CONTRIBUTIONS TO THE THEORY OF FINITE FIELDS*

BY

OYSTEIN ORE

The present paper contains a number of results in the theory of finite fields or higher congruences. The method may be considered as an application of the theory of p-polynomials, which I have developed in a recent paper† *On a special class of polynomials*. In this special case the p-polynomials form a commutative ring. However, this paper may be read without reference to the former investigations and one may say that the method applied is the representation of the finite field in its group ring. It should be mentioned at this point that a number of the results have direct applications in the theory of algebraic numbers.

In chapter 1 the special properties of the p-polynomials with coefficients in a finite field have been derived and the main results are the theorems that every p-polynomial has primitive roots and that every p-modulus is simple. A corollary is the theorem of Hensel, that every finite field has a basis consisting of conjugate elements. Through the introduction of a symbolic multiplication of elements in a p-modulus we make every such modulus a ring usually containing divisors of zero. The results of this first chapter I have previously given without proofs.‡

In chapter 2 various theorems of decomposition and theorems on prime polynomials belonging to a product of p-polynomials have been derived. Theorems 4 and 5 seem to be the most interesting of the results. In the next chapter these results are applied to the construction of irreducible polynomials. Theorem 1 gives a general type of irreducible polynomials. Next the complete prime polynomial decomposition of the simplest p-polynomials are given, and it is shown how most known irreducible polynomials (mod p) can be obtained in this way, thus obtaining a unified method for deriving various formerly known results. In the last paragraph one finds a new class of irreducible polynomials closely related to the linear fractional substitutions. The last chapter contains a few rudiments of the theory of finite fields considered as cyclic fields and also a particularly simple proof for the general law of reciprocity.

* Presented to the Society, October 28, 1933; received by the editors December 1, 1933.

† These Transactions, vol. 35 (1933), pp. 559–584.

‡ O. Ore, *Einige Untersuchungen über endliche Körper*, Proceedings 7th Scandinavian Mathematical Congress, Oslo, 1930, pp. 65–67.

Chapter 1. Theorems on finite fields

1. **Fundamental properties of p-polynomials.** In the following, polynomials with rational integral coefficients will be studied for a rational prime modulus p; since almost all congruences occurring in this paper are taken with respect to this modulus, we shall, when no ambiguity is to be feared, replace congruences (mod p) by equalities.

A polynomial of the form

$$F(x) = a_0x^{p^n} + a_1x^{p^{n-1}} + \cdots + a_{n-1}x^p + a_nx \tag{1}$$

shall be called a *p-polynomial.* $F(x)$ is *reduced* when $a_0=1$. The polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \tag{2}$$

is called the *polynomial corresponding to* $F(x)$; the degree n of $f(x)$ is called the *exponent* of $F(x)$.

The system of all p-polynomials forms a modulus, but not a ring, since the ordinary product of two p-polynomials is not a p-polynomial. One finds, however, that the pth power of a p-polynomial (mod p) is again a p-polynomial; this shows that if

$$G(x) = b_0x^{p^m} + b_1x^{p^{m-1}} + \cdots + b_{m-1}x^p + b_mx \tag{3}$$

is a second p-polynomial with the corresponding polynomial

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m, \tag{4}$$

then the result of substituting $F(x)$ in $G(x)$ is also a p-polynomial $G(F(x))$. We therefore are led to the definition of a symbolic multiplication

$$G(x) \times F(x) = G(F(x)), \tag{5}$$

and a simple investigation of the symbolic product gives the following results:

Theorem 1. *The symbolic multiplication is commutative and distributive and the polynomial corresponding to a symbolic product is equal to the product of the corresponding polynomials of the symbolic factors.*

If consequently

$$F_1(x), \cdots, F_r(x)$$

are p-polynomials with the corresponding polynomials

$$f_1(x), \cdots, f_r(x),$$

then the symbolic product

$$\Pi(x) = F_1(x) \times \cdots \times F_r(x)$$

has the corresponding polynomial

$$\pi(x) = f_1(x) \cdots f_r(x).$$

We shall say that $P(x)$ is a *symbolic prime polynomial*, when it is reduced and no symbolic decomposition $P(x) = A(x) \times B(x)$ exists except when one of the factors has the exponent zero. One could also have used the correspondence stated in Theorem 1 and defined $P(x)$ as a prime p-polynomial when the corresponding polynomial $p(x)$ is irreducible (mod p). This correspondence immediately shows

THEOREM 2. *The decomposition of a p-polynomial in symbolic prime factors is unique.*

One could also have concluded this from the fact that there exists a Euclid algorithm for the symbolic multiplication. When two p-polynomials $A(x)$ and $B(x)$ are given, one can find two others $Q(x)$ and $R(x)$ such that

$$A(x) = B(x) \times Q(x) + R(x) \tag{6}$$

where the exponent of $R(x)$ is smaller than the exponent of $B(x)$. From (6) the existence of a Euclid algorithm follows; there exists a greatest common symbolic factor for any two or more p-polynomials. When $A(x)$ and $B(x)$ have only the trivial symbolic common factor x, we say that $A(x)$ and $B(x)$ are *symbolically relatively prime.*

It should be observed that when $A(x)$ is symbolically divisible by $D(x)$, then $A(x)$ is also divisible by $D(x)$ in the ordinary sense and conversely. From $A(x) = Q(x) \times D(x)$ follows, namely, when $Q(x) = q_1(x) \cdot x$, that $A(x) = q_1(D(x)) \cdot D(x)$. On the other hand, let $A(x)$ be divisible by $D(x)$ in the ordinary sense; one can divide $A(x)$ symbolically by $D(x)$ and obtain

$$A(x) = Q(x) \times D(x) + R(x) = q_1(D(x)) \cdot D(x) + R(x). \tag{7}$$

Here the degree of $R(x)$ is smaller than the degree of $D(x)$, and the second equation (7) shows that $R(x) = 0$. This reasoning also shows that the symbolic Euclid algorithm will contain the same residues as the ordinary Euclid algorithm. One obtains in particular

THEOREM 3. *The greatest common symbolic factor of two p-polynomials is the same as the ordinary greatest common factor of the p-polynomials.*

When therefore $A(x)$ and $B(x)$ are symbolically relatively prime, then the ordinary greatest common factor of $A(x)$ and $B(x)$ is x and conversely. Let us also observe that in this case one can determine two p-polynomials $X(x)$ and $Y(x)$ such that

$$X(x) \times A(x) + Y(x) \times B(x) = x. \tag{8}$$

The p-polynomials of the greatest interest in the following are the well known

$$F_n(x) = x^{p^n} - x \tag{9}$$

with the corresponding polynomial

$$f_n(x) = x^n - 1. \tag{10}$$

Theorem 1 shows

THEOREM 4. *When $f_n(x)$ has the ordinary prime factor decomposition*

$$x^n - 1 = \phi_1(x) \cdots \phi_r(x) \tag{11}$$

then $F_n(x)$ has the symbolic prime factor decomposition

$$x^{p^n} - 1 = \Phi_1(x) \times \cdots \times \Phi_r(x), \tag{12}$$

where $\phi_i(x)$ $(i=1, 2, \cdots, r)$ is the polynomial corresponding to $\Phi_i(x)$.

2. **The roots of p-polynomials.** We shall now discuss the properties of the roots of a p-polynomial $F(x)$ defined by (1). Since $F(x)$ can be represented as the ordinary product of prime factors, it is obvious that the roots will belong to some finite field K. For a p-polynomial one has $F'(x) = a_n$ and this shows that $F(x)$ can only have equal roots when $a_n = 0$; this case will always be excluded in the following considerations.

Let μ and ν be roots of

$$F(x) = 0; \tag{13}$$

due to the special form of a p-polynomial one sees that $\mu \pm \nu$ is also a root of (13) and, furthermore, that the pth power μ^p will also be a root.

We shall say that a finite modulus M_p is a p-modulus, if it has the property that the pth power of every element is contained in it. This definition implies that every p-modulus lies in some finite field. We can now show

THEOREM 5. *The roots of a p-polynomial form a p-modulus and every p-modulus is the set of roots of a p-polynomial.*

The first part of the theorem follows from the remarks made above. Since a p-modulus M_p always has elements in some finite field, and since μ^p for each μ is the conjugate of μ it follows that the totality of elements of M_p will satisfy an equation with rational coefficients. In order to show that this is a p-polynomial, let

$$M_p = r_1\mu_1 + \cdots + r_n\mu_n \qquad (r_i = 0, 1, \cdots, p-1)$$

be a representation of M_p by a basis. Then all elements of M_p are seen to satisfy the equation

$$F(x) = \begin{vmatrix} \mu_1 & \cdots & \mu_n & x \\ \mu_1^p & \cdots & \mu_n^p & x^p \\ \cdot & \cdot & \cdot & \cdot \\ \mu_1^{p^n} & \cdots & \mu_n^{p^n} & x^{p^n} \end{vmatrix} = 0$$

and the fact that the elements $\mu_1, \cdots, \mu_n$ form a basis shows that the highest coefficient does not vanish.

Theorem 5 gives a correspondence between p-moduli and p-polynomials; we shall derive a few simple consequences. Let $F(x)$ be a p-polynomial with the p-modulus M_p; when $F(x)$ is symbolically reducible,

$$F(x) = F_1(x) \times F_2(x) = F_1(F_2(x)),$$

it follows that M_p must contain as a sub-modulus the roots M_p' of $F_1(x)$ (or $F_2(x)$). Conversely, if M_p contains a sub-p-modulus M_p' corresponding to a p-polynomial $F_1(x)$, then according to §1, $F_1(x)$ must divide $F(x)$ both in the ordinary and in the symbolic sense.

THEOREM 6. *The necessary and sufficient condition that $F(x)$ be symbolically reducible is that its p-modulus M_p contain a sub-p-modulus.*

We shall say that M_p is a *prime p-modulus*, when it contains no sub-p-modulus except the zero modulus. The necessary and sufficient condition that M_p be prime is that the corresponding p-polynomial be symbolically irreducible. When M_p and N_p are two p-moduli corresponding to $F(x)$ and $G(x)$, it is easily seen that M_p+N_p is also a p-modulus corresponding to the least common multiple $[F(x), G(x)]$, and that the cross-cut (M_p, N_p) is a p-modulus corresponding to the greatest common factor $(F(x), G(x))$.

Now let μ be an arbitrary element of a finite field; all elements of the form

$$S_p = k_0\mu + k_1\mu^p + k_2\mu^{p^2} + \cdots \tag{14}$$

obviously form a p-modulus and a p-modulus generated in this way by a single element shall be called *simple*. There must exist a smallest exponent a such that a relation

$$\mu^{p^a} + m_1\mu^{p^{a-1}} + \cdots + m_{a-1}\mu^p + m_a\mu = 0$$

holds, and the elements of the simple p-modulus (14) can then be represented uniquely in the form

$$S_p = k_0\mu + k_1\mu^p + \cdots + k_{a-1}\mu^{p^{a-1}}. \tag{15}$$

From the definition of a prime p-modulus it follows that every prime p-modulus is simple. It is one of the main results of this theory that

THEOREM 7. *Every p-modulus is simple.*

This theorem will be proved in §4.

3. Polynomials belonging to a p-polynomial. Let $\phi(x)$ be an arbitrary polynomial of degree m; it will be shown that $\phi(x)$ always divides a p-polynomial $F(x)$. In order to find the p-polynomial $F(x)$ of smallest degree having this property, we divide the successive powers x^{p^i} by $\phi(x)$ and obtain a set of congruences

$$x^{p^i} \equiv a_1^{(i)} x^{m-1} + \cdots + a_m^{(i)} \pmod{\phi(x)} \quad (i = 0, 1, \cdots). \tag{16}$$

Through linear elimination one can obtain a relation (mod $\phi(x)$) between the powers x^{p^i}, eliminating $1, x, x^2, \cdots, x^{m-1}$ from the right-hand side of (16). If $\nu+1$ is the first index such that there exists a linear homogeneous relation between the first $\nu+1$ polynomials on the right-hand side, then $\phi(x)$ will divide a p-polynomial $F(x)$ with the exponent ν. The construction of $F(x)$ shows that it is the p-polynomial with smallest exponent divisible by $\phi(x)$ and we shall say that $\phi(x)$ *belongs* to $F(x)$. The following is then easily seen:

THEOREM 8. *Every polynomial $\phi(x)$ of degree m belongs to a unique p-polynomial $F(x)$ with the exponent $\nu \leqq m$. Every p-polynomial divisible by $\phi(x)$ is symbolically divisible by $F(x)$.*

Let next $F(x)$ be an arbitrary p-polynomial without equal roots, and let $f(x)$ be the corresponding polynomial. Since each prime factor of $f(x)$ divides some x^n-1, it follows that there exists a smallest exponent N such that x^N-1 is divisible by $f(x)$. This gives, when applied to $F(x)$,

THEOREM 9. *There exists for each p-polynomial $F(x)$ without equal roots a smallest number N such that*

$$x^{p^N} - x = G(x) \times F(x). \tag{17}$$

We shall call N the *index* of $F(x)$; every irreducible ordinary factor of $F(x)$ has then a degree dividing the index.

Since every polynomial belongs to some p-polynomial, it follows, in particular, that every prime polynomial $\phi(x)$ belongs to some $F(x)$, and it is easily seen that one can assume that $F(x)$ has no equal roots. The degree N' of $\phi(x)$ is then a divisor of the index N of $F(x)$, according to (17). On the other hand, $\phi(x)$ is a divisor of the p-polynomial

$$F_{p^{N'}}(x) = x^{p^{N'}} - x,$$

and $F(x)$ is therefore also a symbolic divisor of the p-polynomial $F_{p^{N'}}(x)$. This shows, conversely, that N is a divisor of N', and we obtain

THEOREM 10. *An irreducible polynomial of degree N belongs to a p-polynomial with the index N, and conversely, every irreducible ordinary factor belonging to a p-polynomial with the index N has the degree N.*

At the close of these considerations I should like to make another observation. When one wishes to find the prime function decomposition (mod p) of an ordinary polynomial $f(x)$, one usually determines the smallest exponent N such that $f(x)$ divides $x^{p^N}-x$.* In order to obtain this, one can construct the system of congruences (16); instead of continuing the divisions until

$$x^{p^N} \equiv x \qquad (\text{mod } f(x)),$$

it is usually simpler to eliminate the powers of x on the right-hand side and find the p-polynomial $\Phi(x)$ which $f(x)$ divides. When $\Phi(x)$ corresponds to $\phi(x)$ it is only necessary to find the N for which $\phi(x)$ divides x^N-1.

4. **Primitive roots.** The problem now naturally arises to find the number of irreducible polynomials belonging to a given p-polynomial $F(x)$. When $F(x)$ has the exponent N, these polynomials are all of degree N. One may state the problem in a somewhat different form. We shall say that a root μ is a *primitive root* of $F(x)=0$ when it satisfies no p-equation of lower degree. Our problem is then equivalent to the determination of the primitive roots. Now let

$$F(x) = \Phi_1(x)^{(e_1)} \times \cdots \times \Phi_r(x)^{(e_r)} \tag{18}$$

be the symbolic prime function decomposition of $F(x)$, in which the exponents signify the repetition of equal factors; the exponent of $\Phi_i(x)$ is m_i. The primitive roots of $F(x)$ are obtained when one omits all the roots of the polynomials $F(x)\times\Phi_i(x)^{-1}$ and a common argument in number theory shows that

$$\begin{aligned} N_F &= p^m - \sum_i p^{m-m_i} + \sum_{i,j} p^{m-m_i-m_j} + \cdots \\ &= p^m\left(1-\frac{1}{p^{m_1}}\right)\cdots\left(1-\frac{1}{p^{m_r}}\right) \end{aligned} \tag{19}$$

represents the number of primitive roots.

The expression (19) can also be interpreted in a different way. Let $f(x)$ be the polynomial corresponding to $F(x)$; then according to (18)

$$f(x) = \phi_1(x)^{e_1}\cdots\phi_r(x)^{e_r} \tag{20}$$

* See for instance A. Arwin, *Über Kongruenzen von dem fünften und höheren Graden nach einem Primzahlmodulus*, Arkiv för Matematik, Astronomi och Fysik, vol. 14 (1918).

is the prime polynomial decomposition of $f(x)$. Now let $\Phi(f(x))$ denote the number of residues (modd $p, f(x)$) which are relatively prime to $f(x)$; one finds then for this generalized Φ-function exactly the expression (19). This gives

THEOREM 11. *When the p-polynomial $F(x)$ with the corresponding polynomial $f(x)$ has the symbolic prime function decomposition* (18), *then $F(x)$ has exactly*

$$\Phi(f(x)) = p^m\left(1 - \frac{1}{p^{m_1}}\right) \cdots \left(1 - \frac{1}{p^{m_r}}\right) \tag{21}$$

primitive roots; here the m_i denote the exponents of the different prime factors of $F(x)$.

This theorem permits a series of applications. It shows the following, first of all:

There exist primitive roots for all p-polynomials.

Furthermore:

The number of irreducible polynomials belonging to $F(x)$ is $(1/N)\Phi(f(x))$, where N is the index of $F(x)$.

Since there always exist prime functions of degree N dividing $F(x)$, it follows that every p-polynomial has the following property in common with $x^{p^N} - x$:

The degrees of the ordinary irreducible factors of a p-polynomial always divide the degree of the prime divisor of highest degree.

Since every p-modulus M_p forms the set of roots of a p-polynomial $F(x)$, and since $F(x)$ has primitive roots, it follows that M_p can be generated in the form (15) by a primitive root of $F(x)$. This gives the proof of Theorem 7:

Every p-modulus is simple.

An important special case is the case where the p-modulus is a finite field with p^n elements; the corresponding p-polynomial is then $x^{p^n} - x$. Theorem 11 shows that there exist $\Phi(x^n - 1)$ numbers μ such that every element can be represented in the form

$$\omega = a_0\mu + a_1\mu^p + \cdots + a_{n-1}\mu^{p^{n-1}}.$$

We have therefore proved

THEOREM 12. *In a finite field of degree n there exist $(1/n)\Phi(x^n - 1)$ different bases consisting of conjugate elements:*

$$\mu, \mu^p, \cdots, \mu^{p^{n-1}}.$$

Theorem 12 gives the answer to a problem proposed already by Eisenstein*, and partly solved by Schönemann.† The first complete solution was given by Hensel‡; it should also be observed that the existence of such a basis is a consequence of a much more general theorem by Noether and Deuring§, proving the existence of a basis consisting of conjugate elements for an arbitrary Galois field.

5. **Symbolic multiplication.** Let $F(x)$ be a p-polynomial with the exponent $n, f(x)$ the corresponding polynomial and M_p the p-modulus of the roots. All elements of M_p are then of the form

$$Q(\mu) = a_0\mu + \cdots + a_{n-1}\mu^{p^{n-1}} \tag{22}$$

where μ is a primitive root. The number $Q(\mu)$ belongs to some divisor $F_1(x)$ of $F(x)$ and this divisor can easily be found. If namely $F(x) = F_1(x) \times F_2(x)$ and $F_1(Q(\mu)) = 0$, then one must have $F_1(x) \times Q(x) \equiv 0 \pmod{F(x)}$ or $Q(x) \equiv 0 \pmod{F_2(x)}$, and one finds

THEOREM 13. *When $F_1(x) \times F_2(x) = F(x)$, then an element* (22) *in M_p belongs to $F_1(x)$ if and only if*

$$Q(x) = Q_1(x) \times F_2(x),$$

where $Q_1(x)$ is relatively prime to $F_1(x)$.

The primitive elements of M_p consequently consist of those $Q(\mu)$ for which $Q(x)$ is relatively prime to $F(x)$.

The existence of a primitive element also permits us to introduce a symbolic multiplication in a p-modulus and make the p-modulus a ring; and this can even be done in several ways. Let μ as formerly be a primitive element; to define the product of two elements

$$\alpha = A(\mu), \qquad \beta = B(\mu),$$

we put

$$\alpha \times \beta = \beta \times \alpha = [A(x) \times B(x)]_{x=\mu}. \tag{23}$$

This product is associative, distributive and commutative; it should be observed that the definition (23) depends essentially upon the choice of the primitive element μ, because μ must be the unit element of the symbolic mul-

* G. Eisenstein, *Über irreduzible Kongruenzen*, Journal für Mathematik, vol. 39 (1850), p. 182.

† Schönemann, *Über einige von Herrn Dr. Eisenstein aufgestellte Lehrsätze* etc., Journal für Mathematik, vol. 40 (1850), pp. 185–187.

‡ K. Hensel, *Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*, Journal für Mathematik, vol. 103 (1888), pp. 230–237.

§ M. Deuring, *Galoissche Theorie und Darstellungstheorie*, Mathematische Annalen, vol. 107 (1932), pp. 140–144.

tiplication. The *ring* M_p defined by a particular μ is seen to be isomorphic to the ring of all residue-classes (mod $f(x)$), where $f(x)$ is the polynomial corresponding to $F(x)$; M_p is a *field* only when $F(x)$ is symbolically *irreducible.* When applied to a finite field, one obtains in particular

THEOREM 14. *Let μ be a primitive element in a finite field K_μ, such that the conjugates of μ form a basis. Each element in K_μ is then a p-polynomial in μ and the symbolic multiplication of these p-polynomials introduces a new definition of multiplication in K_μ. With regard to this multiplication K_μ is a ring isomorphic to the ring of residue-classes for the double modulus* (modd p, x^n-1).

Now let $F(x)$ be a p-polynomial with the symbolic prime polynomial decomposition

$$F(x) = \Phi_1(x)^{(e_1)} \times \cdots \times \Phi_r(x)^{(e_r)} \tag{24}$$

and let us put

$$A_i(x) = F(x) \times \Phi_i(x)^{(-e_i)} \qquad (i = 1, 2, \cdots, r).$$

The primitive roots of $\Phi_i(x)^{(e_i)}=0$ are then $Q_i(\mu)\times A_i(\mu)$, where $Q_i(x)$ is not divisible by $\Phi_i(x)$, and where μ as before denotes a primitive root of $F(x)=0$. Every root ω of $F(x)$ is representable uniquely in the form

$$\omega = \sum_{i=1}^{r} R_i(\mu) \times A_i(\mu),$$

where the degree of $R_i(x)$ is smaller than the degree of $\Phi_i(x)^{(e_i)}$. This shows that each root is uniquely representable in the form

$$\omega = \mu_1 + \mu_2 + \cdots + \mu_r,$$

where μ_i is a root of

$$\Phi_i(x)^{(e_i)} = 0. \tag{25}$$

The root ω is primitive if and only if all μ_i are primitive roots of their corresponding equations (25).

Now let

$$G(x) = \Phi_1(x)^{(f_1)} \times \cdots \times \Phi_r(x)^{(f_r)} \tag{26}$$

be a second p-polynomial and

$$\nu = \nu_1 + \nu_2 + \cdots + \nu_r, \qquad \Phi_i(\nu_i)^{(f_i)} = 0,$$

the representation of one of its primitive roots. The number

$$\mu \pm \nu = (\mu_1 \pm \nu_1) + \cdots + (\mu_r \pm \nu_r)$$

is then a root of the union $[F(x), G(x)]$. When for an index i we have $e_i > f_i$, then the element $\lambda_i = \mu_i \pm \nu_i$ is a primitive root of $\Phi_i(x)^{(e_i)} = 0$ as one easily sees, and correspondingly for $f_i > e_i$. When $e_i = f_i$ it may happen, however, that λ_i is not a primitive root, but when $p \neq 2$ it is always possible even to a fixed μ_i to choose a ν_i such that λ_i is a primitive root, for instance $\nu_i = \pm\mu_i$. When $p = 2$ and $\Phi_i(x)$ has the exponent 1, one finds that no primitive root ν_i with the property indicated exists.

THEOREM 15. *Let $F(x)$ be two p-polynomials with the symbolic prime polynomial decompositions* (24) *and* (26), *and let μ and ν be two primitive roots. When for all i $e_i \neq f_i$, then $\lambda = \mu \pm \nu$ is a primitive root of the least common multiple $[F(x), G(x)]$. If $e_i = f_i$ for some i and $p \neq 2$, one can always to every primitive μ find a primitive ν such that λ is a primitive root of the union.*

6. p^f-polynomials. We shall finally make a slight generalization of the former theory by considering p^f-polynomials

$$F(x) = \alpha_0 x^{p^{fn}} + \alpha_1 x^{p^{f(n-1)}} + \cdots + \alpha_{n-1} x^{p^f} + \alpha_n x,$$

where the coefficients α_i are elements of a finite field K_f of degree f. The polynomial corresponding to $F(x)$ is

$$F(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n.$$

One can define the symbolic multiplication by substitution as in §1, and one finds that the symbolic multiplication is commutative and that the polynomial corresponding to a symbolic product is equal to the product of the corresponding factors; Theorems 2 and 3 also hold without change.

The decomposition of

$$x^{p^{fn}} - x$$

into p^f-factors corresponds uniquely to the decomposition of $x^n - 1$ into irreducible factors in K_f.

The roots of a p^f-polynomial form a *p^f-modulus*, i.e., a modulus with the following properties:

1. When μ belongs to M_{p^f}, then $\alpha\mu$ also belongs for all elements α of K_f.
2. When μ belongs to M_{p^f}, then μ^{p^f} also belongs. Every p^f-modulus forms the set of roots of a p^f-polynomial.

One finds that every polynomial with coefficients in K_f belongs to a p^f-polynomial. The smallest exponent N such that $F(x)$ divides

$$x^{p^{fN}} - x$$

is called the index of $F(x)$, and Theorem 10 will hold unchanged. One can then prove the existence of primitive roots for a p^f-polynomial and obtain

similar formulas for their number. It follows that every p^f-modulus is simple and can be represented in the form

$$M_{p^f} = \alpha_0\mu + \alpha_1\mu^{p^f} + \cdots + \alpha_{n-1}\mu^{p^{f(n-1)}}.$$

When applied to a finite field of degree ff' this gives

THEOREM 16. *In a finite field $K_{ff'}$ of degree ff' one can always find bases with respect to K_f consisting of conjugate elements*

$$\mu, \mu^{p^f}, \cdots, \mu^{p^{f(f'-1)}}.$$

The analogue of Theorem 15 can easily be deduced.

CHAPTER II. DECOMPOSITION THEOREMS

1. **Identities for $x^{p^n}-x$.** Let $F(x)$ and $G(x)$ be two p-polynomials, and let α be an arbitrary root of $F(x)=0$ and β an arbitrary root of $G(x)=0$. From the definition of the symbolic multiplication it follows that the following identities must hold:

$$F(x) \times G(x) = \prod_\beta (F(x) - \beta) = \prod_\alpha (G(x) - \alpha). \tag{1}$$

This simple remark gives, when applied to $x^{p^n}-x$,

THEOREM 1. *Let $f(x)$ and $g(x)$ be two complementary divisors of x^n-1 such that*

$$x^n - 1 = f(x)g(x), \tag{2}$$

and let $F(x)$ and $G(x)$ be the corresponding p-polynomials. Then

$$x^{p^n} - x = \prod_\beta (F(x) - \beta) = \prod_\alpha (G(x) - \alpha) \tag{3}$$

where α runs through all the roots of $F(x)=0$ and β through all the roots of $G(x)=0$.

Using p^f-polynomials one obtains a similar theorem for the decomposition of $x^{p^{fn}}-x$. Since x^n-1 always has the two factors

$$f(x) = x^{n-1} + \cdots + x + 1, \qquad g(x) = x - 1,$$

one obtains as a special case of the decomposition (3) the decompositions given by Mathieu*:

---

* E. Mathieu, *Mémoire sur l'étude de fonctions de plusieurs quantités* etc., Journal de Mathématiques, (2), vol. 6 (1861), pp. 241–323.

$$
\begin{aligned}
x^{p^n} - x &= \prod_{a=0}^{p-1} (x^{p^{n-1}} + \cdots + x^p + x + a) \\
&= \prod_{\beta} (x^p - x - \beta),
\end{aligned} \tag{4}
$$

where β runs through all solutions of

$$x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x^p + x = 0. \tag{5}$$

When p^f-polynomials are applied one obtains

$$
\begin{aligned}
x^{p^{fn}} - x &= \prod_{\alpha} (x^{p^{f(n-1)}} + \cdots + x^{p^f} + x + \alpha) \\
&= \prod_{\beta} (x^{p^f} - x - \beta),
\end{aligned} \tag{6}
$$

where α runs through all elements of K_f, while β runs through the roots of

$$x^{p^{f(n-1)}} + x^{p^{f(n-2)}} + \cdots + x^{p^f} + x = 0. \tag{7}$$

The significance of the conditions (5) and (7) is seen to be the following: When β is a root of (7) it is an element of the finite field K_{nf} of relative degree n with respect to K_f, and it therefore satisfies an irreducible equation in K_f of degree n_β, where n_β divides n. When $\alpha_1^{(\beta)}$ denotes the coefficient of $x^{n_\beta - 1}$ in this equation, one finds

$$\beta^{p^{f(n-1)}} + \cdots + \beta^{p^f} + \beta = -\frac{n}{n_\beta}\alpha_1^{(\beta)},$$

and the condition (7) is equivalent to

$$\frac{n}{n_\beta}\alpha_1^{(\beta)} \equiv 0 \pmod{p}, \tag{8}$$

or simply $\alpha_1^{(\beta)} \equiv 0 \pmod{p}$ when n is not divisible by p.

2. **Decomposition theorems.** The object of the following considerations is to give a method to determine the prime polynomials belonging to a product $F(x) = F_1(x) \times F_2(x)$ of two p^f-polynomials, when the prime factors of $F_1(x)$ and $F_2(x)$ are known. According to (1) we have the decomposition

$$F(x) = \prod_{\alpha_2} (F_1(x) - \alpha_2) = \prod_{\alpha_1} (F_2(x) - \alpha_1), \tag{9}$$

where α_1 and α_2 run through the roots of $F_1(x) = 0$ and $F_2(x) = 0$ respectively. Each root of $F(x)$ then satisfies an equation

$$F_2(x) = \alpha_1. \tag{10}$$

We shall determine all equations (10) satisfied by primitive roots of $F(x)$;

first, it is obvious that a primitive root can only satisfy (10) when α_1 is a primitive root of $F_1(x)$. Next let μ be a primitive root of $F(x)$; then according to Theorem 16, α_1 must have the form $\alpha_1 = Q(\mu) \times F_2(\mu)$, where $Q(x)$ is relatively prime to $F_1(x)$; when $R(\mu)$ denotes an arbitrary root of (10), then one obtains

$$F_2(x) \times (R(x) - Q(x)) \equiv 0 \qquad (\text{mod } F(x))$$

or

$$R(x) = Q(x) - K(x) \times F_1(x). \tag{11}$$

The relation (11) gives the general form of a root of (10), including also the case where α_1 is not a primitive root of $F_1(x)$.

Let us next write

$$F_1(x) = G_1(x) \times D_1(x), \qquad F_2(x) = G_2(x) \times D_2(x), \tag{12}$$

where $G_1(x)$ and $G_2(x)$ are relatively prime and $D_1(x)$ and $D_2(x)$ contain only prime factors which are common to $F_1(x)$ and $F_2(x)$. When $Q(x)$ is relatively prime to $F_1(x)$ it follows from (11) that any common factor of $R(x)$ and $F(x)$ must be a divisor $\overline{G}_2(x)$ of $G_2(x)$, and this shows that every root of (10) belongs to a polynomial

$$\overline{\overline{G}}_2(x) \times D_2(x) \times F_1(x), \tag{13}$$

where $G_2(x) = \overline{\overline{G}}_2(x) \times \overline{G}_2(x)$.

In order to determine the exact number of roots of (10) belonging to a given polynomial (13), we observe that $R(x)$ must be of the form $R_1(x) \times \overline{G}_2(x)$, where $R_1(x)$ is relatively prime to (13); comparing this with (11) one finds

$$R_1(x) \times \overline{G}_2(x) + K(x) \times F_1(x) = Q(x) \tag{14}$$

and our problem is equivalent to the determination of the number of solutions $R_1(x)$ of degree less than the degree of (13) and relatively prime to this polynomial, i.e., relatively prime to $\overline{\overline{G}}_2(x)$ since no solution of (14) can have a factor in common with $F_1(x)$. Since $\overline{G}_2(x)$ is relatively prime to $F_1(x)$, it follows that (14) has a special solution $R_1^{(0)}(x)$ such that the general solution is

$$R_1(x) = R_1^{(0)}(x) + M(x) \times F_1(x), \tag{15}$$

where $M(x)$ is an arbitrary polynomial whose degree is smaller than the degree of $\overline{\overline{G}}_2(x) \times D_2(x)$. The total number of polynomials $M(x)$ is then p^{f^*}, where $f^* = f(\overline{\overline{g}}_2 + d_2)$ and where $\overline{\overline{g}}_2$ and d_2 are the exponents of $\overline{\overline{G}}_2(x)$ and $D_2(x)$. One finds by the usual argument in number theory that the number of solutions of (15) which are relatively prime to $\overline{\overline{G}}_2(x)$ will be

$$N = p^{fd_2}\Phi(\bar{\bar{g}}_2(x)), \tag{16}$$

where $\bar{g}_2(x)$ is the polynomial corresponding to $\bar{\bar{G}}_2(x)$ and Φ is the generalized Euler function introduced in §4, chapter 1. A well known property of the Φ-function shows that the sum of all numbers (16) taken over all divisors $\bar{g}_2(x)$ of $g_2(x)$ is equal to the degree of $F_2(x)$ as one should expect.

THEOREM 2. *Let $F(x)=F_1(x)\times F_2(x)$ be the product of two p^f-polynomials and*

$$F(x) = \prod_{\alpha_1} (F_2(x) - \alpha_1)$$

the corresponding decomposition, where α_1 runs through all roots of $F_1(x)$. The primitive roots of $F(x)$ are roots of the equations

$$F_2(x) = \alpha_1, \tag{17}$$

where α_1 runs through the primitive roots of $F_1(x)$. When

$$F_1(x) = G_1(x) \times D_1(x), \qquad F_2(x) = G_2(x) \times D_2(x),$$

where $D_1(x)$ and $D_2(x)$ contain the prime factors which are common to $F_1(x)$ and $F_2(x)$, then every root of (17) *belongs to a polynomial*

$$\bar{D}(x) \times D_2(x) \times F_1(x), \tag{18}$$

where $\bar{D}(x)$ is a divisor of $G_2(x)$. The exact number of roots belonging to a given polynomial (18) *is*

$$N(\bar{D}) = p^{fd_2}\Phi(\bar{d}(x)), \tag{19}$$

where d_2 is the exponent of $D_2(x)$ and $\bar{d}(x)$ the polynomial corresponding to $\bar{D}(x)$.

This theorem shows, in particular, that the number of roots of the various categories of an equation (17) is the same for all primitive α_1 and the number of primitive roots is $p^{fd_2}\Phi(g_2(x))$, where $g_2(x)$ is the polynomial corresponding to $G_2(x)$.

Instead of considering (17) one could have determined the primitive roots of $F(x)$ as a root of an equation

$$F_1(x) = \alpha_2. \tag{20}$$

The common roots of two equations (20) and (17) can be obtained in the following manner: one can write α_2 in the symbolic form $\alpha_2=Q_1(\mu)\times F_1(\mu)$ and one finds as in (11) that the general root of (20) has the form

$$R_1(x) = Q_1(x) - L(x) \times F_2(x). \tag{21}$$

The comparison of (21) with (11) shows that in case of a common root the polynomials $K(x)$ and $L(x)$ must satisfy the condition

$$Q(x) - Q_1(x) = K(x) \times F_1(x) - L(x) \times F_2(x). \tag{22}$$

This equation is solvable if and only if

$$Q(x) \equiv Q_1(x) \pmod{T(x)}, \tag{23}$$

where $T(x)$ is the greatest common factor of $F_1(x)$ and $F_2(x)$; when the condition (23) is satisfied, one obtains exactly p^{ft} common solutions from (22), where t denotes the exponent of $T(x)$. A special case of particular importance is the following:

THEOREM 3. *Let $F_1(x)$ and $F_2(x)$ be two p^f-polynomials without common factor; the equations*

$$F_1(x) = \alpha_2, \qquad F_2(x) = \alpha_1, \tag{24}$$

where α_1 is a root of $F_1(x)$ and α_2 is a root of $F_2(x)$, have then exactly one root in common.

The common root can be found from (22); when α_1 is a primitive root of $F_1(x)$ and α_2 is a primitive root of $F_2(x)$, then the common root μ in (24) is a primitive root of $F(x) = F_1(x) \times F_2(x)$, and this remark gives a simple method for determining all primitive roots of $F(x)$.

3. **Applications.** The theorems derived in §2 have a number of applications. Let us use the former notation and let $\phi_1(x)$ be an irreducible polynomial in K_f belonging to the p^f-polynomial $F_1(x)$. When α_1 is an arbitrary root of $\phi_1(x)$, then

$$\phi_1(F_2(x)) = (F_2(x) - \alpha_1)(F_2(x) - \alpha_1^{p^f}) \cdots (F_2(x) - \alpha_1^{p^{f(N_1-1)}}), \tag{25}$$

where N_1 is the degree of $\phi_1(x)$. We now join all factors in (9) in the form (25) and Theorem 2 gives the following result:

THEOREM 4. *Let $\phi_1(x)$ be an irreducible polynomial of degree N_1 belonging to the p^f-polynomial $F_1(x)$; let $F_2(x)$ be a second p^f-polynomial and*

$$F_1(x) = G_1(x) \times D_1(x), \qquad F_2(x) = G_2(x) \times D_2(x),$$

where $D_1(x)$ and $D_2(x)$ contain the prime factors common to $F_1(x)$ and $F_2(x)$. The polynomial $\phi_1(F_2(x))$ is then equal to a product of prime polynomials belonging to p^f-polynomials

$$\bar{D}(x) \times D_2(x) \times F_1(x), \tag{26}$$

where $\overline{D}(x)$ is a divisor of $G_2(x)$. The number of prime polynomials belonging to a given polynomial (26) *is*

$$\frac{N_1}{\overline{N}} p^{fd_2}\Phi(\overline{d}(x)),$$

where $\overline{N}$ is the index of (26), *d_2 the exponent of $D_2(x)$ and $\overline{d}(x)$ the polynomial corresponding to $\overline{D}(x)$.*

There are several cases of Theorem 4 which are of special interest. Since all prime factors of $\phi_1(F_2(x))$ belong to a multiple of $F_1(x)$, it is clear that the degrees of all prime polynomials are divisible by N_1. In the case where $F_1(x)$ is relatively prime to $F_2(x)$, all prime factors of $\phi_1(F_2(x))$ belong to some $\overline{D}(x)\times F_1(x)$, where $\overline{D}(x)$ is a divisor of $F_2(x)$ and the number of prime factors belonging to such a given polynomial is simply

$$\frac{N_1}{\overline{N}} \Phi(\overline{d}(x)),$$

where $\overline{N}$ is the index of $\overline{D}(x)\times F_1(x)$. There will be exactly

$$\frac{(N_1, N_2)}{N_2} \Phi(f_2(x))$$

irreducible factors belonging to $F_1(x)\times F_2(x)$, where N_2 is the index of $F_2(x)$, while there will be only one prime polynomial belonging to $F_1(x)$ and dividing $\phi_1(F_2(x))$. The roots of this prime polynomial can easily be obtained from (11).

Theorem 3 gives a surprisingly simple method for determining the prime polynomials belonging to a product of p^f-polynomials when those of the factors are known:

THEOREM 5. *Let $F_1(x)$ be relatively prime to $F_2(x)$ and let $\phi_1(x)$ be a prime polynomial belonging to $F_1(x)$ while $\phi_2(x)$ belongs to $F_2(x)$. The greatest common factor of the two polynomials*

$$\phi_1(F_2(x)), \qquad \phi_2(F_1(x)) \tag{27}$$

is then a prime polynomial belonging to $F_1(x)\times F_2(x)$ and all prime polynomials belonging to the product can be determined in this way.

CHAPTER III. CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS

1. A class of irreducible polynomials. One of the most interesting but also most difficult problems in the theory of higher congruences is the determination of irreducible polynomials of a given degree in explicit form. At the pres-

ent time this problem has only been solved for very special cases, but it is of interest to observe that almost all of the results obtained are closely related to the theory of p^f-polynomials.

Before we illustrate this fact, we shall however use some of the former results to obtain a new class of irreducible polynomials. Let $f(x)$ be an ordinary irreducible polynomial of degree n with coefficients in a finite field K_f. We shall suppose in addition that $f(x)$ is a primitive polynomial, i.e. $p^{fn}-1$ is the smallest exponent such that

$$x^{p^{fn}-1} \equiv 1 \qquad (\text{mod } f(x)).$$

For the p^f-polynomial $F(x)$ corresponding to $f(x)$ one then has symbolically

$$x^{p^f(p^{fn}-1)} - x \equiv 0 \qquad (\text{mod } F(x))$$

and the index of $F(x)$ is $p^{fn}-1$. Theorem 10 then shows that any ordinary prime polynomial $\neq x$ dividing $F(x)$ has the degree $p^{fn}-1$. This gives

THEOREM 1. *When*

$$f(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$$

is an irreducible primitive polynomial in K_f, then

$$\phi(x) = x^{p^{fn}-1} + \alpha_1 x^{p^f(n-1)} + \cdots + \alpha_{n-1} x^{p^f-1} + \alpha_n$$

is an irreducible polynomial in the same field.

A consequence of Theorem 1 is obviously that the polynomial

$$\phi_1(x) = x^{(p^{fn}-1)/(p^f-1)} + \alpha_1 x^{(p^f(n-1)-1)/(p^f-1)} + \cdots + \alpha_{n-1} x + \alpha_n$$

is irreducible.

As an illustration of Theorem 1 we may take $f(x) = x - \alpha$ and we obtain the well known result that

$$\phi(x) = x^{p^f-1} - \alpha$$

is irreducible when α belongs to the exponent p^f-1 and hence

$$\phi(x) = x^\delta - \alpha$$

is also irreducible when δ is any divisor of p^f-1.

2. **Substitution of a prime polynomial.** Our next considerations are based on Theorem 4, chapter 2, and this theorem shall be applied particularly for the case where $F_2(x)$ is an irreducible p-polynomial. We use the former notations, letting N_1 and N_2 be the indices of $F_1(x)$ and $F_2(x)$, while $f_1(x)$ and $f_2(x)$ denote the polynomials corresponding to $F_1(x)$ and $F_2(x)$.

Let us first deal with the case where $F_2(x)$ symbolically divides $F_1(x)$ and $F_1(x)$ contains $F_2(x)$ symbolically e times. Furthermore let $N_1 = p^A N_1'$, where N_1' is not divisible by p. The exponent A is obviously the smallest number such that p^A is not surpassed by any of the exponents occurring in the symbolic prime function decomposition of $F_1(x)$. If now $e+1 \leqq p^A$, then $F_2(x) \times F_1(x)$ still has the index N_1, and when $\phi_1(x)$ is a polynomial belonging to $F_1(x)$ and hence of degree N_1, then according to Theorem 4 $\phi_1(F_2(x))$ decomposes into irreducible factors of degree N_1. If however $e+1 > p^A$, then e is the largest exponent occurring in $F_1(x)$ and the index of $F_1(x) \times F_2(x)$ must be pN_1, and hence $\phi_1(F_2(x))$ decomposes into factors of degree pN_1.

Next let $F_1(x)$ not be divisible by $F_2(x)$. The index of the product $F_1(x) \times F_2(x)$ is

$$[N_1, N_2] = \frac{N_1 N_2}{(N_1, N_2)}$$

and each irreducible factor of $\phi_1(F_2(x))$ will, according to Theorem 4, belong to $F_1(x) \times F_2(x)$ or to $F_1(x)$, and there will be one prime polynomial of degree N_1 belonging to $F_1(x)$ and

$$\frac{(N_1, N_2)}{N_2} \Phi(f_2(x)) = \frac{(N_1, N_2)}{N_2} (p^{f n_2} - 1)$$

polynomials of degree $[N_1, N_2]$ belonging to $F_1(x) \times F_2(x)$, where n_2 denotes the degree of $f_2(x)$.

THEOREM 2. *Let $F_1(x)$ and $F_2(x)$ be two p^f-polynomials with the indices N_1 and N_2; we shall suppose that $F_2(x)$ is symbolically irreducible and that $\phi_1(x)$ is a prime polynomial belonging to $F_1(x)$. When $F_2(x)$ divides $F_1(x)$, then $\phi_1(F_2(x))$ is the product of prime polynomials of degree N_1 except when N_1 is divisible exactly by p^A and $F_1(x)$ contains $F_2(x)$ to the same power p^A; then $\phi_1(F_2(x))$ is the product of prime polynomials of degree pN_1.*

When $F_2(x)$ does not divide $F_1(x)$, then $\phi_1(F_2(x))$ contains one prime factor of degree N_1, while the remaining factors have the degree $[N_1, N_2]$.

3. Prime polynomials whose degrees are divisible by p. We shall now apply the first part of Theorem 2 to obtain various irreducible polynomials whose degrees are divisible by p. We shall suppose for the moment that all polynomials have rational coefficients, and we put

$$F_2(x) = x^p - ax, \qquad a^d = 1,$$

where the exponent d of a divides $p-1$ and is identical with the index of $F_2(x)$. Since we shall suppose that $F_1(x)$ is divisible by $x^p - ax$, we must have

$x^{N_1}-1$ divisible by $x-a$, which in turn shows that $N_1 \equiv 0 \pmod{d}$. To insure that the exceptional case of Theorem 2 occurs, we shall have to suppose furthermore that $F_1(x)$ divides $x^{pN_1}-x$ but not

$$(x^{pN_1} - x) \times (x^p - ax)^{-1} = x^{pN_1-1} + ax^{pN_1-2} + \cdots + a^{N_1-1}x.$$

This shows

THEOREM 3. *Let a be a rational integer belonging to the exponent d and $\phi(x)$ a prime polynomial of degree N divisible by d. Then $\phi(x^p-ax)$ is a prime polynomial of degree pN, when $\phi(x)$ does not divide*

$$x^{pN-1} + ax^{pN-2} + \cdots + a^{N-1}x.$$

When $a=1$, then $d=1$ and the last condition of Theorem 3 is equivalent to $a_1 \neq 0$, where a_1 is the coefficient of x^{N-1} in $\phi(x)$. This gives the following well known result:

When $\phi(x)$ is a prime polynomial of degree N in which the coefficient of x^{N-1} does not vanish, then $\phi(x^p-x)$ is a prime polynomial of degree pN.

When applied to $\phi(x)=x+a$, this shows that

$$x^p - x + a, \qquad a \neq 0,$$

is irreducible. I observe without proof that Theorem 3 can be modified to hold in an arbitrary field K_f.

We shall also make an application of the first part of Theorem 2 to obtain in a simple way the results of Serret* and Dickson† on prime polynomials in a field K_f, whose degrees are powers of p. Let us denote by $\Pi_r(x)$ the product of r equal symbolic factors $x^{p^f}-x$

$$(1) \qquad \Pi_r(x) = (x^{p^f} - x)^{(r)} = x^{p^f r} - \binom{r}{1} x^{p^f(r-1)} + \cdots + (-1)^r x.$$

For $r=p^n$ one obtains simply

$$(2) \qquad \Pi_{p^n}(x) = x^{p^f p^n} - x.$$

The polynomial corresponding to $\Pi_r(x)$ is $(x-1)^r$ and all symbolic divisors of $\Pi_{p^n}(x)$ are of the form $\Pi_r(x)$. Since a prime polynomial of degree p^n must divide (2) every prime polynomial having this degree must belong to a unique polynomial

$$\Pi_r(x) \qquad (r = p^{n-1}+1, p^{n-1}+2, \cdots, p^n).$$

---

* See Serret, *Cours d'Algèbre.*

† See Dickson, *Linear Groups.*

In this way one obtains a division of all prime polynomials of degree p^n into p^n-p^{n-1} classes. The class corresponding to $r=p^{n-1}+1$ shall be called the *first class* and the class corresponding to $r=p^n$ the *last class of degree* p^n. Since

$$\Pi_r(x) = \Pi_{r-1}(x) \times (x^{p^f} - x) = \Pi_{r-1}(x)^{p^f} - \Pi_{r-1}(x),$$

and since all polynomials dividing, but not belonging to, $\Pi_r(x)$ must divide $\Pi_{r-1}(x)$, it follows that

$$\Gamma_r(x) = \Pi_{r-1}(x)^{p^f-1} - 1 = \prod_\alpha \Big(\Pi_{r-1}(x) - \alpha \Big),$$

where $\alpha \neq 0$ runs through all of the elements of K_f, represents the product of all prime polynomials belonging to $\Pi_r(x)$. The first part of Theorem 2 gives immediately

THEOREM 4. *When $\phi(x)$ is a prime polynomial of degree p^n belonging to the class ρ, then $\phi(x^{p^f}-x)$ is the product of p^f different prime polynomials of the class $\rho+1$ except in the case where $\phi(x)$ belongs to the last class of degree p^n, when $\phi(x^{p^f}-x)$ is the product of p^{f-1} prime polynomials of the first class of degree p^{n+1}.*

4. **Further applications.** The second part of Theorem 2 may also be used to obtain results on irreducible polynomials. We saw that, with the same notation as before, $\phi_1(F_2(x))$ contains one irreducible polynomial of degree N_1 belonging to $F_1(x)$ and

$$T = \frac{(N_1, N_2)}{N_2}(p^{fn_2} - 1)$$

irreducible polynomials of degree $[N_1, N_2]$ belonging to $F_1(x) \times F_2(x)$. We see that $T=1$ only when the indices N_1 and N_2 are relatively prime and $N_2=p^{fn_2}-1$. We can then write $\phi_1(F_2(x))=\lambda(x)\cdot\mu(x)$ where $\lambda(x)$ has the degree N_1N_2 and $\mu(x)$ divides $F_1(x)$. Hence we can write

$$\mu(x) = (\phi_1(F_2(x)), F_1(x))$$

and this gives the following: *Let $f_2(x)$ be an irreducible primitive polynomial of degree n_2 and let $f_1(x)$ be an arbitrary polynomial belonging to the exponent N_1, where $(N_1, p^{fn_2}-1)=1$. When $F_1(x)$ and $F_2(x)$ are the corresponding p^f-polynomials and $\phi_1(x)$ a prime polynomial belonging to $F_1(x)$, then*

$$\lambda(x) = \frac{\phi_1(F_2(x))}{(\phi_1(F_2(x)), F_1(x))}$$

is a prime polynomial of degree $N_1(p^{fn_2}-1)$. It may be observed that this

result contains Theorem 1 for $F_1(x)=x$. We shall give a further application to the case where

$$F_1(x) = x^p - x.$$

One then has $N_1=1$ and $\phi_1(x)=x-\alpha$. Let us suppose

$$F_2(x) = x^{p^{fn}} + \beta_1 x^{p^{f(n-1)}} + \cdots + \beta_n x,$$

and hence

$$\phi_1(F_2(x)) = x^{p^{fn}} + \beta_1 x^{p^{f(n-1)}} + \cdots + \beta_n x - \alpha.$$

According to the general result this polynomial must contain a linear factor $x-\gamma$ and we find

$$\gamma = \frac{\alpha}{1+\beta_1+\cdots+\beta_n}.$$

THEOREM 5. *Let $f(x)$ be an irreducible primitive polynomial of degree n and let $F(x)$ be the corresponding p^f-polynomial. Then*

$$\psi(x) = \frac{F(x)-\alpha}{x - \dfrac{\alpha}{F(1)}}$$

is an irreducible polynomial of degree $p^{fn}-1$.

This theorem may be considered as a restatement of Theorem 1.

5. **Decompositions of p^f-polynomials.** We shall now give the complete decomposition into prime factors of a few simple p^f-polynomials, thus also illustrating the general theorems.

1. In the simplest case

$$F(x) = x^p - \alpha x,$$

let δ be the smallest exponent such that $\alpha^\delta=1$. The index of $F(x)$ is δ and one finds the prime polynomial decomposition

$$F(x) = x \prod_\beta (x^\delta - \beta),$$

where β runs through all of the roots of

$$\beta^{(p^f-1)/\delta} = \alpha.$$

2. When

$$F(x) = (x^{p^f} - x) \times (x^p - x)$$

the irreducible factors must have the degrees 1 and p, and since

$$F(x) = \prod_{\alpha} (x^{p^f} - x - \alpha),$$

where α runs through all of the elements of K_f, it is sufficient to decompose the factors of this product. One finds

$$x^{p^f} - x - \alpha = \prod_{\beta} (x^p - \alpha^{p-1}x - \beta), \quad \alpha \neq 0,$$

where $\beta\alpha^{-p}$ runs through all solutions of

$$x^{p^{f-1}} + \cdots + x^p + x = 1.$$

One can also show that

$$f(x) = x^p - \alpha^{p-1}x - \beta$$

is reducible if and only if $\beta\alpha^{-p}$ satisfies

$$x^{p^{f-1}} + \cdots + x^p + x = 0.$$

3. In the case

$$F(x) = (x^{p^f} - \alpha x) \times (x^{p^f} - x), \quad \alpha^\delta = 1,$$

it follows from the general theory that the irreducible factors are of degree 1 and δ. One obtains

$$F(x) = \prod_{\beta} (x^{p^f} - \alpha x - \beta),$$

and putting $\sigma = \beta/(1-\alpha)$ one finds

$$x^{p^f} - \alpha x - \beta = (x - \sigma) \prod_{\gamma} ((x - \sigma)^\delta - \gamma),$$

where γ runs through all solutions of

$$\gamma^{(p^f-1)/\delta} = \alpha.$$

At this point it may be of interest to determine the decomposition of a polynomial

$$f(x) = x^p - \alpha x - \beta.$$

This problem occurs in connection with the determination of prime ideal decompositions in relative Kummer fields. The number

$$a = \alpha^{(p^f-1)/(p-1)}$$

is rational and we can suppose $a \neq 1$ since this case has been treated under 2. One finds that $f(x)$ has the root

$$\sigma = \frac{1}{1-a}\sum_{i=1}^{f}\beta^{p^f-i}\alpha^{(p^f-p^{f-i+1})/(p-1)}$$

in K_f and consequently

$$x^p - \alpha x - \beta = (x-\sigma)\prod_{\lambda}((x-\sigma)^{\Delta} - \lambda),$$

where

$$\alpha^{\delta} = 1, \qquad \Delta = \left(\frac{p^f-1}{\delta}, p-1\right), \qquad \lambda^{(p-1)/\Delta} = \alpha.$$

6. **Irreducible polynomials and linear substitutions.** Now let

$$F(x) = x^{p^{2f}} + \alpha x^{p^f} + \beta x \tag{3}$$

be a p^f-polynomial whose corresponding polynomial

$$f(x) = x^2 + \alpha x + \beta \tag{4}$$

is irreducible in K_f. In order to study the prime polynomial decomposition of $F(x)$ we put $t = x^{p^f-1}$ and obtain

$$\Phi(t) = F(x)\cdot x^{-1} = x^{p^{2f}-1} + \alpha x^{p^f-1} + \beta = t^{p^f+1} + \alpha t + \beta. \tag{5}$$

Any root of $\Phi(t)$ must satisfy the relation

$$t^{p^f} = -\alpha - \frac{\beta}{t},$$

and so we are naturally led to the study of irreducible polynomials whose roots are connected by linear substitutions

$$x^{p^f} = \frac{\alpha x + \beta}{\gamma x + \delta}. \tag{6}$$

Such prime polynomials are obviously divisors of

$$\Psi(x) = \gamma x^{p^f+1} + \delta x^{p^f} - \alpha x - \beta. \tag{7}$$

In (6) and (7) we can always assume $\gamma \neq 0$ since the polynomials

$$x^{p^f} + \lambda x + \mu \tag{8}$$

have been completely decomposed in Nos. 2 and 3 of the preceding section. We are also mainly interested in the case where the linear substitution (6) leaves no element of K_f unchanged. We suppose then that the equation

$$x = \frac{\alpha x + \beta}{\gamma x + \delta}$$

has no solution in K_f and this is equivalent to the statement that the equation

$$\psi(x) = \gamma x^2 + (\delta - \alpha)x - \beta = 0 \tag{9}$$

is irreducible in K_f.

If namely $\psi(x)$ in (9) has the root ρ in K_f, then $\Psi(x)$ in (7) also has the root ρ and one finds after putting $y = x - \rho$

$$\Psi(x) = \gamma y \cdot \left[y^{p^f} + \left(\rho + \frac{\delta}{\gamma}\right) y^{p^f - 1} + \rho - \frac{\alpha}{\gamma} \right].$$

The second factor in this product is again of the type (8) when z is substituted for $1/y$.

We suppose, then, that (9) is irreducible and has the two roots ψ_1 and ψ_2. This corresponds in our first special case to the assumption that the polynomial (4) is irreducible. In this case $\Psi(x)$ has no linear factors.

From (6) one obtains through iteration

$$x^{p^{fn}} = \frac{\alpha_n x + \beta_n}{\gamma_n x + \delta_n} \tag{10}$$

and one verifies that the coefficients of this substitution are given by*

$$\begin{aligned} (\omega_1 - \omega_2)\alpha_n &= (\alpha - \omega_2)\omega_1^n - (\alpha - \omega_1)\omega_2^n, \\ (\omega_1 - \omega_2)\beta_n &= \beta(\omega_1^n - \omega_2^n), \\ (\omega_1 - \omega_2)\gamma_n &= \gamma(\omega_1^n - \omega_2^n), \\ (\omega_1 - \omega_2)\delta_n &= (\omega_1 - \alpha)\omega_1^n - (\omega_2 - \alpha)\omega_2^n, \end{aligned} \tag{11}$$

where ω_1 and ω_2 are the roots of

$$\omega(x) = x^2 - (\alpha + \delta)x + \alpha\delta - \beta\gamma = 0 \tag{12}$$

and hence

$$\omega_1 = \gamma\psi_1 + \delta, \qquad \omega_2 = \gamma\psi_2 + \delta.$$

Now let n be the degree of an irreducible factor of $\Psi(x)$. Then n is the smallest number such that the roots of the factor satisfy the equation

$$x^{p^{fn}} = x = \frac{\alpha_n x + \beta_n}{\gamma_n x + \delta_n}. \tag{13}$$

If $\gamma_n \neq 0$ one finds that a solution ρ of (13) is also a solution of (9), and since

* These expressions were given by Serret, *Sur les fonctions rationnelles linéaires prises suivant un module premier* etc., Comptes Rendus, Paris, vol. 48 (1859), pp. 112–117.

such a root cannot be a root of $\Psi(x)$, we shall have to suppose $\gamma_n = 0$ and hence according to (11)

$$\omega_1^n = \omega_2^n. \tag{14}$$

In this case one obtains from (11) that the right-hand side of (10) reduces to x and it follows that the degree of any factor of $\Psi(x)$ is the smallest exponent such that (14) is satisfied. Since the number $\omega_1/\omega_2 = \phi_1$ is a root of the congruence

$$\phi(x) = x^2 + \left(\frac{(\alpha+\delta)^2}{\beta\gamma - \alpha\delta} + 2\right)x + 1 \tag{15}$$

and since the irreducibility of (9) follows from the irreducibility of (15), we conclude:

THEOREM 6. *Let*

$$\Psi(x) = \gamma x^{p^f+1} + \delta x^{p^f} - \alpha x - \beta, \qquad \gamma \neq 0,$$

be a polynomial with coefficients in K_f chosen such that the polynomial

$$\phi(x) = x^2 + \left(\frac{(\alpha+\delta)^2}{\beta\gamma + \alpha\delta} + 2\right)x + 1$$

is irreducible in K_f. When $\phi(x)$ belongs to the exponent n, then $\Psi(x)$ is the product of $(p^f+1)/n$ irreducible factors of degree n, and when $\phi(x)$ belongs to the maximal exponent p^f+1, $\Psi(x)$ is irreducible.

It is also possible to give the complete prime polynomial decomposition of $\Psi(x)$ and hence to exhibit explicitly irreducible polynomials having a degree equal to an arbitrary divisor of p^f+1. One finds, namely, that $\Psi(x)$ may be brought into the form

$$\Psi(x) = \alpha_1(x - \psi_1)^{p^f+1} + \alpha_2(x - \psi_2)^{p^f+1}, \tag{16}$$

where ψ_1 and ψ_2 as formerly denote the roots of (9), while $-\alpha_1/\alpha_2$ is a root ϕ_1 of (15). From (16) we obtain the decomposition

$$\Psi(x) = \prod_i \left(\rho_1^{(i)}(x - \psi_1)^n + \rho_2^{(i)}(x - \psi_2)^n\right) \tag{17}$$

where $\rho_1^{(i)}$ and $\rho_2^{(i)}$ are two conjugate elements in the field K_{2f} such that the quotient $-\rho_2^{(i)}/\rho_1^{(i)}$ runs through all $m = (p^f+1)/n$ solutions of the equation

$$x^m = \phi_1. \tag{18}$$

The actual determination of the roots of (18) may be done in the following way. Any solution can be represented in the form

$$\kappa = (r + \omega_2)/(r + \omega_1)$$

and the equation (18) takes the symmetric form

$$\omega_1(r + \omega_1)^m = \omega_2(r + \omega_2)^m. \tag{19}$$

If we suppose $p \neq 2$ we can write

$$\omega_1 = A + B^{1/2}, \qquad \omega_2 = A - B^{1/2},$$

$$A = \frac{\alpha + \delta}{2}, \qquad B = \frac{(\alpha - \delta)^2}{2} + \beta\gamma,$$

and to satisfy (19) we must have

$$\begin{aligned}(r + A)^m + \binom{m}{2}(r + A)^{m-2}\cdot B + \binom{m}{4}(r + A)^{m-4}\cdot B^2 + \cdots \\ + A\left(\binom{m}{1}(r + A)^{m-1} + \binom{m}{3}(r + A)^{m-3}\cdot B + \cdots\right) = 0.\end{aligned} \tag{20}$$

This congruence must have m different solutions and each solution determines a factor of $\Psi(x)$ in (16).

One can, however, derive these irreducible factors in rational form in a different way, which more clearly shows their relation to the linear substitutions. Let the numbers α, β, γ, δ satisfy the conditions of Theorem 6 and let us construct the expression

$$R(x) = x + \frac{\alpha x + \beta}{\gamma x + \delta} + \cdots + \frac{\alpha_{n-1}x + \beta_{n-1}}{\gamma_{n-1}x + \delta_{n-1}}.$$

For a root λ of $\Psi(x)$ we have

$$R(\lambda) = \lambda + \lambda^{p^f} + \cdots + \lambda^{p^{f(n-1)}} = -a_1,$$

where a_1 is the coefficient of x^{n-1} in the corresponding irreducible factor in (16), hence

$$a_1 = n\frac{\rho_1\psi_1 + \rho_2\psi_2}{\rho_1 + \rho_2} = \frac{n}{\gamma}(r + \alpha).$$

Since the equation of nth degree

$$R(x) = -a_1$$

is satisfied by all roots of the irreducible factor of $\Psi(x)$ having the coefficient a_1, we have

THEOREM 7. *Let $p \neq 2$, and let α, β, γ, δ be chosen such that the polynomial* (15) *is irreducible in K_f, while the order of the linear substitution*

$$x' = \frac{\alpha x + \beta}{\gamma x + \delta}$$

is n, where $n \cdot m = p^f + 1$. The equation of nth degree

$$Q_i(x) = x + \frac{\alpha x + \beta}{\gamma x + \delta} + \cdots + \frac{\alpha_{n-1} x + \beta_{n-1}}{\gamma_{n-1} x + \delta_{n-1}} + \frac{n}{\gamma}(r^{(i)} + \alpha) = 0$$

is then irreducible for all $r^{(i)}$ satisfying (20).

One sees from the proof of this theorem that $\Psi(x)$ may be represented as the product of factors $P_i(x)$ where

$$P_i(x) = (\gamma x + \delta) \cdots (\gamma_{n-1} x + \delta_{n-1}) Q_i(x).$$

It should also be observed that one can obtain similar results through a consideration of the product of the linear transformations.

CHAPTER IV. MISCELLANEOUS THEOREMS ON HIGHER CONGRUENCES

1. Elements with unit norm. We shall now deduce a few results which may be considered as the rudiments of the class field theory in finite fields. We show first

THEOREM 1. *The necessary and sufficient condition that a number α in the field $K_{ff'}$ satisfy the relation*

$$\alpha^{(p^{ff'}-1)/(p^f-1)} = 1 \tag{1}$$

is that α be representable in the form

$$\alpha = \beta^{p^f}/\beta. \tag{2}$$

It is obvious that every element of the form (2) satisfies (1). On the other hand, one finds that (1) represents the necessary and sufficient condition that $x^{p^{ff'}} - x$ be symbolically right-hand divisible by $x^{p^f} - \alpha x$, and hence when (1) is satisfied the equation

$$x^{p^f} - \alpha x = 0 \tag{3}$$

has a solution $\beta \neq 0$ in $K_{ff'}$.

If one wishes to determine the form of the number β in the representation (2), we divide $x^{p^{ff'}} - x$ left-hand by $x^{p^f} - \alpha x$ and find

$$x^{p^{ff'}} - x = (x^{p^f} - \alpha x) \times Q(x), \tag{4}$$

where

$$Q(x) = x^{p^f(f'-1)} + \alpha^{p^f(f'-1)} x^{p^f(f'-2)} + \alpha^{p^f(f'-1)+p^f(f'-2)} x^{p^f(f'-3)} + \cdots.$$

The relation (4) shows that

$$\beta = Q(\omega),$$

where ω is an arbitrary element in $K_{ff'}$ such that $Q(\omega) \neq 0$.

The condition (1) may also be written

$$N_f(\alpha) = \alpha \cdot \alpha^{p^f} \cdot \cdots \cdot \alpha^{p^f(f'-1)} = 1,$$

and Theorem 1 is seen to be the analogue of the well known theorem on cyclic fields, that *every element whose norm is unity may be represented as the quotient of two conjugate elements*. The ordinary proof for this theorem could not be applied in our case, since it requires that the field contain an infinite number of elements.

One may also state Theorem 1 in the following equivalent form:

THEOREM 2. *The necessary and sufficient condition that an irreducible polynomial $f(x)$ of degree n with coefficients in K_f belong to an exponent N dividing $(p^{fn}-1)/(p^f-1)$ is that the last coefficient α_n in $f(x)$ be unity, and in this case every root ρ of $f(x)$ may be represented in the form*

$$\rho = \sigma^{p^f}/\sigma$$

where σ is an element of K_{nf}.

One may also express Theorem 1 in a somewhat more general form. Let namely

$$F(x) = x^{p^{fr}} + \gamma_1 x^{p^f(r-1)} + \cdots + \gamma_{r-1} x^{p^f} + \gamma_r x \tag{5}$$

be a p^f-polynomial dividing $x^{p^{ff'}} - x$, and let

$$x^{p^{ff'}} - x = F(x) \times G(x). \tag{6}$$

Expressing the condition that $x^{p^{f'}} - \alpha x$ be a right-hand symbolic divisor of $F(x)$, we find

THEOREM 3. *Let $F(x)$ be a p^f-polynomial given by* (5) *and let $G(x)$ be its complementary polynomial such that* (6) *is satisfied. An element α in $K_{ff'}$ satisfying the condition*

$$\alpha^{(p^{fr}-1)/(p^f-1)} + \gamma_1 \alpha^{(p^f(r-1)-1)/(p^f-1)} + \cdots + \gamma_{r-1}\alpha + \gamma_r = 0$$

is then representable in the form

$$\alpha = \beta^{p^f}/\beta,$$

where β is a root of $F(x) = 0$, hence $\beta = G(\omega)$ for a primitive element ω of $K_{ff'}$.

2. **The law of reciprocity.** There exists for higher congruences a very simple and general law of reciprocity. This was first pointed out by F. K. Schmidt*, although special instances of it were already known to Dedekind.† Recently the theorem has been rediscovered by Carlitz‡, who seems to have overlooked the paper of Schmidt. Carlitz gives two different proofs mapped on the proofs for the quadratic law of reciprocity. In the following I give a new and very simple proof for the law of reciprocity in its most general form.

Let d be a divisor of p^f-1 and let

$$d\cdot\delta = p^f - 1.$$

The equation

$$x^d = 1 \tag{7}$$

is then solvable and has the d roots

$$1 = \epsilon_1, \epsilon_2, \cdots, \epsilon_d \tag{8}$$

in K_f. We define the field K_{nf} over K_f through a root ω of the irreducible equation

$$f(x) = \alpha_0 x^n + \cdots + \alpha_{n-1}x + \alpha_n$$

where we do not, as usual, suppose that $\alpha_0=1$. Let then

$$g(\omega) = \beta_0\omega^m + \cdots + \beta_{m-1}\omega + \beta_m$$

be an arbitrary element in K_{nf}, and hence

$$g(\omega)^{\delta(p^{fn}-1)/(p^f-1)} = \epsilon, \tag{9}$$

where ϵ is one of the roots (8). One may obviously write (9) in the form of a congruence

$$g(x)^{\delta(p^{fn}-1)/(p^f-1)} \equiv \epsilon \qquad (\text{mod } f(x)),$$

and when we introduce the dth power residue symbol

$$\left(\frac{g(x)}{f(x)}\right)_d = \epsilon \equiv g(x)^{\delta(p^{fn}-1)/(p^f-1)} \qquad (\text{mod } f(x)), \tag{10}$$

we find that it has the property

* F. K. Schmidt, *Zur Zahlentheorie in Körpern von der Charakteristik p*, Erlangen Sitzungsberichte, vols. 58–59 (1928), pp. 159–172.

† R. Dedekind, *Abriss einer Theorie der höheren Kongruenzen in Bezug auf einen reellen Primzahlmodulus*, Journal für Mathematik, vol. 54 (1857), pp. 1–26; Werke, vol. 1, pp. 40–67.

‡ L. Carlitz, *The arithmetic of polynomials in a Galois field*, American Journal of Mathematics, vol. 54 (1932), pp. 39–50. See also *On a theorem of higher reciprocity*, Bulletin of the American Mathematical Society, vol. 39 (1933), pp. 155–160.

$$\left(\frac{g(x)\cdot h(x)}{f(x)}\right)_d = \left(\frac{g(x)}{f(x)}\right)_d \left(\frac{h(x)}{f(x)}\right)_d$$

and

$$\left(\frac{g(x)}{f(x)}\right)_d = 1$$

is the necessary and sufficient condition that $g(x)$ be a dth power residue (mod $f(x)$).

This definition (10) gives the dth power residue symbol only for prime $f(x)$. In the general case, where $f(x)$ has the prime factor decomposition

$$f(x) = f_1(x) \cdots f_r(x),$$

we put

$$\left(\frac{g(x)}{f(x)}\right)_d = \left(\frac{g(x)}{f_1(x)}\right)_d \cdots \left(\frac{g(x)}{f_r(x)}\right)_d. \tag{11}$$

To prove the law of reciprocity, let us first consider the symbol for a prime $f(x)$. Then according to (10) we obtain

$$\left(\frac{g(x)}{f(x)}\right)_d = (g(\omega)g(\omega^{p^f}) \cdots g(\omega^{p^{f(n-1)}}))^\delta = \alpha_0^{-m\delta} R(f(x), g(x))^\delta, \tag{12}$$

where $R(f, g)$ denotes the resultant of the two polynomials. The definition (11) then shows that the same formula (12) holds for an arbitrary $f(x)$. For the inverse symbol we obtain in the same way

$$\left(\frac{f(x)}{g(x)}\right)_d = \beta_0^{-n\delta} R(g(x), f(x))^\delta = (-1)^{mn}\beta_0^{-n\delta} R(f(x), g(x))^\delta,$$

and hence

THEOREM 4. *For the dth power residue symbol one has the law of reciprocity*

$$\alpha_0^{m(p^f-1)/d}\left(\frac{f(x)}{g(x)}\right)_d = (-1)^{mn}\beta_0^{n(p^f-1)/d}\left(\frac{g(x)}{f(x)}\right)_d$$

where n and m are the degrees and α_0 and β_0 are the highest coefficients of the relatively prime polynomials $f(x)$ and $g(x)$.

This proof also suggests generalizations of the law of reciprocity using some other symmetric function than the resultant. Let

$$S_{n,m}(u_1, \cdots, u_n; v_1, \cdots, v_m)$$

denote a symmetric function in each of the sets u_i and v_j, and let us suppose in addition that

$$S_{n,m}(u, v) = S_{m,n}(v, u). \tag{13}$$

Various symmetric functions having these properties may be constructed. Now let $f(x)$ and $g(x)$ be two polynomials with the roots $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$, and let us define

$$\left\{\frac{g(x)}{f(x)}\right\} = S_{n,m}(g(x_1), \cdots, g(x_n), f(y_1), \cdots, f(y_m)).$$

It is then obvious according to (13) that

$$\left\{\frac{g(x)}{f(x)}\right\} = \left\{\frac{f(x)}{g(x)}\right\}.$$

YALE UNIVERSITY,
NEW HAVEN, CONN.