ON A SPECIAL CLASS OF POLYNOMIALS*

BY

OYSTEIN ORE

In the present paper one will find a discussion of the main properties of a special type of polynomials, which I have called p-polynomials. They permit several applications to number theory and to the theory of higher congruences as I intend to show in a later paper, and they also possess several properties which are of interest in themselves.

The p-polynomials are defined in a field with prime characteristic p (modular fields); they form a (usually non-commutative) ring, where ordinary multiplication is replaced by symbolic multiplication, i.e., substitution of one polynomial into another. The p-polynomials are completely characterized by the property that the roots form a modulus. This modulus has a basis, and one shows consequently that the p-polynomials will have a great number of properties in common with differential and difference equations, such that the theory of p-polynomials gives an algebraic analogue to the theory of linear homogeneous differential equations. One finds that the theorems on the representation of differential polynomials will hold also for p-polynomials; the decomposition in symbolic prime factors is not unique, but the factors in two different representations will be similar in pairs. One can introduce the system of multipliers and the adjoint of a p-polynomial and even the Picard-Vessiot group of rationality; it corresponds in this case to a representation of the ordinary Galois group of the p-polynomial by means of matrices in the finite field (mod p). When this representation is reducible, the p-polynomial is symbolically reducible and conversely.

In this paper I have given only the fundamental properties in the theory of p-polynomials; various interesting problems could only be mentioned, while most applications of the theory had to be reserved for another communication. There are a few applications to higher congruences in §5, chapter 1, giving new proofs for theorems by Moore and Dickson; in §6 I give a new and simplified proof for the theorem of Dickson on the complete set of invariants for the linear group (mod p). The invariants are, as one will see, the coefficients of a certain p-polynomial, and a slight generalization of the proof of the fundamental theorem on symmetric functions gives the desired result.

---

* Presented to the Society, February 25, 1933; received by the editors February 3, 1933.

CHAPTER 1. PROPERTIES OF p-POLYNOMIALS

1. **Definition of p-polynomials.** Let K be an arbitrary field of *characteristic* p where p is a rational prime. In many of the most important applications K is a finite field, but this will not be assumed at this stage.*

A polynomial of the form

$$F_p(x) = a_0x^{p^m} + a_1x^{p^{m-1}} + \cdots + a_{m-1}x^p + a_mx \tag{1}$$

with coefficients in K shall be called a *p-polynomial*; the number m is called the *exponent* of $F_p(x)$. When $a_0=1$, $F_p(x)$ is said to be *reduced*. At times polynomials of the form

$$G_{p^f}(x) = a_0x^{p^{fm}} + a_1x^{p^{f(m-1)}} + \cdots + a_{m-1}x^{p^f} + a_mx \tag{2}$$

will be considered; their properties are quite analogous to those of p-polynomials (1).

The p-polynomials form a modulus, since they are reproduced by addition and subtraction. The pth power of a p-polynomial is again a p-polynomial.

The product of two p-polynomials is not a p-polynomial. It is however fundamental that a new *symbolic multiplication* can be introduced such that the product of two p-polynomials is again a p-polynomial. This multiplication is usually not commutative so that the p-polynomials will form a non-commutative ring.

Let namely

$$G_p(x) = b_0x^{p^n} + b_1x^{p^{n-1}} + \cdots + b_{n-1}x^p + b_nx \tag{3}$$

be a second p-polynomial; we then define the symbolic product $F_p(x)G_p(x)$ as

$$F_p(x) \times G_p(x) = F_p(G_p(x)) \tag{4}$$

and correspondingly $G_p(x)\times F_p(x) = G_p(F_p(x))$. It follows that

$$F_p(x) \times G_p(x) = c_0x^{p^{n+m}} + c_1x^{p^{n+m-1}} + \cdots + c_{n+m-1}x^p + c_{n+m}x, \tag{5}$$

where

$$\begin{aligned} c_0 &= a_1b_0^{p^m}, \\ c_1 &= a_0b_1^{p^m} + a_1b_0^{p^{m-1}}, \\ c_2 &= a_0b_2^{p^m} + a_1b_1^{p^{m-1}} + a_2b_0^{p^{m-2}}, \\ &\cdots\cdots\cdots \quad \cdots\cdots \\ c_{n+m} &= a_mb_n. \end{aligned} \tag{6}$$

* For several of the following theorems it is not even necessary to assume that the coefficient field is commutative.

The exponent of a product is the sum of the exponents of the factors.

One immediately observes, that the theory of p-polynomials is a special case of the theory which I have discussed in the paper *Theory of non-commutative polynomials.** One has only to introduce the correspondence

$$y^0 \rightarrow x,\ y \rightarrow x^p,\ y^m \rightarrow x^{p^m},\ y^{n+m} = y^n y^m \rightarrow x^{p^n} x^{p^m} = x^{p^{n+m}}$$

giving in general

$$F_p(x) \rightarrow a_0 y^m + \cdots + a_{m-1} y + a_m,$$

to recognize the formal identity of the two theories. Since

$$x^p \times ax = a^p x^p \rightarrow ya = a^p y$$

one sees that the two operations *conjugation* and *differentiation* in the general theory are here simply

$$\bar{a} = a^p,\ a' = 0.$$

From the general theory one can now deduce a great number of facts: In the ring of p-polynomials the symbolic multiplication is associative and distributive with respect to both right-hand and left-hand multiplication. The unit element is $E_p(x) = x$ and there are no divisors of zero, i.e., an identity $A_p(x)B_p(x) = 0$ implies $A_p(x) = 0$ or $B_p(x) = 0$.

A p-polynomial $F_p(x)$ is said to be symbolically right-hand divisible by $D_p(x)$ if $F_p(x) = Q_p(x) \times D_p(x)$. One observes that *when $F_p(x)$ is right-hand symbolically divisible by $D_p(x)$, then $F_p(x)$ is also divisible by $D_p(x)$ in the ordinary sense.* When $F_p(x) = D_p(x) \times Q_p(x)$ we say that $F_p(x)$ is left-hand symbolically divisible by $D_p(x)$.

Let us now consider division for p-polynomials; supposing $m \geqq n$ in (1) and (3) one finds that the differences

$$F_p(x) - a_0 b_0^{-p^{m-n}} x^{p^{m-n}} G_p(x),$$

$$F_p(x) - G_p(x) \times (a_0 b_0^{-1})^{1/p^n} x^{p^{n-m}}$$

do not contain any terms of higher degree than $x^{p^{m-1}}$. It follows, by repetition of this process, that one can write

$$(7) \qquad \begin{aligned} F_p(x) &= Q_p(x) \times G_p(x) + R_p(x), \\ F_p(x) &= G_p(x) \times P_p(x) + S_p(x), \end{aligned}$$

where the exponents of $R_p(x)$ and $S_p(x)$ are smaller than n. The coefficients

* To appear shortly in the Annals of Mathematics. This paper will be quoted as Ore I.

of $R_p(x)$ are all in K, while the coefficients of $S_p(x)$ lie in some radical field over K.

THEOREM 1. *Symbolic right-hand division of polynomials is always possible, while symbolic left-hand division can only be performed in K, when K is perfect.**

When left-hand divisibility is discussed in the following we shall always assume that K is perfect.

Theorem 1 shows that right-hand (and left-hand) Euclid algorithms exist, and this shows in turn the existence of a unique (reduced) cross-cut $(F_p(x), G_p(x)) = D_p(x)$. When $D_p(x) = x$ we say that $F_p(x)$ and $G_p(x)$ are right-hand symbolically relatively prime, and we can then find such polynomials $A_p(x)$ and $B_p(x)$ of exponents less than m and n respectively that

$$A_p(x) \times F_p(x) + B_p(x) \times G_p(x) = x. \tag{8}$$

We shall finally prove the following theorem:

THEOREM 2. *The symbolical right-hand cross-cut of $F_p(x)$ and $G_p(x)$ is equal to the ordinary cross-cut of these polynomials.*

This follows from our former remark that every symbolic right-hand divisor is also an ordinary divisor of a polynomial and the symbolic Euclid algorithm can therefore also be considered as an ordinary Euclid algorithm.

2. Linear factors. Let us now find the condition that a p-polynomial (1) be divisible symbolically by a linear factor $x^p - \alpha x$. One finds easily

$$F_p(x) = Q_p(x)\,(x^p - \alpha x) + Ax,$$

where

$$A = a_0\alpha^{(p^{m-1}-1)/(p-1)} + a_1\alpha^p + \cdots + a_{m-2}\alpha^{p+1} + a_{m-1}\alpha + a_m. \tag{9}$$

THEOREM 3. *The necessary and sufficient condition that the linear p-polynomial $x^p - \alpha x$ be a symbolic divisor of $F_p(x)$ is that α be a root of*

$$a_0 y^{(p^m-1)/(p-1)} + a_1 y^{(p^{m-1}-1)/(p-1)} + \cdots + a_{m-2}y^{p+1} + a_{m-1}y + a_m = 0, \tag{10}$$

i.e., α is equal to the $(p-1)$st power of a root of the equation $F_p(x) = 0$.

One can in the same way find the necessary and sufficient condition that $F_p(x)$ be left-hand divisible by $x^p - \alpha x$. The result is, in this case, a little more complicated, namely α must be a root of the equation

$$a_0^{1/p^m} y^{(p^m-1)/((p-1)p^{m-1})} + a_1^{1/p^{m-1}} y^{(p^{m-1}-1)/((p-1)p^{m-2})} + \cdots + a_{m-2}^{1/p^2} y^{(p+1)/p} + a_{m-1}^{1/p} y + a_m = 0. \tag{11}$$

* Compare Theorem 6, chapter I, Ore I.

From Theorem 3 follows immediately that every p-polynomial will decompose into linear symbolic factors in some finite algebraic extension of K. We shall discuss this decomposition later on.

For the product of linear factors one finds

$$(x^p + a_2x) \times (x^p + a_1x) = x^{p^2} + (a_1^p + a_2)x^p + a_1a_2x,$$

and the following theorem can be proved by induction:

THEOREM 4. *We have*

$$(x^p + a_nx) \times \cdots \times (x^p + a_2x) \times (x^p + a_1x) = x^{p^n} + A_1^{(n)}x^{p^{n-1}} + \cdots + A_{n-1}^{(n)}x^p + A_n^{(n)}$$

where

$$A_i^{(n)} = \sum a_{s_1}^{p^{\alpha_1}} a_{s_2}^{p^{\alpha_2}} \cdots a_{s_i}^{p^{\alpha_i}}, \quad s_1 < s_2 < \cdots < s_i,$$

where the sum is to be extended over all s and α such that

$$s_r + \alpha_r = n - i + r.$$

In the simplest case where all a's are equal to one, it is seen that

$$(x^p + x)^{[n]} = x^{p^n} + \binom{n}{1}x^{p^{n-1}} + \binom{n}{2}x^{p^{n-2}} + \cdots + \binom{n}{1}x^p + x.$$

3. **The roots of p-polynomials.** The roots of p-polynomials have several interesting and characteristic properties. Let us consider an equation

$$F_p(x) = 0; \tag{12}$$

it is obvious that $x=0$ is always a root. Furthermore if ω_1 and ω_2 are roots, it is seen without difficulty that $\omega_1 \pm \omega_2$ are roots.

THEOREM 5. *The roots of an equation* (12) *form a finite modulus.*

When $a_m \neq 0$ we find $F_p'(x) = a_m \neq 0$ and the equation (12) cannot have equal roots. The corresponding modulus must have finite basis and we can state

THEOREM 6. *When $a_m \neq 0$ the roots of $F_p(x) = 0$ form a finite modulus M of rank m. There exists a basis*

$$\omega_1, \omega_2, \cdots, \omega_m \tag{13}$$

for M, such that every root is uniquely representable in the form

$$\omega = k_1\omega_1 + \cdots + k_m\omega_m \quad (k_i = 0, 1, \cdots, p-1). \tag{14}$$

A modulus of the form (14) we shall call a p-modulus. It can be shown that m roots (13) form a basis for M if and only if

$$\Delta(\omega_1, \omega_2, \cdots, \omega_m) = \begin{vmatrix} \omega_1 & \omega_2 & \cdots & \omega_m \\ \omega_1^p & \omega_2^p & \cdots & \omega_m^p \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \omega_1^{p^{m-1}} & \omega_2^{p^{m-1}} & \cdots & \omega_m^{p^{m-1}} \end{vmatrix} \tag{15}$$

does not vanish.

It should be observed at this point, that if one considers the root of a p^f-equation $G_{p^f}(x)=0$, where $G_{p^f}(x)$ is given by (2), the roots will also form a modulus M and one can find a basis

$$\Omega_1, \Omega_2, \cdots, \Omega_m$$

such that every root is representable in the form

$$\Omega = \kappa_1\Omega_1 + \cdots + \kappa_m\Omega_m$$

where the κ_i run through all the elements of a finite field with p^f elements.

4. **Polynomials with given roots.** We shall next consider the inverse problem: *Given a p-modulus $M_p^{(n)}$ of rank n; to construct a p-polynomial $F(x)$ of exponent n having the elements of $M_p^{(n)}$ for roots.* Let $\omega_1, \cdots, \omega_n$ be a basis for $M_p^{(n)}$. When $n=1$ we find simply

$$F(x) = x(x-\omega_1)(x-2\omega_1)\cdots(x-(p-1)\omega_1) = x^p - \omega_1^{p-1}x. \tag{16}$$

The general expression can now be found by induction. Let $F_n(x)$ be the p-polynomial having the roots

$$k_1\omega_1 + \cdots + k_{n-1}\omega_{n-1} \qquad (k_i = 0, 1, \cdots, p-1).$$

The elements of $M_p^{(n)}$ will then satisfy the equation

$$F_n(x) = F_{n-1}(x)\cdot F_{n-1}(x-\omega_n)\cdots F_{n-1}(x-(p-1)\omega_n) = 0,$$

and since all occurring polynomials are p-polynomials,

$$F_n(x) = F_{n-1}(x)(F_{n-1}(x) - F_{n-1}(\omega_n))\cdots(F_{n-1}(x) - (p-1)F_{n-1}(\omega_n)),$$

or finally, as in the case $n=1$,

$$F_n(x) = F_{n-1}(x) - F_{n-1}(\omega_n)^{p-1}F_{n-1}(x), \tag{17}$$

which shows that $F_n(x)$ also is a p-polynomial. Using symbolic multiplication, we can write $F_n(x)$ in the form

$$F_n(x) = (x^p - F_{n-1}(\omega_n)^{p-1}x) \times F_{n-1}(x). \tag{18}$$

This gives by repeated application

THEOREM 7. *The p-polynomial $F_n(x)$ having the elements of a p-modulus $M_p^{(n)}$ for its roots can be written*

$$(19)\quad F_n(x) = (x^p - F_{n-1}(\omega_n)^{p-1}x) \times (x^p - F_{n-2}(\omega_{n-1})^{p-1}x) \times \cdots \times (x^p - \omega_1^{p-1}x)$$

where $\omega_1, \cdots, \omega_n$ is an arbitrary basis for $M_p^{(n)}$. One has also the formula

$$(20)\quad F_n(x) = \frac{\Delta(\omega_1, \cdots, \omega_n, x)}{\Delta(\omega_1, \cdots, \omega_n)}$$

where Δ denotes the determinant defined by (15).

It is obvious that the polynomial (20) has $\omega_1, \cdots, \omega_n$ and hence all elements of $M_p^{(n)}$ for its roots.

THEOREM 8. *The necessary and sufficient condition that the roots of a polynomial form a modulus is that the polynomial be a p-polynomial.*

The modulus must be finite, and the field of the coefficients must consequently have the characteristic p. The theorem then follows from Theorems 6 and 7.

5. **Applications to higher congruences.** The results of §4 immediately give various theorems on congruences (mod p).

From the definition of $F_n(x)$ and from (20) follows

$$(21)\quad \frac{\Delta(\omega_1, \cdots, \omega_n, x)}{\Delta(\omega_1, \cdots, \omega_n)} \equiv \prod_{i=1}^{n} \prod_{k_i=0}^{p-1} (x - (k_1\omega_1 + \cdots + k_n\omega_n)) \pmod{p}$$

which is a generalization of well known identities in higher congruences. When one compares the last term in x on both sides one obtains the following generalization of Wilson's theorem:

THEOREM 9. *Let $M_p^{(n)}$ be a finite modulus* (mod p) *and let $\omega_1, \cdots, \omega_n$ be a basis for the modulus; then*

$$(22)\quad \prod_{\omega} \omega \equiv (-1)^n \Delta(\omega_1, \cdots, \omega_n)^{p-1} \pmod{p}$$

where $\omega \neq 0$ runs through all elements of $M_p^{(n)}$.

Let us finally apply the formula (21) to the case of $n-1$ basis elements $\omega_1, \cdots, \omega_{n-1}$ and let us put $x = \omega_n$. This gives

$$\Delta(\omega_1, \cdots, \omega_n) \equiv \Delta(\omega_1, \cdots, \omega_{n-1}) \prod_{i=1}^{n-1} \prod_{k_i=0}^{p-1} (\omega_n + k_{n-1}\omega_{n-1} + \cdots + k_1\omega_1) \pmod{p}$$

and we have a simple proof of a theorem by E. H. Moore.*

* E. H. Moore, Bulletin of the American Mathematical Society, vol. 2 (1896), p. 189.

THEOREM 10. *The following identity holds*:

$$(23)\quad \Delta(\omega_1, \cdots, \omega_n) \equiv \prod_{i=1}^{n-1} \prod_{k_{i-1}=0}^{p-1} \cdots \prod_{k_1=0}^{p-1} (\omega_i + k_{i-1}\omega_{i-1} + \cdots + k_1\omega_1) \pmod{p}.$$

It can be stated by saying that $\Delta(\omega_1, \cdots, \omega_n)$ is congruent to the product of all different linear expressions in the ω_i, considering two such expressions equal if they are proportional.

Another result is the following:

Let $H_p(x) = A_p(x) \times B_p(x)$; *then*

$$H_p(x) = \prod_{\omega} (B_p(x) + \omega)$$

where ω *runs through the modulus of all roots of* $A_p(x) = 0$ *and the product sign indicates ordinary multiplication.*

This simple remark contains and generalizes various theorems on higher congruences by Mathieu* and Dickson.†

6. **The invariants of linear groups** (mod p). We shall now consider the symmetric functions of the roots of a p-polynomial. From (20) it follows that the p-polynomial corresponding to given modulus $M_p^{(n)}$ has the form

$$(24)\quad F_p(x) = x^{p^n} + A_1 x^{p^{n-1}} + \cdots + A_{n-1}x^p + A_n x,$$

where

$$(25)\quad A_i = (-1)^i \frac{\Delta^{(i)}(\omega_1, \cdots, \omega_n)}{\Delta(\omega_1, \cdots, \omega_n)} \qquad (i = 1, 2, \cdots, n),$$

and where $\Delta^{(i)}(\omega_1, \cdots, \omega_n)$ denotes the minor of the term x^{p^i} in the determinant $\Delta(\omega_1, \cdots, \omega_n, x)$. Every symmetric function of the elements of $M_p^{(n)}$ can therefore be expressed by the rational function (25) of the ω_i.

We shall now consider the inverse problem: When is a rational function $F(x_1, \cdots, x_n)$ a symmetric function of the $p^n - 1$ linear forms

$$(26)\quad \phi_{k_1 \cdots k_n}(x_1, \cdots, x_n) = k_1 x_1 + \cdots + k_n x_n \qquad (k_i = 0, 1, \cdots, p-1),$$

the combination $k_1 = \cdots = k_n = 0$ excluded. We shall prove

THEOREM 11. *The necessary and sufficient condition that* $F(x_1, \cdots, x_n)$ *be a symmetric function of the linear forms* (26) *is that* $F(x_1, \cdots, x_n)$ *be an absolute invariant of the full linear group of order* n (mod p).

When $F(x_1, \cdots, x_n)$ is representable as a symmetric function of the forms

---

* E. Mathieu, Journal de Mathématiques, (2), vol. 6 (1861), pp. 241–323.

† L. E. Dickson, Bulletin of the American Mathematical Society, vol. 3 (1897), pp. 381–389.

(26) it is representable by the coefficients A_i in (24). From the representation (25) it is easily seen that these coefficients are absolute invariants by all linear substitutions of the ω_i with non-vanishing determinant (mod p).

To prove the converse, let $F(x_1, \cdots, x_n)$ be an absolute invariant; one can assume, without loss of generality, that $F(x_1, \cdots, x_n)$ is integral. If we write

$$F(x_1, \cdots, x_n) = \sum_i B_i(x_2, \cdots, x_n) x_1^{\alpha_i}, \tag{27}$$

the $B(x_2, \cdots, x_n)$ must be absolute invariants of the linear group on the $(n-1)$ variables $x_2, \cdots, x_n$. Let us put

$$\Delta = \prod_{k_2, \cdots, k_n=0}^{p-1} (x_1 + k_2 x_2 + \cdots + k_n x_n)^{p-1} = x_1^{p^n - p^{n-1}} + \cdots, \tag{28}$$

where the coefficients of Δ as polynomial in x_1 are also invariants of the group in $n-1$ variables. We can now divide $F(x_1, \cdots, x_n)$ by the powers of Δ and obtain a representation of the form

$$F(x_1, \cdots, x_n) = R_t(x_1)\Delta^t + R_{t-1}(x_1)\Delta^{t-1} + \cdots + R_0(x_1), \tag{29}$$

where the coefficients $R_i(x_1)$ are polynomials of degree smaller than the degree of Δ in x_1 and with coefficients which are invariants in the $n-1$ remaining variables. We shall now show that x_1 does not occur in any $R_i(x_1)$. Let us suppose namely that

$$R_i(x_1) = S_0(x_2, \cdots, x_n) + x_1 S_1(x_2, \cdots, x_n) + \cdots. \tag{30}$$

It follows from the representation (28) that Δ is invariant under an arbitrary substitution of the form

$$\begin{aligned} &x_1 \to k_1 x_1 + \cdots + k_n x_n, \quad k_1 \not\equiv 0, \\ &x_i \to x_i. \end{aligned} \tag{31}$$

Since the representation (29) is unique, all coefficients in (29) must also be invariant under the substitutions (31). From (30) we obtain, however,

$$R_i(x_1) - S_0(x_2, \cdots, x_n) = x_1 K(x_1),$$

and applying all substitutions (31) to this identity we find that the difference $R_i(x_1) - S_0(x_2, \cdots, x_n)$ is divisible by Δ, giving $R_i(x_1) = S_0(x_2, \cdots, x_n)$. This gives the special form

$$F(x_1, \cdots, x_n) = R_t(x_2, \cdots, x_n)\Delta^t + \cdots + R_0(x_2, \cdots, x_n) \tag{32}$$

for the representation (29).

The remaining part of the proof is analogous to the proof for the principal

theorem on symmetric functions. The terms of $F(x_1, \cdots, x_n)$ are arranged in decreasing order as usual in this proof, and we assume that

$$ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}, \quad \alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_n, \tag{33}$$

is the principal term. α_1 is then the highest exponent of any power of x_i which occurs in $F(x_1, \cdots, x_n)$; according to (32) α_1 must be divisible by $p^n - p^{n-1}$; α_2 is the highest power of x_2 contained in the invariant $R_i(x_1, \cdots, x_n)$ and it is therefore by the same reason divisible by $p^{n-1} - p^{n-2}$ etc. It follows that the principal term (33) must have the form

$$ax_1^{t_1(p^n-p^{n-1})}x_2^{t_2(p^{n-1}-p^{n-2})}\cdots x_n^{t_n(p-1)}. \tag{34}$$

The invariant A_i in (25) has the principal term

$$\pm\, x_1^{p^n-p^{n-1}}x_2^{p^{n-1}-p^{n-2}}\cdots x_i^{p^{n-i+1}-p^{n-i}}$$

and the difference

$$F(x_1, \cdots, x_n) - (\pm\, aA_1^{t_1-t_2}A_2^{t_2-t_3}\cdots A_n^{t_n})$$

only contains terms lower than (34) and one obtains a representation of $F(x_1, \cdots, x_n)$ by the A_i through repetition of this process. It also follows that if

$$F(x_1, \cdots, x_n) = R(A_1, \cdots, A_n)$$

is the representation of the integral invariant $F(x_1, \cdots, x_n)$ then the coefficients of R belong to the ring generated by the coefficients of F.

An immediate consequence of this proof is

THEOREM 12. *The polynomials*

$$A_i(x_1, \cdots, x_n) = \frac{\Delta^{(i)}(x_1, \cdots, x_n)}{\Delta(x_1, \cdots, x_n)} \qquad (i = 1, \cdots, n) \tag{35}$$

form a fundamental system for all the absolute invariants of the linear group of n variables (mod p).

A relative invariant of the linear group is an expression $G(x_1, \cdots, x_n)$ which is only multiplied by a power of the substitution determinant by a linear substitution (mod p); $\Delta(x_1, \cdots, x_n)$ is a relative invariant and by multiplying by a suitable power of $\Delta(x_1, \cdots, x_n)$ one obtains a very simple proof of a theorem by Dickson*:

* L. E. Dickson, these Transactions, vol. 12 (1911), pp. 75–98.

THEOREM 13. *The polynomials*

$$\Delta(x_1, \cdots, x_n),\ A_i(x_1, \cdots, x_n) \qquad (i = 1, \cdots, n-1) \tag{36}$$

form a fundamental system for all relative invariants of the linear group on n variables (mod p).

The polynomial $A_n(x_1, \cdots, x_n)$ in (36) has been omitted since

$$A_n(x_1, \cdots, x_n) = \Delta(x_1, \cdots, x_n)^{p-1}.$$

Dickson has proved Theorem 13 for the somewhat more general case in which the linear group is supposed to have coefficients in an arbitrary finite field. Our proof holds with slight modifications also for this case. In the same paper Dickson considers the "Formenproblem" of the invariants: i.e., the problem of finding the values of the variables x_i for which the invariants assume prescribed values. From our point of view, this is identical with the problem of solving the equation defined by the corresponding p-polynomial, a problem which has already been discussed at some length.

7. **The resultant.** An important invariant of two p-polynomials $F_p(x)$ and $G_p(x)$ defined by (1) and (3) respectively is the so-called p-resultant $R_p(F_p(x), G_p(x))$. Let

$$\omega_1, \cdots, \omega_m;\ \psi_1, \cdots, \psi_n$$

be the basis elements of the two corresponding p-moduli; the determinant $\Delta(\omega_1, \cdots, \omega_m, \psi_1, \cdots, \psi_n)$ is then according to (22) equal to the product of all possible different linear combinations

$$a_1\omega_1 + \cdots + a_m\omega_m + b_1\psi_1 + \cdots + b_n\psi_n \tag{37}$$

in which not all coefficients vanish, and where two expressions (37) are considered to be equal if one can be obtained from the other through multiplication with a rational integer. We then define the p-resultant of $F_p(x)$ and $G_p(x)$ by putting

$$R_p(F, G) = \frac{\Delta(\omega_1, \cdots, \omega_m, \psi_1, \cdots, \psi_n)}{\Delta(\omega_1, \cdots, \omega_m)\Delta(\psi_1, \cdots, \psi_n)}. \tag{38}$$

This resultant is, we see, the product of the differences of all non-vanishing roots of the two polynomials, considering as before two differences $\omega - \psi$ and $k(\omega - \psi)$ as being equal. It is therefore

$$R_p(F, G) = R\left(\frac{F_p(x)}{x},\ \frac{G_p(x)}{x}\right)^{p-1}$$

where R denotes the ordinary resultant. I mention without proof that the p-resultant of $F_p(x)$ and $G_p(x)$ can be represented in the form

$$(39)\qquad R_p(F_p, G_p) = \frac{\Delta(F_p(\psi_1), \cdots, F_p(\psi_n))}{\Delta(\psi_1, \cdots, \psi_n)} = \frac{\Delta(G_p(\omega_1), \cdots, G_p(\omega_m))}{\Delta(\omega_1, \cdots, \omega_m)}.$$

One can also find a representation of R_p by means of the coefficients of $F_p(x)$ and $G_p(x)$.

8. **The adjoint of a p-polynomial.** To a given modulus $M_p^{(n)}$ we construct the adjoint modulus $\overline{M}_p^{(n)}$

$$(40)\qquad \bar{\omega}_1 = (-1)^{n+1}\frac{\Delta(\omega_2, \cdots, \omega_n)}{\Delta(\omega_1, \cdots, \omega_n)},\quad \bar{\omega}_2 = (-1)^{n+2}\frac{\Delta(\omega_1, \omega_3, \cdots, \omega_n)}{\Delta(\omega_1, \cdots, \omega_n)}, \cdots,$$
$$\bar{\omega}_n = \frac{\Delta(\omega_1, \cdots, \omega_{n-1})}{\Delta(\omega_1, \cdots, \omega_n)}.$$

We show simply that these numbers are linearly independent and therefore can be regarded as the basis of a modulus $\overline{M}_p^{(n)}$.

In §4, we have found that the reduced polynomial $F_p(x)$ having the modulus $M_p^{(n)}$ for roots will be left-hand divisible by $x^p - \beta x$, where according to (18) and (20)

$$\beta = F_{n-1}(\omega_n)^{p-1} = \frac{\Delta(\omega_1, \cdots, \omega_n)^{p-1}}{\Delta(\omega_1, \cdots, \omega_{n-1})^{p-1}} = \frac{1}{\bar{\omega}_n^{p-1}}.$$

By changing the order of the basis elements ω_i of $M_p^{(n)}$ one can deduce in the same way that $F_p(x)$ is left-hand divisible by all factors

$$x^p - \bar{\omega}_i^{-(p-1)}x,$$

and finally also by all factors

$$x^p - \bar{\omega}^{-(p-1)}x,$$

where $\bar{\omega}$ is an arbitrary element of the adjoint modulus $\overline{M}_p^{(n)}$.

Let on the other hand $\bar{\omega}$ be an element such that

$$(41)\qquad F_p(x) = (x^p - \bar{\omega}^{-(p-1)}x) \times Q_p(x).$$

The roots of $Q_p(x)$ will form a submodulus $M_p^{(n-1)}$ of $M_p^{(n)}$, and since a basis of $M_p^{(n-1)}$ may be completed to a basis for $M_p^{(n)}$ we see that $\bar{\omega}$ must be an element of $\overline{M}_p^{(n)}$. This leads to the following result which may also be used as a definition of $\overline{M}_p^{(n)}$:

THEOREM 14. *The adjoint modulus $\overline{M}_p^{(n)}$ to $M_p^{(n)}$ consists of all elements $\bar{\omega}$ such that the corresponding p-polynomial $F_p(x)$ to $M_p^{(n)}$ has a decomposition of the form* (41).

We shall express this result in a somewhat different form. From (41) we obtain

$$\bar{\omega}^p F_p(x) = ((x\bar{\omega})^p - \bar{\omega}x) \times Q_p(x) = (x^p - x) \times \bar{\omega}x \times Q_p(x). \tag{42}$$

An element κ such that

$$\kappa F_p(x) = (x^p - x) \times R_p(x) \tag{43}$$

shall be called a *multiplier* of $F_p(x)$. It is obvious that the multipliers form a modulus, and from (42) and Theorem 14 we find

THEOREM 15. *The multipliers of a polynomial $F_p(x)$ form a modulus $N_p^{(n)}$ of rank n which is equal to the modulus of the pth powers of the adjoint modulus $\overline{M}_p^{(n)}$ to the modulus $M_p^{(n)}$ of the roots of $F_p(x)=0$.*

Let us now determine the p-polynomial corresponding to the adjoint modulus $\overline{M}_p^{(n)}$ or to the modulus $N_p^{(n)}$ of the multipliers, which is virtually the same problem. If $F_p(x)$ is left-hand divisible by $x^p-\beta x$, then $\beta=\kappa^{-(p-1)/p}$, where κ is a multiplier, and the condition (11) for left-hand linear factors gives

THEOREM 16. *The multipliers of*

$$F_p(x) = x^{p^n} + A_1 x^{p^{n-1}} + \cdots + A_n x \tag{44}$$

are the roots of the equation

$$\overline{F}_p(x) = (A_n x)^{p^n} + (A_{n-1}x)^{p^{n-1}} + \cdots + (A_1 x)^p + x = 0. \tag{45}$$

Since the roots of $x^p-x=0$ are $0, 1, \cdots, p-1$, we observe the following result: If κ is a multiplier of $F_p(x)$ giving the decomposition (43), then

$$\kappa F_p(x) = \prod_{i=0}^{p-1}(R_p(x) + i) \tag{46}$$

where the product sign denotes ordinary multiplication.

We have in the preceding supposed $F_p(x)$ to be reduced. If $F_p(x)$ in (44) has the highest coefficient A_0 then the multipliers will be $\kappa' A_0^{-1}$, where κ' is a multiplier of the corresponding reduced polynomial.

In general we shall call the polynomial

$$\overline{F}_p(x) = (A_n x)^{p^n} + (A_{n-1}x)^{p^{n-1}} + \cdots + (A_1 x)^p + A_0 x \tag{47}$$

the adjoint of $F_p(x)$. The adjoint of $\overline{F}_p(x)$ is

$$\overline{\overline{F}}_p(x) = A_0^{p^n} x^{p^n} + A_1^{p^n} x^{p^{n-1}} + \cdots + A_n^{p^n} = x^{p^n} \times F_p(x) \times x^{p^{-n}},$$

and for the adjoint of a product one finds

$$\overline{F_p(x) \times G_p(x)} = x^{p^n} \times \overline{G_p(x)} \times x^{p^{-n}} \times \overline{F_p(x)}.$$

It may be more simple to introduce fractional powers and define the adjoint polynomial by putting

$$\overline{F}_p(x) = A_n x + (A_{n-1}x)^{1/p} + \cdots + (A_1 x)^{p^{-n+1}} + (A_0 x)^{p^{-n}}.$$

This expression has the same roots as (47) and it has the simpler properties that the adjoint of a sum is the sum of the adjoints, the adjoint of a product is equal to the product of the adjoints in inverse order, and also simply $\overline{\overline{F}}_p(x) = F_p(x)$.

Let us finally determine when $F_p(x) = \overline{F}_p(x)$, using the definition (47). We obtain the relations

$$A_i^{p^i} = A_i \qquad (i = 0, 1, \cdots, n) \tag{48}$$

and also

$$A_{n-i}^{p^{n-i}} = A_i \qquad (i = 0, 1, \cdots, n),$$

giving

$$A_i^{p^n} = A_i \qquad (i = 0, 1, \cdots, n).$$

THEOREM 17. *When a polynomial $F_p(x)$ is self-adjoint, all coefficients must belong to a finite field of p^n elements; in addition the relations* (48) *must hold.*

CHAPTER 2. FORMAL THEORY

1. **The union of p-polynomials.** Let $F_p(x)$ and $G_p(x)$ be two p-polynomials given by (1) and (3); the reduced polynomial

$$M_p(x) = [F_p(x), G_p(x)]$$

of smallest degree with coefficients in K which is right-hand symbolically divisible by both $F_p(x)$ and $G_p(x)$ is called the *least common multiple* or the *union* of $F_p(x)$ and $G_p(x)$. From the existence of a Euclid algorithm the existence of the union follows; it has the exponent $m+n-d$, where d is the exponent of the cross-cut $D_p(x) = (F_p(x), G_p(x))$.

Let as before

$$M_p^{(m)} = (\omega_1, \cdots, \omega_m), \quad N_p^{(n)} = (\psi_1, \cdots, \psi_n) \tag{1}$$

be the basis of the two moduli formed by the roots of the two polynomials $F_p(x)$ and $G_p(x)$. The modulus corresponding to $D_p(x)$ is then the modulus formed by the common elements of $M_p^{(m)}$ and $N_p^{(n)}$ while the modulus of the union is

$$T_p^{(n+m-d)} = (\omega_1, \cdots, \omega_m, \psi_1, \cdots, \psi_n).$$

When $F_p(x)$ is relatively prime to $G_p(x)$ we find

$$[F_p(x), G_p(x)] = \frac{\Delta(\omega_1, \cdots, \omega_m, \psi_1, \cdots, \psi_n, x)}{\Delta(\omega_1, \cdots, \omega_m, \psi_1, \cdots, \psi_n)}, \tag{2}$$

because the right-hand side is a reduced polynomial having the same roots as the union. For the same reason we see that also

$$\begin{aligned}[F_p(x), G_p(x)] &= \frac{\Delta(F_p(\psi_1), \cdots, F_p(\psi_n), F_p(x))}{\Delta(F_p(\psi_1), \cdots, F_p(\psi_n))} \\ &= \frac{\Delta(G_p(\omega_1), \cdots, G_p(\omega_m), G_p(x))}{\Delta(G_p(\omega_1), \cdots, G_p(\omega_m))}\end{aligned} \tag{3}$$

represent the union.

As an application let us determine the union of a reduced polynomial $F_p(x)$ and a linear factor $x^p - ax$. Since the roots of the latter are $ka^{1/(p-1)}$ $(k=0, 1, \cdots, p-1)$, we find, using formula (17), chapter 1,

$$M_p(x) = F_p(x)^p - F_p(a^{1/(p-1)})^{p-1} F_p(x).$$

If we put

$$\phi(x) = x^{(p^n-1)/(p-1)} + A_1 x^{(p^{n-1}-1)/(p-1)} + \cdots + A_n, \tag{4}$$

a simple reduction shows

THEOREM 1. *The union of a reduced polynomial $F_p(x)$ and a linear polynomial $x^p - ax$ is*

$$\begin{aligned}M_p(x) &= F_p(x) - a\phi(a)^{p-1} F(x) \\ &= x^{p^n} + (A_1{}^p - a\phi(a)^{p-1})x + (A_2{}^p - a\phi(a)^{p-1}A_1)x \\ &\quad + \cdots - a\phi(a)^{p-1}A_n x,\end{aligned} \tag{5}$$

where $\phi(x)$ is defined by (4).

2. **Transformation of p-polynomials.** The existence of a union for two arbitrary p-polynomials permits us to introduce a new operation on p-polynomials, which we shall call *transformation.*

The polynomial

$$A_p^{(1)}(x) = a_0 b_0{}^{p^{n-d}}[A_p(x), B_p(x)] \times B_p(x)^{-1} = B_p A_p(x) B_p^{-1} \tag{6}$$

is called the transform of $A_p(x)$ by $B_p(x)$. The notation is such that $A_p(x)$ has the exponent n, $B_p(x)$ the exponent m, while d is the exponent of the cross-cut

(7) $D_p(x) = (A_p(x), B_p(x)), A_p(x) = \overline{A}_p(x)D_p(x), B_p(x) = \overline{B}_p(x)D_p(x).$

Finally, a_0 and b_0 are the highest coefficients of $A_p(x)$ and $B_p(x)$ and the numerical constant in (6) is chosen such that the transform has the same highest coefficient as $A_p(x)$.

When $A_p(x)$ is relatively prime to $B_p(x)$, we say that (6) is a *special transformation*; the transform has then the exponent n. When a cross-cut $D_p(x)$ exists we call the transformation *general*, and the transform has the exponent $n-d$. The general transformation can always be reduced to a special transformation, since it follows from (6) and (7) that

(8) $$B_pA_p(x)B_p^{-1} = a_0b_0p^{n-d}[\overline{A}_p(x), \overline{B}_p(x)] \times \overline{B}_p(x)^{-1} = \overline{B}_p\overline{A}_p(x)\overline{B}_p^{-1}.$$

When the polynomial $A_p^{(1)}(x)$ is obtained from $A_p(x)$ by a special transformation, we say that $A_p^{(1)}(x)$ is similar to $A_p(x)$. It can be shown that *the notion of similarity is symmetric, reciprocal and associative.*

There exist a large number of results on the transformation of p-polynomials which can all be deduced from the general polynomial theory. They will be given here without proof:*

When $B_p^{(1)}(x) \equiv B_p^{(2)}(x) \pmod{A_p(x)}$ then

(9) $$B_p^{(1)}A_p(x)(B_p^{(1)})^{-1} = B_p^{(2)}A_p(x)(B_p^{(2)})^{-1}.$$

Furthermore

(10) $$(C_pB_p)A_p(x)(C_pB_p)^{-1} = C_p(B_pA_p(x)B_p^{-1})C_p^{-1}.$$

From (9) and (10) it follows that if $A_p^{(1)}(x) = B_pA_p(x)B_p^{-1}$, where $B_p(x)$ is relatively prime to $A_p(x)$, then $A_p(x) = B_p^{(1)}A_p^{(1)}(x)(B_p^{(1)})^{-1}$, when $B_p^{(1)}(x)$ is determined such that

$$B_p^{(1)}(x)B_p(x) \equiv x \pmod{A_p(x)},$$

which is always possible according to (8), chapter 1.

For the transformation of a union one finds simply

(11) $$C_p[A_p(x), B_p(x)]C_p^{-1} = [C_pA_p(x)C_p^{-1}, C_pB_p(x)C_p^{-1}];$$

the corresponding formula does not hold for the cross-cut. For the transform of a product of reduced factors one finds

(12) $$C_p(B_p(x) \times A_p(x))C_p^{-1} = C_p^{(1)}B_p(x)(C_p^{(1)})^{-1} \times C_pA_p(x)C_p^{-1}$$

where $C_p^{(1)}(x) = A_pC_p(x)A_p^{-1}$. For an arbitrary number of factors one finds

* The proofs follow from Ore I.

a corresponding result, which gives the theorem that the transform of a product is made up of factors which are similar to the factors in the original product.

The following theorem has some important applications in the formal representations of p-polynomials.

If a product $A_p(x) \times B_p(x)$ is divisible by $C_p(x)$ and $C_p(x)$ is relatively prime to $B_p(x)$, then $A_p(x)$ is divisible by $B_p C_p(x) B_p^{-1}$.

Let us now consider the expression for the transform in terms of the roots of the polynomials. From (3) and the definition of transformation follows

THEOREM 2. *When $B_p(x)$ is relatively prime to $A_p(x)$, we have*

$$B_p A_p(x) B_p^{-1} = a_0 \frac{\Delta(B_p(\omega_1), \cdots, B_p(\omega_n), x)}{\Delta(B_p(\omega_1), \cdots, B_p(\omega_n))} \tag{13}$$

where the ω_i form a basis for the roots of $A_p(x)$.

When ω is an arbitrary element in the modulus of $A_p(x)$, then the modulus of $B_p A_p(x) B_p^{-1}$ consists of all numbers $B_p(\omega)$ and this holds even in the general case. The transformation is consequently analogous to the Tschirnhausen transformation for algebraic equations.

As an application let us find the transform of a linear polynomial $x^p - ax$ by an arbitrary polynomial $F_p(x)$. From Theorem 1 follows

$$F_p(x^p - ax) F_p^{-1} = x^p - a\phi(a)^{p-1} x. \tag{14}$$

One can easily determine when two linear expressions

$$x^p - ax, \quad x^p - bx \tag{15}$$

are similar. According to (14) every polynomial similar to a linear polynomial can be obtained from it by transformation with an expression cx, and there follows from (14)

THEOREM 3. *Two linear polynomials* (15) *are similar when the quotient $ab^{-1} = c^{p-1}$ is a $(p-1)$st power in K.*

3. **Decomposition into prime factors.** We shall say that two reduced polynomials $A_p(x)$ and $B_p(x)$ are *transmutable* if $A_p(x)$ can be represented in the form

$$A_p(x) = B_p A_p^{(1)}(x) B_p^{-1},$$

where $A_p^{(1)}(x)$ is similar to $A_p(x)$. In this case the product

$$A_p(x) \times B_p(x) = [A_p^{(1)}(x), B_p(x)] = A_p^{(1)} B_p(x) A_p^{(1)}$$

can be written in two ways, such that the factors are similar, but occur in

different order. We shall say that one representation is obtained from the other by *transmutation*. As an example let us find when two linear factors are transmutable. Let

$$A_p(x) = x^p - ax,\ B_p(x) = x^p - bx,\ A_p^{(1)}(x) = x^p - cx;$$

then according to (14)

$$B_p A_p^{(1)}(x) B_p^{-1} = x^p - c(c-b)^{p-1}x$$

and c must be a root of the equation

$$c(c-b)^{p-1} = a.$$

A prime polynomial $P_p(x)$ in K is a polynomial which has no reduced symbolical divisors except itself and x. Every polynomial similar to a prime polynomial is also prime. One can then prove the following theorem*:

THEOREM 4. *Every reduced polynomial has a decomposition into prime factors. Two different decompositions of the same polynomial will have the same number of factors; the factors will be similar in pairs by a suitable ordering, and one decomposition can be obtained from the other through transmutation of factors.*

It is easily seen that one cannot expect the decomposition to be unique; if $F_p(x)$ is an arbitrary polynomial with the exponent n, then $F_p(x)$ is divisible by all p linear factors $x^p - \omega^{p-1}$, x, where ω is an arbitrary root.

4. **Completely reducible polynomials.** We shall say that a polynomial $F_p(x)$ in K is *completely reducible* when it is the union of prime polynomials. It can then be represented by a basis

$$F_p(x) = [P_1(x), \cdots, P_r(x)]$$

where each prime polynomial $P_i(x)$ is relatively prime to the union of the others. We can also show the following:

The necessary and sufficient condition that a polynomial be completely reducible is that two consecutive prime factors in an arbitrary prime polynomial decomposition always be transmutable.

The union of all prime polynomials, which divide an arbitrary polynomial $F_p(x)$ on the right, we shall call the *maximal completely reducible factor* of $F_p(x)$ and denote by $H_p^{(1)}(x)$. Then

$$F_p(x) = F_p^{(1)}(x) \times H_p^{(1)}(x),$$

and $F_p^{(1)}$ can be treated the same way; there follows

* Ore I, Theorem 1, chapter 2.

THEOREM 5. *Every polynomial has a unique representation as product of maximal completely reducible factors.*

From the general theory a large number of results on completely reducible polynomials can be deduced.* We shall however only mention a few facts, which we shall apply at a later point.

We shall say that a completely reducible polynomial is uniform, when it is only divisible by similar prime polynomials. The necessary and sufficient condition that a completely reducible polynomial be uniform is that the basis contain only similar prime polynomials.

Let $F_p(x)$ now be an arbitrary completely reducible polynomial; the union of all prime divisors of $F_p(x)$ which are similar to a given prime polynomial $P_p(x)$, we shall call a maximal uniform component of $F_p(x)$. It then follows that

Every completely reducible polynomial is uniquely representable as the union of maximal uniform components.

Let finally

$$F_p(x) = [P_p^{(1)}(x), \cdots, P_p^{(r)}(x)]$$

be an arbitrary completely reducible polynomial. If $F_p(x)$ is to be divisible by any prime polynomial $P_p(x)$ different from the basis elements, then at least two basis elements must be similar. Any prime divisor of $F_p(x)$ has to be similar to one of the basis elements, and if $P_p^{(1)}(x) = AP_p(x)A^{-1} \neq P_p(x)$ we could have constructed the basis such that $P_p(x)$ and $P_p^{(1)}(x)$ were basis elements. When conversely an arbitrary polynomial $F_p(x)$ is divisible both by $P_p(x)$ and the similar polynomial $P_p^{(1)}(x)$, we see that

$$F_p(x) \equiv 0, \qquad F_p(x) \times A_p(x) \equiv 0 \pmod{P_p(x)}$$

and from a theorem in §2, it follows that $F_p(x)$ is also divisible by all polynomials $BP_p(x)B^{-1}$, where $B_p(x)$ is an arbitrary polynomial of the form

$$B_p(x) = k_1 x + k_2 A_p(x) \quad (k_1, k_2 = 0, 1, \cdots, p-1).$$

Since the roots of $P_p^{(1)}(x)$ are different from those of $P_p(x)$, it is easily seen that $BP_p(x)B^{-1}$ is different from $P_p(x)$ and $P_p^{(1)}(x)$ when $k_1 \neq 0$ and $k_2 \neq 0$. This shows that

The necessary and sufficient condition that a completely reducible polynomial be divisible by a prime polynomial different from those occurring in a basis representation is that the basis representation contain at least two similar prime polynomials.

* See Ore I, §2, chapter 2.

One can also state this by saying that *the basis representation of a completely reducible polynomial is unique, when none of the components are similar.*

5. **Decomposable and distributive polynomials.** In Theorem 4 and Theorem 5 we have found two different representations of p-polynomials; several others can be found, but only two other representations of importance will be mentioned briefly.

A polynomial is said to be *decomposable* when there exists a representation

$$F_p(x) = [A_p(x), B_p(x)] \tag{16}$$

where $A_p(x)$ is relatively prime to $B_p(x)$; $F_p(x)$ is said to be *indecomposable* when no such representation exists. We can prove

THEOREM 6. *Every polynomial can be represented as the union of a number of indecomposable polynomials*

$$F_p(x) = [A_p^{(1)}(x), \cdots, A_p^{(r)}(x)], \tag{17}$$

where each indecomposable polynomial $A_p^{(i)}(x)$ is relatively prime to the union of the others; when two or more different representations (17) *exist, they will all have the same number of components, which will be similar in pairs.*

A polynomial $F_p(x)$ shall be said to be *distributive* when there exists a decomposition (16), where $A_p(x)$ and $B_p(x)$ are *proper divisors* of $F_p(x)$; a cross-cut $C_p(x)$ of $A_p(x)$ and $B_p(x)$ may perhaps exist; when no such decomposition (16) exists, we shall say that $F_p(x)$ is *non-distributive.*

For the proofs of the following theorems it is necessary to assume that K *is perfect*; one can then state

THEOREM 7. *The necessary and sufficient condition that a polynomial $F_p(x)$ be non-distributive is that $F_p(x)$ have only a single left-hand prime divisor $P(x)$.*

We shall say that the non-distributive polynomial $F_p(x)$ *belongs to* $P(x)$. It is easily seen that every left-hand divisor of $F_p(x)$ is also non-distributive and belongs to the same prime polynomial $P(x)$. One can also prove

THEOREM 8. *Let the completely reducible polynomial*

$$A_p(x) = [P_1(x), \cdots, P_r(x)] \tag{18}$$

be the union of all prime polynomials dividing a given polynomial $F_p(x)$ on the left. Then every representation of $F_p(x)$ as the union of non-distributive components has the form

$$F_p(x) = [C_1(x), \cdots, C_r(x)], \tag{19}$$

where the non-distributive polynomial $C_i(x)$ belongs to a prime polynomial similar to $P_i(x)$ $(i = 1, 2, \cdots, r)$.

We have supposed that (19) is a *shortest* representation; i.e., we have omitted all components which divide the union of the others.

6. **The invariant ring.** We shall now define a certain characteristic group G_I, *the invariant group*, and also a characteristic ring R_I, *the invariant ring*, corresponding to an arbitrary p-polynomial $F_p(x)$. We make the following definition:

The polynomial $I_p(x)$ is said to be an invariant transformer of $F_p(x)$, when $I_pF_p(x)\ I_p^{-1}$ is a divisor of $F_p(x)$.

It is easy to determine the invariant transformers in some simple cases. Let first $F_p(x)=x^p-ax$; it can then be assumed that $I_p(x)=cx$, and from §2 follows

$$I_pF_p(x)I_p^{-1} = x^p - ac^{p-1}x,\ c \neq 0,$$

giving the values $c=0$ and $c^{p-1}=1$, i.e., $c=0, 1, \cdots, p-1$. Let next $F_p(x)=x^{p^m}$; using the definition of the transform, one easily finds that every polynomial is an invariant transformer.

The definition of the invariant transformers can easily be modified in the following way:

THEOREM 9. *The necessary and sufficient condition that $I_p(x)$ be an invariant transformer of $F_p(x)$ is that*

$$F_p(x) \times I_p(x) \equiv 0 \pmod{F_p(x)}. \tag{20}$$

This condition (20) immediately shows that the sum, difference, and product of two invariant transformers is again an invariant transformer, and the ring of all invariant transformers is the invariant ring of $F_p(x)$.

When an invariant transformer $I_p(x)$ is relatively prime to $F_p(x)$ we must have

$$I_pF_p(x)I_p^{-1} = F_p(x). \tag{21}$$

The invariant transformers satisfying (21) form the invariant group. It is obvious that the product of two such polynomials has the same property, and to show the group property it only remains to show the existence of an inverse. Since $I_p(x)$ is relatively prime to $F_p(x)$, we can determine an $I_p^{(1)}(x)$ such that

$$I_p^{(1)}(x) \times I_p(x) \equiv x \pmod{F_p(x)},$$

and it is easily seen that also $I_p^{(1)}(x)$ satisfies (21).

Let now α be a root of

$$F_p(x) = 0. \tag{22}$$

from (20) follows that $I_p(\alpha)$ is also a root of (22) for an arbitrary root α and an arbitrary invariant transformer $I_p(x)$. The invariant transformer therefore permutes the roots of (22), or, expressed in a different way, it transforms the modulus formed by the roots of (22) into itself or a submodulus. When all the roots of (22) are different, the invariant transformer $I_p(x)$ is uniquely determined by the transformation it produces, since $I_p(\alpha)=I_p^{(1)}(\alpha)$ for all α implies $I_p(x)\equiv I_p^{(1)}(x) \pmod{F_p(x)}$. Since the number of roots of (22) is finite we obtain

THEOREM 10. *When all the roots of $F_p(x)=0$ are different, the invariant ring and the invariant group are finite.*

When $F_p(x)=0$ has equal roots, then

$$F_p(x) = x^{p^r}G_p(x),$$

and the invariant ring of $F_p(x)$ will be identical with the invariant ring of $G_p(x)$, when considered (mod $G_p(x)$). Incidentally, these remarks also show that the polynomials cx^{p^r} are the only ones for which all the polynomials are invariant transformers.

From the fact that the invariant ring is finite follows that it is an algebra over the finite field (mod p) and the invariant ring has a basis, such that every element can be represented in the form

$$I_p(x) \equiv c_1 I_p^{(1)}(x) + \cdots + c_r I_p^{(r)}(x) \pmod{F_p(x)}$$

where $c_i=0, 1, \cdots, p-1$. The invariant ring defined here should more specifically be called the right-hand invariant ring. There also exists a left-hand invariant ring having similar properties; for a left-hand invariant transformer $J_p(x)$ one must have as in (20)

$$J_p(x) \times F_p(x) = F_p(x) \times I_p(x), \tag{23}$$

and here $I_p(x)$ must be a right-hand invariant transformer according to definition. When conversely $I_p(x)$ is an invariant right-hand transformer it is easily seen that

$$J_p(x) = F_p(x) \times I_p(x) \times F_p(x)^{-1} \tag{24}$$

is a left-hand invariant transformer of $F_p(x)$.

THEOREM 11. *The left-hand and right-hand invariant rings and groups are directly isomorphic through the correspondence* (24).

Let us finally determine the invariant ring of a prime polynomial $P_p(x)$. In this case every $I_p(x)\not\equiv 0 \pmod{F_p(x)}$ has an inverse, and the invariant

ring is a field. Since this field has a finite number of elements, it follows from a theorem of Wedderburn that it is commutative.

THEOREM 12. *The invariant ring of a prime polynomial $P_p(x)$ is a commutative, finite field.*

The invariant ring of a p-polynomial is closely connected with the structure and representations of the given polynomial and several interesting results can be obtained. It will however carry us too far to study these problems here.

CHAPTER 3. CONNECTION BETWEEN p-POLYNOMIALS AND ORDINARY POLYNOMIALS

1. **Polynomials belonging to a p-polynomial.** We shall finally study some of the connections between p-polynomials and ordinary polynomials in K. First of all we shall show that an arbitrary polynomial $f(x)$ of nth degree always divides a p-polynomial. Let us divide all pth powers of x by $f(x)$; this gives relations of the form

$$x^{p^i} \equiv c_{n-1}^{(i)} x^{n-1} + \cdots + c_0^{(i)} \pmod{f(x)} \quad (i = 0, 1, 2, \cdots). \tag{1}$$

The powers $1, x, x^2, \cdots$ on the right-hand side of the $\nu \leqq n$ first congruences (1) can now be eliminated, and on the left-hand side this gives a p-polynomial $F_p(x)$ with the exponent ν which is divisible by $f(x)$. Since $F_p(x)$ obviously is the p-polynomial with the smallest exponent having this property, it follows from Theorem 2, chapter 1, that every other p-polynomial $\phi_p(x)$ having the same property must be symbolically divisible by $F_p(x)$.

THEOREM 1. *Every polynomial $f(x)$ of degree n belongs to a unique, reduced p-polynomial $F_p(x)$ with exponent $\nu \leqq n$, such that $f(x)$ divides $F_p(x)$ and every other p-polynomial $\phi_p(x)$ divisible by $f(x)$ is symbolically divisible by $F_p(x)$.*

The number ν shall be called the *exponent* of $f(x)$. It is easily seen that one can determine $F_p(x)$, when the p-polynomials corresponding to the irreducible factors of $f(x)$ are known. Let namely

$$f(x) = \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \tag{2}$$

be the prime-function decomposition of $f(x)$; we denote by $g(x)$ the product of all different prime factors of $f(x)$:

$$g(x) = \phi_1(x) \cdots \phi_r(x). \tag{3}$$

When $g(x)$ belongs to $G_p(x)$, then $F_p(x)$ must be symbolically divisible by

$G_p(x)$, and since $F_p(x)$ cannot contain equal factors, except when the last coefficient vanishes, it follows that $F_p(x)$ has the form

$$F_p(x) = x^{p^t} \times G_p(x),$$

where t is the smallest exponent such that p^t exceeds all e_i in (2).

One can consequently assume that the polynomial to be considered has no equal factors and therefore is of the form (3). One finds, that when the irreducible factor $\phi_i(x)$ belongs to $\phi_p^{(i)}(x)$, then $g(x)$ belongs to the union

$$G_p(x) = [\phi_p^{(1)}(x), \cdots, \phi_p^{(r)}(x)].$$

2. **The degrees of the factors.** When the roots of the polynomial $f(x)$ are known, the corresponding p-polynomial $F_p(x)$ can be determined in a different way. Let

$$f(x) = (x - \theta_1) \cdots (x - \theta_n), \tag{4}$$

and let us assume that all roots are different and non-vanishing. In the field $K(\theta_1, \cdots, \theta_n)$ a linear factor $x - \theta_i$ belongs to $x^p - \theta_i^{p-1}x$, and from the last remarks of §1 we obtain

THEOREM 2. *Let the n different non-vanishing numbers*

$$\theta_1, \theta_2, \cdots, \theta_n \tag{5}$$

be the roots of a polynomial $f(x)$ in K; then $f(x)$ belongs to

$$F_p(x) = [x^p - \theta_1^{p-1}x, \cdots, x^p - \theta_n^{p-1}x]. \tag{6}$$

It is obvious that the coefficients of $F_p(x)$ belong to K, since they are symmetric functions of the elements (5).

It should be noted that there are always polynomials belonging to an arbitrary p-polynomial $F_p(x)$, for instance $F_p(x)$. There are however not always irreducible polynomials belonging to a given p-polynomial, and consequently there exist p-polynomials without primitive roots, i.e., such that every root of $F_p(x) = 0$ satisfies a p-equation with lower exponent. As an example let us take

$$F_p(x) = [x^p - ax, x^p - ab^{p-1}x].$$

$F_p(x)$ is the union of two similar p-polynomials with the exponent 1, and its roots are of the form

$$\theta = k_1 a^{1/(p-1)} + k_2 b a^{1/(p-1)} \quad (k_1, k_2 = 0, 1, \cdots, p - 1),$$

and θ satisfies the equation with exponent 1

$$x^p - (k_1 + k_2 b)^{p-1} a x = 0.$$

It would be an interesting problem to determine the necessary and sufficient condition for the existence of primitive roots.

Let us now suppose that the p-polynomial $F_p(x)$ is generated by an ordinary polynomial $f(x)$ with the roots (5) as indicated in Theorem 2. The roots of $F_p(x)$ are then according to (6)

$$M_p = k_1\theta_1 + \cdots + k_n\theta_n \quad (k_i = 0, 1, \cdots, p-1;\ i = 1, \cdots, n). \tag{7}$$

All factors $g(x)$ of $F_p(x)$ have therefore roots lying in the Galois field $K(\theta_1, \cdots, \theta_n)$ and if N is the degree of this Galois field, it follows that the degree of each factor is a divisor of N. This gives in particular

THEOREM 3. *When $F_p(x)$ is generated by an irreducible Galois polynomial $f(x)$ of degree N, then all factors of $F_p(x)$ have degrees equal to N or a factor of N.*

It is possible that even for an arbitrary p-polynomial $F_p(x)$ the theorem holds that if N is the degree of the maximal factor of $F_p(x)$, then all other factors have degrees equal to N or a factor of N. I have only been able to prove this theorem under certain limiting conditions. It should be observed that Theorem 2 gives a generalization of a well known property of the polynomial $x^{p^\nu} - x \pmod p$.

3. **The Galois group.** Let $F_p(x)$ be a p-polynomial and $f(x)$ a polynomial belonging to $F_p(x)$; when the roots of $f(x)$ are given by (5), then the roots of $F_p(x)$ form the modulus (7). The following is therefore obvious:

THEOREM 4. *The exponent of $f(x)$ is equal to the rank of the modulus* (7).

Choosing the notation in a suitable manner, one can write the modulus (7) in the reduced form

$$M_p = k_1\theta_1 + \cdots + k_\nu\theta_\nu \quad (k_i = 0, 1, \cdots, p-1;\ i = 1, \cdots, \nu). \tag{8}$$

The equations $F_p(x) = 0$ and $f(x) = 0$ define the same Galois field, as one sees from the representation (8) of the roots. Let G be the Galois group of $f(x)$; any permutation S in G will then produce a substitution on the linear expressions (8), and it is easily seen that two different permutations will produce different substitutions. This shows

THEOREM 5. *When ν is the exponent of the polynomial $f(x)$, then there exists a true representation of the Galois group G of $f(x)$ by means of matrices of rank ν in the finite field* (mod p).

We have in the introduction mentioned the analogy between p-polynomials and differential polynomials. To those who are familiar with the Picard-Vessiot theory of linear homogeneous differential equations, it will be clear that the group of linear substitutions on the expressions (8) correspond-

ing to the Galois group G is the analogue of the group of rationality of a differential equation. One may of course obtain a different representation of G by using a different basis for the roots of $F_p(x)$, but it is easily seen that all such representations are similar.

Almost all theorems on the group of rationality have analogues in the theory of p-polynomials. I shall here only mention two results, analogous to theorems by Loewy on differential equations:

THEOREM 6. *The necessary and sufficient condition that a p-polynomial be reducible in K is that the representation of G be reducible.*

When the representation of G is reducible, one can choose a basis for the modulus of the roots, such that there exists a submodulus G' which is transformed into itself by all substitutions of G. The submodulus G' defines a factor $G_p(x)$ of $F_p(x)$ and since $G_p(x)$ is left unchanged by all substitutions in G it has coefficients in K. When conversely $F_p(x)$ has a symbolic factor $Q_p(x)$ it is clear that a reducible representation of G exists. In a similar way we show

THEOREM 7. *When* $F_p(x)$ *is decomposable,*

$$F_p(x) = [A_p(x), B_p(x)],$$

then the representation of G is also decomposable and equal to the sum of two representations corresponding to $A_p(x)$ *and* $B_p(x)$, *and conversely.*

YALE UNIVERSITY,
NEW HAVEN, CONN.