ON SOME ALGEBRAIC PROPERTIES OF THE BESSEL POLYNOMIALS

BY

EMIL GROSSWALD

1. **Introduction.** For integral n, the differential equation

$$x^2y'' + 2(x+1)y' - n(n+1)\,y = 0$$

is satisfied by the polynomials of degree n

$$y_n(x) = \sum_{\nu=0}^{n} (n+\nu)!(x/2)^\nu/\{(n-\nu)!\nu!\} \tag{1}$$
$$= 1 + n(n+1)x/2 + \cdots + (2n)!x^n/n!2^n.$$

These polynomials are orthogonal on the unit circle, with weight function $w(x) = e^{-2/x}$, so that, for $m \neq n$, $\int_{|x|=1} y_m(x)\cdot y_n(x)\cdot e^{-2/x}dx = 0$. They satisfy also the recurrence relations (see [10])[1]:

$$y_{n+1} = (2n+1)xy_n + y_{n-1}, \tag{2}$$
$$x^2y_n' = (nx-1)y_n + y_{n-1}, \tag{3}$$
$$x^2y_{n-1}' = y_n - (nx+1)y_{n-1}. \tag{4}$$

These polynomials seem to have been considered first by S. Bochner[2] [1]. H. L. Krall and O. Frink [10] generalized them, so as to include also the polynomial solutions of the differential equation

$$x^2y'' + (ax+b)y' - n(n+a-1)y = 0,$$

which reduces to the first, for $a=b=2$. H. L. Krall and O. Frink called them "Bessel polynomials"[3] on account of their connection with the Bessel functions. They studied in detail properties of the BP and the generalized BP, such as recurrence relations, orthogonality, equivalent of Rodrigues' formula, generating function, and so on. In the present paper, we intend to establish some asymptotic formulas and to study algebraic properties of the BP. The main results are:

(1) Let $Y_n(x) = (2n)!x^ne^{1/x}/n!2^n$, $U_n(x) = \exp\,(n^2x/2)$. Then, for fixed x

Presented to the Society, December 29, 1949; received by the editors December 22, 1949 and, in revised form, December 1, 1950.

[1] Numbers in brackets refer to the references at the end of the paper.

[2] They were also mentioned by W. Hahn [5] and H. L. Krall [11]. Remark also that, if D stands for the symbol of derivation, $x^ny_n(2/x) = (1-D)^{-n-1}x^n = (-1)^{n-1}A_n(x)$. The polynomials $A_n(x)$ defined by this relation have been used in the proofs of the transcendency of e and π (see [17]).

[3] In this paper the abbreviation BP stands for Bessel polynomials.

with $|x| \geqq 1$, $\lim_{n\to\infty} y_n(x) = Y_n(x)$ and for fixed $n > 3$, $\lim_{x\to 0} y_n(x) = U_n(x)$.

(2) All zeros of BP are simple and inside the unit circle (except $x_1 = -1$, the zero of $y_1(x)$, which is *on* the unit circle). The BP of even degree have no real zeros, those of odd degree have exactly one real zero. Let x_n be the real zero of $y_n(x)$ (n odd); then

$$-1 = x_1 < x_3 < \cdots < x_{n-2} < x_n < \cdots < 0.$$

(3) The BP are algebraically irreducible in the field of rational numbers, at least up to the degree $n \leqq 400$, and also for $n > 400$, whenever n is of one of a set of specified forms. If not irreducible, they contain always an irreducible factor of degree greater than or equal to $A_n \cdot n$, where $A_n > 16/17$ and approaches one, when n increases.

(4) The Galois group of the irreducible BP is the symmetric group on n symbols (except, perhaps, for $n = 9$, 11, and 12).

2. **Asymptotic formulas.** By (1), $y_n(x) = \{(2n)!x^n/n!2^n\} \sum_{\nu=0}^{n} a_\nu x^{-\nu}$ with $a_0 = 1$, $a_\nu = (1/\nu!) \prod_{i=1}^{\nu} (2n-2i+2)/(2n-i+1)$, $\nu = 1, 2, \cdots, n$. Keeping ν fixed, let $n \to \infty$; then $\lim_{n\to\infty} a_\nu = 1/\nu!$ and

$$y_n(x) \sim k_n x^n \sum_{\nu=0}^{\infty} x^{-\nu}/\nu! = k_n x^n e^{1/x} \qquad \text{where } k_n = (2n)!/n!2^n.$$

Let[4] $Y_n(x) = k_n x^n e^{1/x}$ and evaluate the "error term" $R_n(x) = y_n(x) - Y_n(x)$ for fixed n and x. We have

$$R_n(x) = k_n x^n \left\{ \sum_{\nu=1}^{n} \frac{1}{\nu! x^\nu} \left(\frac{2^\nu n!(2n-\nu)!}{(n-\nu)!(2n)!} - 1 \right) - \sum_{\nu=n+1}^{\infty} \frac{1}{\nu! x^\nu} \right\},$$

so that

$$(5) \qquad |R_n(x)| \leqq k_n X^n \left\{ \sum_{\nu=2}^{n} A(n, \nu) X^{-\nu} + \sum_{\nu=n+1}^{\infty} X^{-\nu}/\nu! \right\},$$

where $X = |x|$ and $A(n, \nu) = (1 - \prod_{i=1}^{\nu-1} (2n-2i)/(2n-i))/\nu!$. We have

$$(6) \qquad A(n, \nu) \leqq 1/2(\nu-2)!(2n-1) \qquad \text{for } \nu \geqq 2.$$

The relation holds for $\nu = 2$ and is proven, in general, by induction on ν, with the help of the inequality:

$$\frac{1}{2(\nu-2)!(\nu+1)(2n-1)} + \frac{\nu}{(\nu+1)!(2n-\nu)} \prod_{i=1}^{\nu-1} \left(\frac{2n-2i}{2n-i} \right) \leqq \frac{1}{(\nu-1)!2(2n-1)},$$

[4] It is precisely the property of BP to approximate an exponential, which permits their use in the proof of the transendency of e. (See footnote 2.)

which is valid for $\nu \geqq 2$, because the product is smaller than one. From (5) and (6) it follows that

$$\begin{aligned} | R_n(x) | &\leqq k_n X^n \left(\left\{ \sum_{\nu=2}^{n} X^{-\nu}/(\nu-2)! \right\} \Big/ 2(2n-1) + \sum_{\nu=n+1}^{\infty} X^{-\nu}/\nu! \right) \\ &\leqq k_n \{ X^{n-2} e^{1/x}/2(2n-1) + (n+2)/(n+1)!((n+2)X-1) \}. \end{aligned}$$

For $X \geqq 2/(n-2)$ and $n \geqq 6$ it follows further that $| R_n(x) | \leqq k_n X^{n-2} e^{1/x}/4(n-1)$ so that $| y_n/Y_n - 1 | \leqq e^{1/X}/\{4(n-1)X^2 | e^{1/x} | \}$ and the right-hand side tends to zero when x is kept fixed and $n \to \infty$. In particular, if x is real, $| y_n/Y_n - 1 | \leqq e^{2x}/4(n-1)x^2$.

For small values of X, the above formulas are not satisfactory, because the error term becomes important. In this case let $U_n(x) = e^{n^2 x/2}$, and consider, for fixed x and n, the difference $R_n'(x) = y_n(x) - U_n(x)$. We have $| R_n'(x) | \leqq \sum_{\nu=1}^{n} \{ n^{2\nu-1} | a_\nu | X^\nu / 2^\nu (\nu-1)! \} + \sum_{\nu=n+1}^{\infty} (n^2 X/2)^\nu/\nu!$, with

$$a_\nu = \frac{(n+\nu)!}{(n-\nu)! n^{2\nu-1} \cdot \nu} - \frac{n}{\nu} \cdot \tag{7}$$

For all ν, $| a_\nu | < (n/2)^{1/2}$. Indeed, $a_\nu \leqq (n+\nu)/\nu - n/\nu = 1$ follows directly from (7); for $2 \leqq \nu \leqq (2n)^{1/2}$, $a_\nu > -1$, which holds for $\nu = 2$ and follows then by induction on ν. The induction is valid, provided $(n-\nu+1)^2/n^2 > (n-\nu)/(n+\nu)$, and, a fortiori, for $\nu \leqq (2n)^{1/2}$. Finally, from (7), for $\nu > (2n)^{1/2}$, $a_\nu > -n/\nu > -(n/2)^{1/2}$ and $| a_\nu | < (n/2)^{1/2}$. Using this upper bound for $| a_\nu |$ we obtain

$$\begin{aligned} | R_n'(x) | &\leqq \left(\frac{n}{2} \right)^{1/2} \cdot \frac{nX}{2} \sum_{\nu=1}^{n} \frac{(n^2 X/2)^{\nu-1}}{(\nu-1)!} \\ &\quad + \left(\frac{n^2 X}{2} \right)^{n+1} \frac{1}{(n+1)!} \left\{ 1 + \frac{n^2 X}{2(n+2)} + \cdots \right\} \\ &\leqq (n/2)^{3/2} X \exp (n^2 X/2) + \frac{(n^2 X/2)^{n+1}}{(n+1)!} \cdot \frac{2(n+2)}{2(n+2) - n^2 X} \cdot \end{aligned}$$

For $X \leqq 1/n$ and $n > 3$, the second term is smaller than $(2^{1/2}-1)(n/2)^{3/2} X \cdot \exp (n^2 X/2)$, so that $| R_n'(x) | \leqq 2^{-1} n^{3/2} X \exp (n^2 X/2)$, and, consequently, $| y_n/U_n - 1 | \leqq n^{3/2} X/2$, and the right-hand side tends to zero with x, if n is kept constant.

3. Some properties of the zeros of BP.

THEOREM 1. *The zeros of BP are all simple.*

Proof. Assume that x_0 is a multiple zero of $y_n(x)$. Then $y_n(x_0) = y_n'(x_0) = 0$ and, by (3), $y_{n-1}(x_0) = 0$. Using (4) it follows that also $y_{n-1}'(x_0) = 0$, so that, if x_0 is a multiple zero of $y_n(x_0)$, it is also a multiple zero of $y_{n-1}(x_0)$. The argument holds for all n, down to $y_1(x_0)$, which has no multiple zero; consequently,

$y_n(x)$ cannot have any either.

THEOREM 2. *All zeros of BP are inside the unit circle, except for $y_1(x)=x+1$, whose zero lies on the unit circle.*

Proof. From a theorem of Kakeya (see [9]) it follows that if $a_0 \geqq a_1 \geqq \cdots \geqq a_n \geqq 0$, then all zeros of the polynomial $a_n+a_{n-1}x+\cdots+a_0x^n$ are inside, or on the unit circle. For BP, by (1), $a_n=1$, $a_{n-k}=a_{n-k+1}\cdot(n+k)(n-k+1)/2k$, $k=1, 2, \cdots, n$. As $(n+k)(n-k+1)/2k \geqq 1$, with equality only for $k=n$, the conditions of Kakeya's theorem are satisfied and the zeros of BP are inside, or on the unit circle. By Hurwitz's refinement (see [7]) of Kakeya's theorem, the necessary and sufficient condition that a zero be on the unit circle is that the coefficients a_ν $(\nu=1, 2, \cdots, n)$ fall into equal groups of consecutive, equal coefficients, that is,

$$a_0 = a_1 = \cdots = a_{m-1} > a_m = a_{m+1} = \cdots$$
$$= a_{2m-1} > \cdots > a_{n-m+1} = a_{n-m+2} = \cdots = a_n.$$

As seen, $a_{n-k} \neq a_{n-k+1}$, except for $k=n$; therefore, Hurwitz's condition is satisfied only for $n=1$, when $a_0=a_1=1$, which finishes the proof.

THEOREM 3. *For*[5] *even n, $y_n(x)$ has no real zeros.*

For its proof, we need the following lemmas.

LEMMA 1. *Let $L_n=\sum_{i=0}^{n-1}(4i+1)y_{2i}$; then*

$$y_{2n} = (4n-1)x^2L_n + (4n-1)x + y_{2n-2}. \tag{8}$$

Proof. Since $y_1=x+1$, a simple induction from (2) shows that $y_{2n-1}=1+xL_n$ and, by (2) again,

$$y_{2n} = (4n-1)x(1+xL_n) + y_{2n-2},$$

proving (8).

LEMMA 2. *If for some ν and some $x_0<0$ we have $y_{2\nu-2}(x_0)>0$ and $y_{2\nu-1}(x_0) \leqq 0$, then $y_{2n}(x_0)>0$, $y_{2n+1}(x_0)<0$ hold for all $n \geqq \nu$.*

Proof. The lemma follows immediately from (2), on account of the asumption.

LEMMA 3. *Any real zero of $y_{2n}(x)$ satisfies $x_0>-1/4$.*

Proof. By direct computation we find that the only real zero of $y_7(x)$ is $x_7=-0.219\cdots$ and that all zeros of $y_{2n}(x)$ $(n=1, 2, 3)$ are complex. Therefore, if $x<x_7$, we have $y_6(x)>0$, $y_7(x)<0$, and the same inequalities hold, by Lemma 2, for all $y_{2n}(x)$ and $y_{2n+1}(x)$ with $n>3$. Consequently, if $y_{2n}(x_0)=0$,

[5] The author wishes to acknowledge his indebtedness to the referee, whose suggestions permitted a considerable shortening and streamlining of this and some other proofs.

then $x_0 > x_7 = -0.219 \cdots$, proving the lemma.

LEMMA 4. *If* $-1/4 < x < 0$, *then*

$$y_{2\nu}(x) \geqq (1+x)^{2\nu}/(2\nu)!. \tag{9}$$

Proof. (9) holds for $\nu = 0$, as $y_0 = 1$, and for $\nu = 1$, when it becomes

$$3x^2 - 3x + 1 \geqq (1+x)^2/2!, \tag{10}$$

which is equivalent to $5x^2 - 8x + 1 \geqq 0$, which is true for $x < 0$. Now we use induction on ν, assuming that (9) holds for $0 \leqq \nu \leqq m-1$. Write $u = x+1$. Then, by (8) and the induction assumption (9), we have

$$y_{2m} \geqq (4m-1)x^2 f_m(u) + (4m-1)x + u^{2m-2}/(2m-2)!,$$

where $f_m(u)$ is obtained by replacing y_{2i} in L_m by $u^{2i}/(2i)!$, according to (9), so that $f_m(u) = \sum_{j=0}^{m-1} (4j+1)u^{2j}/(2j)!$. In order to prove (9) for $\nu = m$, we therefore have to show that

$$(4m-1)x^2 f_m(u) + (4m-1)x + u^{2m-2}/(2m-2)! \geqq u^{2m}/(2m)!. \tag{11}$$

This we prove by induction on m. For $m = 1$, (11) reduces to (10). Assume now that (11) holds for $m-1$. Multiply this inequality by $(4m-1)/(4m-5)$, and subtract the result from (11) itself. This yields

$$\begin{aligned} &\{(4m-1)(4m-3)x^2 + 1\}u^{2m-2}/(2m-2)! \\ &\qquad + [(4m-1)/(4m-5)]u^{2m-4}/(2m-4)! \\ &\qquad \geqq u^{2m}/(2m)! - [(4m-1)/(4m-5)]u^{2m-2}/(2m-2)!. \end{aligned} \tag{12}$$

In order to prove (12), write $u-1$ for x in the first bracket, pass all terms to the left, and obtain, after obvious simplifications,

$$\begin{aligned} &u^4(4 - 1/m(m-1/2)(4m-1)(4m-3)) \\ &\qquad + u^2((1-2u)/m(m-1/2) + 2/(4m-1)(4m-3)m(m-1/2) \\ &\qquad + 4/(4m-1)(4m-3)(4m-5)m(m-1/2)) \\ &\qquad - 8(m-1)(2m-3)/(4m-3)(4m-5) \geqq 0. \end{aligned} \tag{13}$$

Now (13) will be satisfied, if $u > u_m$, where u_m is the largest root of the corresponding equation. For $m \to \infty$, (13) becomes $4u^4 - 1 \geqq 0$, which is satisfied for $u \geqq 1/2^{1/2}$. For finite[6] $m \geqq 2$, $u_m < 1/2^{1/2}$. As $u = x+1$ and, by assumption, $x > -1/4$, it follows that $u > 3/4 > 1/2^{1/2} > u_m$, so that (13) holds. This proves (12) and finishes the induction proof of (11); consequently, (9) holds for $\nu = m$, proving the lemma.

Proof of Theorem 3. All coefficients of y_{2n} are positive; therefore, any real zero of y_{2n} has to be negative; by Lemma 3, however, y_{2n} can have no real

[6] For $m = 2$, $u_m = .85 \cdots /2^{1/2}$; for $m > 2$, u_m approaches rapidly $1/2^{1/2}$.

zero in the interval $(-\infty, -1/4)$, and by Lemma 4, it can have no real zero in $(-1/4, 0)$, proving the theorem.

THEOREM 4. *For odd n, $y_n(x)$ has a single real, negative zero.*

Proof. Assume, contrary to the theorem, that, for $x_1 < x_2$,

$$y_n(x_1) = y_n(x_2) = 0. \tag{14}$$

Then there exists one, or an odd number of values x_3, such that $y_n'(x_3) = 0$, $x_1 < x_3 < x_2$, so that in any case

$$y_n'(x_1) \cdot y_n'(x_2) < 0. \tag{15}$$

Substituting successively x_1 and x_2 in (3) and multiplying the results, we obtain, by (14) and (15), $y_{n-1}(x_1) \cdot y_{n-1}(x_2) < 0$, showing that $y_{n-1}(x) = 0$ has a real root. As $n-1$ is even, this contradicts Theorem 3; consequently, Theorem 4 holds.

THEOREM 5. *For odd n, let x_n be the real zero of $y_n(x)$. Then*

$$-1 = x_1 < x_3 < \cdots < x_{n-2} < x_n < \cdots < 0.$$

Proof. From (2) written for $n-1$ follows, for $x = x_{n-2}$, that $y_n(x_{n-2}) = (2n-1)x_{n-2}y_{n-1}(x_{n-2})$. As $x_{n-2} < 0$ and $y_{n-1}(x_{n-2}) > 0$ by Theorem 3, it follows that $y_n(x_{n-2}) < 0$. As $y_n(x_n) = 0$, and also, by (1), $y_n(0) = 1$, it follows, using Theorem 4, that $x_{n-2} < x_n < 0$; hence, as $x_1 = -1$, the theorem.

COROLLARY. *Let $n_1 < n_2 < n_3$ be three odd numbers. Then the real zero of y_{n_2} separates those of y_{n_1} and y_{n_3}.*

4. **On the irreducibility of BP.** It seems very likely that all BP are ir reducible in the field of rational numbers. In what follows, we show only that $y_n(x)$ is irreducible for $n \leqq 400$, and also for $n > 400$ provided that n is of one of the forms[7]: $n = p^m$, $q \cdot p - 1$, $q \cdot p$, $p^m - 1$, $q \cdot p^m$ (with some restrictions in the last three cases). Here p is an odd prime, m and q are positive integers, and $q < p^m$ (throughout this section, p, m, and q will keep their meaning). We show also that $y_n(x)$ contains always an i.f. (in this section i.f. stands for irreducible factor) of degree $A_n n$, where $16/17 < A_n \leqq 1$ and A_n approaches one when n increases. Our main tool will be the following theorem.

THEOREM OF DUMAS (*see* [4]). *Let $f(x) = \sum_{\nu=0}^{n} a_\nu p^{e_\nu} x^{n-\nu}$, $p \nmid a_\nu$, with a_ν, e_ν rational integers, p prime, and consider the corresponding Newton's polygon*[8]. *Let l_r be the horizontal, k_r the vertical projection of the rth side*

[7] It is easy to increase the number of such forms of n; but this seems not to be of great interest, as we cannot prove the irreducibility for any set of forms, which should exhaust all possibilities for n.

[8] The (unique) polygon, with vertices at points of coördinates $(n-\nu, e_\nu)$ convex downwards and with all points $(n-\nu, e_\nu)$ on or above its sides. See [4, p. 213] and [6, p. 44].

$\lambda_r=(l_r, k_r)$ *their greatest common divisor*, $l_r=\lambda_r s_r$, *and* m *the number of sides. Then all irreducible factors of* $f(x)$ *have a degree of the form* $\sum_{r=1}^{m}\mu_r s_r$, *where the integers* μ_r *satisfy* $0\leqq\mu_r\leqq\lambda_r$. *If, in particular,* $e_0=0$, $e_\nu\geqq\nu e_n/n$ *for* $\nu=1, 2, \cdots, n$, *then* $m=1$ *and all i.f. of* $f(x)$ *have degrees* $\mu_r n/\lambda$, *where* $\lambda=(n, e_n)$ *and* $1\leqq\mu_r\leqq\lambda$; *if* $(n, e_n)=1$, *then* $f(x)$ *is irreducible.*

Dumas' theorem contains as a particular case the following theorem.

THEOREM OF PERRON (*see* [14, *Theorem* 6]). *Let*

$$f(x) = x^n + \sum_{\nu=1}^{i} a_\nu x^{n-\nu} + \sum_{\mu=1}^{n-i-1} p^{[(e/(n-i))\mu]+1}a_i x^{n-i-\mu} + p^e a_n,\ p\nmid a_i,\ p\nmid a_n,$$

$(e, n-i)=1$. *Then* $f(x)$ *has at least one i.f. of degree greater than or equal to* $n-i$.

Whenever $y_n(x)$ is irreducible, so is $z_n(x)=x^n y_n(1/x)$, and to each i.f. of $y_n(x)$ corresponds an i.f. of the same degree of $z_n(x)$, and conversely. It is, therefore, sufficient to study the irreducibility of the polynomials $z_n(x)$. From (1) it follows that

$$z_n(x) = \sum_{\nu=0}^{n} a_\nu x^{n-\nu} = \sum_{\nu=0}^{n} \frac{(n+\nu)!}{(n-\nu)!\nu!2^\nu}\, x^{n-\nu}. \tag{16}$$

Let e_ν be the highest power to which the odd prime p divides a_ν, so that $a_\nu=p^{e_\nu}\alpha_\nu$, $p\nmid\alpha_\nu$. Let p_1 be the highest prime satisfying $n=p_1+k_1$ with $k_1\geqq 0$. Then, by (16), $e_\nu=0$ for $0\leqq\nu\leqq k_1$; $e_\nu=1$ for $k_1+1\leqq\nu\leqq n$, and it follows from Perron's theorem that $z_n(x)$ contains an i.f. of degree greater than or equal to $n-k_1$. Similarly, if p_2 is the smallest prime satisfying $n=p_2-k_2-1$, with $k_2\geqq 0$, it follows by the same argument that $z_n(x)$ contains an i.f. of degree greater than or equal to $n-k_2$. If we take, in particular, k_1, respectively k_2, equal to zero it follows that z_n is irreducible if $n=p$, or $n=p-1$. In general, if $k=\min(k_1, k_2)$, then z_n contains an i.f. of degree greater than or equal to $n-k$.

Let $\epsilon>0$; then (see [13]) there exists an $N(\epsilon)$ such that for $n\geqq N(\epsilon)$ there exists always a prime satisfying $x<p\leqq(1+\epsilon)x$. Hence it follows by a simple computation that, for a given n, there exists either a $k_1\leqq n/(2/\epsilon+1)$ or a $k_2\leqq n/(2/\epsilon+1)-1$, so that always $k\leqq n/(2/\epsilon+1)<n\epsilon/2$ and z_n contains an i.f. of degree greater than or equal to $n-k>n(1-\epsilon/2)$, where, for sufficiently large n, ϵ can be made arbitrarily small. The function $N(\epsilon)$ is not known in general, but we know that $N(1/8)=48$ (see [2]). Taking $\epsilon=1/8$, it follows then, for $n>50$, that $k\leqq n/17$ and z_n contains an i.f. of degree greater than or equal to $n-k\geqq 16n/17$. For $n<50$ we check directly that $k\leqq 2$ if $n\leqq 25$ and $k\leqq 3$ otherwise, with corresponding conclusions for the degrees of the i.f. of z_n. We condense these results into the following two lemmas:

LEMMA 1. *Let $k=\min(|n-p|, |n+1-p|)$, where p runs through all primes; then z_n contains an i.f. of degree greater than or equal to $n-k$ and, consequently, no factor of degree d, with $k<d<n-k$.*

LEMMA 2. *All*[9] *polynomials z_n contain an i.f. of degree greater than or equal to $A_n n$, where $A_n>16/17$ and approaches one when n increases; consequently, no i.f. of z_n can have a degree d with $n/17<d<16n/17$.*

Before we proceed to examine particular forms of n, we need some estimates of the highest power to which a prime p divides a factorial. Let $n!=b\cdot p^e$, $p\nmid b$. Then

$$e=(n-1)/(p-1) \text{ if } n=p^m, \qquad e\leqq (n-2)/(p-1) \text{ otherwise}[10]. \tag{17}$$

As[11] $e=[n/p]+[n/p^2]+\cdots$, it follows also that

$$e\geqq \sum_{i=1}^{r}\frac{n}{p^i}-r=\frac{n(p^r-1)}{p^r(p-1)}-r \qquad \text{for any } r\geqq 1. \tag{18}$$

(i) Let $n=p^m$. Then, by (16) and (17) we find: $e_0=0$, $e_\nu\geqq \nu/(p-1)$ for $1\leqq\nu\leqq n-1$, and $e_n=(n-1)/(p-1)$. As $e_\nu\geqq \nu e_n/n$ it follows that the Newton polygon reduces to a single segment and, as $(e_n, n)=1$ by Dumas' Theorem, that z_n is irreducible.

(ii) Let $n=q\cdot p-1$, q prime or composite. If $q<p$, it follows, as before, that $e_0=0$, $e_\nu=[(\nu-1)/p]+1$, for $1\leqq\nu\leqq n$; in particular, $e_n=q$. As $e_\nu\geqq\nu e_n/n$, the Newton polygon reduces to a single segment. As also $(e_n, n)=(q, qp-1)=1$, it follows, by Dumas' Theorem, that z_n is irreducible.

(iii) In case $n=q\cdot p$, p, q as before, the construction of the Newton polygon is the same as under (ii); but now $(e_n, n)=(q, qp)=q$ and z_n may have i.f.of degrees $k\cdot n/q=kp$, $1\leqq k\leqq q$. In case $n>50$ and $q\leqq 17$, no such factor different from z_n itself can exist, as it would have a degree $d\geqq n/q>n/17$, contrary to Lemma 2. In case $q>17$ and $p>k$, z_n is irreducible by Lemma 1. This holds also, in particular, for all $n=q\cdot p<50$.

(iv) Let $n=p^m-1$. Then, by (16) and (17), $e_0=0$ and $e_n=n/(p-1)$. For $0<\nu<n$, we observe from (16) that p is contained in a_ν as often as in $\prod_{i=1}^{\nu}(n+i)=(n+1)\prod_{i=2}^{\nu}(n+i)=(n+1)\prod_{i=1}^{\nu-1}(n+1+i)$. As $n+1=p^m$, $e_\nu=m+d_\nu$ where d_ν is the power of p contained in $\prod_{i=1}^{\nu-1}(n+1+i)$, and this is the same as the power of p contained in $(\nu-1)!$. Let $p^r\leqq\nu-1<p^{r+1}$, $r\leqq m-1$. Then, by (18), for $r\leqq m-2$, $d_\nu\geqq(\nu-1)(p^r-1)/p^r(p-1)-r$ and

$$e_\nu\geqq(\nu-1)(p^r-1)/p^r(p-1)-r+m. \tag{19}$$

[9] We shall prove without use of the lemma, that, for $n<50$, all BP are irreducible. Therefore, and in order not to complicate uselessly the statement, we use the word "all," although the lemma was proven—and will be used—only for $n>50$.

[10] For $p=2$, the statement was known to Lagrange. The general case follows from Theorem 27, p. 13 in [12].

[11] $[x]$ represents here the largest integer not exceeding x.

If $r=m-1$, then $\nu-1=\sum_{i=1}^{t} c_i p^{m-i}$, $t\leqq m$, $c_1\geqq 1$, max $c_i\leqq p-1$, so that

$$d_\nu = \sum_{\alpha=1}^{m-1} [(\nu-1)/p^\alpha] = \sum_{i=1}^{t} c_i(p^{m-i}-1)/(p-1)$$

$$= \left(\nu - \sum_{i=1}^{t} c_i\right)\Big/(p-1) \geqq \nu/(p-1) - t$$

and

$$e_\nu \geqq \nu/(p-1) + m - t \geqq \nu/(p-1). \tag{20}$$

We assert that

$$e_\nu \geqq \nu e_n/n = \nu/(p-1) \qquad \text{for } 1 \leqq \nu \leqq n-1. \tag{21}$$

For $r=m-1$, (21) follows directly from (20). For $r\leqq m-2$, (21) is a consequence of (19) and of $(\nu-1)(p^r-1)/p^r(p-1)-r+m\geqq \nu/(p-1)$. This can be written also as $\nu-1\leqq p^r\{(m-r)(p-1)-1\}$ and holds, since $\nu-1<p^{r+1}$, provided $p\leqq(m-r)(p-1)-1$, or, as $r\leqq m-2$, for $p\geqq(m-r+1)/(m-r-1)$ $=1+2/(m-r-1)\geqq 3$. This finishes the proof of (21). The Newton polygon reduces, therefore, to a single side. From $(e_n, n)=(n/(p-1), n)=n/(p-1)$ it follows now, by Dumas' Theorem, that the i.f. of z_n are of degrees which are multiples of $p-1$. If $k<p-1$, then, by Lemma 1, no such factor, different from z_n itself, can exist, and z_n is irreducible. In particular, if $m=1$, $n=p-1$ and always $k<n$, so that we find again that, for $n=p-1$, z_n is irreducible. The same conclusion holds, by Lemma 2, if $m=2$ and $7<p\leqq 17$ (so that $n>50$). Example: $n=120=11^2-1$, $e_n=n/(p-1)=12$, $(n, e_n)=(120, 12)=12$. As 127 is a prime, $k=127-n=7<12$; therefore, z_{120} is irreducible.

(v) Let $n=qp^m$, $p\nmid q$, $q\gtrless p^m$. This case is much more difficult than (iii), as the Newton polygon consists, in general, of several sides. The consideration of this case is useful, mainly in order to establish the irreducibility of a given polynomial. From (16) it follows that $a_{\nu+1}=a_\nu(n-\nu)(n+\nu+1)/(\nu+1)$, so that $e_{\nu+1}=e_\nu$, unless $p\,|\,\nu(\nu+1)$. Consequently, the Newton polygon may have corners only for $\nu=hp$ and, exceptionally, for $\nu=h\cdot p^\alpha=1$, $\alpha\geqq m-1$. Let $n=p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}$ and assume that no exceptional case arises in the Newton polygon for any p_i $(i=1, 2, \cdots, r)$. Then, by Dumas' Theorem, any i.f. of z_n is of degree $d\equiv 0 \pmod{p_1p_2\cdots p_r}$ and is irreducible if k $<p_1p_2\cdots p_r$. That the exceptional case can actually arise can be seen from the example $n=15$, $p=3$, with corners at $\nu=9$ and $\nu=11$. Everything said here holds also for the case $n=qp^m-1$ as is obvious from (16).

Using from previous criteria only those of unrestricted validity, we find that, up to $n\leqq 400$, all but 19 polynomials are irreducible. Also these 19 are found to be irreducible, as the i.f. which they may have are of degrees inadmissible by Lemma 1.

5. The Galois group of the BP.

THEOREM 6. *If y_n is an irreducible BP, then its Galois group G_n is the symmetric group on n symbols (except, possibly, for $n=9$, 11, 12).*

In the proof, we shall use the following theorem.

THEOREM OF SCHUR (*see* [16]). *Let $f(x)=\sum_{i=0}^{n} a_i x^{n-i}$, of discriminant Δ, be irreducible in the field of rationals, and let G_n be its Galois group. If there exists a prime p such that $p^m | \Delta$, $m \geqq n$; $p | a_n$; $p^2 \nmid a_n$; and also $f(x) \equiv x^k \phi(x)$ (mod p); $p | \delta$, where δ is the discriminant of $\phi(x)$, then the order of G_n is divisible by p. If, furthermore, $n/2 < p < n-2$, then G_n is the alternating group if Δ is a perfect square, the symmetric group otherwise.*

We shall again find it more convenient to study, instead of $y_n(x)$, the polynomial $z_n(x)=x^n y_n(1/x)$. This transformation leaves G_n and the discriminant unchanged.

Let D_n be the discriminant of y_n, let $a_0=(2n)!/n!2^n$ and $a_n=1$ be, respectively, the coefficient of x^n and the constant term in $y_n(x)$, and let $R_n=R(y_{n-1}, y_n)$ be the resultant of y_n and y_{n-1}. In (2) replace x by a root x_ν of $y_n(x)$ to get $y_{n+1}(x_\nu)=y_{n-1}(x_\nu)$. The product of these equations for $\nu=1, 2, \cdots, n$ gives

$$a_0^{-n-1} R_{n+1} = a_0^{-n+1} R_n, \quad \text{or} \quad R_{n+1} = a_0^2 R_n,$$

whence, using the value of a_0,

$$R_n = \left\{ 2^{-n(n-1)/2} \prod_{k=1}^{n-1} (2k)!/k! \right\}^2. \tag{22}$$

Similarly, $x=x_\nu$ in (3) gives $x^2 y_n'(x_\nu)=y_{n-1}(x_\nu)$. Taking the product of these equations, for $\nu=1, 2, \cdots, n$, and observing that $\prod_{\nu=1}^{n} x_\nu = 1/a_0$, one obtains

$$a_0^{-n-1} R(y_n, y_n') = a_0^{-n+1} R(y_n, y_{n-1}). \tag{23}$$

But $R(y_n, y_n')=a_0 D_n$. This combined with (22) and (23) yields

$$D_n = \prod_{k=0}^{n-1} (2n - 2k - 1)^{2k+1}. \tag{24}$$

We observe from (24) that any odd integer smaller than n is contained in D_n to a power larger than n and also that, for $n>1$, D_n cannot be a perfect square.

Let us consider those values of n, for which there exists some prime p satisfying

$$(2n - 1)/3 < p < n - 2. \tag{25}$$

Schur has shown (see [15]) that such primes always exist, if $(2n-1)/3 \geqq 23$, that is, for $n \geqq 35$. For $n<35$ we find by trial that primes satisfying (25) exist for all $n \geqq 14$ and also for $n=10$. From (16) and (24) it follows that primes satisfying (25) satisfy also the first set of three assumptions in Schur's theorem. Furthermore, let $p=n-\nu$, so that $2<\nu<(n+1)/3$. Observing that the coefficients of x^i in (16), with $i<n-\nu$, are divisible by $n-\nu$ and that $n \equiv \nu \pmod{(n-\nu)}$, it follows that $z_n(x) \equiv x^{n-\nu} z_\nu(x) \pmod{(n-\nu)}$. From (24) we see that no prime larger than $2\nu-1$ divides the discriminant D_ν of $z_\nu(x)$. From $\nu<(n+1)/3$ it follows also that $2\nu-1<(2n-1)/3<p$; therefore, $p \nmid D_\nu$. Consequently, if $z_n(x)$ is irreducible, all conditions of Schur's Theorem are fulfilled. As already seen, the discriminant D_n is not a perfect square and hence G_n is the symmetric group whenever (25) holds, that is, for $n \geqq 14$ and $n=10$. For the other values of n, we proceed as follows. As there are no primes satisfying (25), we try to find primes satisfying at least

$$(2n-1)/3 < p < n. \tag{26}$$

The cases $n=2$ and $n=3$ are trivial[12]. For each other $n \leqq 13$ ($n \neq 10$) except for $n=5$ and $n=11$, we find exactly one prime p_n satisfying (26), namely,

$$p_4 = 3, \quad p_6 = p_7 = 5, \quad p_8 = p_9 = 7, \quad p_{12} = p_{13} = 11. \tag{27}$$

As the corresponding polynomials are irreducible, their G_n are transitive. Furthermore, by Schur's Theorem, their order is divisible by the corresponding primes from (27) and, as also in each case $p_n>n/2$, it follows: (a) that the G_n are each isomorphic to a primitive permutation group; (b) that the degree of transitivity is in each case[13]: $l_n \geqq n-p_n+1$, so that, by (27): $l_4 \geqq 2$; $l_6 \geqq 2$; $l_7 \geqq 3$; $l_8 \geqq 2$; $l_9 \geqq 3$; $l_{12} \geqq 2$; $l_{13} \geqq 3$. We can now settle immediately the cases $n=4$, 7, and 13. As D_n is not a perfect square, it is sufficient to show that G_n contains in each case the corresponding alternating group. For $n=4$, there are no primitive groups, except the symmetric and alternating groups (see [3, §166, (ii), p. 214]). For $n=7$, the only triply transitive groups are the symmetric and alternating groups (ibid. (v), p. 216). For $n=13$, we observe that $p_1=5>3$ and $p_2=2 \cdot p_1+1=11$ are both primes; then there exists no triply transitive groups of order $2p_1+3=13$, which does not contain the alternating group (ibid. §165, p. 214, Ex.).

The remaining cases can be settled, as shown, in what follows, for $n=5$, 6, 8 using the following theorem.

THEOREM OF DEDEKIND (*see* [16, p. 445]). *If a congruence*

$$f(x) \equiv f_1(x) \cdot f_2(x) \cdots f_r(x) \pmod{p} \tag{28}$$

exists, where the polynomials $f_i(x)$ $(i=1, 2, \cdots, r)$ *are irreducible and incon-*

[12] The corresponding equations are irreducible and the discriminants are not perfect squares; consequently, G_2 and G_3 are the symmetric groups on 2, respectively 3, symbols (see [16, §3]). The method for $n \leqq 13$ follows, in the main, that of [16, §3].

[13] See [8, Note C].

gruent (mod p), *then the Galois group of* $f(x)$ *contains at least one permutation of* r *cycles, each cycle corresponding to one of the factors in* (28) *and being of the same order as the degree of the polynomial to which it corresponds.*

For $n=5$ we have:

$$\begin{aligned} z_5(x) &= x^5 + 15x^4 + 105x^3 + 420x^2 + 945x + 945 \\ &\equiv (x^3 + x^2 + 4x + 5)(x - 2)(x - 1) \pmod{17}. \end{aligned}$$

As $g(x) = x^3+x^2+4x+5$ is irreducible (mod 17), it follows by Dedekind's Theorem that G_5 contains a cycle of third order. Therefore, the order of G_5 is divisible by 3; the only transitive groups of degree 5 whose orders are divisible by 3 are, however, the symmetric and the alternating groups (see [3, §166, (iii), p. 214]). Similarly:

$$z_6(x) \equiv (x + 3)(x^2 + x - 1)(x^3 + 4x^2 - 3x + 6) \pmod{13}$$

where the factors are irreducible (mod 13). It follows from Dedekind's Theorem that G_6 contains a permutation of the form

$$P = (a, b)(c, d, e).$$

It contains, therefore, also the element $P^3 = (a, b)$, and as this is a transposition and G_6 is primitive, it is the symmetric group. For $n=8$,

$$(29)\quad z_8(x) \equiv (x + 6)(x^2 + 2x + 2)(x^5 + 9x^4 - 7x^3 + 8x^2 - 7x + 4) \pmod{19}.$$

As the factors are irreducible (mod 19), by the same argument as before, G_8 contains a permutation of the form $P = (a, b)(c, d, e, f, g)$ and consequently also $P^2 = (c, e, g, d, f)$, which is an element of fifth order. The order of G_8 is then divisible by 5, so that (see [3, §166, (vi), p. 218]) it contains the alternating group.

In general[14], if p^e is the highest power of p contained in $n!$, and if $p < 2n/3$, then p^{e-1} is the highest power of p contained in the order of any primitive group of degree n which does not contain the alternating group. It is, therefore, sufficient to show that G_9 contains an element of order 5 and that G_{11} and G_{12} contain elements of order 7, in order to have ascertained that they contain the alternating group. The method used for $n = 5$, 6, and 8 is still applicable; but the numerical difficulties involved in the establishment of congruences like (29) are so great that we abstained.

As the only difficult part of the proof is to establish such congruences, it may be of interest to give some details of the method. The only primes to be considered are $p \geqq 2n+1$, as, for smaller values, $a_0 \equiv a_1 \equiv 0 \pmod{p}$, $z_n \equiv x^2\phi(x)$, and Dedekind's Theorem is no longer applicable because we have a repeated factor. Starting with the smallest prime $p \geqq 2n+1$, we separate

[14] This follows from the argument used in [3, p. 207], in the proof of the corollary to Theorem 1.

first all linear factors (mod p), then all quadratic factors, and so on. If no suitable decomposition (mod p) can be found, we repeat the same process with the next higher prime, and so on. In particular, for $z_8(x)$ the steps are as follows:

(a) $p=17$. Linear factors: none, as $z_8(s)\not\equiv 0$ (mod 17) for integral s.

(b) Quadratic factors: As no linear factors exist, a decomposition of the form $(x^2+\alpha x+\beta)(x^6+\alpha' x^5+ \cdots)$ (mod 17) is of no use, as it cannot be decomposed further to obtain factors of the fifth degree, for which we are looking. We look, therefore, directly for a congruence like:

(c) $z_8(x)\equiv x^8+2x^7+x^6-6x^5+6x^4+4x^3-3x^2-4x-4\equiv(x^3+\alpha x^2+\beta x+\gamma)\cdot(x^5+\alpha' x^4+\cdots+\epsilon')$ (mod 17). In order to find the coefficients, we have to solve a system of simultaneous congruences, which turns out to have no solution.

(d) We pass, therefore, to the next higher prime, $p=19$. As $z_8(-6)\equiv 0$(mod 19), we can write:

$$\begin{aligned} z_8(x) &\equiv x^8-2x^7+3x^6-5x^5-9x^4-5x^3-8x^2-9x-9 \\ &\equiv (x+6)(x^7-8x^6-6x^5-7x^4-5x^3+6x^2-6x+8) \pmod{19}, \end{aligned} \tag{30}$$

and no other linear factors exist.

(e) We look now for a congruence like

$$\begin{aligned} &x^7-8x^6-6x^5-7x^4-5x^3+6x^2-6x+8 \\ &\qquad \equiv (x^2+\alpha' x+\beta')(x^5+\alpha x^4+\beta x^3+\gamma x^2+\delta x+\epsilon) \pmod{19}, \end{aligned} \tag{31}$$

which leads to the system of simultaneous congruences (mod 19):

$$\begin{array}{ll} \alpha+\alpha' \equiv -8, & \epsilon+\alpha'\delta+\beta'\gamma \equiv +6, \\ \beta+\alpha'\alpha+\beta' \equiv -6, & \alpha'\epsilon+\beta'\delta \equiv -6, \\ \gamma+\alpha'\beta+\beta'\alpha \equiv -7, & \beta'\epsilon \equiv +8. \\ \delta+\alpha'\gamma+\beta'\beta \equiv -5, & \end{array}$$

This system has a solution, which, substituted in (31), leads, by (30), to (29). Before we can use Dedekind's Theorem, we must still prove that all factors in (29) are irreducible (mod 19). As there are no linear factors in (31), the only possible decomposition would be of the form

$$\begin{aligned} &x^5+9x^4-7x^3+8x^2-7x+4 \\ &\qquad\qquad \equiv (x^2+\alpha x+\beta)(x^3+\alpha' x^2+\beta' x+\gamma') \pmod{19}. \end{aligned}$$

In order to determine the coefficients, we are led again to solve a system of simultaneous congruences, which turns out to have no solution. The factors of (29) are, consequently, irreducible (mod 19) and Dedekind's Theorem applies.

Added in proof. At the time when the present paper went to the printer, a paper by Professor J. Burchnall appeared in the Canadian Mathematical Journal, January 1951, with several of the results of the present paper.

Bibliography

1. S. Bochner, *Ueber Sturm-Liouvillesche Polynomsysteme,* Math. Zeit. vol. 29 (1929) pp. 730–736.

2. R. Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates,* Math. Zeit. vol. 34 (1932) pp. 505–524.

3. W. Burnside, *The theory of groups of finite order,* 2d ed., Cambridge University Press, 1911.

4. M. G. Dumas, *Sur quelques cas d'irréductibilité . . . ,* J. Math. Pures Appl. (6) vol. 2 (1906) pp. 191–258.

5. W. Hahn, *Ueber die Jacobischen Polynome . . . ,* Math. Zeit. vol. 39 (1935) pp. 634–638.

6. K. Hensel and O. Landsberg, *Theorie der algebraischen Funktionen,* Leipzig, Teubner, 1902.

7. A. Hurwitz, *Ueber einen Satz des Herrn Kakeya,* Tôhoku Math. J. vol. 4 (1913) pp. 89–93.

8. C. Jordan, *Traité des substitutions,* Paris, 1870.

9. S. Kakeya, *On the limits of the roots of an algebraic equation . . . ,* Tôhoku Math. J. vol. 2 (1912) pp. 140–142.

10. H. L. Krall and O. Frink, *A new class of orthogonal polynomials: the Bessel polynomials,* Trans. Amer. Math. Soc. vol. 65 (1949) pp. 100–115.

11. H. L. Krall, *On derivatives of orthogonal polynomials.* II, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 261–264.

12. E. Landau, *Vorlesungen über Zahlentheorie,* Leipzig, Hirzel, 1927.

13. ———, *Handbuch der Lehre von der Verteilung der Primzahlen,* Leipzig, Teubner, 1909.

14. O. Perron, *Ueber die Anwendung der Idealtheories . . . ,* Math. Ann vol. 60 (1905) pp. 448–458.

15. J. Schur, *Einige Sätze über Primzahlen,* Preuss. Akad. Wiss. Sitzungsber. (1929) pp. 125–136.

16. ———, *Gleichungen ohne Affekt,* ibid. (1930) pp. 443–449.

17. C. L. Siegel, *Transcendental numbers,* Princeton University Press, 1949.

University of Saskatchewan,
Saskatoon, Sask., Canada