NEW TYPES OF IRREDUCIBILITY CRITERIA

GRACE MURRAY HOPPER

[illegible]

[illegible]

[illegible]
[illegible]

A Dissertation
Presented to the Faculty
of the Graduate School of Yale University
in Candidacy for the Degree of
Doctor of Philosophy
[illegible]

NEW TYPES OF IRREDUCIBILITY CRITERIA

Grace Murray Hopper

A.B. Vassar College 1928
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.

PREFACE

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

CHAPTER I

HISTORICAL INTRODUCTION

1. Earliest Theorems on Irreducibility.[1]

Given a polynomial

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

where the coefficients $a_0, a_1, \ldots, a_n$ are rational integers. It is frequently necessary to decide whether or not there exists a decomposition,

$$f(x) = f_1(x) f_2(x) \ldots f_r(x)$$

where $f_i(x) = b_{i0} x^{n_i} + b_{i1} x^{n_i - 1} + \ldots + b_{in_i}, (i = 1, 2, \ldots, r)$, 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

---

1. Ore, "Über die Reduzibilität von algebraischer Gleichungen." Christiania Videnskapsselskapets Skrifter. Pt. I. (1923) #22.

Kronecker[2], Runge[3], and Mandl[4]. 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[5];

<u>Theorem</u>: Given

$$f(x) = \phi^t(x) + pM(x).$$

Then $f(x)$ is irreducible if

$$M(x) \not\equiv 0 \left(\text{modd } p \quad \phi(x)\right),$$

$\phi(x)$ 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[6].

<u>Theorem</u>: Given

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

---

2. Kronecker, "Uber die Irreductibilität von Gleichungen" <u>Monatsberichte, Akademie der Wissenschaften Berlin.</u> (1880), 155-162.
3. Runge, "Uber die Zerlegung ganzer ganzzahliger Funktionen in irreductible Factoren." <u>Journal für Mathematik</u>. XCIX (1887), 89-97.
4. Mandl, "Uber die Zerlegung ganzer ganzzahliger Funktionen in irreductible Factoren." <u>Journal für Mathematik</u>. CXIII (1894), 252-261.
   "Eine Methode zur Zerlegung ganzer ganzzahliger Funktionen in irreducible Factoren." <u>Jahresberichte der Deutsche Mathematiker Vereinigung</u>. IV (1897), 95-96.
5. Schönemann, "Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reale Primzahl ist." <u>Journal für Mathematik</u>. XXXI (1845), 269-325.
   "Von denjenigen Modulen, welche Potenzen von Primzahlen sind." <u>Journal für Mathematik</u>. XXXII (1846), 93-100.
6. Eisenstein, "Uber die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen lemniscate abhangt." <u>Journal für Mathematik</u>. XXXIX (1850), 166.

where the coefficients a_i are rational integers, $a_n \neq 0$.

If $a_i \equiv 0 \pmod p$, $(i = 1, 2, \ldots n)$, and $a_n \not\equiv 0 \pmod{p^2}$; then $f(x)$ is irreducible.

That the theorem of Eisenstein is a special case of Schönemann's[7] theorem is apparent when

$$\phi(x) = x^n, \quad M(x) = b_1 x^{n-1} + \ldots + b_n.$$

2. <u>Generalizations of the Theorem of Eisenstein.</u>

Not until much later did any further theorems appear. Königsberger in his first paper[8] gives little but results, but his second[9] contains proofs for two theorems.

<u>Theorem:</u> Given

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

If $a_i = b_i\, p^{e\left(\frac{ir}{n}\right)+1}$, $(i = 1, 2, \ldots, n-1)$,

$a_n = b_n p^r$, $b_n \not\equiv 0 \pmod p$, $a_0 \not\equiv 0 \pmod p$,

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

<u>Theorem:</u> Given

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

If $a_0 \not\equiv 0 \pmod p \not\equiv 0 \pmod q$,

$a_i = p^{c\left(\frac{i-1}{\mu}\right)+1+c\left(\frac{i}{\mu}\right)}\, q^{c\left(\frac{i-1}{\nu}\right)+1+c\left(\frac{i}{\nu}\right)}\, b_i$, $(i = 1, 2, \ldots n-1)$,

$a_n = p^\mu q^\nu b_n$ $\quad b_n \not\equiv 0 \pmod p \not\equiv 0 \pmod q$,

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

---

7. Schönemann, "Uber einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze irreductible Congruenzen betreffend." <u>Journal für Mathematik</u>. XL(1850), 188.
8. Königsberger, "Uber den Eisensteinschen Sätz von der Irreductibilität algebraischer Gleichungen." <u>Sitzungsberichte, Akademie der Wissenschaften Berlin</u>. (1894) Pt.2, 1135-1139.
9. Königsberger, "Uber den Eisensteinschen Sätz von der Irreductibilität algebraischer Gleichungen." <u>Journal für Mathematik</u>. CXV (1895), 53-78.

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[10] gives several theorems concerning the number and degrees of possible factors of certain types of polynomials.

Theorem: Given

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

If $a_i = pb_i$, $(i = 1, 2, \dots, \alpha - 1)$,

$a_i = p^2 b_i$, $(i = \alpha, \alpha+1, \dots, n)$,

$b_n \not\equiv 0 \pmod p$ and $n > 2\alpha$;

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

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

If $a_i = pb_i$, $(i = 0, 1, \dots, n-2\alpha-2)$,

$a_i = p^2 b_i$, $(i = n-2\alpha-1, \dots, n-\alpha-1)$,

$a_i = p^3 b_i$, $(i = n-\alpha, \dots, n)$,

$b_n \not\equiv 0 \pmod p$ and $n > 3\alpha$;

---

10. Netto, "Uber die Irreductibilitat ganzer ganzzahliger Functionen." Mathematische Annalen. XLVIII (1897) 81-88.

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

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.

In 1900 Königsberger[11] gives a more general criterion.

Theorem: Given

$$\begin{aligned} f(x) = x^n &+ p^{\delta^{(2)}_{\mu_2-1}} a_{n-1} x^{n-1} + \dots + p^{\delta^{(2)}_{\alpha}} a_\nu x^\nu + p^{\delta^{(2)}_{\alpha-1}} q^{\varepsilon_{\nu-1}} a_{\nu-1} x^{\nu-1} + \dots \\ &+ p^{\delta^{(2)}_2} q^{\varepsilon_{\mu_1+2}} a_{\mu_1+2} x^{\mu_1+2} + p^{\delta^{(2)}_1} q^{\varepsilon_{\mu_1+1}} a_{\mu_1+1} x^{\mu_1+1} + p^{\delta^{(1)}_{\mu_1}} q^{\varepsilon_{\mu_1}} a_{\mu_1} x^{\mu_1} + \dots \\ &+ p^{\delta^{(1)}_2} q^{\varepsilon_2} a_2 x^2 + p^{\delta^{(1)}_1} q^{\varepsilon_1} a_1 x + p^{\rho_1+\rho_2} q^{\sigma} a_0 , \end{aligned}$$

where p and q are two different rational primes.

If
$$\begin{aligned} \delta^{(1)}_{\gamma_1} &= e\left[(\mu_1-\gamma_1)\tfrac{\rho_1}{\mu_1}+\rho_2\right] \text{ or } e\left[(\mu_1-\gamma_1)\tfrac{\rho_1}{\mu_1}+\rho_2\right]+1 \\ \delta^{(2)}_{\gamma_2} &= e\left[(\mu_2-\gamma_2)\tfrac{\rho_2}{\mu_2}\right] \text{ or } e\left[(\mu_2-\gamma_2)\tfrac{\rho_2}{\mu_2}\right]+1 \\ \varepsilon_\gamma &= e\left[(\nu-\gamma)\tfrac{\sigma}{\nu}\right] \text{ or } e\left[(\nu-\gamma)\tfrac{\sigma}{\nu}\right]+1 \end{aligned}$$

according as e is or is not an integer,

$$\mu_1+\mu_2=n, \quad \nu=\mu_1+\alpha, \quad \nu>\mu_1, \quad \nu>\mu_2$$

$\frac{\rho_1}{\mu_1} > \frac{\rho_2}{\mu_2}$, the fractions $\frac{\rho_1}{\mu_1}, \frac{\rho_2}{\mu_2}, \frac{\sigma}{\nu}$ are irreducible,

$$a_0 \not\equiv 0 \pmod p \not\equiv 0 \pmod q$$

$$a_{\mu_1} \not\equiv 0 \pmod p, \quad a_\nu \not\equiv 0 \pmod q;$$

then $f(x)$ is irreducible.

Bauer's[12] extension of this theorem made it applicable

---

11. Konigsberger, "Uber die Entwickelungsform algebraischer Functionen und Irreductibilität algebraischer Gleichungen." Journal für Mathematik. CXXI (1900), 320-359.
12. Bauer, "Beitrag zur Theorie der irreduzibeln Gleichungen." Journal für Mathematik. CXXVIII (1905), 298-301.

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

Theorem: Given

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

If 1) $n = \prod_{s=1}^{r} n_s$ where the n_s are all relatively prime,

2) $a_i = \prod_{s=1}^{r} p^{\left[\frac{i\alpha_s - 1}{n_s}\right]+1} C_i$ where the α_s are positive integers such that $(\alpha_s, n_s) = 1$. (The symbol $\left[\frac{a}{b}\right]$ denotes the largest rational integer less than or equal to $\frac{a}{b}$.)

3) $(C_n, \prod_{s=1}^{r} p_s) = 1$, $p_1, p_2, \dots, p_r$ are different rational primes; then $f(x)$ is irreducible.

All of the previous theorems are included in one given by Perron[13] 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 nth power of a prime ideal if the degree of the field containing the prime is divisible by n.

Theorem: Given

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

If $a_i = \prod_{s=1}^{r} p_s^{\left[\frac{i\alpha_s}{n}\right]+1} C_i$, $(i=1,2, \dots, n-1)$,

$a_n = \prod_{s=1}^{r} p_s^{\alpha_s} C_n$, $(C_n, \prod_{s=1}^{r} p_s) = 1$,

and the r+1 numbers $n, \alpha_1, \alpha_2, \dots, \alpha_r$, 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.

---

13. Perron, "Uber eine Anwendung der Idealtheorie auf die Fräge nach der Irreduzibilität algebraischer Gleichungen." Mathematische Annalen. LX (1905), 448-458.

Ore[14] further extended these theorems to reducibility in an arbitrary algebraic field, using the prime ideals $\mathfrak{p}_s$ in place of the primes p_s .

Theorem: Given

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

where the a_i are integers in an algebraic field $K(\vartheta)$.

If $a_i = \prod_{s=1}^{r} \mathfrak{p}_s^{\left\lceil \frac{\alpha_s i}{n} \right\rceil} b_i$, $(i=1,2, \dots, n)$,

$(b_n, \prod_{s=1}^{r} \mathfrak{p}_s) = 1$, $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ are prime ideals. Here $\left\lceil \frac{a}{b} \right\rceil$ indicates the rational integer next greater than $\frac{a}{b}$ if $\frac{a}{b}$ is not integral and $\frac{a}{b}$ if it is integral. If $n, \alpha_1, \alpha_2, \dots, \alpha_r$ have no common factor $f(x)$ is irreducible. If e is the greatest common factor of $n, \alpha_1, \alpha_2, \dots, \alpha_r$ and γ is one of the numbers $1,2, \dots, e$; then $f(x)$ can only have factors of degree $m = \frac{\gamma n}{e}$.

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

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

If $a_n \not\equiv 0 \pmod p$; then $f(x)$ will be irreducible in all algebraic fields $K(\vartheta)$ in which p does not divide the discriminant of ϑ .

3. Generalizations of the Theorem of Schonemann.

The first such theorems are given by

---

14. Ore, "Uber die Reduktibilität in algebraischen Zahlkörpern." Norsk Matematisk Forening Skrifter. (1922), ser.1, #9.

Kahan.[15]

Theorem: Given the polynomial

$$f(x) = x^n + c_{n-1}x^{n-1} + p(c_{n-2}x^{n-2} + \dots + c_2x^2 + c_1x \pm 1).$$

If $c_{n-1} \not\equiv 0 \pmod p \not\equiv \pm 1 \pmod p$; then $f(x)$ is irreducible.

Theorem: Given the polynomial

$$f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + p(c'_{n-3}x^{n-3} + \dots + c_1x \pm 1),$$

where $c_{n-1} \not\equiv 0 \pmod p) \not\equiv \pm 1 \pmod p$. If no root of this polynomial is equal to ± 1; the polynomial is irreducible.

The next theorem, a more direct generalization, was proved by Bauer[16] in 1905. The proof is completed by means of ideal theory.

Theorem: Given $f(x) = \phi^t(x) + p^\alpha M(x)$

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

2) $(t, \alpha) = 1$,

3) the degree of $M(x)$ is less than mt, and

4) $M(x) \not\equiv 0 (\text{modd } p, \phi(x))$; then $f(x)$ is irreducible.

This theorem was included in a more general one by Ore.[17]

Theorem: Given

$$f(x) = \prod_{i=1}^{s} f_i(x)^{e_i} + p^\alpha M(x), \ f(x) \text{ of degree } n.$$

---

15. Kahan, "Uber einige irreducible Polynome." Jährbuch über die Fortschritte der Mathematik. XXX(1899),100.
16. Bauer, "Verallgemeinerung eines Sätzes von Schönemann." Journal für Mathematik. CXXVIII (1905), 87-89.
17. Ore, "Uber die Reduzibilität von algebraischen Gleichungen." Christiania Videnskapsselskapets Skrifter. (1923), Pt.I,#22.

If 1) $f_i(x)$ is a prime function of degree n ,

2) $(e_i, \alpha) = b_i$,

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

$$r_i = \sum_{i=1}^{s} k_i \frac{e_i}{b_i} n_i ,$$

where k_i is one of the numbers 1,2, ... b_i.

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 $f(x) = \prod_{i=1}^{s} f_i(x)^{e_i} + kM(x)$, $k = \prod_{j=1}^{r} p_j^{\alpha_j}$, and states this theorem for the case of $s = 1$.

<u>Theorem</u>: Given $f(x) = \phi(x)^e + \prod_{j=1}^{r} p_j^{\alpha_j} M(x)$

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

2) $(e, \alpha_1, \alpha_2, \ldots, \alpha_r) = b$,

3) the degree of $M(x)$ is less than em, and

4) $M(x) \not\equiv 0 \pmod{p, \phi(x)}$; then $f(x)$ can only have factors of degree $r = k\frac{e}{b}m$ where k is one of the numbers 1,2, ..., b.

4. <u>The Newtonian Polygon.</u>

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

If $a_i = p^{\alpha_i} b_i$, $b_i \not\equiv 0 \pmod p$;

then $P_i = (n-i, \alpha_i)$.

In 1906 Dumas[18] proved that the polygon of a product coincides

18. Dumas, "Sur quelques cas d'irreductibilité des polynomes à coefficients rationnels." <u>Journal de Mathématiques</u>. ser.6.II (1906), 191-256.

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

$$\tan \phi_i = \frac{k_i}{l_i}$$

If $(k_i, l_i) = e_i$ then $k_i = e_i \varkappa_i$, $l_i = e_i \lambda_i$ and

$$\tan \phi_i = \frac{\varkappa_i}{\lambda_i} \qquad (\varkappa_i, \lambda_i) = 1.$$

Dumas' product theorem then gives the theorem:

<u>Theorem</u>: $f(x)$ can have factors of degree r only when r is of the form

$$r = \sum_{i=1}^{m} \mu_i \lambda_i$$

where μ_i is one of the numbers $0, 1, 2, \ldots, e_i$.

Fürtwangler[19] states a similar theorem in the

---

19. Fürtwangler, "Uber Kriterien für irreduzible und für primitive Gleichungen." <u>Mathematische Annalen</u>. LXXXV (1922), 34-40.

form:

Theorem: Given the polynomial

$$f(x) = a_0 x^n + p^{e_1} a_1 x^{n-1} + \dots + p^{e_{n-1}} a_{n-1} x + p^{e_n} a_n.$$

where $a_i \not\equiv 0 \pmod p$.

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

2) If $(e_{n-k}, n-k) = 1$; then $f(x)$ if 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 $\frac{n}{t}$ where $t = (n, e_n)$.

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

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

However in the same year, Ore[21] extended the definition of the Newtonian polygong to completely generalize the Schönemann-Eisenstein theorems.

Given the polynomial,

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

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

---

20. Kürschak, "Irreduzible Formen." Journal für Mathematik. CLII(1923), 180-191.

21. Ore, "Zur Theorie der Irreduzibilitäts-Kreiterien." Mathematische Zeitschrift. XVIII (1923), 278-288.

be written in the form:

$$f(x) = \sum_{i=0}^{s} a_i Q_i(x) p^{\alpha_i} \phi^{i}(x),$$

where $a_i \not\equiv 0 \pmod p$, and $Q_i(x)$ 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

$$f(x) = a_0 \phi^{n}(x) + a_1 Q_1(x) \phi^{n-1}(x) + \dots + a_n Q_n(x).$$

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

2) $a_i = \alpha_i p^{\left[\frac{ir}{n}\right]}$, $a_n = \alpha_n p^{r}$,

$\alpha_0 \not\equiv 0 \pmod p$, $\alpha_n \not\equiv 0 \pmod p$,

3) the degree of $Q_i(x)$ is at most m-1, and

4) $Q_n(x) \not\equiv 0 \pmod p$;

then f(x) can only have factors of degree

$$t = m \frac{n}{e} \tau$$

where $e = (n,r)$ and τ is one of the numbers 1, 2, ..., e.

5. Criteria Dependent Upon Values for Integral Arguments.

In 1908 Schur[22] proposed the problem:

When are the polynomials

$$f_1(x) = (x-a_1)(x-a_2)\dots(x-a_n)-1$$

$$f_2(x) = (x-a_1)(x-a_2)\dots(x-a_n)+1$$

reducible or irreducible in the rational field?

Westlund[23] showed that $f_1(x)$ is always irreducible

---

22. Schur, "Problem 226." Archiv der Mathematik und Physik. ser.3.XIII (1908),368.
23. Westlund, "On the irreducibility of certain polynomials." American Mathematical Monthly. XVI (1909), 66-67.

and that $f_2(x)$ is reducible only if it is a perfect square.

Flügel[24] in solving the problem set by Schur gave the more complete solution that $f_1(x)$ 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[25] set a second problem: Show that

$$f_1(x) = (x-a_1)^2(x-a_2)^2 \dots (x-a_n)^2+1$$

$$f_2(x) = (x-a_1)^4(x-a_2)^4 \dots (x-a_n)^4+1$$

are irreducible in the rational field.

A few years later Stäckel[26] 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)

---

24. Flügel, "Solution of a Problem by Schur." Archiv der Mathematik und Physik. ser.3.XV (1909), 271.
25. Schur, "Problem 275." Archiv der Mathematik und Physik. ser.3.XV (1909), 259.
26. Stäckel, "Arithmetische Eigenschaften ganzer Functionen." Journal für Mathematik. CXLVIII (1918), 101-112.

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

<u>Theorem</u>: 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 $k > S$

$$S = 2 + \frac{A n! (n-1)^{\frac{1}{2}(n^2+n+2)}}{1! 2! 3! \cdots (n-1)!}$$

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

Polyá[27] in order to prove three criteria makes use of the auxiliary theorem:

If a polynomial $f(x)$ of nth degree is such that for $n+1$ values γ_i of x,

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

then $f(x)$ is not integral.

<u>Theorem</u>: If the polynomial $f(x)$ of nth degree is such that for n values γ_i of x, no $f(\gamma_i) = 0$ and

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

then $f(x)$ is irreducible.

<u>Theorem</u>: If there exist n integers $\gamma_1, \gamma_2, \ldots, \gamma_n$ such that the difference btween 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

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

then $f(x)$ is irreducible.

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

---

27. Polyá, "Verscheidene Bemerkungen zur Zahlentheorie." <u>Jahresberichte der Deutsche Mathematiker. Vereinigung</u> XXVIII (1919), 31-40.

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[28] included a solution of Schur's second problem. Where

$$P(x) = (x-a_1)(x-a_2)\dots(x-a_n)$$

the three authors showed that:

<u>Theorem:</u> If $G(x) = z^4+1$; then $G\left[P(x)\right]$ is irreducible.

<u>Theorem:</u> If $G(x) = cz^4+1$ where c is a positive integer is irreducible; then $G\left[P(x)\right]$ is irreducible.

<u>Theorem:</u> If $G(x) = z^8+1$; then $G\left[P(x)\right]$ is irreducible.

<u>Theorem:</u> If $G(x) = c_1 z^4+c_2 z^3+c_3 z^2+c_4 z+1$ is an irreducible integral polynomia; 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:

z^4-z^2+1	$8z^4-4z^2+1$
z^4+2z^2+3z+1	$8z^4+3z^3-z^2-3z+1$
z^4+2z^2-3z+1	$8z^4-3z^3-z^2+3z+1$
$27z^4-9z^2+1$	

---

28. Brauer, Brauer and Hopf, "Uber die Irreduzibilitäts einiger Spezielle Klassen von Polynomen." <u>Jahresberichte der Deutsche Mathematiker Vereinigung</u>. XXXV (1926), 99-112.

In the same year Ille[29] 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 γ_i of x, $f(\gamma_i) \neq 0$,

$$|f(\gamma_i)| < \frac{k}{2^{2k-1}}$$

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

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

<u>Theorem</u>: If $G(x) = az^4 + bz^3 + cz^2 + dz + 1$ is an irreducible polynomial, $P(x) = (x-a_1)(x-a_2) \ldots (x-a_n)$ where the a_i are all different; then $G[P(x)]$ can have no factors of degree less than k.

Wegner[30] 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.

<u>Theorem</u>: If $P(x) = (x-a_1)(x-a_2) \ldots (x-a_n)$, $n > 5$, d a rational integer not a perfect square and $d \not\equiv 3 \pmod 4$; then

$$[P(x)]^4 + d \text{ is irreducible.}$$

---

29. Ille, "Einige Bermerkung zur einem von G. Polyá herrührenden Irreduzibilitätskriterium." <u>Jahresberichte der Deutsche Mathematiker Vereinigung</u>. XXXV (1926), 204-208.
30. Wegner, "Uber die Irreduzibilität einer Klasse von ganzen rationalen Funktionen." <u>Jahresberichte der Deutsche Mathematiker Vereinigung</u>. XL (1931), 239-241.

The paper by Dorwart and Ore[31] 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 nth degree taking the values $+1$ at m points $a_1, a_2, \ldots a_n$ where $4 < m \leq n$ can have factors only of the form

$$g(x) = (x-a_1)(x-a_2)\ldots(x-a_n)h(x)+1.$$

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

These lead to the theorems:

<u>Theorem</u>: The polynomials

$$f(x) = a(x-a_1)(x-a_2)\ldots(x-a_n)+1$$

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.

<u>Theorem</u>: The polynomials

$$F[P(x)] = b_0 P(x)^2 + b_1 P(x) + 1$$

---

31. Dorwart and Ore, "Criteria for the irreducibility of polynomials." <u>Annals of Mathematics</u>. 2 ser. XXXIV (1933), 81-94.

where $F(x) = b_0 x^2 + b_1 x + 1$ 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

$$f(x) = c(x-a_1)^2 (x-a_2)^2 \ldots (x-a_n)^2 + 1$$

are always irreducible if $c \neq -b^2$ except when $f(x)$ is equivalent to

$$-8(x-1)^2 x^2 (x-1)^2 + 1 = (2x-1)(-4x^4 + 6x^2 - 1).$$

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 $\geq \frac{m}{2}$.

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 $n \leq 10$ it is found that this theorem holds except when $n = 3$ where $f(x)$ is reducible only for the two polynomials

$$(x-1)(x+1)(x+p) + p = x(x^2 + px - 1)$$

$$4x(x-1)(2x+p-1) + p = (2x-1)(4x^2 + 2px - 4x - p)$$

Theorem: A polynomial taking the values ± 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[32] in 1929 added criteria for several special types of polynomials. Four similar types are defined.

Theorem: Every polynomial of the form

$$f(x) = 1 + a_1\frac{x}{1!} + a_2\frac{x^2}{2!} + \cdots + a_{n-1}\frac{x^{n-1}}{(n-1)!} \pm \frac{x^n}{n!}$$

where the a_i are rational integers, is irreducible.

Theorem: Every polynomial of the form

$$f(x) = 1 + a_1\frac{x^2}{u_2} + a_2\frac{x^4}{u_4} + \cdots + a_{n-1}\frac{x^{2n-2}}{u_{2n-2}} \pm \frac{x^{2n}}{u_{2n}}$$

where the a_i are rational integers,

$u_{2i} = 1.2.3. \ldots (2i-1)$, is irreducible.

Theorem: In general every polynomial of the form

$$f(x) = 1 + a_1\frac{x^2}{u_4} + a_2\frac{x^4}{u_6} + \cdots + a_{n-1}\frac{x^{2n-2}}{u_{2n}} \pm \frac{x^{2n}}{u_{2n+2}}$$

is irreducible. The exception is the case where $2n$ is of the form 3^r-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

$$f(x) = 1 + a_1\frac{x}{2!} + a_2\frac{x^2}{3!} + \cdots + a_{n-1}\frac{x^{n-1}}{n!} \pm \frac{x^n}{(n+1)!}$$

will in general be irreducible. If however n is of the form 2^r-1 $(r\geq 2)$, then $f(x)$ may have factors

---

32. Schur, "Einige Sätze uber Primzahlen mit Andwendung auf Irreductibilitätsfragen." Akademie der Wissenschaften. Berlin. Sitzungsberichte (1929) Part I. 125-136, 370.

of the form $x\pm2$. If $n=8$ then $f(x)$ may have two irreducible factors one of degree 2 and the other of degree 6.

In 1907 Perron[33] 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 $f(x)=x^n+a_1x^{n-1}+\dots+a_n=0$, where the a_i are rational integers, $a_n\neq0$; 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 α such that

$$|a_1+\alpha| > A+1-|a_1|-|\alpha|$$

where $A=|a_1|+|a_2|+\dots+|a_n|$;

then $|\alpha|>1$ and the absolute values of the other n-1 roots are less than one. This leads to the theorems:

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

<u>Theorem</u>: 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 $A=|a_1|+|a_2|+\dots+|a_n|$; 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

---

33. Perron, "Neue Kriterien für die Irreduzibilität algebraischer Gleichungen." <u>Journal für Mathematik</u>. CXXXII (1907), 288-307.

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:

<u>Theorem:</u> If

$$\sqrt{a_2} \geq 4^{n-1} \quad (|a_1| + |a_3| + \ldots + |a_n|)$$

then f(x) is irreducible.

If f(x) is of degree ≥ 5 it is irreducible if

$$\sqrt{a_2} \geq \left(\tfrac{7}{2}\right)^{n-1} \left(|a_1| + |a_3| + \ldots + |a_n| \right).$$

Of interest in connection with the auxiliary theorems used by Perron is a paper by Mayer.[34] Using a problem in probability and its difference equation Mayer showed that:

<u>Theorem:</u> Given $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ where the a_i are real or imaginary. If

$$|a_k| > |a_1| + |a_2| + \ldots + |a_{k-1}| + |a_{k+1}| + \ldots + |a_n|;$$

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

In 1921 Tajima[35] showed that if

$$|a_k| = |a_1| + |a_2| + \ldots + |a_{k-1}| + |a_{k+1}| + \ldots + |a_n|$$

and at least two of the quantities

$$\frac{a_1}{a_2}, \quad \frac{a_2}{a_3}, \quad \ldots, \quad \frac{a_{n-1}}{a_n} \text{ are not equal;}$$

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

---

34. Mayer, "Sur les équations algébriques." <u>Nouvelles Annales de Mathématiques</u>. ser.3.X (1891), 111-124.
35. Tajima, "On the roots of an algebraic equation." <u>Tohôku Mathematical Journal</u>. XIX (1921), 173-174.

CHAPTER II.

THE CLOSED CONVEX POLYGON

1. The Polygon of f(xy).

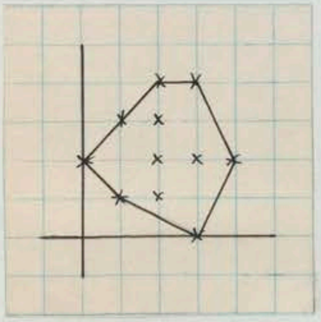
In the rapid tracing of algebraic curves in two variables a form of Newton's polygon is used to determine approximating[36] curves. This polygon is closed and convex in form and is defined by the powers of x and y appearing in the terms of the polynomial. We consider a polynomial

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

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, $f(xy) = x^4y^2 - 5x^3y^4 + 3x^3y^2 - 2x^3 - 15x^2y^4 + x^2y^3 + 10x^2y^2 + 13x^2y - 62xy^3 - 2xy + 13y^2$.

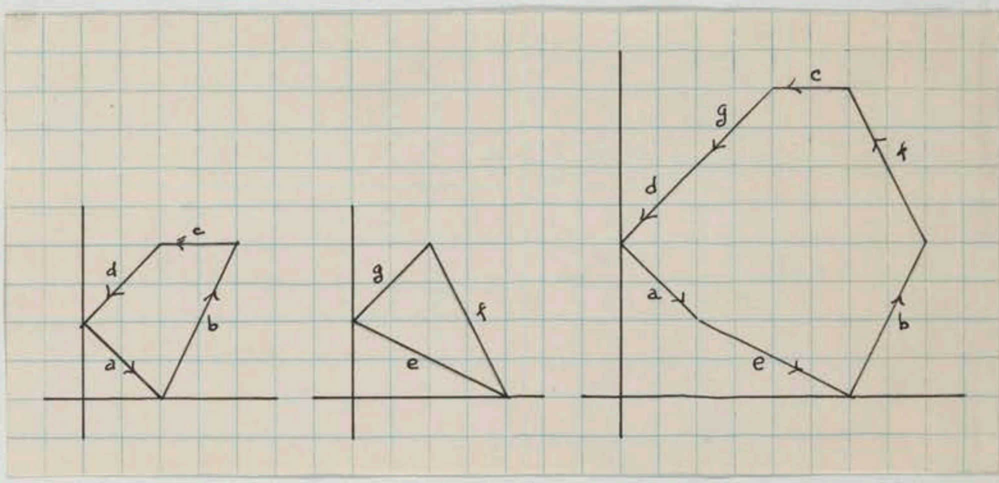


The starting point of such a polygon may be defined as

36. For a full discussion of this use of the polygons see W. W. Johnson. Curve Tracing in Cartesian Co-ordinates. New York, 1884.

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[37] 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

$$P \equiv y^n + P_{n-1}(x)y^{n-1} + \dots + P_1(x)y + P_0(x)$$

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 $a_{i0} \neq 0$ and one $a_{0j} \neq 0$;

$$g(xy) = \sum_{k=0}^{n'} \sum_{l=0}^{m'} a'_{kl} x^k y^l$$

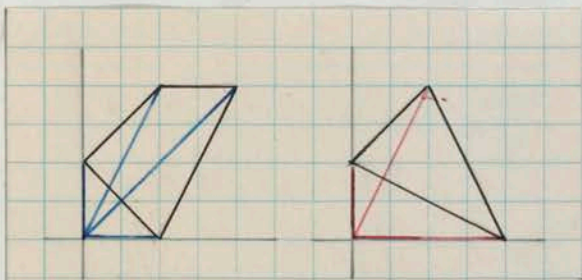
where at least one $a'_{k0} \neq 0$ and one $a'_{0l} \neq 0$.

Then $h(xy) = f(xy)g(xy)$

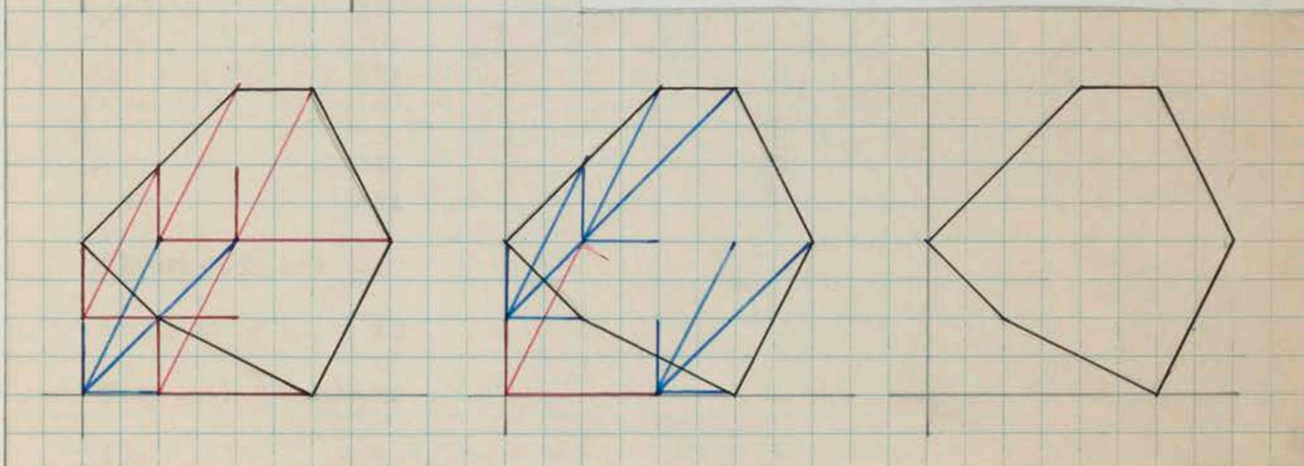
$$= \sum_{k=0}^{n+n'} \sum_{l=0}^{m+m'} c_{uv} x^u y^v$$

where $c_{uv} x^u y^v = \sum_{\substack{u=i+k \\ v=j+l}} a_{ij} a'_{kl} x^{i+k} y^{j+l}$.

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



To every point (i,j) of P_f and (k, l) of P_g is drawn a vector from the origin. By the laws of vector combin-



ation $P_f + P_g$ is then nothing more than the polygon defined by all those points whose vectors from the origin are vector sums of the vectors from the origin of P_f and P_g, considered in paris one being from P_f and one from P_g. That is, $P_f + P_g$ is the least convex polygon containing the set of points $(i+k, j+l)$.

By definition the polygon P_{fg} 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_{fg} and $P_f + P_g$ 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

$$i+k = i'+k' = i''+k'' = \dots = u$$

$$j+l = j'+l' = j''+l'' = \dots = v$$

or $$c_{uv} = a_{ij}a'_{kl} + a_{i'j'}a'_{k'l'} + a_{i''j''}a'_{k''l''} + \dots\dots$$

Consider any two of these terms

$$a_{ij}a_{kl}\ x^{i+k}y^{j+l} \text{ and } a_{i'j'}a'_{k'l'}x^{i'+k'}y^{j'+l'},$$

These are derived from the terms

$$a_{ij}x^iy^j,\ a'_{kl}x^ky^l \text{ and } a_{i'j'}x^{i'}y^{j'},\ a'_{k'l'}x^{k'}y^{l'}$$

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

$$a_{ij}a'_{k'l'}x^{i+k'}y^{j+l'},\ a_{i'j'}a'_{kl}x^{i'+k}y^{j'+l}.$$

These terms define the points

$$(i+k',\ j+l')\ (i'+k,\ j'+l).$$

The midpoint of the line joining these points is

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

or since $i+k = i'+k' = u$, $j+l = j'+l' = v$, this midpoint is the missing point (u,v) of P_{fg}.

That is, if a point P of P_{fg} corresponding to a point of $P_f + P_g$ 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_{fg} 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

$$a_{i0}x^i + a_{i1}x^iy + \dots + a_{i\,m-1}x^iy^{m-1} + a_{im}x^iy^m$$

the first and last of these for which $a_{ij} \neq 0$ 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

$$f(x) = x^n + A_1x^{n-1} + \dots + A_n$$

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

$$f(x) = \sum_{i=0}^{n} \sum_{j=0}^{\alpha_i} r_{ij}\; x^{n-i}p^j$$

where p is a rational prime and the coefficients r_{ij} 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 polygon, 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 $x = n-i$ corresponds to the highest power of p dividing A_i and the maximum point on the ordinate is $(n-i, \alpha_i)$ 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.

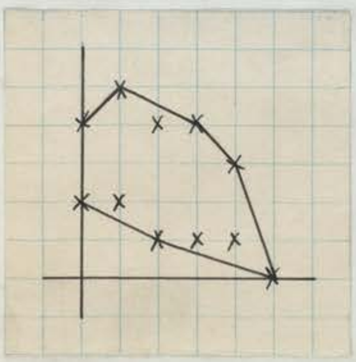
Evidently we need not plot all of the points (i,j) for our purpose, hence we shall define the <u>polygon of f(x)</u> thus:

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

$A_i \neq 0$, $A_i \equiv 0 \pmod{p^{a_i}} \not\equiv 0 \pmod{p^{a_i+1}}$

$$p^{\alpha_i} \leq |A_i| < p^{\alpha_i+1}.$$

The points $(n-i, a_i)$ $(n-i, \alpha_i)$ are plotted in a Cartesian co-ordinate system (if $A_i \neq 0$ no point is plotted on the ordinate $x = n-i$) and the least



<u>closed</u> <u>convex</u> polygon including these points is constructed. For example: $f(x) = x^5 - 14x^4 + 30x^3 - 30x^2 - 60x + 28$.

$a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 2$, $a_5 = 2$,
$\alpha_1 = 3$, $\alpha_2 = 4$, $\alpha_3 = 4$, $\alpha_4 = 5$, $\alpha_5 = 4$.

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.[38]

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).[39]

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 $P_f + P_g$ and P_{fg} coincide by Dumas' theorem, the correspondence between the upper sides is no longer exact. Consider

$$f(x) = \sum_{i=0}^{n} \sum_{j=0}^{\alpha_i} r'_{ij} \; x^i p^j$$

$$g(x) = \sum_{k=0}^{m} \sum_{l=0}^{\beta_k} r''_{kl} \; x^k p^l$$

$$h(x) = f(x)g(x) = \sum_{u=0}^{n+m} \sum_{v=0}^{\gamma_u} r_{uv} \; x^u p^v$$

The points defining the upper sides of P_f and P_g are respectively

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

These points define the points

$$(n+m-i-k, \alpha_i + \beta_k) \text{ of } P_f + P_g.$$

---

38. See pages 9 to 12 .
39. See pages 20 to 21 .

Consider the terms defining a corresponding point in $h(x)$; i.e., $u = i + k$. It consists of all the terms for which $i + k = u$,

$$\sum_{j=0}^{\alpha_i} \sum_{l=0}^{\beta_k} r'_{ij} r''_{kl} x^{n+m-i-k} \quad p^{j+l}$$

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

$$r'_{i\alpha_i} \; r''_{k\beta_k} \; p^{\alpha_i + \beta_k}$$

In $f(xy)$ the coefficient $r'_{i\alpha_i} \; r''_{k\beta_k}$ could not affect the powers of y, it may now however affect the powers of p. If

$$r'_{i\alpha_i} \; r''_{k\beta_k} \geq p$$

we have a term containing p to the power $\alpha_i + \beta_k + 1$, and the point defining P_{fg} lies above the corresponding point defining $P_f + P_g$. Correspondingly if in the coefficient

$$r'_{i\,\alpha_i - 1} \quad r''_{k\beta_k} \quad p^{\alpha_i + \beta_k - 1}$$

$$r'_{i\,\alpha_i - 1} \quad r''_{k\beta_k} > p,$$

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_{fg} may fall below the point defining $P_f + P_g$. 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

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n$$

with complex coefficients. For all non-vanishing coefficients a we plot the points

$$P_i = (i, \log |a_i|) \qquad (i = 1, 2, \dots, n)$$

in a Cartesian coordinate system and construct the lowest convex polygon lying above all points. We shall denote the sides of this polygon by

$$S_1, S_2, \dots, S_r$$

The projections of these sides on the X-axis are

$$l_1, l_2, \dots l_r,$$

and these numbers are all positive integers, while the projections

$$h_1, h_2, \dots, h_r$$

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.) $$k_i = \operatorname{tg} \phi_i = \frac{h_i}{l_i} = \log \mathcal{K}_i \; (i = 1, 2, \dots, r).$$

The first and last point of the i-th side are respectively $(l_1 + \ldots + l_{i-1}, \log|a_{l_1+\cdots+l_{i-1}}|)$, $(l_1 + \ldots + l_i, \log|a_{l_1+\cdots+l_i}|)$ and hence one finds for the slope

$$k_i = \operatorname{tg}\varphi_i = \frac{1}{l_i}\left(\log|a_{l_1+\cdots+l_i}| - \log|a_{l_1+\cdots+l_{i-1}}|\right)$$

or

$$\log|a_{l_1+\cdots+l_i}| = \log|a_{l_1+\cdots+l_{i-1}}| + l_i k_i$$

or also according to (1)

$$\varkappa_i = \left|\frac{a_{l_1+\cdots+l_i}}{a_{l_1+\cdots+l_{i-1}}}\right|^{\frac{1}{l_i}}.$$

Now let

$$\lambda_i = l_1 + \ldots + l_i$$

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_{λ_i+j} lying to the right of P_{λ_i}. Since all such points are lying on or below the (i + 1)-st side S_{i+1}, we have

$$\log|a_{\lambda_{i}+j}| \leq \log|a_{\lambda_i}| + jk_{i+1} = \log|a_{\lambda_i}| + j\log\varkappa_{i+1}$$

or

(3)
$$|a_{\lambda_i+j}| \leq |a_{\lambda_i}|\varkappa_{i+1}^{j}.$$

In the same way one finds for the points to the left of P_{λ_i}

$$\log|a_{\lambda_i-j}| \leq \log|a_{\lambda_i}| - jk_i = \log|a_{\lambda_i}| - j\log\varkappa_i$$

or

(4)
$$|a_{\lambda_i-j}| \leq |a_{\lambda_i}|\varkappa_i^{-j}.$$

These two inequalities (3) and (4) are fundemental in the following considerations.

2. Next let

$$g(x) = x^m + b_1 x^{m-1} + \ldots + b_m$$

be another polynomial and let us construct the corresponding polygon with the sides

$$S'_1, S'_2, \dots S'_s$$

and the slopes

$$k'_i = \log \varkappa'_i \qquad (i = 1, 2, \dots, s).$$

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

(5) $$|b_{\mu_i+j}| \leq |b_{\mu_i}| \varkappa'^{\,j}_{i+1}, \quad |b_{\mu_i-j}| \leq |b_{\mu_i}| \varkappa'^{\,-j}_{i}.$$

We shall now form the product

$$h(x) = f(x)g(x) = x^{n+m} + c_1 x^{n+m-1} + \dots + c_{n+m}$$

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_{fg} 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_{fg} 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_{fg} 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_{fg} of P_{fg} may be than the corresponding ordinate y_{f+g} of $P_f + P_g$. The coefficients in the product have the form

$$c_i = a_i + b_1 a_{i-1} + \dots + b_{i-1} a_1 + b_i$$

and hence

$$(6) \qquad |c_i| \le |a_i| + |b_1||a_{i-1}| + \dots + |b_{i-1}||a_1| + |b_i| .$$

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

$$(7) \qquad \begin{cases} t_i = i + 1 & \text{for } i \le m \\ t_i = m + 1 & \text{for } n \ge i \ge m \\ t_i = n + m + 1 - i & \text{for } i \ge n . \end{cases}$$

In every case we have

$$(8) \qquad t_i \le m + 1 \le \frac{N}{2} + 1 .$$

The point $(i, \log |c_i|)$ lies on or below the polygon P_{fg}. From the construction of the sum polygon $P_f + P_g$ it follows that no expression $\log |a_s||b_{i-s}|$ can exceed the ordinate y_{f+g} of $P_f + P_g$ at this point. Hence we obtain from (6)

$$(9) \qquad \log |c_i| \le y_i + \log t_i$$

for all i and hence we obtain

$$(10) \qquad y_{fg} - y_{f+g} \le \log t_i \le \log (m + 1) \le \log \left(\frac{N}{2} + 1\right)$$

which is the result we wanted to establish.

4. The more difficult proposition is to show that the polygon P_{fg} cannot fall very much below $P_f + P_g$. We shall show this by considering the difference of the ordinates of the two polygons at a corner point of $P_f + P_g$. The ordinate y_{f+g} at this point is

$$(11) \qquad y_{f+g} = \log |a_r| + \log |b_s| ,$$

where

(12) $\quad (r, \log |a_r|), \quad (s, \log |b_s|)$

are corner points of P_f and P_g respectively. We shall then have to determine a bound for the absolute value of the difference

(13) $$\delta = \left| \log |c_{r+s}| - \log |a_r| - \log |b_s| \right| = \left| \log \frac{|c_{r+s}|}{|a_r| |b_s|} \right|.$$

For c_{r+s} we have the expression

$$c_{r+s} = a_r b_s + a_{r-1} b_{s+1} + \dots + a_{r+1} b_{s-1} \dots$$

and hence from (13)

(14) $$\delta = \left| \log \left| 1 + \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \frac{a_{r-2}}{a_r} \frac{b_{s+2}}{b_s} + \dots \right.\right.$$
$$\left.\left. + \frac{a_{r+1}}{a_r} \frac{b_{s-1}}{b_s} \frac{a_{r+2}}{a_r} \frac{b_{s-2}}{b_s} + \dots \right| \right|$$

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

(15) $$\left| \frac{a_{r-i}}{a_r} \right| \leq \mathcal{H}_\alpha^{-i} \qquad \left| \frac{a_{r+i}}{a_r} \right| \leq \mathcal{H}_{\alpha+1}^{i}$$
$$\left| \frac{b_{s-i}}{b_s} \right| \leq \mathcal{H}_\beta'^{-i} \qquad \left| \frac{b_{s+i}}{b_s} \right| \leq \mathcal{H}_{\beta+1}'^{i}$$

We then find

(16) $$\left| \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \frac{a_{r-2}}{a_r} \frac{b_{s+2}}{b_s} + \dots \right| \leq \frac{\mathcal{H}'_{\beta+1}}{\mathcal{H}_\alpha} + \left(\frac{\mathcal{H}'_{\beta+1}}{\mathcal{H}_\alpha} \right)^2 + \dots$$
$$\frac{\mathcal{H}'_{\beta+1}}{\mathcal{H}_\alpha} \; \frac{1}{1 - \frac{\mathcal{H}'_{\beta+1}}{\mathcal{H}_\alpha}}$$

and in the same way

(17) $$\left| \frac{a_{r+1}}{a_r} \frac{b_{s-1}}{b_s} + \frac{a_{r+2}}{a_r} \frac{b_{s-2}}{b_s} + \dots \right| < \frac{\mathcal{H}_{\alpha+1}}{\mathcal{H}'_\beta} \; \frac{1}{1 - \frac{\mathcal{H}_{\alpha+1}}{\mathcal{H}'_\beta}}$$

It should be observed that

$$\mathcal{H}_\alpha > \mathcal{H}_{\alpha+1}, \quad \mathcal{H}'_\beta > \mathcal{H}'_{\beta+1}$$

and from the construction of the sum polygon follows

$$\mathcal{H}'_\beta > \mathcal{H}_{\alpha+1}, \quad \mathcal{H}_\alpha > \mathcal{H}'_{\beta+1}$$

We shall now introduce the <u>sharpness</u> of a corner of a polygon, defining the sharpness σ_α of the α-th corner of the polygon P_f through the relation

$$\mathcal{H}_\alpha = \sigma_\alpha \mathcal{H}_{\alpha+1} .$$

In the same way σ'_β is the sharpness of the β-th corner of P_g, where

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

Let us now consider the sharpness σ of the corner C of $P_f + P_g$. We have four different possibilities

$$\mathcal{H}'_\beta \geq \mathcal{H}_\alpha > \mathcal{H}_{\alpha+1} \geq \mathcal{H}'_{\beta+1}$$
$$\mathcal{H}_\alpha \geq \mathcal{H}'_\beta > \mathcal{H}'_{\beta+1} \geq \mathcal{H}_{\alpha+1}$$
$$\mathcal{H}_\alpha \geq \mathcal{H}'_\beta > \mathcal{H}_{\alpha+1} \geq \mathcal{H}'_{\beta+1}$$
$$\mathcal{H}'_\beta \geq \mathcal{H}_{\alpha} > \mathcal{H}'_{\beta+1} \geq \mathcal{H}_{\alpha+1}$$

and in the respective cases we find the four values for σ

$$\sigma_\alpha, \ \sigma'_\beta, \ \frac{\mathcal{H}'_\beta}{\mathcal{H}_{\alpha+1}}, \ \frac{\mathcal{H}_\alpha}{\mathcal{H}'_{\beta+1}}$$

A simple consideration shows that in all cases

$$(18) \qquad \frac{\mathcal{H}'_{\beta+1}}{\mathcal{H}_\alpha} \leq \frac{1}{\sigma} \qquad , \qquad \frac{\mathcal{H}_{\alpha+1}}{\mathcal{H}'_\beta} \leq \frac{1}{\sigma}$$

and from (16) and (17) we obtain

$$\left| \frac{a_{r-1}}{a_r} \frac{b_{s+1}}{b_s} + \ldots + \frac{a_{r+1}}{a_r} \frac{b_{s-1}}{b_s} + \ldots \right| < \frac{2}{\sigma - 1} .$$

This in turn gives the following limits for δ

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

or

$$(19) \qquad \frac{\sigma + 1}{\sigma - 1} |a_r||b_s| > |c_{r+s}| > \frac{\sigma - 3}{\sigma - 1} |a_r||b_s|$$

which is the result we desired to deduce. It shows that at a sharp corner point of $P_f + P_g$ the point C of the product cannot differ greatly from it. We have for instance for $\sigma = 4$ and $\sigma = 5$ respectively.

$$\frac{1}{3}|a_r||b_s| < |c_{r+s}| < \frac{5}{3}|a_r||b_s|$$

(20)

$$\frac{1}{2}|a_r||b_s| < |c_{r+s}| < \frac{3}{2}|a_r||b_s|$$

I also observe that under certain conditions C will also be a corner point of P_{fg} and the sharpness of the corner can only slightly exceed σ.

5. We shall now investigate how much the polygon P_{fg} may fall below $P_f + P_g$ at any point at which the sharpness of $P_f + P_g$ is less than 4. We consider two consecutive sharp points P_1 and P_2 of $P_f + P_g$ corresponding to the abscissae s and $s+t$. At P_1 and P_2 the polygon P_{fg} cannot fall more than log 3 below $P_f + P_g$. The polygon $P_f + P_g$ is made up of parts of P_f and P_g 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 $P_f + P_g$ is

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

where the k_j are the slopes of P_f and P_g arranged in decreasing order. We also suppose for simplicity, that every point of $P_f + P_g$ 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) $$y_i = \log|a_r| + \log|b_s| + \frac{i}{t}\sum_{j=1}^{t} k_j.$$

We are mainly interested in the difference between these ordinates which is found to be

$$(24) \qquad \Delta_i = \sum_{j=1}^{i} k_j - \frac{i}{t}\sum_{j=1}^{t} k_j = \left(1 - \frac{i}{t}\right)\sum_{j=1}^{i} k_j - \frac{i}{t}\sum_{j=i+1}^{t} k_j .$$

We want to determine the maximal value of this expression. To this end we introduce the $\mathcal{H}_i$ by the relation $k_i = \log \mathcal{H}_i$ and obtain

$$(25) \qquad \Delta_i = \left(1 - \frac{i}{t}\right)\sum_{j=1}^{i} \log \mathcal{H}_j - \frac{i}{t}\sum_{j=i+1}^{t} \log \mathcal{H}_j$$

$$= \log \left(\mathcal{H}_1 \ldots \mathcal{H}_i\right)^{1-\frac{i}{t}} \left(\mathcal{H}_{i+1} \ldots \mathcal{H}_t\right)^{-\frac{i}{t}} .$$

We shall next use the fact that the sharpness of any corner of $P_f + P_g$ in this interval is less than 4. The sharpness σ_i was defined by the relation

$$(26) \qquad \mathcal{H}_i = \sigma_i \mathcal{H}_{i+1} , \quad \sigma_i \geq 1 .$$

or

$$(27) \qquad \log \mathcal{H}_i = \log \mathcal{H}_{i+1} + \log \sigma_i .$$

From (26) one easily deduces

$$(28) \qquad \mathcal{H}_j = \sigma_j \sigma_{j+1} \ldots \sigma_{t-1} \mathcal{H}_t$$

or

$$\log \mathcal{H}_j = \log \sigma_j + \log \sigma_{j+1} + \ldots + \log \sigma_{t-1} + \log \mathcal{H}_t .$$

From this relation follows

$$(29) \qquad \sum_{j=1}^{i} \log \mathcal{H}_j = \log \sigma_1 + 2 \log \sigma_2 + \ldots + i \log \sigma_i$$
$$+ i \left(\log \sigma_{i+1} + \ldots + \log \sigma_{t-1}\right) + i \log \mathcal{H}_t ,$$

and

$$(30) \qquad \sum_{j=i+1}^{t} \log \mathcal{H}_j = \log \sigma_{i+1} + 2 \log \sigma_{i+2} + \ldots +$$
$$+ (t - i - 1) \log \sigma_{t-1} + (t - 1) \log \mathcal{H}_t .$$

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

$$\Delta_i = \left(1 - \frac{i}{t}\right) \left(\log \sigma_1 + 2 \log \sigma_2 + \ldots + i \log \sigma_i\right)$$
$$\frac{i}{t}\left((t - i - 1) \log \sigma_{i+1} + (t - i - 2) \log \sigma_{i+2} + \ldots + \log \sigma_{t-1}\right).$$

Since the coefficients in all of these terms are positive we obtain the maximal value for Δ_i by making $\sigma_j = \sigma = 4$ for all j. This gives

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

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

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

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

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

CHAPTER IV.

IRREDUCIBILITY CRITERIA

1. The Application of the Convex Polygon

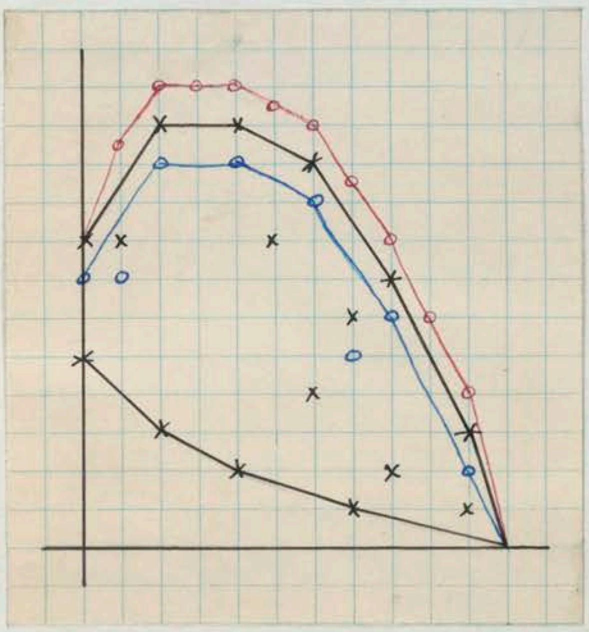
There remains to be demonstrated the method for the application of these polygons.

Given

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

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 $A_i \neq 0$;

$$A_i \equiv 0 (\text{mod } p^{a_i}) \not\equiv 0 (\text{mod } p^{a_i+1})$$
$$p^{\alpha_i} \leq |A_i| < p^{\alpha_i+1}$$



The points $(n-i, a_i)(n-i, \alpha_i)$ (indicated by X) are plotted and the least convex polygon is constructed. On any ordinate $x = n-i$ the distance $\underline{\Delta_i + 1}$, $i = 1,2,\dots,n-1$ (indicated by o) above the point where this polygon crosses the ordinate is laid off, where

$$\Delta_i = \log_p (3.2^{i(n-i)})$$

On any ordinate $x = n-i$, $i = 1,2,\dots,n$, the distance $\underline{\delta_i + 1}$ is laid off below the point $(n-i, \alpha_i)$ (indicated by ○), where

$$\delta_i = \log_p(t_i)$$

where $$t_i = i+1 \quad \text{for } i \leq \frac{n}{2}$$

$$t_i = n-i+1 \quad \text{for } i \geq \frac{n}{2}$$

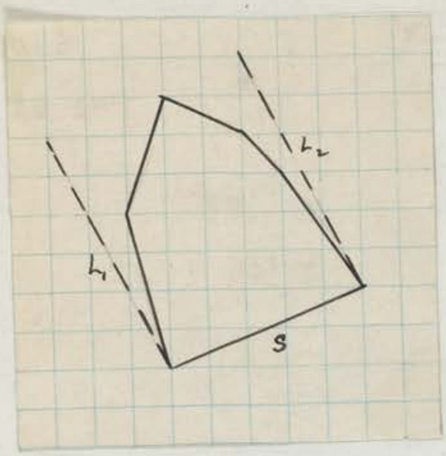
The least convex polygon lying above and including these two sets of points are the limits of a region R (upper limit polygon — , lower limit polygon —). It is evident by the considerations of Chapter III. that if the polynomial is reducible the product of the polygons of its factors must lie nn the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

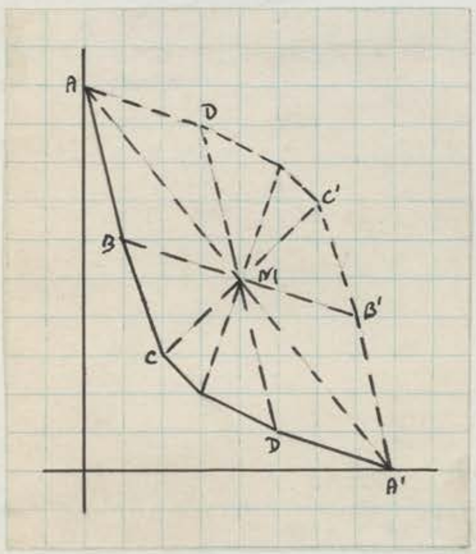
2. Irreducible Polygons

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_1, 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 $ABC\ldots DA'$. With the mid-point M of this line as center construct above the line the corner points, lattice points on the sides $(B'C'\ldots D')$ 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

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

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 lines through A' and B' and lying above $A'B'$ which is contrary to the hypothesis that the points $B', C', \ldots\ldots, D'$ are not included by the upper limit polygon of P.

Suppose ABC...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.

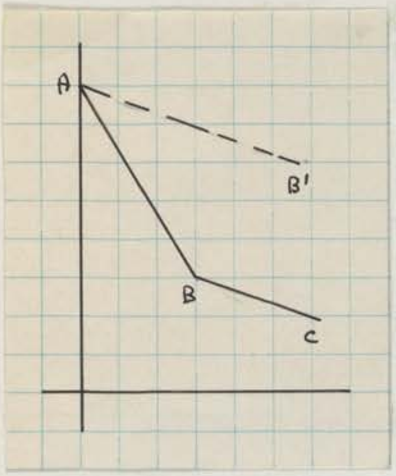
3. <u>Polygons of Type I.</u>

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. <u>The irreducible side S forms the Dumas polygon.</u>

This is the Dumas criterion.

2. <u>The irreducible side S is the first side of the Dumas polygon.</u>



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

$A = (0, a_n)$ $B = (n-k, a_k)$ $C = (n-l, a_l)$

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

The conditions defining the side BC are:

3.) $\dfrac{a_k - a_l}{k-l} < \dfrac{a_n - a_k}{n-k}$

4.) $a_l + j\left(\dfrac{a_k - a_l}{k-l}\right) \leq a_{l+j}$ $\quad j = 1, 2, \ldots, k-l-1$

The condition on the remaining sides of the Dumas polygon is:

5.) $a_l + (i-l)\left(\dfrac{a_k - a_l}{k-l}\right) \leq a_i$ $\quad i = 1, 2, \ldots, l-1$

Let $\alpha_r \geq \alpha_i$, $\quad i = 1, 2, \ldots, n-1$

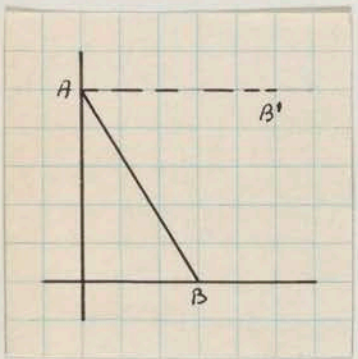
We now desire to insure that no point of the upper limit polygon falls on or above the line AB parallel to BC. There are two necessary conditions, 6.) $\alpha_n = a_n > \frac{n}{k-l} (a_k - a_l)$

7.) $\frac{\alpha_n - \alpha_r}{n-1} - \frac{\Delta_i + 1}{n-i} \frac{a_k - a_l}{k-l}$ $i = 1,2,\ldots,n-1$

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.) $\frac{a_n}{n-k} \leq \frac{a_{k+j}}{j}$ $j = 1,2,\ldots,n-k-1$

6a.) $\alpha_n = a_n > 0$

7a.) $\frac{\alpha_n - \alpha_r}{n-1} > \frac{\Delta_i + 1}{n-i}$

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

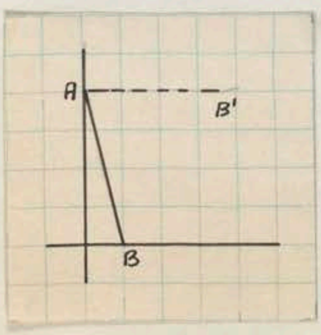
$$x^n \pm kx^m \pm l p^v, \quad n > m,$$

where $(m,v) = 1$, $k \not\equiv 0 \pmod p$,

$0 < k < p^{v-2(n-1)}$ $0 < l < p$ and $p > 3.2^{\frac{n^2}{4}}$

is irreducible.

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



1b.) $a_{n-1} = 0$

6b.) $\alpha_n = a_n > 0$

7b.) $\frac{\alpha_n - \alpha_r}{n-1} > \frac{\Delta_i + 1}{n-i}$ $i = 1,2,\ldots,n-1$

or $\alpha_n > \frac{(n-1)}{(n-i)} (\Delta_i + 1) + \alpha_r$

For example:

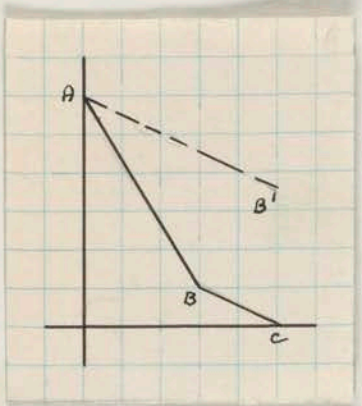
$$x^n \pm kx \pm lp^v,$$

where $\quad k \not\equiv 0 \pmod{p}, \; 0 < k < p^{v-2(n-1)}$

$$0 < l < p, \quad \text{and } p > (3.2)^{\frac{n^2}{4}}$$

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

3c.) $\frac{a_k}{k} < \frac{a_n - a_k}{n-k}$

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

6c.) $\alpha_n = a_n \ge \frac{n}{k}\ a_k$

7c.) $\frac{\alpha_n - \alpha_r}{n-1} - \frac{\Delta_i + 1}{n-1} > \frac{a_k}{k} \qquad i = 1,2,\ldots,n-1$

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

For example:

$$x^n \pm kp^u x^m \pm lp^v, \; n > m$$

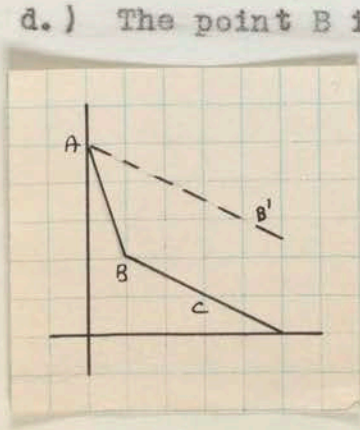
where $\quad (v-u, m) = 1, \quad \frac{u}{n-m} < \frac{v-u}{m}$

$$0 < l < p, \qquad k \not\equiv 0 \pmod{p},$$

$$0 < k < p^{v-u-(n-1)\left(\frac{u}{n-m}+2\right)}, \quad \text{and } p > 3.2^{\frac{n^2}{4}}$$

is irreducible.

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



3d.) $\frac{a_{n-1} - a_l}{n-l-1} < a_n - a_{n-1}$

4d.) $a_l + j\left(\frac{a_{n-1} - a_l}{n-l-1}\right) \le a_{l+j} \qquad j = 1,2,\ldots,n-l-2$

5d.) $a_l + (i-l)\left(\frac{a_k - a_l}{k-l}\right) \le a_i \quad i = 1,2,\ldots,l-1$

6d.) $\alpha_n = a_n \geq \frac{n}{n-l-1}(a_{n-1} - a_l)$

7d.) $\frac{\alpha_n - \alpha_r}{n-1} - \frac{\Delta_i + 1}{n-i} > \frac{a_{n-1} - a_l}{n-l-1}$ $\quad i \quad 1,2,\ldots,n-1$

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

For example:

$$x^n \pm kp^u x^m \pm lp^v$$

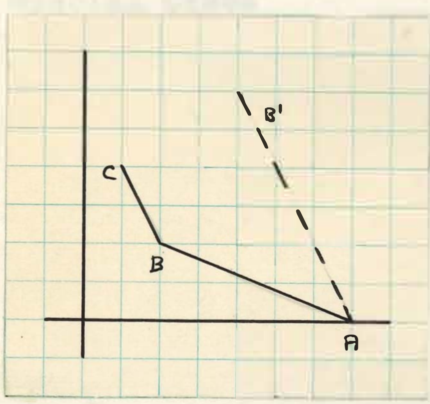
where $v > u + \frac{u}{n-1}$, $\quad 0 < l < p$,

$k \not\equiv 0 \pmod{p}$, $\quad 0 < k < p^{v-2(n-u-1)}$

and $p > 3.2^{n^2/4}$

is irreducible.

3. <u>The irreducible side S is the last side of the Dumas polygon.</u>



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

$$A = (n,0) \quad B = (n-k, a_k) \quad C \quad (n-l, a_l)$$

It is 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:

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

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

The conditions defining the side BC are:

10.) $\frac{a_l - a_k}{l-k} > \frac{a_k}{k}$

11.) $a_k + j\left(\frac{a_l - a_k}{l-k}\right) \leq a_{k+j}$ $\qquad j = 1,2,\ldots,l-k-1$

The conditions on the remaining sides of the Dumas polygon is

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

Let $\quad \alpha_r \geq \alpha_i \qquad\qquad i = 1,2,\ldots,n-1$

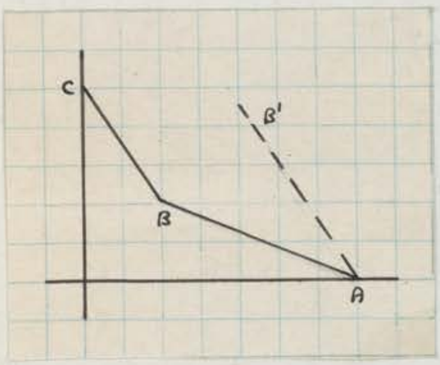
The condition is now imposed that no point of the upper limit polygon fall on or above the line AB parallel to BC, this is

$$13.)\quad \alpha_r + \frac{\Delta_i + 1}{i} < \frac{a_l - a_k}{l-k} \qquad i = 1,2,\ldots,n-1$$

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

Special Cases

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



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

$$9a.)\quad \frac{a_k}{k} < \frac{a_i}{i} \qquad i = 1,2,\ldots,k-1$$

$$10a.)\quad \frac{a_n - a_k}{n-k} > \frac{a_k}{k}$$

$$11a.)\quad a_l + j\left(\frac{a_n - a_k}{n-k}\right) \leq a_{h+j} \qquad j = 1,2,\ldots,l-k-1$$

$$13a.)\quad \alpha_r + \frac{\Delta_i + 1}{i} < \frac{a_n - a_k}{n-k} \qquad i = 1,2,\ldots,n-1$$

Any polygon f(x) satisfying these conditions is irreducible. For example:

$$x^n \pm kp^u x^m \pm lp^v, \qquad n > m$$

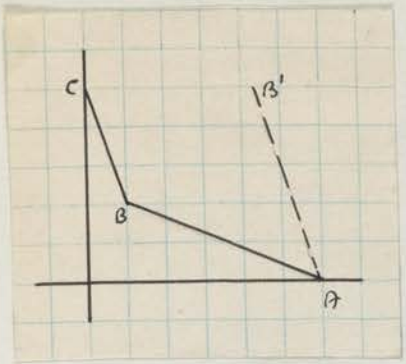
where $\quad (u, n-m) = 1, \qquad \frac{v}{n} > \frac{u}{n-m},$

$$0 < l < p, \quad k \not\equiv 0 \pmod{p}, \quad 0 < k < p^{\frac{v-(m+1)u}{m} - 2}$$

and $\quad p > 3.2^{\frac{n^2}{4}}$

is irreducible.

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



$C = (0, a_n)$

8b.) $(a_{n-1}, n-1) = 1$

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

10b.) $a_n - a_{n-1} > \frac{a_{n-1}}{n-1}$

13b.) $\alpha_r + \frac{\Delta_i + 1}{i} < a_n - a_{n-1}$ $\qquad i = 1, 2, \ldots, n-1$

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

For example:

$$x^n \pm kp^u x \pm l p^v$$

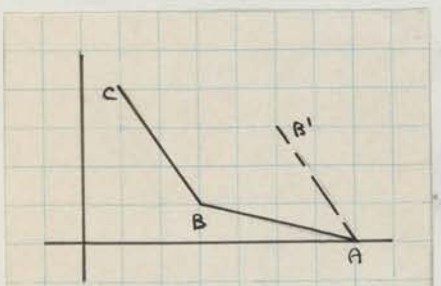
where $\qquad (u, n-1) = 1, \qquad \frac{v}{n} > \frac{u}{n-1},$

$$0 < l < p, \quad k \not\equiv 0 \pmod p, \quad 0 < k < p^{v-2(u+1)}$$

and $\qquad p > 3.2^{n^2/4}$

is irreducible.

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



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

10c.) $\frac{a_l - 1}{l - k} > \frac{1}{k}$

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

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

13c.) $\alpha_r + \frac{\Delta_i + 1}{i} < \frac{a_l - 1}{l - k}$ $\qquad i = 1, 2, \ldots, n-1$

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

For example:

$$x^n \pm kpx^m \pm l p^v$$

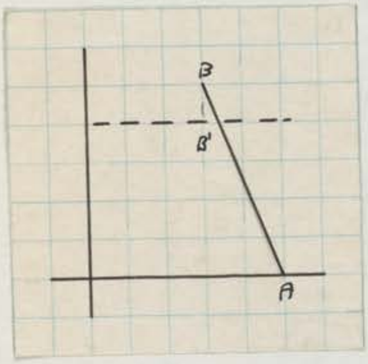
where $\qquad v > \dfrac{n}{n-m}$, $\qquad 0 < l < p$,

$$k \not\equiv 0 \pmod{p}, \qquad 0 < k < p^{\frac{v-1}{m}-3}$$

and $\qquad p > 3.2^{n^2/4}$

is irreducible.

4. <u>The irreducible side S is the first side of the upper polygon.</u>



Let AB be the irreducible side S.

$A = (n,0) \qquad B = (n-k, \alpha_k)$

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 $x = n-k$.

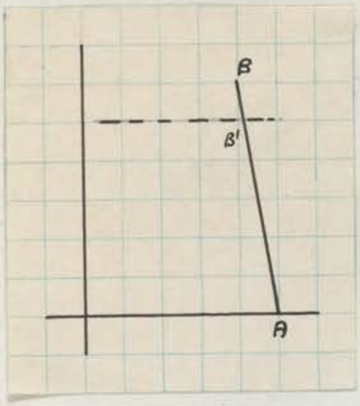
If α_r is the maximum of the numbers $\alpha_{k+1}, \ldots, \alpha_n$, the condition that no point of the upper limit polygon fall above the line through B' is

$$14.) \quad \alpha_k - \alpha_r > (\delta_k + \Delta_i)\left(\frac{n-k}{i-k}\right) \qquad i = k+1, \ldots, n$$

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

$$\alpha_1 - \alpha_r > (1 + \Delta_i)\left(\frac{n-1}{i-1}\right) \qquad i = 2,3,\ldots,n$$

Special Case



If $p > 3.2^{\frac{n^2}{4}}$, $\Delta_i < 1$

$\alpha_1 - \alpha_r > \frac{2(n-1)}{i-1}$

or $\alpha_1 > 2(n-1) + \alpha_n$

This condition expressed in terms of the coefficients is

$$|A_1| > p^{2(n-1)} |A_r|$$

where $|A_r| \geq |A_i|$ $i = 2,\dots,n$

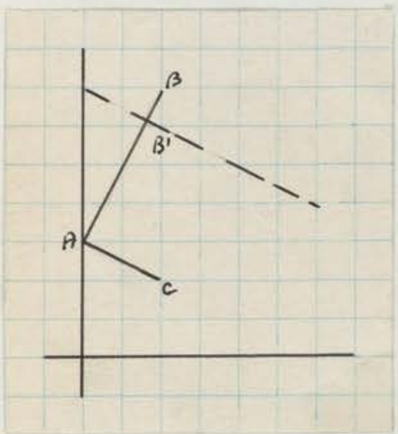
Or it may be written

$$|A_1| > p^{2(n-1)} \quad (|A_2| + |A_3| + \dots + |A_n|),$$

where $p > 3.2^{\frac{n^2}{4}}$.

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

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

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.) $a_l + j\left(\frac{a_n-a_l}{n-l}\right) \le a_{l+j}$ $\quad j = 1,2,\dots,n-l-1$

$\alpha_n = a_n$

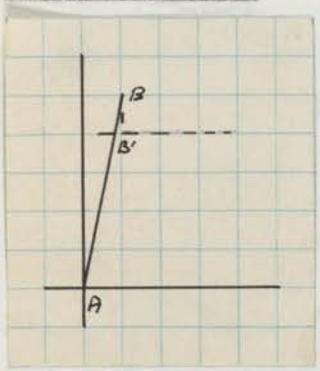
The condition that no point of the upper limit polygon fall on or above $B'C'$ is

$$\frac{\alpha_k - \alpha_r}{k-1} > \frac{\Delta_i + \delta_k + 2}{k-i} \quad \frac{a_n - a_l}{n-l} \qquad i = 1,2,\dots,k-1$$

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

16.) $\frac{\alpha_{n-1} - \alpha_r}{n-2} > \frac{\Delta_i + 3}{n-i-1} + \frac{a_n - a_l}{n-l} \qquad i = 1,2,\dots,(n-2)$

<u>Special Cases</u>



a.) If $\alpha_n = a_n = 0$ this becomes

16a.) $\frac{\alpha_{n-1} - \alpha_r}{n-2} > \frac{\Delta_i + 3}{n-i-1}$

b.) If in addition to $\alpha_n = a_n = 0$, $p > 3.2^{n^2/4}$

$\Delta_i = 1$ and we have

16b.) $\alpha_{n-1} > 4(n-2) + \alpha_r$

In terms of the coefficients,

If $\quad |A_n| < p \quad , \; p > 3.2^{n^2/4}$

and $\quad |A_{n-1}| > p^{4(n-2)} \, |A_r|$

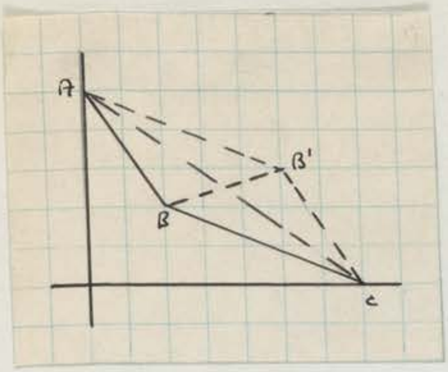
where $\quad |A_r| \ge |A_i| \qquad i = 1,2,\dots,(n-2)$

then $f(x)$ is irreducible.

4. <u>Polygons of Type II</u>.

The application of this type of polygon leads for the greater part to theorems concerning the numbers and degrees of possible factors.

1. <u>The Dumas polygon consists of two straight lines.</u>



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:

$$1.)\quad a_k + j\left(\frac{a_n-a_k}{n-k}\right) \le a_{k+j} \qquad j = 1,2,\dots,n-k-1$$

The line BC is defined by the conditions:

$$2.)\quad \frac{a_k}{k} < \frac{a_n-a_k}{n-k}$$

$$3.)\quad \frac{a_k}{k} \le \frac{a_i}{i} \qquad i = 1,2,\dots,k-1$$

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 $y = a_n-a_k-m(x-k)$

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

Therefore the condition is

$$\alpha_i < a_n-a_k-m(n-i-k)-1-\max\Delta_i \qquad i = 1,2,\dots,n$$

or

$$4.)\quad \alpha_i < a_n-a_k+\frac{a_n}{n}(i+k)-1-\Delta_{n/2}$$

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 $n-k+\varepsilon\frac{k}{e}$ and one ore more factors of degree $\varepsilon\frac{k}{e}$ where ε is one of the number $1,2,\ldots,e-1$.

If $(a_n-a_k, n-k)=t$ and $(a_k, k)=1$ then $f(x)$ if reducible has one or more factors of degree

$$\tau\frac{n-k}{t}+k$$

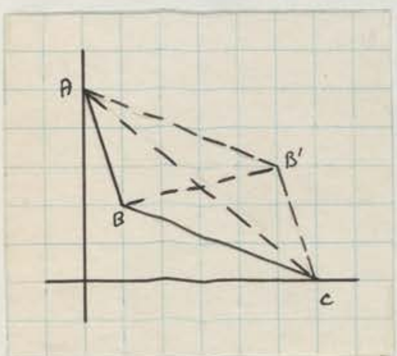
and one or more factors of degree $\tau\frac{n-k}{t}$ when τ is one of the numbers $1,2,\ldots,t-1$.

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 $\tau\frac{n-k}{t}+\varepsilon\frac{k}{e}$ where $\tau=0,1,2,\ldots\ldots,t-1$

$$\varepsilon=0,1,2,\ldots\ldots,e-1$$

That is, it may not have factors whose Dumas polygons are the lines AB, BC.

Special Cases



a.) If $p>3.2^{n^2/2}$, $\Delta_i<1$

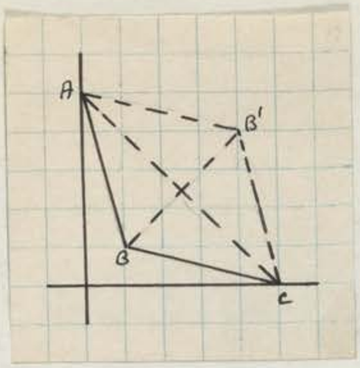
If also the point B lies on the ordinate $x=1$; i.e., $B=(1,a_{n-1})$,

2a.) $\frac{a_{n-1}}{n-1}<a_n-a_{n-1}$

3a.) $\frac{a_{n-1}}{n-1}<\frac{a_i}{i}$ $\quad i=1,2,\ldots,n-2$

4a.) $\alpha_i<2a_n-a_{n-1}-2+\frac{a_n}{n}$ $(i-1)$

If $(a_{n-1}, n-1)=1$ the polynomial is irreducible.



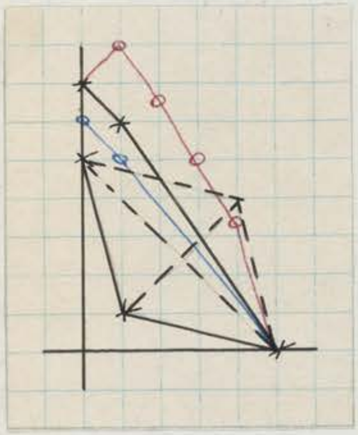
b.) If the point $B = (1,1)$; i.e., $a_{n-1} = 1$ and $p > 3.2^{n^2/4}$, the further conditions under which the polynomial is irreducible are:

2b.) $a_n > 1$

3b.) $a_i \geq 1 \qquad i = 1,2,\ldots,n-2$

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

Thus all polynomials of the form



$x^n \pm kpx \pm p^v m \qquad v > 3$

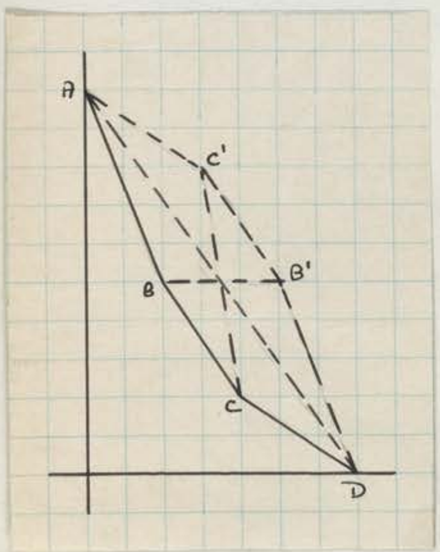
where $k \not\equiv 0 \pmod p$, $0 < k < p^{2v-4}$,

$m \not\equiv 0 \pmod p$, $0 < m < p^{v-3}$

and $\quad p > 3.2^{n^2/4}$

are irreducible.

2. <u>The Dumas polygon consists of three straight lines.</u>



The Dumas polygon is defined by the points $A = (0, a_n)$ $B = (n-k, a_k)$ $C = (n-l, a_l)$ $D = (n, 0)$. 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,

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

$$(a_k - a_l\ , k-l) = 1$$

$$(a_l, l) = 1.$$

The condition must now be applied that the upper limit polygon shall not include the points B' and C'. These points are $B' = (k, a_n - a_k)$ $C' = (l, a_n - a_l)$. The line $B'C'$ is

$$y = \frac{(k-l+1)a_l - a_k}{(k-l)}(x-l)$$

Therefore the condition is

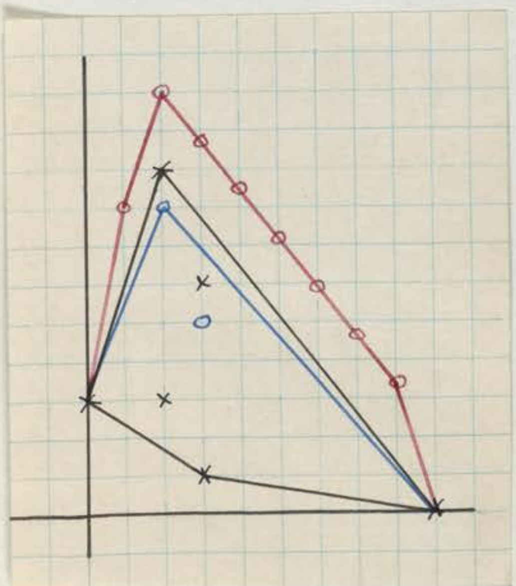
5.) $$\frac{(k-l+1)a_l - a_k}{(k-l)}(n-i-l)-1-\max\Delta_i$$

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

5. Numerical Cases

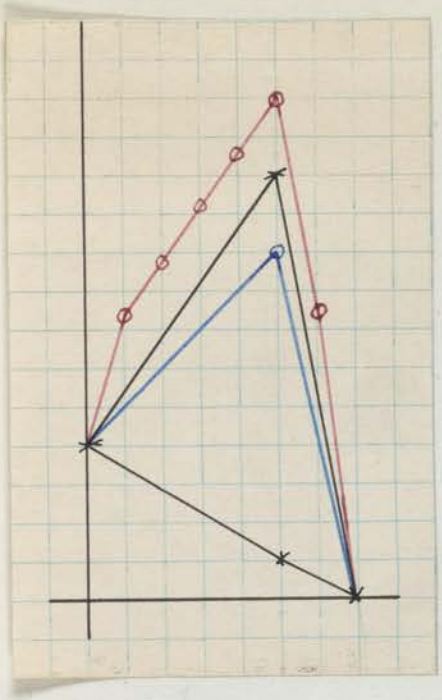
Further application of these polygons to derive algebraic criteria does not seem advisable since they are so complicated in statement.

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: $f(x) = x^9 \pm (p^6+p)x^3 \pm (p^9+p^3)x^2 \pm p^3$, $p > 3.2^{81/4}$ is irreducible since it is impossible to decompose any of its possible polygons into closed convex factor polygons.

So also is:



$f(x) = x^7 \pm (p^{11} + p)x^5 \pm p^4$ where $p > 3.2^{49/4}$ irreducible for the same reason.

Two other forms of irreducible polynomials are:

a.) $f(x) = x^n \pm kx^2 \pm l p^{2v+1}$

where $0 < k < p^{2(v-2)}$, $k \not\equiv 0 \pmod p$,

$0 < l < p$ and $p > 3.2^{n^2/4}$

is irreducible. The pòlygon is of type I, case 2a.)

b.) $f(x) = x^n \pm kp^2 x^{n-m} \pm l p^v$

where $m = 2m' + 1$,

$v \geq 4(n-m) + 2$,

$0 < k < p^{\frac{m}{n}v-2}$, $k \not\equiv 0 \pmod p$,

$0 < l < p$ and $p > 3.2^{n^2/4}$

is irreducible. The polygon is of type I, case 3a.)

CHAPTER V

BIBLIOGRAPHY

1. Chronological Bibliography

1845 Schönemann, "Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist." Journal für Mathematik. XXXI (1845), 269-325.

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

1850 Eisenstein, "Uber die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhangt." Journal für Mathematik. XXXIX (1850), 166.

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

1880 Kronecker, "Uber die Irreductibilität von Gleichungen" Monätsberichte, Akademie der wissenschaften Berlin. (1880), 155-162.

1887 Runge, "Uber die Zerlegung ganzer ganzzahliger Funktionen in irreductible Factoren." Journal für Mathematik XCIX (1887), 89-97.

1891 Mayer, "Sur les équations algébriques." Nouvelles Annales de Mathématiques. ser.3.X (1891),111-124.

1894 Mandl, "Uber die Zerlegung ganzer, ganzzahliger Funktionen in irreductible Factoren." Journal für Mathematik CXIII (1894), 252-261.

Königsberger, "Uber die Eisenstein'schen Satz von Irreductibilität algebraischer Gleichungen." Sitzungsberichte, Akademie der wissenschaften Berlin (1894) Pt.I,1135-1139.

1895 Königsberger, "Uber den Eisenstein'schen Satz von Irreductibilität algebraischer Gleichungen." Journal fur Mathematik. CXV (1895), 53-78.

1897 Netto, "Uber 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.

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

1900 Königsberger, "Uber die Entwickelungsform algebraischer Functionen und Irreductibilität algebraischer Gleichungen." Journal fur Mathematik. CXXI (1900), 320-359.

1905 Bauer, "Verallgemeinerung eines Sätzes von Schönemann." Journal für Mathematik. CXXVIII (1905), 87-89.

Bauer, "Beitrag zur Theorie der irreduziblen Gleichungen." Journal für Mathematik. CXXVIII (1905), 298-301.

Perron, "Uber eine Anwendung der Idealthoerie auf die Frage nach der Irreduzibilität algebraischer Gleichungen." Mathematische Annalen. LX (1905), 448-458.

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

1907 Perron, "Neue Kriterien für die Irreduzibilität algebraischer Gleichungen." Journal für Mathematik. CXXXII (1907), 288-307.

1908 Schur, "Problem 226" Archiv der Mathematik und Physik. ser.3. XIII (1908), 368.

1909 Westlund, "Ontheirreducibility of certain polynomials." American Mathematical Monthly. XVI (1909),66-67

Flügel, "Solution of a problem by Schur." Archiv der Mathematik und Physik. ser.3XV (1909), 271.

Schur, "Problem 275." Archiv der Mathematik und Physik. ser.3.XV (1909), 259.

1918 Stäckel, "Arithmetische Eigenschaften ganzer Funktionen." Journal für Mathematik. CXLVIII (1918), 101-112.

1919 Polyà, "Verscheidene Bermerkungen zur Zahlentheorie." Jahresberichte der Deutsche Mathematiker Vereinigung. XXVIII (1919), 31-40.

1921 Tajima, "On the roots of an algebraic equation." Tohôku Mathematical Journal. XIX (1921), 173-174.

1922 Fürtwangler, "Uber Kriterien für irreduzible und für primitive Gleichungen und uber die Aufstellung affektfreier Gleichungen." Mathematische Annalen. LXXXV (1922), 34-40.

Ore, "Uber die Redktibilität in algebraischen Zahlkorpern." Norsk Matematisk Forenings Skrifter. (1922) ser.1.#9.

1923 Dines," A theorem on the factorization of polynomials of certain types," American Mathematical Society Bulletin. XXIX (1923), 440.

Kürschak,"Irreducible Formen." Journal für Mathematik. CLII (1923), 180-191.

Ore, "Uber die Reduzibilität von algebraischer Gleichungen." Christiania Videnskapsselskapets Skrifter. (1923) Pt.I.#22.

Ore, "Zur Theorie der Irreduzibilitätskreiterien." Mathematische Zeitschrift. XVIII (1923), 278-288.

1926 Brauer, Brauer and Hopf, "Uber die Irreduzibilitäts einige Spezielle Klassen von Polynomen." Jahresberichte der Deutsche Mathematiker Vereinigung. XXXV (1926),99-112.

Ille, "Einige Bermerkung zu einem von G. Polyà herrührenden Irreduzibilitätskriterium," Jahresberichte der Deutsche Mathematiker Vereinigung. XXXV (1926), 204-208.

1929 Schur, "Einige Sätze uber Primzahlen mit Anwendung auf Irreduzibilitätsfragen." Sitzungsberichte, Akademie der wissenschaften Berlin. (1929) Pt.I. 125-136,370.

1931 Wegner, "Uber die Irreduzibilitäts einer Klasse von genzen rationalen Funktionen." Jahresberichte der Deutsche Mathematiker Vereinigung. XL (1931), 239-241.

1933 Dorwart and Ore, "Criteria for the irreducibility of polynomials." Annals of Mathematics. ser.2.XXXIV (1933), 81-94.

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

2. Supplementary Bibliography

1854 Heine, "Untersuchungen uber ganze Functionen." Journal für Mathematik. XLVIII (1854), 237-266.

1857 Dedekind, "Beweis fur die Irreductibilitäts der Kreistheilung-Gleichungen." Journal für Mathematik. LIV (1857), 27-30.

1882 Kronecker, "Grundzüge einer arithmetischen Theorie der algebraischen Grössen." Journal für Mathematik. XCII (1882), 10-12.

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

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

Capelli, see also Netto, "Vorlesungen uber Algebra." Leipzig, vol. II, 39, 395.

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, "Uber die Irreductibilität algebraischer Functionalgleichungen und linear Differentialgleichungen." Mathematische Annalen. LIII (1900), 49-80.

1905 Bauer, "Zür Theorie der irreduziblen Gleichungen." Mathematik und Natur wissenschaftliche berichte aus Ungarn. XX (1905), 30-33.

1906 Mandl, "Uber die Zerlegung von Functionen mehrerer variablen in irreduktible Faktoren." Journal für Mathematik. CXXXI (1906), 40-48.

1907 Dickson, "Criteria for the irreducibility of functions in a finite field." American Mathematical Society Bulletin. ser.2. XIII (1907), 1-8.

1908 Bauer, "Elementare Irreduzibilitätsuntersuchungen." Journal für Mathematik. CXXXIV (1908), 15-22.

Dickson, "Criteria for the irreducibility of a reciprocal 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

1916 Blumberg, "on the factorization of expressions of various types." American Mathematical Society Transactions. XVII (1916), 517-544.

Glenn, "Relating to the quadratic factors of a polynomial." American Mathematical Monthly. XXIII (1916), 313-315.

1917 Frumweller, "Quadratic factors of a polynomial." American Mathematical Monthly. XXIV (1917), 208-212.

1919 Mazzoni, "Sul problema dell' irreductibilitá di un equazione in un campo di razionalitá generale." Atti della Reale Accademia Nazionale dei Lincei. ser.5a. XXVIII (1919), 129.

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

Fujiwara, "Über Kriterien fur Irreduzibilität ganzzahliger algebraisches Gleichungen." Tohôku Mathematical Journal. XVII (1920), 10-17.

1921 Oishi, "Criteria for the irreducibility of a polynomial." Tohôku Mathematical Journal XX (1921), 37-40

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

Chlàdek, "Eine neue Methoden fur die Zerlegung reduktibler Polynome einer variabeln." Casopsis LI (1922), 97-101.

1922 Huttinger, "Nôte sur la décomposition en facteurs des équations algébriques." Association francaise pour l'avancement de science. XLVI (1922), 121-122.

Noether, "Ein algebraisches Kriterium fur absolute Irreduzibilität." Mathematische Annalen. LXXXV (1922), 26-33.

Rados, "Uber Krongruenzbedingungen der rationalen Lösbarkeit von algebraischen Gleichungen." Mathematische Annalen. LXXXVII (1922), 78-83.

1923 Darbi, "Sulla riduttibilitá dell' equazioni algebriche." Atti della Reale Accademia Nazionale dei Lincei. ser.5a. XXXII (1923), 76.

Huttinger, "Nôte sur la décomposition en facteurs des équations algébriques." Association française pour l'avancement de science. XLVII (1923), 98-99.

1924 Chládek, "Einige Satze über die Zerlegung von Polynomen einer Veränderlichen." Casopsis. LIII (1924), 247-251.

Ore, "Zür Theorie der Eisensteinschen Gleichungen." Mathematische Zeitschrift. XX (1924), 267-279.

Sopman, "Ein Kriterium fur Irreduzibilität ganzer Funktionen in einem beliebigen algebraischen Korper." Mathematische Annalen. XCI (1924), 60-61.

1925 Fischer, "Uber absolute Irreduzibilität." Mathematische Annalen. XCIV (1925), 163-165.

1926 Dörge, "Zum Hilbertschen Irreduzibilitätssätz." Mathematische Annalen. XCV (1926), 84-97.

Dörge, "Uber die reduziblen Polynome und der Normal Gleichungen." Mathematische Annalen. XCV (1926) 247-249.

Ostrowski, "Uber eine Erweiterung der Irreduzibilität begriffs und ihre Anwendung auf ein funktionen theoretisches Problem." Jahresberichte der Deutsche Mathematiker Vereinigung. XXXV (1926), 91-96.

1927 Dörge, "Einfacher Beweis der Hilbertschen Irreduzibilitätssätz." Mathematische Annalen. XCVI (1927), 176-182.

1929 Dörge, "Bemerkung zum Hilbertschen Irreduzibilitätssätz." Mathematische Annalen. CII (1930), 521-530.

Dörge, "Uber die Reduzibilitäts von Polynomen im Korper der reelen Zahlen." Mathematische Annalen. CII (1930), 726-737.

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) 485-501.

von der Waerden, "Eine Bermerkung uber die Unzerlegbarkeit von Polynomen." Mathematische Annalen. CII (1930) 738-739

Netto, "Vorlesungen uber Algebra" Leipzig. 1896. Vol. I, 56.

Polya und Szego, "Aufgaben und Lehrsätze aus der Analysis." Berlin. 1925. Vol. II, 137, 347-350.

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

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

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

$$P = (n-i, a_i)$$

where a_i 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 <u>closed</u> 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

$$f(x)=\sum_{i=0}^{n}\sum_{j=0}^{\alpha_i} r_{ij}\,x^{i}p^{j}$$

where the coefficients r_{ij} are all less than p. Then the plotting of the points (i,j) will again define a <u>closed</u> 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_{fg} do not necessarily exactly coincide with those of the product of the polygons P_f+P_g. 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.

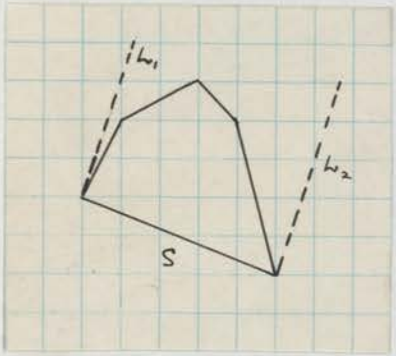
It can however be shown for this upper polygon that if a polynomial is considered as the product of factors, f(x) and g(x), the product of the polygons of the factors $P_f + P_g$ lies on or within certain limits about the polygon of the product P_{fg}. That is, we plot the points defined by a given polynomial and construct its polygon P_{fg}. 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 $P_f + P_g$ 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 $P_f + P_g$ on the ordinate $x = n-i$ may not lie more than $\log(3.2^{i(n-i)})$ above and not more than $\log(\frac{n}{2}+1)$ below the polygon P_{fg} when this is defined by the points $\log|A_i|$. 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 <u>sharpness</u> 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 $P_f + P_g$ and the corresponding point of P_{fg} cannot differ greatly. For a corner point whose sharpness is less than four the previously stated limit is found.

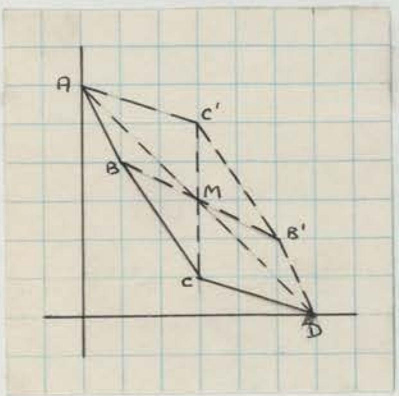
Applying these polygons to the deduction of irreducibility criteria, we find certain types of polygons which are irreducible. The irreducibility criteria thus derived are algebraic in form similar to those given by Perron in 1907 but more general.

First, suppose that P is a polygon with one



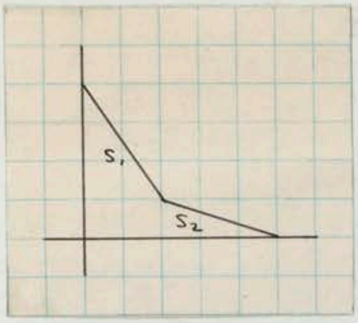
irreducible side S. If it is possible to find a pair of parallels L_1, L_2 through the end-points of S such that P lies entirely within these parallels, then P is irreducible.

Second, consider the convex polygon of a polynomial. Draw the line connecting the end-points



of the Dumas polygon (AD). 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 (B',C'). 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.