Generators for groups of permutation polynomials over finite fields

By CHARLES WELLS in Cleveland (Ohio, U. S. A.)*)

1. Introduction. Let $GF(q)$ denote the finite field of order $q=p^n$. If Φ is a function from $GF(q)$ to $GF(q)$, a polynomial f over $GF(q)$ is said to represent Φ if $f(\xi)=\Phi(\xi)$ for all $\xi\in GF(q)$. If follows from the Lagrange interpolation formula that every such function Φ is represented by a unique polynomial f of degree $\leqq q-1$. (No such simple theorem is true over the ring of integers (mod p^n); see CARLITZ [5], NÖBAUER [12], RÉDEI and SZELE [13].)

A *permutation polynomial* is simply a polynomial which represent a permutation. The first systematic investigation of permutation polynomials was undertaken by DICKSON [8, 9]; the permutation polynomials over $GF(p)$ had previously been investigated by HERMITE [11]. Other references to early work done on special cases may be found in DICKSON [8].

DICKSON's work suggested much of the work done since with permutation polynomials. His longest and most detailed investigation culminated in his listing of all the permutation polynomials of degree $\leqq 6$ for all $GF(q)$. (We note here that CAVIOR [6] extended these results partially to octic binomial permutation polynomials.)

By means of this list DICKSON proved that the symmetric group on 7 letters was generated by the permutations x^5 and $\alpha x+\beta$ (α, $\beta\in GF(7)$, $\alpha\neq 0$). This suggested our Theorem 4. 1, first proved by CARLITZ [2]. By a modification of CARLITZ's method, FRYER [10] found generators for the alternating group on p letters (Theorem 4. 6).

The present paper contains a number of new theorems on generators of the symmetric group on q letters and its subgroups. These include a sharpening of CARLITZ's result (Theorem 4. 2) and the presentation of generators of three small subgroups (Theorem 4. 4). A more interesting result is the discovery of several sets of generators for the alternating group on q letters (Theorems 4. 7 and 4. 8).

*) Supported by National Science Foundation Grant GF—1891.

None of these sets of generators is a direct generalization of FRYER's Theorem; it may be that that result cannot be generalized in a satisfactory way.

Theorems on generators of S_{q+1} and A_{q+1} are found in Sections 6—8 by means of a device used by BURNSIDE [1; p. 185], CARLITZ [3], and others. An element ∞ is added to $GF(q)$, forming the extended domain $\overline{GF(q)}$. Rational functions $f(x)/g(x)$ (where f and g are polynomials over $GF(q)$) are well defined as mappings of $\overline{GF(q)}$ into $\overline{GF(q)}$, and all permutations of $\overline{GF(q)}$ are representable by rational functions, as CARLITZ showed [3, p. 326—327]. Theorems 7. 2, 7. 3, 8. 2, and 8. 3 exhibit generators of S_{q+1} and A_{q+1} in terms of rational functions.

2. Preliminaries. Throughout the following, q will be assumed to be fixed and greater than 2. Many of the theorems are false for $q=2$ (for example Lemma 4. 3).

$GF(q)$ always includes $GF(p)$. In this paper the elements of $GF(p)$ will be written as integers; it will be understood that k and $k+mp$ are the same element of $GF(p)$ for all m. It is in this sense that a formula like (3. 2) below should be understood.

If two polynomials represent the same function, then they differ by a polynomial multiple of x^q-x. The *reduced form* of a polynomial will here be taken to be the remainder obtained when the polynomial is divided by x^q-x. When two permutation polynomials are combined by the operation of composition, the result may be assumed to be in reduced form; in this sense the set of permutation polynomials of degree $\leqq q-1$ represents the symmetric group S_q. It is not hard to prove that in fact a permutation polynomial cannot have degree $q-1$.

It is convenient to write

$$\langle g(x)\rangle \langle f(x)\rangle = \langle h(x)\rangle \tag{2. 1}$$

when $f(g(x))\equiv h(x)$ (mod x^q-x). Then $\langle g(x)\rangle$ is the function represented by $g(x)$. However, except when it is convenient to write out formulas like (2. 1), we shall follow the usual practice of identifying the polynomial and the function.

3. We collect here some elementary facts about permutation polynomials. In the first place, it follows from the cancellation laws that αx and $x+\beta$ are permutation polynomials for any β and any $\alpha\neq 0$ in $GF(q)$. It follows from a theorem of DICKSON [9; p. 59] that x^b is a permutation polynomial for any integer b such that $(b, q-1)=1$. This may also be proved directly: let ϱ be a primitive root of $GF(q)$, set $\alpha=\varrho^r$, $\beta=\varrho^s$, and note that $\alpha^b=\beta^b$ if and only if $rb\equiv sb$ (mod $q-1$).

In particular, x^{q-2} is a permutation polynomial. It is, in fact, the function that takes every nonzero element into its inverse.

For later use we note the following rules of calculation:

(3. 1) $$\langle x+\alpha\rangle\langle x+\beta\rangle=\langle x+\alpha+\beta\rangle \qquad (\alpha,\ \beta\in GF(q)).$$

(3. 2) $$\langle x+\alpha\rangle^s=\langle x+s\alpha\rangle \qquad (\alpha\in GF(q),\ s \text{ any integer}).$$

(3. 3) $$\langle \alpha x\rangle^s=\langle \alpha^s x\rangle \qquad (\alpha\in GF(q),\ \alpha\neq 0,\ s \text{ any integer}).$$

(3. 4) $$\langle x^{q-2}\rangle^2=\langle x\rangle.$$

(3. 5) $$\langle \alpha x\rangle\langle x+\beta\rangle=\langle \alpha x+\beta\rangle \qquad (\alpha,\ \beta\in GF(q),\ \alpha\neq 0).$$

(3. 6) $$\langle x^{q-2}\rangle\langle \alpha x\rangle=\langle \alpha x^{q-2}\rangle \qquad (\alpha\in GF(q),\ \alpha\neq 0).$$

Since the composition of two permutations is a permutation, it follows that the functions on the right side of the above equations are all permutations.

4. Generators of $A_q^{\prime}$. In [2] CARLITZ proved:

Theorem 4. 1. *S_q is generated by*

(4. 1) $$\alpha x+\beta,\ x^{q-2} \qquad (\alpha,\ \beta\in GF(q),\ \alpha\neq 0).$$

The proof consists in noting that the polynomial

(4. 2) $$g_\gamma(x) = -\gamma^2[((x-\gamma)^{q-2}+\gamma^{-1})^{q-2}-\gamma]^{q-2}$$

represents the transposition (0γ).

Of course, several sets of generators of the abstract symmetric group are known; see, for example, COXETER and MOSER [7; pp. 63—66]. The transpositions form such a set. The value of the generators found in this section is that they are simple as polynomials; it is evident from (4. 2) that simplicity as polynomials and simplicity as permutations are not equivalent.

We may simplify Theorem 4. 1 as follows. Let ϱ be a primitive root of $GF(q)$.

Theorem 4. 2. *S_q is generated by*

(4. 3) $$\varrho x,\ x+1, \text{ and } x^{q-2}.$$

Proof. Let $\alpha,\ \beta\in GF(q)$, $\alpha\beta\neq 0$. Let $\alpha=\varrho^s$, $\beta=\varrho^t$. Then the proof follows from (3. 3) and

(4. 4) $$\langle \alpha x+\beta\rangle=\langle \varrho x\rangle^{s-t}\langle x+1\rangle\langle \varrho x\rangle^t.$$

By an elaboration of these methods we may find generators for the alternating group A_q. Since the polynomials given in (4. 1) and (4. 3) do not necessarily represent even permutations, we first prove

Lemma 4. 3. *For all α, $x+\alpha$ and $(x^{q-2}+\alpha)^{q-2}$ are even; αx is even if and only if α is a nonzero square; x^{q-2} is even if and only if $q\equiv 3 \pmod 4$.*

Proof. By (3. 1) $x+\alpha$ is composed of p^{n-1} cycles of length p. Thus, if p is odd, or if $q=2^n$ and $n>1$, then $x+\alpha$ is even. Since $\langle (x^{q-2}+\alpha)^{q-2}\rangle = \langle x^{1-2}\rangle \cdot \langle x+\alpha\rangle \langle x^{q-2}\rangle$, it is even regardless of what x^{q-2} is.

By (3. 3) αx is a power of ϱx (as permutations), which is a cycle of length $q-1$. The second clause follows from this and the fact that every element of $GF(2^n)$ is square.

As a permutation, x^{q-2} consists of disjoint transpositions containing all elements of $GF(q)$ except 0, 1, -1. It therefore contains $\frac{1}{2}(q-3)$ transpositions when q is odd and $\frac{1}{2}(q-2)$ when q is even (since then $1=-1$). This proves the lemma.

We now define the following sets:

$$L_q = \{\alpha x+\beta \mid \alpha,\ \beta\in GF(q),\ \alpha\neq 0\}$$

$$AL_q = \{\alpha^2 x+\beta \mid \alpha,\ \beta\in GF(q),\ \alpha\neq 0\}$$

$$Q_q = \{(x^{q-2}+\alpha)^{q-2} \mid \alpha\in GF(q)\}.$$

The following equations imply that L_q, AL_q, and Q_q are actually groups

$$\langle \alpha x+\beta\rangle\langle \gamma x+\delta\rangle = \langle \alpha\gamma x+\beta\gamma+\delta\rangle \tag{4. 5}$$

$$\langle (x^{q-2}+\alpha)^{q-2}\rangle\langle (x^{q-2}+\beta)^{q-2}\rangle = \langle (x^{q-2}+\alpha+\beta)^{q-2}\rangle. \tag{4. 6}$$

Evidently the order of L_q is $q(q-1)$, that of AL_q is $\frac{1}{2}q(q-1)$, q odd, and that of Q_q is q. Q_q is isomorphic to the additive group of $GF(q)$. We have

Theorem 4. 4. *L_q is generated by ϱx and $x+1$. AL_q is generated by $\varrho^2 x$ and $x+1$. The elements of Q_q may be obtained from $(x^{q-2}+1)^{q-2}$ and $\varrho^2 x$. Furthermore, $AL_q \subseteqq A_q$, $Q_q\subseteqq A_q$.*

Proof. The first two sentences follow from (4. 4) and the fact that every element in a finite field is the sum of two squares (see [12; p. 46]). The third sentence follows from the last mentioned fact, (3. 3), and

$$\langle (x^{q-2}+\alpha^2)^{q-2}\rangle = \langle \alpha^2 x\rangle\langle (x^{q-2}+1)^{q-2}\rangle\langle \alpha^{-2}x\rangle. \tag{4. 7}$$

The last sentence follows from Lemma 4. 3.

The groups L_q and AL_q were first considered by Burnside [1; pp. 181—185].

We now prove a lemma on generators for the alternating group A_n on n letters $\{0, 1, \cdots, n-1\}$. Let $R=(0\ 1\ 2)$ and $S=(0\ 1\ 2\ \cdots\ n-1)$.

Lemma 4. 5. *For odd n, A_n is generated by R and S.*

Proof. We have

$$(0\ 1\ 3) = S^{-1}R^{-1}SR$$

and

$$(0\ 1\ i+1) = (0\ 1\ i)S^{-i+1}RS^{i-1}(0\ 1\ i)^{-1}(0\ 1\ i-1),$$

for $i=3, \cdots, n-1$. Since the permutations $(0\ 1\ i)$ $(i=2, 3, \cdots, n-1)$ generate A_n, this proves the lemma.

Using this lemma, FRYER [10] proved

Theorem 4. 6. *Let p be an odd prime. Then A_p is generated by $x+1$ and mx^{p-2}, where m is any square if* $p\equiv 3 \pmod 4$ *and any nonsquare if* $p\equiv 1 \pmod 4$. *Otherwise $x+1$ and mx^{p-2} generate S_p.*

Now FRYER's proof depends on the fact that in $GF(p)$ the permutation $x+1$ is a single cycle containing all the elements of the field, and so is the S of Lemma 4. 5. But for general $GF(p^n)$, $x+1$ contains n cycles and FRYER's proof does not work.

However, we may find generators for the general case using (4. 2). For the elements $(0\ 1\ \alpha)$ $(\alpha \in GF(q))$ generate A_q, and

$$(0\ 1\ \alpha) = (0\ 1)(0\ \alpha) = \langle g_1(x)\rangle\langle g_\alpha(x)\rangle =$$

$$= \langle x-1\rangle Q\langle x+1\rangle Q\langle x-1\rangle Q\langle -x\rangle\langle x-\alpha\rangle Q\langle x-\alpha^{-1}\rangle Q\langle x-\alpha\rangle Q\langle -\alpha^2 x\rangle,$$

where Q denotes the permutation x^{q-2}.

Now for $q\equiv 0$ or $1 \pmod 4$ this has the form

$$E(OEO)E(OEEO)E(OEO)E \tag{4. 8}$$

where E stands for any even permutation and O for any odd one. Grouping in the manner shown we obtain the generators $\alpha^2 x+\beta$ $(\alpha, \beta\in GF(q), \alpha\neq 0)$ and $(x^{q-2}+\gamma)^{q-2}(\gamma\in GF(q))$. For $q\equiv 3 \pmod 4$ we have

$$EEEEEEOEEEEEEO, \tag{4. 9}$$

but we may bring the two odd permutations together by noting that $-x$ commutes (as a permutation) with αx and with x^{q-2}, and that

$$\langle -x\rangle\langle x+1\rangle = \langle x-1\rangle\langle -x\rangle.$$

After this is done we may group them as in (4. 8) to obtain the same set of generators. We therefore have

Theorem 4. 7. *The alternating group A_q is generated by its subgroups AL_q and Q_q.*

Of course, (4. 9) implies the existence of a simpler set of generators, which is incorporated in the following theorem:

Theorem 4. 8. *The alternating group A_q is generated by $\varrho^2 x$, $x+1$, and any one of the elements in the following list:*

(i) $(x^{q-2}+1)^{q-2}$ (*all q*),

(ii) x^{q-2} ($q \equiv 3 \pmod 4$),

(iii) αx^{q-2} ($q \equiv 1 \pmod 4$, *α not square; or* $q \equiv 3 \pmod 4$, *α square*).

Proof. The theorem follows from Theorems 4. 4 and 4. 7, and from (4. 9), Lemma 4. 3, and the following formula:

$$\langle (x^{q-2}+1)^{q-2} \rangle = \langle \alpha x^{q-2} \rangle \langle x+\alpha \rangle \langle \alpha x^{q-2} \rangle. \tag{4. 10}$$

5. Another method of proof. The fact that AL_q and x^{q-2} generate A_q whenever αx^{q-2} is even may also be deduced independently by a method resembling the proof of Fryer's Theorem (Theorem 4. 6). It follows from Lemma 4. 5 by properly renumbering the elements of $GF(q)$ that the permutations

$$(0\ 1\ \varrho) \quad \text{and} \quad T=(0\ 1\ \varrho\ \varrho^2 \cdots \varrho^{q-2}) \tag{5. 1}$$

generate A_q. Let $s=1$ if $q \equiv 1 \pmod 4$ and $s=2$ if $q \equiv 3 \pmod 4$, and let U be the permutation $\varrho^s x^{q-2}$. A lengthy calculation shows that

$$(0\ 1\ \varrho) = T^{-1}[(T\,U\,T)^2\, U (T\,U\,T)^2]^4 T$$

so that T and U generate A_q.

Since $T=\langle \varrho x \rangle \langle g_1(x) \rangle$, we may deduce by a method like that in (4. 8) and (4. 9) that A_q is generated by

$$(\varrho x-1)^{q-2}, \quad (x^{q-2}-1)^{q-2}, \quad \varrho^2 x, \quad x+1, \quad \text{and} \quad \varrho x^{q-2} \tag{5. 2}$$

when $q \equiv 1 \pmod 4$ and

$$-\varrho x, \quad x-1, \quad x^{q-2} \quad \text{and} \quad \varrho^2 x^{q-2} \tag{5. 3}$$

when $q \equiv 3 \pmod 4$. But we may replace $(x^{q-2}-1)^{q-2}$ by $(x^{q-2}+1)^{q-2}$ in (5. 2) since the former is merely the p-lst power of the latter (as permutations), and we may eliminate $(\varrho x-1)^{q-2}$ by means of the equation

$$\langle (\varrho x-1)^{q-2} \rangle = \langle \varrho^2 x - p \rangle \langle \varrho x^{q-2} \rangle.$$

We may replace $-\varrho x$ by $\varrho^2 x$ in (5. 3) because the former is the $\frac{1}{4}(q-1)$st power of the latter. Finally we may substitute $\varrho^m x^{q-2}$ for $\varrho^s x^{q-2}$ for m the proper parity (that is, we must have $m \equiv s \pmod 2$) in both (5. 2) and (5. 3) by means of

$$\langle \varrho^s x^{q-2} \rangle = \langle \varrho^m x^{q-2} \rangle \langle \varrho^{s-m} x^{q-2} \rangle.$$

This shows that αx^{q-2} and AL_q generate A_q when αx^{q-2} is even.

6. The extended domain. Let $r(x)=f(x)/g(x)$ be a rational function over $GF(q)$, where f and g are relatively prime polynomials over $GF(q)$ and g is primary. If g has a root $\beta \in GF(q)$, then r does not represent a function from $GF(q)$ into $GF(q)$ since $r(\beta)$ is undefined. We may evade this difficulty by adding an element ∞ to $GF(q)$ obeying the following rules of calculation:

$$r(\beta) = \begin{cases} f(\beta)g(\beta)^{-1} & (g(\beta) \neq 0) \\ \infty & (g(\beta) = 0) \end{cases} \tag{6.1}$$

and

$$r(\infty) = \begin{cases} \infty & (\deg g < \deg f) \\ 0 & (\deg g > \deg f) \\ \operatorname{sgn} f & (\deg g = \deg f). \end{cases} \tag{6.2}$$

From (6. 1) and (6. 2) we may deduce the usual rules of calculation. For example for $\alpha, \beta, \gamma, \delta \in GF(q)$ we have

$$\gamma \cdot \infty = \gamma/0 = \infty \qquad (\gamma \neq 0) \tag{6.3}$$

$$\frac{\alpha\infty + \beta}{\gamma\infty + \delta} = \frac{\alpha}{\gamma} \qquad (\gamma \neq 0) \tag{6.4}$$

$$f(\infty) = \infty \qquad (f \in GF[q, x],\ \deg f \geqq 1). \tag{6.5}$$

The structure obtained from $GF(q)$ by adding ∞ in this manner is called the *extended domain* and is denoted by $\overline{GF(q)}$.

Carlitz [3; pp. 326—327] showed that every permutation of $\overline{GF(q)}$ is representable by a rational function. In fact, he shows that every permutation is representable in the form $g(t(x))$, where g is a polynomial over $GF(q)$, and t is a member of the *general linear fractional group* of functions of the form

$$t(x) = \frac{\alpha x + \beta}{\gamma x + \delta} \qquad (\alpha, \beta, \gamma, \delta \in GF(q),\ \alpha\delta - \beta\gamma \neq 0).$$

7. Generators for S_{q+1}. We may find generators for S_{q+1} by using the following lemma:

Lemma 7. 1. *Let Ψ and Φ be in S_n, with Φ a cycle containing $n-1$ elements and Ψ a transposition containing the element not in Φ. Then Φ and Ψ generate S_n.*

The proof follows from the formula

$$(1\ 2 \cdots n-1)^{-k}(0\ 1)(1\ 2 \cdots n-1)^{k} = (0\ k+1)\ (1 \leqq k \leqq n-2).$$

Now considered as permutations of $\overline{GF(p)}$, $1/x^{p-2}$ is $(0\ \infty)$ and $x+1$ is $(0\ 1\ 2 \cdots p-1)$, so by the lemma they generate S_{p+1}.

For the general case $q=p^n$ we consider the permutation $\varrho x+1$, where ϱ is a primitive root of $GF(q)$. This permutation takes $\infty \to \infty$, and

$$0 \to 1 \to \varrho+1 \to \varrho^2+\varrho+1 \to \varrho^3+\varrho^2+\varrho+1 \to \cdots \to \varrho^{q-2}+\varrho^{q-3}+\cdots+\varrho+1=0.$$

Since ϱ is a primitive q-1st root of unity, it follows that the above series contains no zeros except for the first and last elements. Hence, $\varrho x+1$ is a Ψ as in the lemma, and we have

Theorem 7. 2. *S_{p+1} is generated by $x+1$ and $1/x^{p-2}$. For all $q=p^n$, S_{q+1} is generated by $\varrho x+1$ and $1/x^{q-2}$.*

From this we have immediately

Theorem 7. 3. *S_{q+1} is generated by $1/x$, x^{q-2}, ϱx, and $x+1$.*

Theorem 7. 3 is, by Theorem 4. 4, equivalent to a theorem proved by CARLITZ [3; p. 328] (his proof uses the canonical form mentioned at the end of Section 6).

8. To find generators for the alternating group A_{q+1}, we first prove a lemma analogous to Lemma 4. 3.

Lemma 8. 1. *The permutation $x+\alpha$ is even over $\overline{GF(q)}$ for all $\alpha \in GF(q)$; x^{q-2} is even if and only if $q \equiv 3 \pmod 4$; $1/x$ is odd if and only if $q \equiv 3 \pmod 4$.*

Proof. The first two clauses follow immediately from Lemma 4. 3, since $x+\alpha$ and x^{q-2} leave ∞ unchanged. The other follows from

$$\langle x^{q-2}\rangle = \left\langle \frac{1}{x} \right\rangle (0\infty). \tag{8.1}$$

This proves the lemma.

Now A_{q+1} is generated by the elements $(0\infty\alpha)$ $(\alpha \in GF(q))$. But

$$(0\infty\alpha) = (\alpha\infty)(0\infty)$$

and for any $\alpha \in F(q)$, including $\alpha = 0$,

$$(\alpha\infty) = \left\langle \frac{1}{(x-\alpha)^{q-2}} + \alpha \right\rangle. \tag{8.2}$$

Since

$$\left\langle \frac{1}{x^{q-2}} \right\rangle = \left\langle \frac{1}{x} \right\rangle \langle x^{q-2} \rangle = \langle x^{q-2} \rangle \left\langle \frac{1}{x} \right\rangle$$

we may write $(0\infty\alpha)$ in two ways:

$$(0\infty\alpha) = \langle x+\alpha \rangle \left\langle \frac{1}{x} \right\rangle \langle x^{q-2} \rangle \langle x+\alpha \rangle \langle x^{q-2} \rangle \left\langle \frac{1}{x} \right\rangle \tag{8. 3}$$

and

$$(0\infty\alpha) = \langle x+\alpha \rangle \langle x^{q-2} \rangle \left\langle \frac{1}{x} \right\rangle \langle x+\alpha \rangle \left\langle \frac{1}{x} \right\rangle \langle x^{q-2} \rangle. \tag{8. 4}$$

Grouping the third, fourth and fifth factors together in each of (8. 3) and (8. 4), we find that when $q \equiv 0$ or 1 (mod 4), A_{q+1} is generated by $1/x$, SL_q, and Q_q, where SL_q is the group of permutations of the form $x+\alpha$ $(\alpha \in GF(q))$; and when $q \equiv 3$ (mod 4), A_{q+1} is generated by x^{q-2}, SL_q, and Q'_q, where Q'_q is the group of permutations $(x^{-1}+\beta)^{-1}(\beta \in GF(q))$.

Now it is easy to see that Q_q, Q'_q, and SL_q are all isomorphic to the additive group of $GF(q)$ in the obvious manner. When $q=p$, these groups are cyclic, and we have the following particularly simple theorem:

Theorem 8. 2. *A_{p+1} is generated by*

$$\frac{1}{x}, \quad x+1, \quad (x^{p-2}+1)^{p-2} \qquad (p \equiv 0, 1 \,(\mathrm{mod}\, 4))$$

or

$$x^{p-2}, \quad x+1, \quad (x^{-1}+1)^{-1} \qquad (p \equiv 3 (\mathrm{mod}\, 4)).$$

By Theorem 4. 4 the elements of Q_q may be obtained from $(x^{q-2}+1)^{q-2}$ and $\varrho^2 x$, and the elements of SL_q from $\varrho^2 x$ and $x+1$ (since $SL_q \subseteqq AL_q$). Similarly $\varrho^2 x$ and $(x^{-1}+1)^{-1}$ give the elements of Q'_q. Hence, we have

Theorem 8. 3. *A_{q+1} is generated by*

$$\frac{1}{x}, \quad x+1, \quad \varrho^2 x, \quad (x^{q-2}+1)^{q-2} \qquad (q \equiv 0, 1 \,(\mathrm{mod}\, 4))$$

or

$$x^{q-2}, \quad x+1, \quad \varrho^2 x, (x^{-1}+1)^{-1} \qquad (q \equiv 3 (\mathrm{mod}\, 4)).$$

References

[1] W. Burnside, *Theory of Groups of Finite Order* (New York, 1955).

[2] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.*, **4** (1953), 538.

[3] L. Carlitz, A note on permutation functions in a finite field, *Duke Math. J.*, **29** (1962), 120—123.

[4] L. Carlitz, Permutations in finite fields, *Acta Sci. Math.*, **24** (1953), 196—203.

[5] L. Carlitz, Functions and polynomials (mod p^n), *Acta Arithmetica*, **9** (1964), 67—78.

[6] S. Cavior, A note on octic permutation polynomials, *Mathematics of Computation*, **17** (1963), 450—452.

[7] H. S. M. Coxeter and W. Moser, *Generators and Relations for Discrete Groups*, second edition (Berlin, 1965).

[8] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Annals of Math.*, **11** (1896—97), 65—110.

[9] L. E. Dickson, *Linear Groups with an Exposition of Galois Field Theory* (New York, 1958).

[10] K. Fryer, Note on permutations in a finite field, *Proc. Amer. Math. Soc.*, **6** (1955), 1—2.

[11] Ch. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Paris.*, **57** (1863), 750—757.

[12] W. Nöbauer, Bemerkungen über die Darstellung von Abbildungen durch Polynome und Rationale Funktionen, *Monatshefte für Math.*, **68** (1964), 138—142.

[13] L. Rédei and T. Szele, Algebraisch-zahlentheoretische Betrachtungen über Ringe. I, *Acta Math.* **79** (1947), 291—320.

(Received February 24, 1966)