ACTA ARITHMETICA
XII (1967)

Classification of irreducible factorable polynomials over a finite field*

by

Andrew F. Long (Laurinburg, N. C.)

1. Introduction. Let $\mathrm{GF}(q)$ denote the finite field of order $q = p^n$, where p is an arbitrary prime and $n \geqslant 1$. A polynomial $M(x_1, \ldots, x_k)$ with coefficients in $\mathrm{GF}(q)$ is *factorable* if

$$M(x_1, \ldots, x_k) = \prod_{i=0}^{m} (a_{i0} + a_{i1}x_1 + \ldots + a_{ik}x_k)$$

where the a_{ij} lie in some finite field $\mathrm{GF}(q^s)$. Ordinary polynomials in a single indeterminate are inherently factorable, and Dickson ([3]) and Serret ([8]) have classified the irreducible polynomials of degree p^r over $\mathrm{GF}(q)$. In this paper we extend this classification to irreducible factorable polynomials of degree $p^r s$ in both the single and multiple indeterminate cases.

The homogeneous and non-homogeneous cases require separate treatment. Let $P(x_0, x_1, \ldots, x_k)$ be a homogeneous factorable irreducible polynomial over $\mathrm{GF}(q)$. Then $(x_0^{q^s} - x_0, x_1^{q^s} - x_1, \ldots, x_k^{q^s} - x_k)$ factors into q^s factorable irreducible polynomials of degree s. In addition the decomposition of $P(x_0^{q^{ms}} - x_0, x_1^{q^{ms}} - x_1, \ldots, x_k^{q^{ms}} - x_k)$ for m an integer greater than 1 is determined.

In the non-homogeneous case, the substitution $x^{q^s} - x$ for x in an irreducible (factorable) polynomial $P(x)$ of a given class of degree $p^r s$, where $p \nmid s$, yields either q^s irreducibles of the next class of degree $p^r s$ or p^{ns-1} irreducibles of the first class of degree $p^{r+1} s$. Additional results include the demonstration that roots of irreducibles of class m of degree ps can be expressed as polynomials of degree m in a root of an irreducible of the first class of degree ps, and the determination of the number $\psi(p^r s, q, m)$ of irreducibles over $\mathrm{GF}(q)$ in class m of degree $p^r s$. The results for factorable irreducibles in more than one indeterminate are for the most part direct analogs of the single indeterminate results.

---

* Supported by National Science Foundation grant GP-1593.

The following notation and definition will be used throughout the paper. Elements of $\mathrm{GF}(q)$ will, in general, be denoted by lower case Greek letters, but at times lower case Roman letters will be used to prevent ambiguity. If in the factorable polynomial $M(x_1, \ldots, x_k)$ of degree m, x_k^m actually appears and has coefficient unity, M is said to be *primary*. Irreducible polynomials over $\mathrm{GF}(q)$ will be denoted by $P(x_1, \ldots, x_k)$ and $Q(x_1, \ldots, x_k)$.

2. Some classical concepts and theorems. The following concepts and theorems pertain to polynomials in a single indeterminate. Most of the results are found in [2] and [4].

A polynomial of the form

$$f(x) = \sum_{i=0}^{s} a_i x^{p^{ni}}$$

is called a *linear polynomial*. If $a_s \neq 0$, then $f(x)$ is of *order* s. Ore ([7], pp. 262, 263) lets $f(x)$ correspond to the ordinary polynomial

$$F(x) = \sum_{i=0}^{s} a_i x^i$$

and proves that given $F(x)$ one can find a unique linear polynomial $g(x)$ of minimum order ($\leqslant s$) divisible by $F(x)$. We say that $F(x)$ *belongs* to $g(x)$.

Let $Q(x)$ be an irreducible of degree p^r over $\mathrm{GF}(p^n)$. Using the concept of linear polynomials, results of Serret ([8], p. 301) for $n = 1$ and Dickson ([3], pp. 384-387) for $n > 1$ imply that Q belongs to

$$z_t(x) = \sum_{i=0}^{t} (-1)^i \binom{t}{i} x^{p^{n(t-i)}},$$

where $p^{r-1}+1 \leqslant t \leqslant p^r$. We say that Q is of the *m-th class* of degree p^r, where $m = t-p^{r-1}$, so that $1 \leqslant m \leqslant p^r-p^{r-1}$.

THEOREM 2.1. *Let $Q(x)$ be irreducible of the m-th class of degree p^r. Then $Q(x^{p^n}-x)$ is the product of p^n irreducibles of the $(m+1)$-th class of degree p^r provided that $m < p^r-p^{r-1}$. If $m = p^r-p^{r-1}$, then $Q(x^{p^n}-x)$ is the product of p^{n-1} irredicibles of the first class of degree p^{r+1}.*

Although Dickson did not give the result, it is possible to calculate the number of irreducibles over $\mathrm{GF}(q)$ in each class of degree p^r.

THEOREM 2.2. *Let $\psi(p^r, q, j)$ denote the number of primary irreducibles of degree p^r over $\mathrm{GF}(q)$ of class j, $1 \leqslant j \leqslant p^r-p^{r-1}$. Then*

$$\psi(p^r, q, j) = (q-1)p^{n(p^{r-1}+j-1)-r}.$$

Proof. From Theorem 2.1 it is clear that

$$\psi(p^r, q, j) = (p^{n-1})(q^{j-1})\psi(p^{r-1}, q, p^{r-1}-p^{r-2}). \tag{2.1}$$

The theorem follows on substituting, with r replaced by $r-1$,

$$\psi(p^r, q, p^r-p^{r-1}) = (q-1)(p^{n(p^{r}-1)-r}) \tag{2.2}$$

in (2.1). (2.2) is easily verified by induction on r.

THEOREM 2.3. *The number $\psi(s, q)$ of primary irreducibles of degree s over $\mathrm{GF}(q)$ is given by*

$$\psi(s, q) = \frac{1}{s} \sum_{ij=s} \mu(i) q^j.$$

DEFINITION 2.1. If a is contained in $\mathrm{GF}(q^f)$ but is not contained in $\mathrm{GF}(q^e)$, $1 \leqslant e < f$, then f is called the *degree of a relative to* $\mathrm{GF}(q)$.

We use the notation $\deg a = f$.

THEOREM 2.4. *$Q(x)$ is an irreducible polynomial of degree s over $\mathrm{GF}(q)$ if and only if*

$$Q(x) = \prod_{j=0}^{s-1} (x-a^{q^j})$$

and $\deg a = s$.

THEOREM 2.5. *Let $\mathrm{GF}(q)$ denote a finite field of order q. Then*

$$x^q-x = \prod_{\lambda \in \mathrm{GF}(q)} (x-\lambda).$$

THEOREM 2.6. *$\mathrm{GF}(q^n)$ is contained in $\mathrm{GF}(q^m)$ if and only if n divides m.*

THEOREM 2.7. *An irreducible polynomial of degree s over $\mathrm{GF}(q)$ decomposes into d factors each an irreducible polynomial of degree s/d over $\mathrm{GF}(q^r)$ where $d = (s, r)$.*

THEOREM 2.8. *Let P be an irreducible polynomial of degree s over $\mathrm{GF}(q)$. Then*

$$P \mid x^{p^{nt}}-x$$

if and only if $s \mid t$.

A result ([6], pp. 229, 230) of a different nature which will be required later is

THEOREM 2.9. (Lucas' Lemma). *Let*

$$m = a_0+a_1p+\ldots+a_rp^r \quad (0 \leqslant a_i < p),$$
$$n = b_0+b_1p+\ldots+b_rp^r \quad (0 \leqslant b_i < p).$$

Then

$$\binom{m}{n} \equiv \prod_{i=0}^{r} \binom{a_i}{b_i} \pmod{p}.$$

3. Some theorems on factorable polynomials. The following theorems of Carlitz ([1]) pertaining to factorable polynomials in several indeterminates will be required.

THEOREM 3.1. *A factorable polynomial $P(x_1, \ldots, x_k)$ of degree s is irreducible over* GF(q) *if and only if*

$$P = \prod_{j=0}^{s-1} (a_0^{q^j} + a_1^{q^j} x_1 + \ldots + a_k^{q^j} x_k) \tag{3.1}$$

and

$$s = [f_0, f_1, \ldots, f_k], \tag{3.2}$$

where f_j is the degree of a_j relative to GF(q).

Let, as in [1],

$$D^s(x_0, x_1, \ldots, x_k) = |x_i^{q^{js}}| \quad (i, j = 0, 1, \ldots, k)$$

denote the Moore determinant.

THEOREM 3.2. *Let $\theta(t)$ denote the product of the primary irreducible factorable $P(x_0, x_1, \ldots, x_k)$ in homogeneous form of degree t. Then*

$$D^s(x_0, x_1, \ldots, x_k) = \prod_{t|s} \theta(t). \tag{3.3}$$

By considering the degree of both members of (3.3) we obtain

THEOREM 3.3. *Let $\psi_k(s, q)$ denote the number of primary irreducible factorable $P(x_1, \ldots, x_k)$ of degree s over* GF(q). *Then*

$$\psi_k(s, q) = \frac{1}{s} \sum_{ij=s} \mu(i)(q^{kj} + q^{(k-1)j} + \ldots + q^j).$$

Note that for $k = 1$ Theorem 3.3 reduces to Theorem 2.3.

4. Decomposition of homogeneous irreducible f---able polynomials in several indeterminates. Let

$$P(x_0, x_1, \ldots, x_k) = \prod_{j=0}^{s-1} (a_0^{q^j} x_0 + a_1^{q^j} x_1 + \ldots + a_k^{q^j} x_k) \quad ([f_0, f_1, \ldots, f_k] = s), \tag{4.1}$$

where f_i is the degree of a_i, $0 \leqslant i \leqslant k$, be an irreducible factorable polynomial in homogeneous form of degree s over GF(q). Substituting $x_i^{q^s} - x_i$ for x_i, $0 \leqslant i \leqslant k$, in (4.1) and making use of Theorem 2.5 we have

$$\begin{aligned} (4.2)\quad P(x_0^{q^s} - x_0, \ldots, x_k^{q^s} - x_k) &= \prod_{j=0}^{s-1} [a_0^{q^j}(x_0^{q^s} - x_0) + \ldots + a_k^{q^j}(x_k^{q^s} - x_k)] \\ &= \prod_{j=0}^{s-1} [(a_0^{q^j} x_0 + \ldots + a_k^{q^j} x_k)^{q^s} - (a_0^{q^j} x_0 + \ldots + a_k^{q^j} x_k)] \\ &= \prod_{\lambda \in \mathrm{GF}(q^s)} \prod_{j=0}^{s-1} (a_0^{q^j} x_0 + \ldots + a_k^{q^j} x_k + \lambda^{q^j}). \end{aligned}$$

The degree f_λ of λ is a divisor of s; hence $[f_0, f_1, \ldots, f_k, f_\lambda] = s$. Applying Theorem 3.1 to the extreme right hand member of (4.2) we obtain

THEOREM 4.1. *Let $P(x_0, x_1, \ldots, x_k)$ be an irreducible factorable polynomial in homogeneous form of degree s over* GF(q). *Then $P(x_0^{q^s} - x_0, x_1^{q^s} - x_1, \ldots, x_k^{q^s} - x_k)$ is the product of q^s irreducible factorable polynomials of degree s over* GF(q).

Next consider the substitutions $x_i^{q^{ms}} - x_i$ for x_i, $0 \leqslant i \leqslant k$, in (4.1) where m is an integer greater than 1. We have

$$P(x_0^{q^{ms}} - x_0, \ldots, x_k^{q^{ms}} - x_k) = \prod_{\lambda \in \mathrm{GF}(q^{ms})} \prod_{j=0}^{s-1} (a_0^{q^j} x_0 + \ldots + a_k^{q^j} x_k + \lambda^{q^j}). \tag{4.3}$$

Since $a_0, a_1, \ldots, a_k$ are fixed, the degrees of the irreducibles in this decomposition are determined by the degree of λ. If the degree of λ divides s, then $[f_0, \ldots, f_k, \deg \lambda] = s$ and

$$\prod_{j=0}^{s-1} (a_0^{q^j} x_0 + \ldots + a_k^{q^j} x_k + \lambda^{q^j})$$

is an irreducible of degree s by Theorem 3.1. If the degree of λ is a multiple ts of s, $t|m$, we expect an irreducible of degree ts to occur. By Theorem 2.7 an irreducible Q of degree ts over GF(q) is the product of s irreducible factors of degree t over GF(q^s), that is

$$\begin{aligned} (4.4)\quad Q(x_1, \ldots, x_k) &= \prod_{i=0}^{ts-1} (a_0^{q^i} x_0 + \ldots + a_k^{q^i} x_k + \lambda^{q^i}) \\ &= \prod_{i=0}^{t-1} \prod_{j=0}^{s-1} (a_0^{q^i} x_0 + \ldots + a_k^{q^i} x_k + \lambda^{q^{j+si}}). \end{aligned}$$

These factors are available in (4.3); hence the irreducible $Q(x_0, \ldots, x_k)$ can be constructed by Theorem 3.1. Now the roots of an irreducible of degree t over GF(q^s) must necessarily be of degree ts relative to GF(q) according to Theorem 2.4. Hence there are $t\psi(t, q^s)$ elements in GF(q^{ms}) of degree ts. Since t of these elements are used to form each irreducible of the form given in (4.4), there are $\psi(t, q^s)$ irreducible polynomials of degree ts in the decomposition of (4.3). This proves:

THEOREM 4.2. *Let $P(x_0, x_1, \ldots, x_k)$ be a factorable irreducible polynomial in homogeneous form of degree s over* GF(q). *Then for m an integer $\geqslant 1$, $P(x_0^{q^{ms}} - x_0, \ldots, x_k^{q^{ms}} - x_k)$ decomposes into $\sum_{t|m} \psi(t, q^s)$ factorable irreducible polynomials over* GF(q), *the decomposition containing $\psi(t, q^s)$ irreducibles of degree ts for t a divisor of m.*

Note that Theorem 4.1 is a special case of Theorem 4.2.

5. Classification of non-homogeneous irreducible polynomials of degree $p^r s$ in a single indeterminate. Before proceeding to a classification of non-homogeneous factorable irreducible polynomials of degree $p^r s$ in two or more indeterminates, it is useful to consider the single indeterminate case. Similar to Dickson's classification of the irreducibles of degree p^r over $\mathrm{GF}(p^n)$ ([4], pp. 28-31), the substitution $x^{q^s}-x$ will be employed; the result however is not so satisfying as Dickson's in that not all irreducibles of degree $p^r s$ will be included in the classes constructed.

Let

$$Q(x) = \prod_{j=0}^{s-1}(x-a^{q^j}) \qquad (\deg a = s) \tag{5.1}$$

be irreducible of degree s over $\mathrm{GF}(q)$. Substituting $x^{q^s}-x$ for x in (5.1) we obtain

$$Q(x^{q^s}-x) = \prod_{j=0}^{s-1}(x^{q^s}-x-a^{q^j}). \tag{5.2}$$

Taking $j = 0$,

$$x^{q^s}-x-a = 0 \tag{5.3}$$

has a root $\lambda_1 \notin \mathrm{GF}(q^s)$ such that

$$\lambda_1^{q^s} = \lambda_1+a,$$
$$\lambda_1^{q^{2s}} = \lambda_1^{q^s}+a^{q^s} = \lambda_1+2a,$$
$$\cdots\cdots\cdots\cdots$$
$$\lambda_1^{q^{ps}} = \lambda_1+pa = \lambda_1,$$

as the characteristic of the field is p. Thus λ_1 has at most degree ps relative to $\mathrm{GF}(q)$. By Theorem 2.6 if λ_1 has a lower degree, it must be of the form pt, $t|s$. Now $pt\nmid s$ for then $\lambda_1^{q^{pt}} = \lambda_1$ would imply $\lambda_1^{q^s} = \lambda_1$, a contradiction to $\lambda_1^{q^s} = \lambda_1+a$. Moreover since a is of degree s and is a polynomial in λ_1, Theorem 2.6 implies that the degree of a must divide the degree of λ_1; that is, $s|pt$. The restrictions $t|s$, $pt\nmid s$, and $s|pt$ taken together imply that $t = s$. Consequently the degree of λ_1 is exactly ps.

All roots of (5.3) are of the form $\lambda_1+\gamma$, $\gamma\in\mathrm{GF}(q^s)$. Hence

$$x^{q^s}-x-a = \prod_{\gamma\in\mathrm{GF}(q^s)}[x+(\lambda_1+\gamma)].$$

Likewise

$$x^{q^s}-x-a^{q^j} = 0 \qquad (j = 1, \ldots, s-1) \tag{5.4}$$

has q^s roots of degree ps. They may be expressed in terms of λ_1 as follows: Raising both sides of (5.3), with λ_1 substituted for x, to the q^jth power we obtain

$$(\lambda_1^{q^j})^{q^s}-\lambda_1^{q^j}-a^{q^j} = 0.$$

Therefore all roots of (5.4) are given by $\lambda_1^{q^j}+\gamma$, where $\gamma\in\mathrm{GF}(q^s)$.

Thus (5.2) becomes

$$Q(x^{q^s}-x) = \prod_{\gamma\in\mathrm{GF}(q^s)}\prod_{j=0}^{s-1}(x+\lambda_1^{q^j}+\gamma) = \prod_{\gamma\in\mathrm{GF}(q^s)}\prod_{j=0}^{s-1}[x+(\lambda_1+\gamma)^{q^j}]. \tag{5.5}$$

Since $\lambda_1+\gamma$ has degree ps, any irreducible formed by Theorem 2.4 from the factors of $Q(x^{q^s}-x)$ as determined by (5.5) will be of the form

$$\prod_{j=0}^{ps-1}[x+(\lambda_1+\gamma)^{q^j}] = \prod_{i=0}^{p-1}\prod_{j=0}^{s-1}[x+(\lambda_1+\gamma)^{q^{is}q^j}].$$

This proves

THEOREM 5.1. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$. Then $Q(x^{q^s}-x)$ is the product of p^{ns-1} irreducibles of degree ps over $\mathrm{GF}(q)$.*

We shall assume in the remainder of this section that $p\nmid s$.

The irreducibles obtained from $Q(x^{q^s}-x)$ in Theorem 5.1 will be called *irreducibles of the first class of degree ps*.

If we now take an irreducible of the first class of degree ps, say,

$$P(x) = \prod_{j=0}^{ps-1}(x-\lambda_1^{q^j}),$$

then

$$P(x^{q^s}-x) = \prod_{j=0}^{ps-1}(x^{q^s}-x-\lambda_1^{q^j}).$$

Taking $j = 0$,

$$x^{q^s}-x-\lambda_1 = 0$$

has a root λ_2, which can be shown to be of degree ps as before, provided that $p > 2$. (If $p = 2$, λ_2 will have degree $p^2 s$; see Lemma 5.1.) Thus

$$x^{q^s}-x-\lambda_1 = \prod_{\gamma\in\mathrm{GF}(q^s)}[x+(\lambda_2+\gamma)]$$

and

$$P(x^{q^s}-x) = \prod_{\gamma\in\mathrm{GF}(q^s)}\prod_{j=0}^{ps-1}[x+(\lambda_2+\gamma)^{q^j}]. \tag{5.6}$$

Since $\lambda_2+\gamma$ is of degree ps relative to $\mathrm{GF}(q)$, the application of Theorem 2.4 yields q^s irreducibles of degree ps in the decomposition (5.6). These irreducibles will be called *irreducibles of the second class of degree ps*.

We could continue constructing new classes from previous ones in this manner, but it is convenient at this point to generalize the procedure by using the following lemma:

LEMMA 5.1. *Let λ_m denote a root of the equation*

$$x^{q^s}-x-\lambda_{m-1}=0,$$

where $\lambda_0 = a$ of (5.1). *Then*

$$\lambda_m^{q^{is}} = \sum_{t=0}^{m} \binom{i}{m-t} \lambda_t, \tag{5.7}$$

where i is any positive integer.

Proof. The proof will be by induction on i. Put $i = 1$ in (5.7). This yields

$$\lambda_m^{q^s} = \lambda_{m-1}+\lambda_m$$

which is the hypothesis.

Assume (5.7) holds for $i = r$, that is,

$$\lambda_m^{q^{rs}} = \sum_{t=0}^{m} \binom{r}{m-t} \lambda_t.$$

Raising both sides to the q^sth power we have

$$\lambda_m^{q^{(r+1)s}} = \sum_{t=0}^{m} \binom{r}{m-t} \lambda_t^{q^s} = \sum_{t=0}^{m} \binom{r}{m-t} (\lambda_t+\lambda_{t-1})$$

$$= \sum_{t=0}^{m} \binom{r}{m-t} \lambda_t + \sum_{t=0}^{m} \binom{r}{m-(t+1)} \lambda_t = \sum_{t=0}^{m} \binom{r+1}{m-t} \lambda_t.$$

This completes the proof of Lemma 5.1.

It is apparent form Lemma 5.1 that for $1 \leqslant m \leqslant p-1$, an irreducible of class m has a root λ_m which is at most of degree ps. That the degree is exactly ps follows from the same argument used to show that λ_1 has exactly degree ps.

For $m = p$ however (5.7) yields

$$\lambda_p^{q^{ps}} = \lambda_p+a$$

showing that λ_p is not of degree ps. In fact

$$\lambda_p^{q^{p^2 s}} = \lambda_p;$$

hence λ_p has at most degree $p^2 s$. By an argument similar to that for λ_1, it can be shown that $\deg \lambda_p = p^2 s$.

If we maintain an orderly procedure of calling λ_m a root of an irreducible formed from the decomposition of one with a root λ_{m-1} on substituting $x^{q^s}-x$ for x, Lemma 5.1 will give λ_m in terms of all previous λ's. Moreover it is easy to determine the m's at which the degree changes with the use of Theorem 2.9. These m's are $1, p, p^2, p^3, \ldots, p^r, \ldots$. We say that λ_p is a *root of an irreducible of the first class of degree* $p^2 s$, λ_{p^2} is a *root of an irreducible of the first class of degree* $p^3 s$, and so on. Thus $\lambda_p, \ldots, \lambda_{p^2-1}$ are all of degree $p^2 s$; $\lambda_{p^2}, \ldots, \lambda_{p^3-1}$ are of degree $p^3 s$; and in general $\lambda_{p^{r-1}}, \ldots, \lambda_{p^r-1}$ are of degree $p^r s$. Hence there are p^2-p classes of degree $p^2 s$, p^3-p^2 classes of degree $p^3 s$, and p^r-p^{r-1} classes of degree $p^r s$.

Irreducible polynomials having roots of the form $\lambda_m+\gamma$, $\gamma \in \mathrm{GF}(q^s)$, of higher degree than ps are formed in an analogous manner to those of degree ps. In particular, irreducibles having roots of the form $\lambda_{p^r}+\gamma$, $\gamma \in \mathrm{GF}(q^s)$, are obtained from the $(p^{r-1}-p^{r-2})$-th (last) class of degree $p^{r-1}s$; there will be p^{ns-1} of them for each irreducible of that class. We have the following theorem:

THEOREM 5.2. *Let $Q(x)$ be an irreducible polynomial over* $\mathrm{GF}(q)$ *of the m-th class of degree $p^r s$, where $p \nmid s$. Then $Q(x^{q^s}-x)$ is the product of q^s irreducible polynomials of the $(m+1)$-th class of degree $p^r s$ provided that $m < p^r-p^{r-1}$. If $m = p^r-p^{r-1}$, then $Q(x^{q^s}-x)$ is the product of p^{ns-1} irreducible polynomials of the first class of degree $p^{r+1}s$.*

It is of interest to determine the form of a root λ_m of an irreducible polynomial of the mth class of degree ps in terms of a root λ_1 of an irreducible of the first class of degree ps. The form of λ_2 is determined as follows:

As a polynomial in λ_1, λ_2 may be written

$$\lambda_2 = a_0+a_1\lambda_1+\ldots+a_{p-1}\lambda_1^{p-1} \quad (a_i \in \mathrm{GF}(q^s)). \tag{5.8}$$

Raising both sides of (5.8) to the q^s-th power, we have

$$\lambda_2^{q^s} = a_0+a_1(\lambda_1+a)+a_2(\lambda_1+a)^2+\ldots+a_{p-1}(\lambda_1+a)^{p-1}. \tag{5.9}$$

Substituting (5.8) and (5.9) in

$$\lambda_2^{q^s}-\lambda_2 = \lambda_1$$

we obtain

$$\sum_{k=0}^{p-2} \sum_{j=k+1}^{p-1} \binom{j}{k} a_j a^{j-k} \lambda_1^k = \lambda_1.$$

Equating coefficients of like powers of λ_1, we find that a_2 is the first nonzero coefficient. Thus λ_2 is quadratic in λ_1, that is

$$\lambda_2 = a_0+a_1\lambda_1+a_2\lambda_1^2. \tag{5.10}$$

Now λ_3 is a polynomial in λ_2, which is itself a polynomial in λ_1; hence λ_3 may be written

$$\lambda_3 = b_0+b_1\lambda_1+\ldots+b_{p-1}\lambda_1^{p-1} \quad (b_i \in \mathrm{GF}(q^s)). \tag{5.11}$$

Also

$$\lambda_3^{q^s} = b_1+b_1(\lambda_1+a)+\ldots+b_{p-1}(\lambda_1+a)^{p-1}. \tag{5.12}$$

Substituting (5.10), (5.11), and (5.12) in

$$\lambda_3^{q^s}-\lambda_3 = \lambda_2$$

and equating coefficients of like powers of λ_1, we find that λ_3 is cubic in λ_1.

In general the following theorem may be stated (compare with § 43 of [4]):

THEOREM 5.3. *The roots of every irreducible $P(x)$ of class m of degree ps, where $p\nmid s$, over $GF(q)$ may be written as polynomials of degree m in λ_1, a root of an irreducible of the first class of degree ps.*

The following example illustrates that not all irreducibles of degree $p^r s$ are included in the preceding classification:

Let $p=2, n=1, r=1$, and $s=3$. By Theorem 2.2 $\psi(3,2)=2$, that is there are two primary irreducibles $P(x)$ and $Q(x)$ of degree 3 over $GF(2)$. On substituting $x^{q^s}-x$ for x, $P(x)$ and $Q(x)$ each decompose into $p^{ns-1}=4$ irreducibles of degree $ps=6$. Since $p-1=1$, there is only one class of degree 6; hence a total of 8 irreducibles of degree 6 are produced. However $\psi(6,2)=9$, indicating that our classification has failed to include one irreducible of degree 6.

The missing irreducible can be determined as follows: Let

$$P(x) = x^3+x+1, \qquad Q(x) = x^3+x^2+1.$$

From Theorem 2.8 it follows that

$$x^{p^{ns}}-x = \prod_{\deg R|s} R(x), \tag{5.13}$$

where the product extends over all primary irreducibles R over $GF(q)$ of degree dividing s. Thus

$$x^8-x = \prod_{\deg R|3} R(x),$$

with the same conditions, for this example. As the irreducibles of degree 1 are x and $x+1$ over $GF(2)$, it follows that

$$P(x)Q(x) = \frac{x^8+x}{x(x+1)}. \tag{5.14}$$

When the substitution $x^{q^s}-x = x^8+x$ is made in (5.14) we obtain

$$P(x^8+x)Q(x^8+x) = \frac{x^{64}+x}{(x^8+x)(x^8+x+1)}.$$

Now

$$x^{64}+x = \prod_{\deg R|6} R(x)$$

from (5.13). Hence $x^{64}+x$ contains all the irreducible sextics. Therefore the denominator $(x^8+x)(x^8+x+1)$ must contain the missing irreducible sextic. Since x^8+x contains no irreducible sextic, x^8+x+1 is the product of a sextic and a quadratic: $x^8+x+1 = (x^2+x+1)(x^6+x^5+x^3+x^2+1)$.

The sextic $x^6+x^5+x^3+x^2+1$ is in fact a primitive irreducible over $GF(q)$ ([4], p. 41).

6. Classification of non-homogeneous irreducible factorable polynomials of degree $p^r s$ in several indeterminates. This section generalizes the work of § 5 to k indeterminates. Let

$$Q(x_1, \ldots, x_k) = \prod_{j=0}^{s-1} (a_0^{q^j}+a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k) \qquad ([f_0, f_1, \ldots, f_k] = s), \tag{6.1}$$

where f_i is the degree of a_i, $0 \leqslant i \leqslant k$, be an irreducible factorable polynomial of degree s over $GF(q)$. Substituting $x_i^{q^s}-x_i$ for x_i, $1 \leqslant i \leqslant k$, in (6.1), we have

$$\begin{aligned} Q(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k) &= \prod_{j=0}^{s-1} [a_1^{q^j}(x_1^{q^s}-x_1)+\ldots+a_k^{q^j}(x_k^{q^s}-x_k)+a_0^{q^j}] \\ &= \prod_{j=0}^{s-1} [(a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k)^{q^s}-(a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k)+a_0^{q^j}] \\ &= \prod_{j=0}^{s-1} \prod_{\lambda} (a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k+\lambda^{q^j}), \end{aligned}$$

where the inner product extends over all λ satisfying

$$\lambda^{q^s}-\lambda+a_0 = 0. \tag{6.2}$$

If λ_1 is a particular root of (6.2), all roots are given by $\lambda_1+\gamma$, $\gamma \in GF(q^s)$. Hence

$$Q(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k) = \prod_{\gamma \in GF(q^s)} \prod_{j=0}^{s-1} [a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k+(\lambda_1+\gamma)^{q^j}].$$

Let h denote the degree of λ_1 relative to $GF(q)$. We show that $[f_1, \ldots, f_k, h] = ps$. Since $\lambda_1^{q^{ps}} = \lambda_1$, $h|ps$. But $h\nmid s$ for this would imply $\lambda_1^{q^s} = \lambda_1$ in contradiction to $\lambda_1^{q^s}-\lambda_1+a_0 = 0$. Hence $h = pt$, $t|s$. If $f_0 = s$, then $s|pt$ as a_0 is a polynomial in λ_1. The conditions $t|s$, $pt\nmid s$, and $s|pt$ imply that $h = ps$; thus $[f_1, \ldots, f_k, h] = ps$. If $f_0 \neq s$, $f_0|s$, then $[f_1, \ldots, f_k] = s$. As $h = pt$, $t|s$ it follows that $[f_1, \ldots, f_k, h] = ps$.

Consequently p of the factors

$$\prod_{j=0}^{s-1} [a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k+(\lambda_1+\gamma)^{q^j}]$$

are used in forming a factorable irreducible in accordance with Theorem 3.1. We have the following analog of Theorem 5.1:

THEOREM 6.1. *Let* $Q(x_1, \ldots, x_k)$ *be an irreducible factorable polynomial of degree s over* GF(q). *Then* $Q(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k)$ *is the product of* p^{ns-1} *irreducible factorable polynomials of degree ps over* GF(q).

In the remainder of this section we shall assume that $p \nmid s$.

As before, the irreducibles obtained in the decomposition of $Q(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k)$ will be called *irreducibles of the first class of degree ps.*

If we next take a factorable irreducible of the first class of degree ps, say,

$$P(x_1, \ldots, x_k) = \prod_{j=0}^{ps-1} (a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k+\lambda_1^{q^j}) \qquad ([f_1, \ldots, f_k, h] = ps),$$

we find that

$$P(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k) = \prod_{\gamma\epsilon \mathrm{GF}(q^s)} \prod_{j=0}^{ps-1} [a_1^{q^j}x_1+\ldots+a_k^{q^j}x_k+(\lambda_2+\gamma)^{q^j}]$$

where λ_2 satisfies $\lambda_2^{q^s}-\lambda_2-\lambda_1 = 0$. Let d denote the degree of λ_2 relative to GF(q). We show that $[f_1, \ldots, f_k, d] = ps$, provided that $p > 2$. Since $\lambda_2^{q^{ps}} = \lambda_2$, $d \mid ps$. But $d \nmid s$ since $\lambda_2^{q^s} \neq \lambda_2$. Hence $d = pv$, $v \mid s$. If $h = ps$, then $ps \mid d$ as λ_1 is a polynomial in λ_2. The conditions $ps \mid pv$ and $v \mid s$ imply that $d = ps$; hence $[f_1, \ldots, f_k, d] = ps$. If $h \neq ps$, then $h = pt$, $t \mid s$ and $[f_1, \ldots, f_k, h] = ps$ implies $[f_1, \ldots, f_k] = s$. Since $d = pv$, $v \mid s$, it follows that $[f_1, \ldots, f_k, d] = ps$.

Applying Theorem 3.1 we see that $P(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k)$ decomposes into q^s factorable irreducibles of degree ps. These irreducibles will be called *irreducibles of the second class of degree ps.*

Lemma 5.1 can be applied in a manner similar to its use in § 5 to prove the following analog of Theorem 5.2:

THEOREM 6.2. *Let* $Q(x_1, \ldots, x_k)$ *be an irreducible factorable polynomial over* GF(q) *of the m-th class of degree* $p^r s$ *where* $p \nmid s$. *Then* $Q(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k)$ *is the product of* q^s *irreducible factorable polynomials of the* $(m+1)$*-th class of degree* $p^r s$ *provided that* $m < p^r-p^{r-1}$. *If* $m = p^r-p^{r-1}$, *then* $Q(x_1^{q^s}-x_1, \ldots, x_k^{q^s}-x_k)$ *is the product of* p^{ns-1} *irreducible factorable polynomials of the first class of degree* $p^{r+1}s$.

Likewise the following analog of Theorem 5.3 holds:

THEOREM 6.3. *The roots of every irreducible* $P(x_1, \ldots, x_k)$ *of class m of degree ps, where* $p \nmid s$, *over* GF(q) *may be written as polynomials of degree m in* λ_1, *a root of an irreducible of the first class of degree ps.*

THEOREM 6.4. *Let* $\psi_k(p^r s, q, j)$ *denote the number of primary factorable irreducibles in k indeterminates over* GF(q) *contained in the j-th class of degree* $p^r s$ *where* $p \nmid s$. *Then*

$$\psi_k(p^r s, q, j) = \psi_k(s, q) p^{ns(p^{r-1}+j-1)-r},$$

where $\psi_k(s, q)$ *is given by Theorem* 3.3.

Proof. From Theorem 6.2 we have

$$\psi_k(p^r s, q, j) = p^{ns-1}q^{(j-1)s}\psi_k(p^{r-1}s, q, p^{r-1}-p^{r-2}). \tag{6.3}$$

It can be proved by induction on r that

$$\psi_k(p^r s, q, p^r-p^{r-1}) = \psi_k(s, q) p^{ns(p^r-1)-r}. \tag{6.4}$$

The theorem follows by substituting (6.4), with r replaced by $r-1$, in (6.3).

The total number of irreducibles $\overline{\psi}_k(ps, q)$ constructed in all the classes of degree ps is

$$\overline{\psi}_k(ps, q) = \psi_k(s, q)(p^{ns-1})(1+q^s+\ldots+q^{(p-2)s}) \tag{6.5}$$

according to Theorem 6.2. It is instructive to take an example to compare $\overline{\psi}_k(ps, q)$ with $\psi_k(ps, q)$:

Let $k = 2$, $p = 2$, $n = 1$, and $s = 3$. From Theorem 3.3, $\psi_2(6, 2) = 679$. Substituting $\psi_2(3, 2) = 22$ in (6.5) and evaluating yields $\overline{\psi}_2(6, 2) = 88$.

References

[1] L. Carlitz, *On factorable polynomials in several indeterminates*, Duke Math. Journ. 2 (1936), pp. 660-670.

[2] — Unpublished notes for a course in arithmetic of polynomials.

[3] L. E. Dickson, *Higher irreducible congruences*, Bull. Amer. Math. Soc. 3 (1897), pp. 381-389.

[4] — *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig 1901.

[5] C. Jordan, *Traité des Substitutions et des Équations Algébriques*, Paris 1870.

[6] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. Journ. Math. 1 (1878), pp. 184-240.

[7] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), pp. 243-274.

[8] J. A. Serret, *Détermination des fonctions entières, suivant un module premier, dans le cas où le degre est égal au module*, Journ. Math. Pures Appl. 2, 18 (1873), pp. 301-304.

Reçu par la Rédaction le 27. 6. 1966