \frac{N}{2} + 1 \right) \]

which is the result we wanted to establish.

4. The more difficult proposition is to show that the polygon \( P_{\xi,\gamma} \) cannot fall very much below \( P_{\xi} + P_j \). We shall show this by considering the difference of the ordinates of the two polygons at a corner point of \( P_{\xi} + P_j \). The ordinate \( y_{\xi,\gamma} \) at this point is

(11) \[ y_{\xi,\gamma} = \log |a_i| + \log |b_i| \],
where

\begin{equation}
(12) \quad (r, \log |a_r|), \ (s, \log |b_s|)
\end{equation}

are corner points of \( P_1 \) and \( P_2 \) respectively. We shall then have to determine a bound for the absolute value of the difference

\begin{equation}
(13) \quad \delta = \left| \log |c_{r,s}| - \log |a_r| - \log |b_s| - \log \frac{|c_{r,s}|}{|a_r|\cdot |b_s|} \right|.
\end{equation}

For \( c_{r,s} \) we have the expression

\[ c_{r,s} = a_r b_s + a_{r-1} b_{s+1} + \ldots + a_r b_s + \ldots \]

and hence from (13)

\begin{align}
(14) \quad \delta &= \left| \log \left( 1 + \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \frac{a_{r-2}}{a_r} \frac{b_{s+2}}{b_s} + \ldots \right. \\
&\quad \left. \quad \quad \quad + \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \frac{a_{r-2}}{a_r} \frac{b_{s+2}}{b_s} + \ldots \right) \right|.
\end{align}

We now determine an upper bound for the sums occurring in these expressions by means of the inequalities (3), (4) and (5), which we write in the following way

\begin{align}
(15) \quad \left| \frac{a_{r-1}}{a_r} \right| \leq \mathcal{K}_\alpha^i, \quad &\left| \frac{a_{r-1}}{a_r} \right| \leq \mathcal{K}_\alpha^{i+1} \\
\left| \frac{b_{s+1}}{b_s} \right| \leq \mathcal{H}_\beta^i, \quad &\left| \frac{b_{s+1}}{b_s} \right| \leq \mathcal{H}_\beta^{i+1}.
\end{align}

We then find

\begin{equation}
(16) \quad \left| \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \frac{a_{r-2}}{a_r} \frac{b_{s+2}}{b_s} + \frac{b_{s+3}}{b_s} + \ldots \right| \leq \mathcal{K}_\alpha^i + \mathcal{H}_\beta^i + \left( \frac{\mathcal{H}_\beta^i}{\mathcal{H}_\alpha^i} \right)^2 + \ldots
\end{equation}

and in the same way

\begin{equation}
(17) \quad \left| \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \frac{a_{r-2}}{a_r} \frac{b_{s+2}}{b_s} + \frac{b_{s+3}}{b_s} + \ldots \right| \leq \mathcal{K}_\alpha^i + \mathcal{H}_\beta^i + \left( \frac{\mathcal{H}_\beta^i}{\mathcal{H}_\alpha^i} \right)^2 + \ldots
\end{equation}

It should be observed that

\[ \mathcal{K}_\alpha > \mathcal{K}_\alpha^i, \quad \mathcal{H}_\beta > \mathcal{H}_\beta^i, \]

and from the construction of the sum polygon follows

\[ \mathcal{H}_\beta > \mathcal{H}_\beta^i, \quad \mathcal{K}_\alpha > \mathcal{K}_\alpha^i, \]
We shall now introduce the sharpness of a corner of a polygon, defining the sharpness $\sigma_\alpha$ of the $\alpha$-th corner of the polygon $P_\alpha$ through the relation

$$d_{\alpha\alpha} = \sigma_\alpha d_{\alpha\alpha+1}.$$  

In the same way $\sigma'_\beta$ is the sharpness of the $\beta$-th corner of $P_\beta$, where

$$d_{\beta\beta}' = \sigma'_\beta d_{\beta\beta+1}'.$$

Let us now consider the sharpness $\sigma$ of the corner C of $P_\beta + P_\alpha$. We have four different possibilities

- $d_\alpha' \geq d_\alpha > d_{\alpha\alpha}, \geq d_{\alpha\alpha}'$  
- $d_\alpha > d_\alpha' > d_{\alpha\alpha}, \geq d_{\alpha\alpha}'$  
- $d_\alpha > d_\alpha' > d_{\alpha\alpha}, \leq d_{\alpha\alpha}'$  
- $d_\alpha' > d_\alpha > d_{\alpha\alpha}, \leq d_{\alpha\alpha}'$

and in the respective cases we find the four values for $\sigma$

$$\sigma_\alpha, \sigma'_\beta, \frac{d_{\alpha\alpha}'}{d_{\alpha\alpha}+1}, \frac{d_{\alpha\alpha}}{d_{\alpha\alpha}+1}.'$$

A simple consideration shows that in all cases

$$\frac{d_{\alpha\alpha}'}{d_{\alpha\alpha}+1} \leq \frac{1}{\sigma}, \quad \frac{d_{\alpha\alpha}}{d_{\alpha\alpha}+1} \leq \frac{1}{\sigma}.$$  

and from (16) and (17) we obtain

$$\left| \frac{a_{r_1}}{a_r} b_{s_1} + \ldots + \frac{a_{r_n}}{a_r} b_{s_n} \right| \leq \frac{2}{\sigma-1}.$$

This in turn gives the following limits for $\sigma$

$$\log \frac{\sigma + 1}{\sigma - 1} > S > \log \frac{\sigma - 3}{\sigma - 1}$$

or

$$\frac{\sigma + 1}{\sigma - 1} |a_r||b_s| > |c_{r+s}| > \frac{\sigma - 3}{\sigma - 1} |a_r||b_s|$$

which is the result we desired to deduce. It shows that at a sharp corner point of $P_\alpha + P_\beta$ the point C of the product cannot differ greatly from it. We have for instance for $\sigma = 4$ and $\sigma = 5$ respectively.
\[
\frac{1}{3} |a_r||b_s| \leq |c_{r,s}| \leq \frac{5}{3} |a_r||b_s|
\]

(20)
\[
\frac{1}{2} |a_r||b_s| \leq |c_{r,s}| \leq \frac{3}{2} |a_r||b_s|
\]

I also observe that under certain conditions \( C \) will also be a corner point of \( P_{r,s} \) and the sharpness of the corner can only slightly exceed \( \sigma \).

5. We shall now investigate how much the polygon \( P_{r,s} \) may fall below \( P_k + P_j \) at any point at which the sharpness of \( P_k + P_j \) is less than 4. We consider two consecutive sharp points \( P_i \) and \( P_{i+1} \) of \( P_k + P_j \) corresponding to the abscissae \( s \) and \( s + t \). At \( P_i \) and \( P_{i+1} \) the polygon \( P_{r,s} \) cannot fall more than \( \log 3 \) below \( P_k + P_j \). The polygon \( P_k + P_j \) is made up of parts of \( P_k \) and \( P_j \) between the two points. At the first point it has the ordinate \( \log |a_r| + \log |b_s| \) and at the \( i \)-th point the ordinate of \( P_k + P_j \) is

(21)
\[
\log |a_r| + \log |b_s| + \sum_{j=1}^{i} k_j,
\]

where the \( k_j \) are the slopes of \( P_k \) and \( P_j \) arranged in decreasing order. We also suppose for simplicity, that every point of \( P_k + P_j \) is a corner point so that some of the \( k_j \) are equal. We assume that \( i = t \) gives us the next sharp point with the ordinate

(22)
\[
\log |a_r| + \log |b_s| + \sum_{j=1}^{t} k_j.
\]

We now join the two sharp corners with a straight line
\[
y - \log |a_r| - \log |b_s| = \frac{\sum_{j=1}^{t} k_j}{t} (x - r - s)
\]
and the ordinate of the point on this line corresponding to (21) is

(23)
\[
y_z = \log |a_r| + \log |b_s| + \frac{1}{t} \sum_{j=1}^{t} k_j.
\]
We are mainly interested in the difference between these ordinates which is found to be

\[ \Delta_i = \frac{1}{t} \sum_{j=1}^{\ell} k_j - \frac{1}{t} \sum_{j=1}^{\ell} k_j = (1 - \frac{1}{t}) \sum_{j=1}^{\ell} k_j - \frac{1}{t} \sum_{j=1}^{\ell} k_j. \]

We went to determine the maximal value of this expression. To this end we introduce the \( h_i \) by the relation \( k_i = \log h_i \) and obtain

\[ \Delta_i = \left(1 - \frac{1}{t}\right) \sum_{j=1}^{\ell} \log h_j - \frac{1}{t} \sum_{j=1}^{\ell} \log h_j \]

\[ = \log (h_1 \ldots h_\ell) - \frac{1}{t} \sum_{j=1}^{\ell} \log h_j. \]

We shall next use the fact that the sharpness of any corner of \( P_t + P_\ell \) in this interval is less than 4.

The sharpness \( \sigma \) was defined by the relation

\[ h_i = \sigma h_i, \quad \sigma \geq 1. \]

or

\[ \log h_i = \log h_i + \log \sigma_i. \]

From (26) one easily deduces

\[ h_j = \sigma_j \sigma_{j+1} \ldots \sigma_{\ell}, \quad h_\ell \]

or

\[ \log h_j = \log \sigma_j + \log \sigma_{j+1} + \ldots + \log \sigma_{\ell}, \quad h_\ell \log h_\ell. \]

From this relation follows

\[ \sum_{j=1}^{\ell} \log h_j = \log \sigma_1 + 2 \log \sigma_2 + \ldots + i \log \sigma_i + \ldots + 1 \log \sigma_{\ell} + (i-1) \log \sigma_{i-1} + 1 \log \sigma_1. \]

and

\[ \sum_{j=1}^{\ell} \log h_j = \log \sigma_1 + 2 \log \sigma_1 + \ldots + \]

\[ + (t-i-1) \log \sigma_{i+1} + (t-1) \log h_\ell. \]

When (29) and (30) are substituted in (25) we obtain an expression containing only the quantities, \( \sigma_i \)

\[ \Delta_i = \left(1 - \frac{1}{t}\right) \left( \log \sigma_1 + 2 \log \sigma_2 + \ldots + i \log \sigma_i \right) + \frac{1}{t} \left( (t-i-1) \log \sigma_{i+1} + (t-1-i) \log \sigma_{i+1} + \ldots + \log \sigma_{\ell} \right). \]
Since the coefficients in all of these terms are positive we obtain the maximal value for $\Delta_2$ by making $\sigma_i = \sigma = 4$ for all $j$. This gives

$$\Delta_2 \leq \frac{i(t - 1)}{2} \log \sigma$$

as the maximal value for the difference. Since the polygon $P_{\sigma_3}$ cannot fall more than $\log \frac{\sigma - 3}{\sigma - 1}$ below $P_\sigma + P_\sigma$ at the sharp corner points we obtain the maximal difference

$$\frac{i(t - 1)}{2} \log \sigma + \log \frac{\sigma - 3}{\sigma - 1}$$

between $P_{\sigma_3}$ and $P_\sigma + P_\sigma$. This result can however probably be considerably improved upon. For $\sigma = 4$ and $t = n$ we find

$$\Delta_2 = \log (3.2^{i(n-i)})$$

$$= \log (3.2^{i(n-i)})$$
CHAPTER IV.

IRREDUCIBILITY CRITERIA

1. The Application of the Convex Polygon

There remains to be demonstrated the method for the application of these polygons.

Given

$$f(x) = x^n + A_1 x^{n-1} + \ldots + A_i$$

In the case where the $A_i$ are rational integers, a rational prime $p$ being chosen, a congruence and an inequality may be written for each $A_i 
eq 0$:

$$A_i = 0 \pmod{p^{a_i}} \neq 0 \pmod{p^{a_i+1}}$$

$$p^{a_i} \leq |A_i| p^{a_i+1}$$

The points $(n-1, e_i)(n-1, \alpha_i)$ (indicated by X) are plotted and the least convex polygon is constructed. On any ordinate $x = n-1$ the distance $\delta_i + 1, \ i = 1, 2, \ldots, n-1$ (indicated by O) above the point where this polygon crosses the ordinate is laid off, where

$$\delta_i = \log_p (3.2^{(n-1)\epsilon})$$

On any ordinate $x = n-1, \ i = 1, 2, \ldots, n$, the distance $\delta_i + 1$ is laid off below the
point \((n-1, \infty)\) (indicated by \(\circ\)), where

\[
\delta_i = \log_p(t_i)
\]

where

\[
t_i = i+1 \quad \text{for } i \leq n/2
\]

\[
t_i = n-i+1 \quad \text{for } i \geq n/2
\]

The least convex polygon lying above and including these two sets of points are the limits of a region \(R\) (upper limit polygon \(-\) , lower limit polygon \(-\)). It is evident by the considerations of Chapter III. that if the polynomial is reducible the product of the polygons of its factors must lie on the limits of, or within, the region \(R\).

If each of the possible polygons in this region considered together with the Dumas polygon is irreducible, the polynomial is irreducible. This theorem will serve as a basis for the deduction of irreducibility criteria.

2. **Irreducible Polygons**

The most evident forms of irreducible polygons are the triangle and the trapezium none of whose sides are reducible. These are however special cases of a type of polygon having one long irreducible side.
Let \( P \) be a convex polygon with one irreducible side \( S \). Then \( P \) is irreducible if a pair of parallels \( L_L', L_2 \) can be drawn through the end-points of \( S \) such that the polygon \( P \) lies entirely within the parallels. If \( P \) is reducible let \( P' \) be the factor polygon containing \( S \). Projecting \( P' \) on \( S \) parallel to \( L \) it follows that \( P' \) must contain all other sides of \( P \). This irreducible polygon will be hereafter referred to as of type \( I \).

Type \( II. \) of the irreducible polygons depends on the construction of a centro-symmetric polygon. Such a polygon has an even number of sides, and the diagonals connecting opposite vertices bisect each other in a point within the polygon, the center of symmetry. Consider the convex polygon of a polynomial. Draw the line \( AA' \) connecting the end-points of the Dumas polygon \( ABC...DA' \). With the midpoint \( M \) of this line as center construct above the line the corner points, lattice points on the sides \( (B'C'...D') \) and sides necessary to form with the existing Dumas polygon a centro-symmetric polygon.

If the upper limit of the polygon \( P \) does not include any
of the corner points or points on the sides of this constructed polygon, then no factor polygon may have as its Dumas polygon a sequence of the first \( k \) sides of the original polygon. By construction

\[
AB \parallel A'B', \quad BC \parallel B'C', \ldots, \quad DA' \parallel D'A
\]

Suppose the contrary; that is, suppose \( AB \) is the Dumas polygon of a factor polygon \( P' \). Then the upper polygon of \( P' \) since it is to be convex must consist of a line equal and parallel to \( AB \) or lines through \( A \) and \( B \) and lying above \( AB \). This indicates a line in \( P \) coinciding with \( A'B' \) or \( A'B' \) lines through \( A' \) and \( B' \) and lying above \( A'B' \) which is contrary to the hypothesis that the points \( B', C', \ldots, D' \) are not included by the upper limit polygon of \( P \).

Suppose \( ABC \ldots D \) forms the Dumas polygon of a factor polygon \( P' \). Then the upper polygon of \( P' \) since it is convex must consist of a line equal and parallel to \( AD \) or lines through \( A \) and \( D \) and lying above \( AD \). This indicates a line in \( P \) coinciding with \( A'D' \) or lines through \( A' \) and \( D' \) and lying above \( A'D' \) which is contrary to the hypothesis.

Continuing thus we see that no sequence of the first \( k \) sides of the Dumas polygon of \( f(x) \) may form the Dumas polygon of a factor of \( f(x) \).

The next step is the application of these two types of irreducible polygons to the derivation of irreducibility criteria.

3. **Polygons of Type I.**

The first type of polygon may be placed on the co-ordinate axes in five different positions, giving rise to five forms of criteria:
1. The irreducible side $S$ forms the Dumas polygon.
   This is the Dumas criterion.

2. The irreducible side $S$ is the first side of the Dumas polygon.

   Let $AB$ be the irreducible side $S$ and $BC$ the next side of the Dumas polygon.
   \[ A = (0, a_n) \quad B = (n-k, a_k) \quad C = (n-l, a_l) \]

   It is then necessary to insure that no point of the upper limit polygon falls on or above the line $AB$ parallel to $BC$.

   The conditions defining the irreducible side $AB$ are:
   
   1. \( (a_n - a_k, n-k) = 1 \)
   2. \( a_{k+j} \left( \frac{a_n - a_k}{n-k} \right) \leq a_{k+j} \quad j = 1, 2, \ldots, n-1 \)

   The conditions defining the side $BC$ are:
   
   3. \( \frac{a_{k-1} - a_l}{k-1} \leq \frac{a_n - a_k}{n-k} \)
   4. \( a_{k+j} + j \left( \frac{a_{k-1} - a_l}{k-1} \right) \leq a_{l+j} \quad j = 1, 2, \ldots, k-2 \)

   The condition on the remaining sides of the Dumas polygon is:
   
   5. \( a_{l+j} + (l-j) \left( \frac{a_{k-1} - a_l}{k-1} \right) \leq a_l \quad i = 1, 2, \ldots, l-1 \)

   Let \( \lambda_i \geq \lambda_i^{*} \quad i = 1, 2, \ldots, n-1 \)

   We now desire to insure that no point of the upper limit polygon falls on or above the line $AB$ parallel to $BC$.

   There are two necessary conditions,
6.) \( a_n = a_n > \frac{n}{k-2} (a_k - a_i) \)

7.) \( \frac{a_n - a_k}{n-1} < \frac{\Delta_i + 1}{n-1} \frac{a_k - a_i}{k-1} \) \( i = 1, 2, \ldots, n-1 \)

Two parallels may now be constructed through the end-points of AB such that they include the polygon P and the upper and lower limit polygons. Hence all polygons in R will also be included by the parallels and therefore are irreducible. Therefore all polynomial \( f(x) \) whose coefficients satisfy conditions 1.) through 7.) are irreducible.

**Special Cases**

a.) The point B is on the x-axis; i.e., \( a_k = 0 \)

1a.) \((a_n, n-k) = 1\)

2a.) \(a_n < \frac{a_{n+j}}{n-k} \) \( j = 1, 2, \ldots, n-k-1\)

6a.) \( a_n = a_n > 0 \)

7a.) \( \frac{a_n - a_k}{n-1} < \frac{\Delta_i + 1}{n-1} \)

If these conditions are satisfied \( f(x) \) is irreducible. For example:

\[ x^n + kx^m + \ell p^v, \quad n > m, \]

where \((m, v) = 1, \quad k \neq 0 \text{ (mod } p), \quad 0 < k \leq \frac{v-2(m-1)}{p} \leq \ell \leq p \) and \( p > 3.2 \)

is irreducible.

b.) The point B is on the x-axis at \((1, 0)\)

1b.) \( a_{n-1} = 0 \)

6b.) \( a_n = a_n > 0 \)

7b.) \( \frac{a_n - a_k}{n-1} < \frac{\Delta_i + 1}{n-1} \) \( i = 1, 2, \ldots, n-1 \)

or \( a_n > \frac{(n-1)}{(n-1)} (\Delta_i + 1) + a_k \)
For example:

\[ x^n + kx + l \]

where \( k \neq 0 \mod p \), \( 0 \leq k \leq \frac{n-2}{p} \)

\( 0 \leq l \leq p \), and \( p > 3.2 \frac{n}{k} \)

is irreducible.

c.) The Dumas polygon consists of but two sides; i.e.,

\[ C = (n,0) \]

1c.) \((a_n - a_k, n-k) = 1\)

2c.) \( a_k + j \left( \frac{a_n - a_k}{n-k} \right) \leq a \)

3c.) \( \frac{a_k - a_n}{k} \leq a_n \)

4 & 5c.) \( i \left( \frac{a_k}{k} \right) \leq a_i , i = 1, 2, \ldots, k-1 \)

6c.) \( a_n \geq n \cdot a_k \)

7c.) \( \frac{a_n - a_k}{n-1} - \frac{k}{n-1} \frac{a_k}{k} \leq j = 1, 2, \ldots, n-1 \)

If these conditions are satisfied \( f(x) \) is irreducible.

For example:

\[ x^n + kp^n + l \]

where \( (v-u,m) = 1 \), \( \frac{u}{n-m} \leq \frac{v-u}{m} \)

\( 0 \leq l \leq p \), \( k \neq 0 \mod p \),

\( 0 \leq k \leq \frac{n-2}{p} \cdot \frac{n-m}{(n-1)k} \), and \( p > 3.2 \frac{n}{k} \)

is irreducible.

d.) The point \( B \) is on the ordinate \( x = 1 \); i.e., \( B (1, a_{n-1} ) \)

3d.) \( \frac{a_n - a_1}{n-1} \leq a_n - a_{n-1} \)

4d.) \( a_i + j \left( \frac{a_{n-1} - a_1}{(n-1)} \right) \leq a_{i+1} , j = 1, 2, \ldots, n-1-2 \)

5d.) \( a_i + (i-1) \left( \frac{a_k - a_{i-1}}{k} \right) \leq a_i , i = 1, 2, \ldots, l-1 \)
6d.) $\omega_n = a_n \frac{n}{n-1} (a_n - a_i)$

7d.) $\omega_n - \omega_n \frac{a_n - a_i}{n-1} \frac{a_n - a_i}{n-1}$ for $i, 1, 2, \ldots, n-1$

If these conditions are satisfied $f(x)$ is reducible.

For example:

$$x^n \pm kp x^{n-1}$$

where

$$v > u + \frac{u}{n-1}, \quad 0 < l < p,$$

and

$$k \not\equiv 0 (\mod p), \quad 0 < k - p \equiv \lambda (n-\lambda)$$

is irreducible.

3. The irreducible side $S$ is the last side of the Dumas polygon.

Let $AB$ be the irreducible side $S$ and $BC$ the next side of the Dumas polygon.

$A = (n, 0) \quad B = (n-k, a_i) \quad C = (n-1, a_i)$

It is necessary to ensure that no point of the upper limit polygon falls on or above the line $AB$ parallel to $BC$.

The conditions defining the irreducible side $AB$ are:

8.) $(a_i, k) = 1$

9.) $\frac{a_i}{k} < \frac{n}{k} \quad x = 1, 2, \ldots, k-1$

The conditions defining the side $BC$ are:

10.) $a_i \frac{a_i}{k} > \frac{a_i}{1-k}$

11.) $a_i \frac{(a_i - a_i)}{k} \frac{a_i}{j} \quad j = 1, 2, \ldots, k-1$

The conditions on the remaining sides of the Dumas
polygon is

\[ a_i + (i-\ell) \left( \frac{a_k-a_i}{i-k} \right) \leq a_i \quad i=\ell+1, \ldots, n \]

Let \( \alpha \geq \alpha_i \quad i=1,2,\ldots,n-1 \)

The condition is now imposed that no point of the upper limit polygon fall on or above the line \( AB \) parallel to \( BC \), this is

\[ \alpha \geq \frac{\alpha_i+1}{i} - \frac{a_i-a_k}{i-k} \quad i=1,2,\ldots,n-1 \]

As before two parallels may be constructed through the ends of \( AB \) which include all possible polygons in \( \mathbb{R} \). Therefore \( f(x) \) satisfying conditions 8. through 13. is irreducible.

**Special Cases**

a.) The Dumas polygon has only two sides; i.e., \( C = (0,a_n) \)

8a.) \( (a_k,k) = 1 \)

9a.) \( a_k < a_i \quad i=1,2,\ldots,k-1 \)

10a.) \( \frac{a_i-a_k}{n-k} > a_i \frac{k}{K} \)

11a.) \( a_i + j \left( \frac{a_i-a_k}{n-k} \right) < a_i \quad j=1,2,\ldots,k-1 \)

13a.) \( \alpha \geq \frac{\alpha_i+1}{i} - \frac{a_i-a_k}{n-k} \quad i=1,2,\ldots,n-1 \)

Any polygon \( f(x) \) satisfying these conditions is irreducible.

For example:

\[ x^n \pm kp^\ell x^m \pm l p^\nu, \quad n > m \]

where \( (u, n-m) = 1, \quad \frac{v}{n} > \frac{u}{n-m} \), \( 0 \leq l < p, \quad k \neq 0 (\mod p), \quad 0 < k < p \frac{v(m+1)}{n-2} \)

and \( p > 3.2 \)

is irreducible.
b.) The point B is on the ordinate $x = 1$; i.e., $B = (1, a_{n-1})$

$$C = (0, a_n)$$

9b.) $(a_{n-1}, n-1) = 1$

9b.) $$\frac{a_{n-1}}{n-1} \geq \frac{a_i}{i} \quad i = 1, 2, \ldots, n-2$$

10b.) $$a_{n-1} - a_{n-i} \geq \frac{a_{n-i}}{n-1}$$

13b.) $$\frac{a_i + 1}{i} \leq a_{n-1} - a_{n-i} \quad i = 1, 2, \ldots, n-1$$

Any polygon $f(x)$ satisfying these conditions is irreducible.

For example:

$$x^n \pm k p x \pm l p'$$

where

$$(u, n-1) = 1, \quad \frac{v}{n} > \frac{u}{n-1},$$

$$0 < l < p, \quad k \neq 0 (\text{mod } p), \quad 0 < k < p$$

and

$$p > 3.2$$

is irreducible.

c.) The point B is on the line $y = 1$; i.e., $B = (n-k, 1)$

9c.) $$\frac{1}{k} \leq \frac{a_i}{i} \quad i = 1, 2, \ldots, k-1$$

10c.) $$\frac{a_i - 1}{i-k} \geq \frac{1}{k}$$

11c.) $$1 + j \left(\frac{a_i - 1}{l-k}\right) \leq a_{k+j} \quad j = 1, 2, \ldots, l-k-1$$

12c.) $$a_l + (i-1) \left(\frac{a_i - 1}{l-k}\right) \leq a_i \quad i = 1, 2, \ldots, n$$

13c.) $$\frac{a_i + 1}{i} \leq \frac{a_i - 1}{l-k} \quad i = 1, 2, \ldots, n-1$$

Any polygon $f(x)$ satisfying these conditions is irreducible.

For example:

$$x^n \pm k p x \pm l p'$$
where \( v > \frac{n}{n-m} \), \( 0 < l < p \),
\( k \neq 0 \mod p \), \( 0 < k \leq \frac{v-1}{m-3} \)
and \( p > 3.2 \).  

is irreducible.

4. **The irreducible side \( S \) is the first side of the upper polygon.**

Let \( AB \) be the irreducible side \( S \).
\( A = (n,0) \) \( B = (n-k, \alpha_k) \)

In order that parallels may be drawn through the end-points of \( S \) which will include all possible polygons, the condition must be imposed that no point of the upper limit polygon shall fall on or above a line parallel to the \( x \)-axis and through the point \( B' \), the lower limit point on the ordinate \( x = n-k \).

If \( \alpha \) is the maximum of the numbers \( \alpha_{k+1}, \ldots, \alpha_n \), the condition that no point of the upper limit polygon fall above the line through \( B' \) is

\[
14.) \quad \alpha_k - \alpha_l > \left( \frac{\delta_k + \delta_l}{\delta_k - \delta_l} \right) \left( \frac{n-k}{1-k} \right) 
\]

The condition that the side \( AB \) be irreducible for all possible polygons is \( k = 1 \). Therefore 14.) becomes

\[
\alpha_l - \alpha_r > (1 + \Delta_i) \left( \frac{n-1}{1-l} \right) 
\]  
\( i = 2, 3, \ldots, n \)
Special Case

If \( p > 3.2^{\frac{n^2}{2}} \), \( \Delta_i < 1 \)

\[ \alpha_i - \alpha_r > \frac{2(n-1)}{i-1} \]

or \( \alpha_i > 2(n-1) + \alpha_r \)

This condition expressed in terms of the coefficients is

\[ |A_r| > p^{2(n-1)} |A_r| \]

where \( |A_r| \geq |A_i| \quad i = 2, \ldots, n \)

Or it may be written

\[ |A_r| > p^{2(n-1)} \left( |A_2| + |A_3| + \ldots + |A_n| \right) \]

where

\[ p > 3.2^{\frac{n^2}{2}} \]

It must be noted here that this is similar in form to Perron's criteria (pp. 21-22).

5. The irreducible side \( S \) is the last side of the upper polygon.

Let \( AB \) be the irreducible side \( S \)

\( A = (0, \alpha_n) \quad B = (n-k, \alpha_k) \)

In order that parallels may be drawn through the end-points of \( S \) which will include all possible polygons, the condition must be imposed that no point of the upper limit polygon shall fall on or above the line \( B'C' \) parallel to \( AC \) the first side of the Dumas polygon and through the point \( B' \) the lower limit point on the ordinate \( x = n-k \).

The condition defining \( AC \) is
15.) \( a_l + j(\frac{a_n-a_l}{n-l}) \leq a_{l+1} \) \( j = 1, 2, \ldots, n-l-1 \)

\( \Delta_n = a_n \)

The condition that no point of the upper limit polygon fall on or above \( B'C' \) is

\[ \frac{\lambda_k - \lambda_l}{k-1} > \frac{\alpha + \beta \lambda_k + 2}{k-1} \frac{a_n-a_l}{n-l} \]

\( 1 = 1, 2, \ldots, k-1 \)

The condition that the side \( AB \) be irreducible for all possible polygons is \( k = n-1 \). Therefore

16.) \[ \frac{\lambda_{n-1} - \lambda_l}{n-2} > \frac{\lambda_{n-1}}{n-1-1} \frac{a_n-a_l}{n-l} \]

\( i = 1, 2, \ldots, (n-2) \)

**Special Cases**

a. If \( \lambda_n - \alpha_l = 0 \) this becomes

16a.) \[ \frac{\lambda_{n-1} - \lambda_l}{n-2} > \frac{\alpha \lambda_{n-1} + 3}{n-1-1} \frac{a_n-a_l}{n-l} \]

b. If in addition to \( \lambda_n = \alpha_l = 0 \), \( p > 3.2 \) and \( \alpha_l = 1 \) and we have

16b.) \[ \lambda_{n-1} > 4(n-2) \alpha_l \]

In terms of the coefficients, \( x' \)

If \( |A_n| < p \), \( p > 3.2 \)

and \( |A_{n-1}| > p^{\frac{\lambda_{n-1}}{2}} |A_l| \)

where \( |A_r| \geq |A_l| \)

\( i = 1, 2, \ldots, (n-2) \)

then \( f(x) \) is irreducible.

4. **Polygons of Type II.**

The application of this type of polygon leads for the greater part to theorems concerning the numbers and degrees of possible factors.
1. The Dumas polygon consists of two straight lines.

The Dumas polygon is defined by the points $A = (0, a_n), B = (n-k, a_k), C = (n, 0)$. The centro-symmetric polygon $AB'C$ is constructed. The condition must now be applied that the upper limit polygon shall not include the point $B'$. The line $AB$ is defined by the conditions:

1. $a_k + j \left( \frac{a_n - a_k}{n-k} \right) = a_k + i \quad j = 1, 2, \ldots, n-k-1$

The line $BC$ is defined by the conditions:

2. $\frac{a_n}{k} \leq \frac{a_n - a_k}{n-k}$

3. $\frac{a_n}{k} \leq \frac{a_n - a_k}{i} \quad i = 1, 2, \ldots, k-1$

The point $B'$ is $(k, a_n - a_k)$

If the upper limit polygon is to fall below the point $B'$ all upper limit polygon points must fall below a line through $B'$.

This is the line $y = a_n - a_k - m(x-k)$

$$\frac{a_n - m}{n} \leq \frac{a_n - a_k}{n-k}$$

Therefore the condition is

$$\alpha_c < a_n - a_k - m(n-i-k) - \max \Delta_c \quad i = 1, 2, \ldots, n$$

or

4. $\alpha_c < a_n - a_k - a_n \frac{(i+k)-1}{n} - \Delta_{\gamma_2}$

If $(a_n - a_k, n-k) = 1$ and $(a_k, k) = 1$; then $f(x)$ is irreducible.
If \((a_n-a_k,n-k) = 1\) and \((a_k,k) = e\), then \(f(x)\) if reducible has one factor of degree \(n-k + \frac{k}{e}\) and one or more factors of degree \(\frac{n-k}{t} + k\) where \(e\) is one of the number \(1, 2, \ldots, e-1\).

If \((a_n-a_k,n-k) = t\) and \((a_k,k) = e\) then \(f(x)\) if reducible has one or more factors of degree \(\frac{n-k}{t} + k\) when \(t\) is one of the numbers \(1, 2, \ldots, t-1\).

If \((a_n-a_k,n-k) = t\) and \((a_k,k) = e\) then \(f(x)\) if reducible has only factors whose degrees are of the form \(\frac{n-k}{t} + \frac{k}{e}\) where \(t = 0, 1, 2, \ldots, t-1\) and \(e = 0, 1, 2, \ldots, e-1\)

That is, it may not have factors whose Dumas polygons are the lines \(AB, BG\).

**Special Cases**

\(a.\) If \(p > 3.2^{\frac{n-1}{2}}\), \(\Delta < 1\)

If also the point B lies on the ordinate \(x = 1\); i.e., \(B = (1, a_{n-1})\),

\[2a. \quad \frac{a_n}{n-1} - \frac{a_{n-1}}{n-1}\]

\[3a. \quad \frac{a_n}{n-1} - \frac{a_k}{i} \quad i = 1, 2, \ldots, n-2\]

\[4a. \quad \Delta < 2a_n - a_{n-1} - 2 + \frac{a_n}{n} (1-1)\]

If \((a_{n-1}, n-1) = 1\) the polynomial is irreducible.
b.) If the point $B = (1,1)$; i.e., $a_{n-1} = 1$ and $p > 3.2^{n/4}$, the further conditions under which the polynomial is irreducible are:

2b.) $a_n > 1$

3b.) $a_i = 1 \quad i=1,2,...,n-2$

4b.) $< - \frac{2a_n - 3x a_n}{n} (1-1) \quad i=1,2,...,n$

Thus all polynomials of the form

$$x^{n} = kpx \pm p \ m \quad v > 3$$

where $k \neq 0 (mod \ p), \ spat k < p^{2n-4}$, $m \neq 0 (mod \ p), \ spat m < p^{r-3}$

and $p > 3.2^{n/4}$

are irreducible.

2. The Dumas polygon consists of three straight lines.

The Dumas polygon is defined by the points $A = (0,a_n) \ spat B = (n-k,a_k)$

$C = (n-1,a_{n-1}) \ spat D = (n,0)$. The centro-symmetric polygon $DB'C'A$

is constructed. For simplicity of algebraic expression let us suppose that the sides $AB, BC, CD$ are irreducible,

$$(a_n - a_k, n-k) = 1$$

$$(a_k - a_1, k-?) = 1$$

$$(a_1, a_1) = 1.$$

The condition must now be applied that the upper limit
polygon shall not include the points \( B' \) and \( C' \). These points are \( B'(k, a_n - a_1) \) \( C'(2, a_n - a_2) \). The line \( B'C' \) is

\[
y = \frac{(k-1) a_1 - a_k}{(k-2)} (x-2)
\]

Therefore the condition is

5.) \( \frac{(k-l+1)a_1-a_k}{(k-l)} (n-l-1)-\max \triangle \)

Then \( f(x) \) has but two factors if reducible; one of degree \( (n-k+2) \) and one of degree \( (k-l) \) whose Dumas polygons are \( AB + CD \) and \( BC \) respectively.

5. Numerical Cases

Further application of these polygons to derive algebraic criteria does not seem advisable since they are so complicated in statement.

The application in numerical cases will however frequently show that the polynomial under consideration is irreducible since closed convex factor polygons cannot be formed from the sides of the polygon of the polynomial.

For example: \( f(x) = x^3 + (p^2 + p)x^2 + (p^3)p^2x^p_2 + p^3 \)

\( p > 3.2^{1/4} \) is irreducible since it is impossible to decompose any of its possible polygons into closed convex factor polygons.

So also is:
Two other forms of irreducible polynomials are:

a.) \[ f(x) = x^7 \pm (p'' + p)x^5 \pm p^x \text{ where } p > 3.2^{47/4} \]
irreducible for the same reason.

b.) \[ f(x) = x^n \pm kp^x \sim_{2(n-2)}^p l \]
where \[ 0 < k < p, \quad k \neq 0 \mod p, \]
\[ 0 < l < p \quad \text{and} \quad p > 3.2^{47/4} \]
is irreducible. The polygon is of type I, case 2a.)

\[ m = 2m' + 1, \]
\[ v \geq 4(n-m) + 2, \]
\[ 0 < k < p^{2(n-2)}, \quad k \neq 0 \mod p, \]
\[ 0 < l < p \quad \text{and} \quad p > 3.2^{47/4} \]
is irreducible. The polygon is of type I, case 3a.)
CHAPTER V

BIBLIOGRAPHY

1. Chronological Bibliography


1846 Schönemann, "Von denjenigen Modulen, welche Potenzen von Primzahlen sind." Journal für Mathematik XXXII (1846), 93-100.


Schönemann, "Über einige von Herrn. Dr. Eisenstein aufgestellte Lehrsätze, irreductible Congruenzen betreffend. "Journal für Mathematik XL (1850), 188.


Netto, "Über die Irreduzibilität ganzer ganzzahliger Funktionen." Mathematische Annalen. XLVIII (1897), 81-88.

Mandl, "Eine methode zur Zerlegung ganzer, ganzzahliger Functionen in irreductible Factoren." Jahresberichte der Deutsche Mathematiker Vereinigung. IV (1897) 95-96.

Kahan, "Über einige irreducible Polynome." Jahrbuch über die Fortschritte der Mathematik. XXX (1899), 100.


Dumas, "Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels." Journal de Mathématiques. ser.6. II (1906), 191-256.


Schur, "Problem 226" Archiv der Mathematik und Physik. ser.3. XIII (1906), 368.


Shanok, "Convex polyhedra and criteria for irreducibility." Dissertation 1933, Yale University.
2. Supplementary Bibliography


1892 Hilbert, "Über die Irreduzibilität ganzer rationaler Functionen mit ganzzahlichen Coefficienten." Journal für Mathematik. CX '1892), 104-129.

1897 Capelli, "Sulla riduttibilità delle equazioni algebriche." Rendiconti di Napoli ser.3 III (1897), 243-252.


1900 Hancock, "Methode de décomposition des polynomes entiers a plusieurs variables." Annales scientifiques de l'école normale superieure a Paris. ser.3 XVII (1900), 89-102.

Königsberger, "Über die Irreductibilität algebraischer Functionalgleichungen und lineer Differentialgleichungen." Mathematische Annalen. LIII (1900), 49-80.


Dickson, "Criteria for the irreducibility of a reciprococal equation." American Mathematical Society Bulletin ser.2.XIV (1908), 426-430.

1913 Glenn, "Theorems on Reducible Quantics." Annals of Mathematics. ser.2.XIV (1913), 27-41


1920 Amato, "Sull metodo di Kronecker per la decomposizione di una funzione razionale intera in un campo ampliata di razionalità." Atti della Reale Accademia Nazionale dei Lincei. ser.5a XXIX (1920), 99.


Ore, "Om Polynomers reduktibilität." Norsk Matematisk Tidsskrift. III (1921), 135-144.


1930 Gourin, "On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves." American Mathematical Society, Transactions. XXXII (1930) 403-501.


Serret, "Cours d'algébre supérieure."
ADDENDA

1. Abstract

Instead of the open Dumas polygon usually applied for the deduction of irreducibility criteria, a closed convex polygon is introduced, depending both on the size and the divisibility properties of the coefficients. For this polygon an approximate multiplication theorem holds and this may be used to deduce irreducibility criteria depending on the size of the coefficients.

2. Report presented to the American Mathematical Society, March 30, 1934

In 1906 Dumas applied Newton's polygon to deduce irreducibility criteria. This polygon for

\[ f(x) = x^n + A_1 x^{n-1} + \ldots + A_n \]

\((A_i \text{ rational integers})\) was defined as the least convex polygon lying below and including the points

\[ P = (n-1, a) \]

where \(a\) is the highest power of a rational prime \(p\) dividing \(A_i\). The product of two polygons was defined as the polygon formed by laying off the sides of the factor polygons in order of increasing inclination. Dumas proved for these polygons a product theorem:
The polygon of the product of two factors is coincident with the product of their polygons. Hence if the polygon of a polynomial cannot be broken up the polynomial is irreducible.

In applying the Newtonian polygon to functions of two variables

\[ f(xy) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j \]

if the points \((i,j)\) are plotted we obtain a closed convex polygon, the least polygon including all of these points. A similar product theorem can be shown for these closed polygons.

Returning then to the consideration of \(f(x)\) it is possible to write \(f(x)\) in the form

\[ f(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} r_{ij} x^i p^j \]

where the coefficients \(r_{ij}\) are all less than \(p\). Then the plotting of the points \((i,j)\) will again define a closed convex polygon, the lower sides of which coincide with the Dumas polygon and the upper sides of which are dependent on the magnitude of the absolute values of the coefficients.

It is found in so doing that such an upper polygon exists but that when we consider a product theorem the upper sides of the polygon of the product \(P \times_2 P_3\) do not necessarily exactly coincide with those of the product of the polygons \(P_2 P_3\). This is due to the fact that in the process of multiplication the summation of terms containing like powers of \(x\) may cause the increase or decrease of the powers of \(p\).
It can however be shown for this upper polygon that if a polynomial is considered as the product of factors, \( f(x) \) and \( g(x) \), the product of the polygons of the factors \( P_{r} \) lies on or within certain limits about the polygon of the product \( P_{s} \). That is, we plot the points defined by a given polynomial and construct its polygon \( P_{r} \). On each ordinate we then lay off certain distances, dependent upon the abscissas, above and below the polygon, and construct the two polygons lying above and including these two sets of points. The product of the polygons of the factors \( P_{r} \) then is one of the polygons lying on the limits of, or within the region defined by the two limit polygons.

These limits of the upper polygon have been proved for all polynomials whose coefficients are real or complex numbers. The point defining \( P_{s} \) on the ordinate \( x = n-1 \) may not lie more than \( \log(3.2^{(n-2)}) \) above and not more than \( \log(\frac{3}{2} + 1) \) below the polygon \( P_{s} \) when this is defined by the points \( \log|A| \). From certain considerations noted in the use of this method, I feel that these can be improved.

The proof depends on the consideration of the sharpness of the corner points of the product of the polygons. Here sharpness of a corner point is defined as the ratio of the slopes of two consecutive sides of the polygon. It is shown that for corner points whose sharpness is greater than or equal to four the point of \( P_{r} \) and the corresponding point of \( P_{s} \) cannot
differ greatly. For a corner point whose sharpness is less than four the previously stated limit is found.

Applying these polygons to the deduction of irreducibility criteria, we find certain types of polygons which are irreducible. The irreducibility criteria thus derived are algebraic in form similar to those given by Perron in 1907 but more general.

First, suppose that P is a polygon with one irreducible side S. If it is possible to find a pair of parallels L₁, L₂ through the endpoints of S such that P lies entirely within these parallels, then P is irreducible.

Second, consider the convex polygon of a polynomial. Draw the line connecting the end-points of the Dumas polygon (ADB). Considering the mid-point M of this line as center, construct above the line the corner points and sides necessary to form with the existing Dumas polygon a centro-symmetric polygon (BC').

If the upper limit polygon contains none of the corner points of this constructed polygon, then no factor polygon may have as its Dumas polygon a sequence of the first k sides of the original polygon.

If under the above conditions the Dumas polygon
has but two sides containing no lattice points, then \( f(x) \) is irreducible.

If it has but three sides \( S_1, S_2, S_3 \), each crossing no lattice points, the only possible factor polygons are those two having as Dumas polygons \( S_1 + S_3 \) and \( S_2 \).