sequences remove the first $r-1$ of the e_1's occurring in the left-hand end position and place this truncated sequence on the same horizontal line with the other and to its right. The resulting sequence of the e's obviously contains each of the n^r permutations exactly twice.

The case of an arbitrary k is then readily disposed of by successive applications of this process.

TRINITY COLLEGE

CRITERIA FOR THE IRREDUCIBILITY OF POLYNOMIALS*

BY LOUIS WEISNER

1. *Introduction.* If a polynomial with integral coefficients is reducible in the field of rational numbers, the task of decomposing it into the product of irreducible polynomials may be expected to involve a great deal of numerical work, commensurate with the degree and coefficients of the polynomial, such as is required by Kronecker's method. But when it is merely required to know whether or not the polynomial is reducible, the amount of labor required by Kronecker's method is altogether too great. As a polynomial is completely determined by a sufficiently extended table of values, these values should suffice to determine the reducibility or irreducibility of the polynomial. We can hardly expect to establish the *reducibility* of a polynomial of degree n, with fewer than $n+1$ entries in its table of values. For this reason criteria establishing the reducibility of a polynomial are unknown. No such criteria are established in the present paper. On the other hand, *one* entry in the table of values of a polynomial may be sufficient to establish its *irreducibility*. The present paper is concerned with criteria of this sort.

One such criterion is available:† if for a sufficiently large integer h, $f(h)$ is a prime, where $f(x)$ is a polynomial with inte-

---

* Presented to the Society, March 30, 1934.

† See P. Stäckel, Journal für Mathematik, vol. 148 (1918), p. 109; Pólya and Szegö, *Aufgaben und Lehrsätze*, vol. 2, p. 137, Ex. 127.

gral coefficients, then $f(x)$ is irreducible.* The applicability of this theorem is clearly limited, for it is well known that an irreducible polynomial may represent no prime. Moreover, the first prime represented by a polynomial may be large, and considerable fruitless calculations may be expended in discovering it.

The criteria described in §3 have a wider range of applicability. The sense of these criteria is that, subject to certain conditions, a polynomial is irreducible if it represents the integer $\pm kp^m$, (p prime), where k is relatively small. These criteria are well adapted to establishing the irreducibility of numerical polynomials and lead to the construction of large classes of irreducible polynomials.

2. *Irreducibility Determined by Leading and Final Coefficients.*

THEOREM 1. *Let L and M be lower and upper bounds, respectively, of the absolute values of the roots of a reducible polynomial*

$$A(x) = \sum_{v=0}^{n} a_v x^{n-v}, \qquad (n \geqq 2,\ a_0 \neq 0),$$

with integral coefficients, and suppose that

$$|a_n| = kp^m, \qquad (k \geqq 1,\ m \geqq 1),$$

where p is a prime which does not divide a_{n-1} if $m > 1$.

A. *If $L \geqq 1$, then $k \geqq L$.* B. *If $M \geqq 1$, then $p^m \leqq |a_0| M^{n-1}$.*

As $A(x)$ is reducible,

$$A(x) = B(x)C(x) = \sum_{v=0}^{r} b_v x^{r-v} \sum_{v=0}^{s} c_v x^{s-v},$$
$$(1 \leqq r \leqq n-1;\ 1 \leqq s \leqq n-1),$$

the b's and c's being integers. We have

$$a_{n-1} = b_{r-1}c_s + b_r c_{s-1},$$
$$kp^m = |a_n| = |b_r|\,|c_s|.$$

* Except where the contrary is explicitly stated, the terms *reducible* and *irreducible* will be understood to apply to the field of rational numbers throughout this paper.

As a_{n-1} is not divisible by p if $m>1$, one of the integers b_r, c_s is not divisible by p. If b_r is not divisible by p, c_s is divisible by p^m. If $m=1$, at least one of the integers b_r, c_s is divisible by p, and we shall suppose that c_s has this property. In both cases c_s is divisible by p^m. Hence

$$|c_s| \geqq p^m, \qquad |b_r| \leqq k.$$

Denoting the roots of $B(x)$ by $\beta_1, \cdots, \beta_r$, we have

$$|\beta_1| \cdots |\beta_r| = \left|\frac{b_r}{b_0}\right| \leqq |b_r| \leqq k.$$

Hence, as the roots of $B(x)$ are roots of $A(x)$,

$$k \geqq L^r,$$

from which the first part of the theorem follows.

Denoting the roots of $C(x)$ by $\gamma_1, \cdots, \gamma_s$, we have

$$|\gamma_1| \cdots |\gamma_s| = \left|\frac{c_s}{c_0}\right| \geqq \frac{p^m}{|c_0|} \geqq \frac{p^m}{|a_0|}$$

as c_0 is a divisor of a_0. Hence

$$p^m \leqq |a_0| M^s,$$

from which the second part of the theorem follows.

The rational roots, and hence the linear factors, of a polynomial with integral coefficients, are readily determined by elementary methods. If $A(x)$ is reducible, but has no linear factors, $2 \leqq r \leqq n-1$, $2 \leqq s \leqq n-2$. Hence we have the following theorem.

THEOREM 2. *With the notation and hypothesis of Theorem* 1, *if* $A(x)$ *is reducible but has no linear factor, then*

$$k \geqq L^2, \qquad p^m \leqq |a_0| M^{n-2}.$$

As an illustration, consider the polynomial

$$x^n + x \pm p^m, \qquad (p^m > 2).$$

Its roots are easily shown to be outside the unit circle. It follows from Theorem 1A, with $k=1$, that the polynomial is irreducible if p^m is any prime-power integer >2.

3. *Irreducibility Determined by Integers Represented by a Polynomial.*

THEOREM 3. *Let M be an upper bound of the absolute values of the roots of a polynomial $A(x)$ of degree n with integral coefficients and leading coefficient $a_0 \neq 0$; and let h be an integer such that*

$$|h| \geqq M + 1, \qquad |A(h)| = kp^m,$$

where p is a prime which does not divide $A'(h)$ if $m > 1$. If $A(x)$ is reducible,

$$k \geqq |h| - M, \qquad p^m \leqq |a_0| (|h| + M)^{n-1}.$$

If $A(x)$ is reducible but has no linear factor,

$$k \geqq (|h| - M)^2, \qquad p^m \leqq |a_0| (|h| + M)^{n-2}.$$

Evidently, $A(x)$ and $A(x+h) = a_0x^n + \cdots + A'(h)x + A(h)$ are simultaneously reducible or irreducible. If ρ is a root of $A(x+h)$, $\rho+h$ is a root of $A(x)$, so that $|\rho+h| \leqq M$. Hence

$$|\rho| = |h - (\rho + h)| \geqq |h| - |\rho + h| \geqq |h| - M,$$

$$|\rho| \leqq |h| + M.$$

As $|h| - M$ and $|h| + M$ are lower and upper bounds, respectively, of the absolute values of the roots of $A(x+h)$, the theorem follows from those of §2.

As an illustration, consider the polynomial

$$A(x) = x^6 - 2x^4 + x^3 + x^2 - x - 3,$$

which represents only multiples of 3, so that Stäckel's criterion (§1) is inapplicable. Here we may take $M = 2$. We find that

$$A(-5) = 3 \cdot 4759,$$

and 4759 is a prime. As the polynomial has no linear factor, and the inequality

$$k \geqq (|h| - M)^2$$

is violated, the polynomial is irreducible.

If M is large, the application of Theorem 2 involves computations with large figures. The next theorem may then be found more practicable. Let

$$A(x, y) = \sum_{v=0}^{n} a_v x^{n-v} y^v$$

be the homogeneous polynomial corresponding to

$$A(x) = \sum_{v=0}^{n} a_v x^{n-v}.$$

The homogeneous polynomial corresponding to $A'(x)$ is denoted by $A'(x, y)$.

THEOREM 4. *Let L be a lower bound of the absolute values of a polynomial $A(x)$ with integral coefficients; and let t and u be integers such that*

$$|u|L - |t| \geqq 1, \qquad |A(t, u)| = kp^m,$$

where p is a prime which does not divide $A'(t, u)$ if $m > 1$. If $A(x)$ is reducible,

$$k \geqq |u|L - |t|.$$

If $A(x)$ is reducible but has no linear factor,

$$k \geqq (|u|L - |t|)^2.$$

It follows, as in the proof of Theorem 3, that $|u|L - |t|$ is a lower bound of the absolute values of the roots of the polynomial

$$A(x + t, u) = a_0 x^n + \cdots + A'(t, u)x + A(t, u),$$

which is reducible if $A(x)$ is. The theorem follows by those of §2.

4. *Certain Classes of Irreducible Polynomials.*

THEOREM 5. *If $f(x)$ is a polynomial with integral coefficients, which has a rational root h, and k is a fixed positive integer, the polynomial $f(x) \pm kp$ is irreducible for all sufficiently large primes p. If, in addition, $f'(h) \neq 0$, the polynomial $f(x) \pm kp^m$ is irreducible for all sufficiently large prime-power integers p^m.*

Let $h = t/u$, where t and u are integers and $u \geqq 1$, and let n be the degree of $f(x)$. If

$$g(x) = u^n f\left(x + \frac{t}{u}\right),$$

then

$$u^n f\left(x + \frac{t}{u}\right) \pm ku^n p^m = g(x) \pm ku^n p^m,$$

and $g(0) = 0$. It is therefore sufficient to prove the theorem for $h = 0$.

If the polynomial

$$A(x) = f(x) \pm kp^m = a_0 x^n + \cdots + a_{n-1}x \pm kp^m, \quad (a_{n-1} \neq 0),$$

has a root whose absolute value is $\leqq k$, then

$$kp^m \leqq |a_0| k^n + \cdots + |a_{n-1}| k.$$

Hence, if p^m is a prime-power integer greater than

$$|a_0| k^{n-1} + \cdots + |a_{n-1}|,$$

all the roots of $A(x)$ are $> k$ in absolute value. It follows from Theorem 1A that $A(x)$ is irreducible unless $m > 1$ and p is a divisor of a_{n-1}.

To treat this case, let p be a prime factor of a_{n-1}, p^μ the highest power of p that divides a_{n-1}, and suppose that $A(x)$ is reducible. With the notation of the proof of Theorem 1, we have

$$b_{r-1}c_s + b_r c_{s-1} = a_{n-1},$$

$$b_r c_s = \pm kp^m.$$

At least one of the integers b_r, c_s is not divisible by $p^{\mu+1}$. If b_r has this property,

$$|b_r| = k_1 p^\nu, \qquad (0 \leqq \nu \leqq \mu),$$

where k_1 is a divisor of k. Hence

$$|b_r| \leqq k |a_{n-1}|.$$

At least one root β of $B(x)$ therefore satisfies the inequality

$$|\beta| \leqq \left(\left|\frac{b_r}{b_0}\right|\right)^{1/r} \leqq (|ka_{n-1}|)^{1/r} \leqq |ka_{n-1}|.$$

On the other hand, by choosing m sufficiently large, the absolute value of every root of $A(x)$ may be made arbitrarily large. Hence $A(x)$ is irreducible for sufficiently large values of m.

That the condition $f'(h) \neq 0$ if $m > 1$ is necessary is shown by the example $x^n - p^m$, which is reducible if p is any prime and m any multiple of n, $(n > 1)$.

THEOREM 6. *Let*

$$A(x) = \sum_{v=0}^{n} a_v x^{n-v}$$

be a polynomial with integral coefficients. If a_n is a power of a prime which does not divide a_{n-1}, and if

$$0 < a_0 < a_1 \cdots < a_{n-1} < a_n,$$

then $A(x)$ is irreducible.

The stated inequalities imply that the absolute value of every root of $A(x)$ is >1.* The theorem follows from Theorem 1, with $k = 1$.

5. *Validity of Preceding Theorems in Other Fields.* There are fields besides the field of rational numbers for which the preceding theorems are valid. Let R be an algebraic field of class number 1. The first five theorems are valid if we understand reducibility to pertain to R and *integer* to mean integer of R. Theorem 6 is valid, with a similar understanding, if the coefficients of $A(x)$ are real numbers.

HUNTER COLLEGE

* See G. Eneström, *Härledning af en allmän formel . . .*, Öfversigt af Kongl. Vetenskaps-Akademiens Förhandlingar, vol. 50 (1893), p. 405–415. French translation in Tôhoku Mathematical Journal, vol. 18 (1920), p. 34. An elegant proof of Eneström's theorem is given by A. Hurwitz, Tôhoku Mathematical Journal, vol. 4 (1914), p. 89.