NOTE ON PERMUTATIONS IN A FINITE FIELD

K. D. FRYER

A recent paper by Carlitz [1] has prompted me to submit the present note. Carlitz proved the

**Theorem (Carlitz).** Every permutation on the numbers of GF(q) can be derived from the permutation polynomials

\[
ax + \beta, \quad x^{q-2} \quad (\alpha, \beta \in GF(q), \alpha \neq 0).
\]

In this paper we prove the following:

**Theorem.** The permutations

\[
P: x' = x + 1, \quad Q: x' = mx^{q-2}
\]

in GF(q), q prime, generate the symmetric group \(S_q\) if:

1. \(m\) is a square of GF(q), \(q = 4n+1\),
2. \(m\) is a nonsquare of GF(q), \(q = 4n+3\),

and generate the alternating group \(A_q\) if:

3. \(m\) is a square of GF(q), \(q = 4n+3\),
4. \(m\) is a nonsquare of GF(q), \(q = 4n+1\).

This result, which arose as a consequence of a theorem in [2], includes the result of Carlitz when \(q\) is prime, in that if all \(\alpha\) are used in (1), then our \(Q\) is present.

**Proof of the theorem.** \(Q\) is of order two, since under \(Q\),

\[
x' = \begin{cases} 
m/x, & x \neq 0, \\
0, & x = 0.
\end{cases}
\]

Hence \(Q\) in standard form is a product of transpositions. If \(m\) is a square of \(GF(q)\), \(Q\) leaves 0 and two other elements fixed. Then \(Q\) is an odd permutation if \(q = 4n+1\), and even if \(q = 4n+3\). \(Q\) has the reverse character if \(m\) is a nonsquare of \(GF(q)\), for then only 0 is left fixed by \(Q\), and \(Q\) contains an extra transposition.

Hence \(\{P, Q\}\) contains even and odd permutations if (2) or (3) holds, but only even permutations if (4) or (5) holds. But \(\{P, Q\}\) contains the permutation

\[
R = P^{-1}QP^mQP^{-1}: x' = -1/x, \quad x \neq 0, 1.
\]

Received by the editors February 15, 1954.
Under this permutation,
\[0 \to -1 \to 1 \to 0,\]
and in standard form \(R = (0 \ -1 \ 1)\) [product of transpositions]. \(R\) is an even permutation for all \(q\).

Then \(R^2 = (0 \ 1 \ -1), \ P^{-1}R^2P = (0 \ 1 \ 2),\) and this permutation and \(P = (0 \ 1 \ 2 \cdots q-1)\) generate \(\mathfrak{S}_q\). The theorem follows.

In particular, the permutations
\[x' = x + 1, \quad x' = -x^{q-2}\]
in \(GF(q),\) \(q\) prime, generate \(\mathfrak{S}_q\) for all \(q\), while the permutations
\[x' = x + 1, \quad x' = x^{q-2}\]
generate \(\mathfrak{S}_q\) if \(q = 4n + 1,\) and \(\mathfrak{A}_q\) if \(q = 4n + 3.\)

Consider now the following sets of permutations in \(GF(q)\):

\[
\begin{align*}
(A) & \quad x' = x + 1, \quad x' = \alpha x, \quad x' = x^{q-2}, \quad \alpha \in GF(q), \alpha \neq 0. \\
(B) & \quad x' = x + 1, \quad x' = mx, \quad x' = x^{q-2}, \quad m \in GF(q), \text{fixed, } m \neq 0. \\
(C) & \quad x' = x + 1, \quad x' = mx^{q-2}, \quad m \in GF(q), \text{fixed, } m \neq 0.
\end{align*}
\]

The permutations (A) are in effect the permutations (1) used in Carlitz’s result.

The sets (A), (B), (C) are equivalent if \(m\) belongs to (2) or (3) in the sense that each set generates \(\mathfrak{S}_q\). Moreover (A) and (B) are equivalent if \(m\) is in (5); each generates \(\mathfrak{S}_q\). (B) will give (C) for this \(m\) but the converse is not true, since (C) then yields the alternating group. Finally (B) and (C) are equivalent for \(m\) in (4), each generating \(\mathfrak{A}_q\), and (B) is equivalent to (A) if \(\alpha\) in (A) is restricted to squares of \(GF(q)\).

**References**


Royal Military College of Canada

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use