Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 4, pp. 1051–1062
DOI : 10.1080/09720529.2021.1974649

Semilinear groups contained in alternating group on a finite-dimensional linear space

Keisuke Hakuta
Institute of Science and Engineering
Shimane University
Academic Assembly
1060 Nishikawatsu-cho
Matsue, Shimane 690-8504
Japan

Abstract

Let $\mathbb{F}_q$ be a finite field with q elements, and n a positive integer with $n \geq 2$, where $q = p^m$ (p : a prime, m : a positive integer). It is natural to ask under which conditions a semilinear group over $\mathbb{F}_q$ is a proper subgroup of the alternating group $\mathrm{Alt}(\mathbb{F}_q^n)$. In this paper, we provide necessary conditions for semilinear groups over $\mathbb{F}_q$ to be subgroups of the alternating group $\mathrm{Alt}(\mathbb{F}_q^n)$ on the n-dimensional linear space $\mathbb{F}_q^n$. We shall show that if $q = 2$ and $n \geq 3$, or $p = 2$ and $n \geq 2$, then the affine semilinear group $\mathrm{A\Gamma L}_n(\mathbb{F}_q)$ (resp. the general semilinear group $\mathrm{\Gamma L}_n(\mathbb{F}_q)$) is a proper subgroup of the alternating group $\mathrm{Alt}(\mathbb{F}_q^n)$, respectively. In addition, we shall also prove that if one of the following five conditions holds: (i) $q = 2$ and $n \geq 3$, (ii) $p = 2$ and $n \geq 2$, (iii) $p \equiv 1 \bmod 4$ and $n \geq 3$, (iv) $p \equiv 3 \bmod 4$ and m : odd, (v) $p \equiv 3 \bmod 4$, m, n : even, then the affine special semilinear group $\mathrm{A\Sigma L}_n(\mathbb{F}_q)$ (resp. the special semilinear group $\mathrm{\Sigma L}_n(\mathbb{F}_q)$) is a proper subgroup of the alternating group $\mathrm{Alt}(\mathbb{F}_q^n)$, respectively. Our results are generalizations and improvements of several known results. These results can be derived from the formula of the sign of the permutation induced by the p^k -th Frobenius maps on $\mathbb{F}_{p^m}$ $(1 \leq k \leq m)$.

Subject Classification: (*2010*) *Primary 15A04, Secondary 12E20, 20B25, 20D06.*

Keywords: *Alternating group, Frobenius automorphism, Semilinear group, Semilinear transformation.*

1. Introduction

Let $\mathbb{K}$ be a field of characteristic $p := \mathrm{char}(\mathbb{K})$, and let n be a positive integer with $n \geq 1$. Let $X_1, \ldots, X_n$ denote n indeterminates over $\mathbb{K}$,

E-mail: **hakuta@cis.shimane-u.ac.jp**

and let $\boldsymbol{x} := (X_1, \ldots, X_n)$ denote the n-tuple of indeterminates over the n-dimensional linear space $\mathbb{K}^n$. We denote by $\mathrm{GL}_n(\mathbb{K})$ (resp. $\mathrm{SL}_n(\mathbb{K})$) the general linear group of degree n over $\mathbb{K}$ (resp. the special linear group of degree n over $\mathbb{K}$). Let $\mathrm{AGL}_n(\mathbb{K}) := \mathbb{K}^n \rtimes \mathrm{GL}_n(\mathbb{K})$ denote the group of all affine transformations $\boldsymbol{x} \mapsto A\boldsymbol{x} + b$ with $A \in \mathrm{GL}_n(\mathbb{K})$ and $\boldsymbol{x}, b \in \mathbb{K}^n$. Let $\mathrm{ASL}_n(\mathbb{K}) := \mathbb{K}^n \rtimes \mathrm{SL}_n(\mathbb{K})$ denote the subgroup of $\mathrm{AGL}_n(\mathbb{K})$ consisting of the affine transformations $\boldsymbol{x} \mapsto A'\boldsymbol{x} + b$ with $A' \in \mathrm{SL}_n(\mathbb{K})$. We use the symbol $\mathrm{Aut}(\mathbb{K})$ to denote the group of field automorphisms of $\mathbb{K}$. Let $\mathbb{F}$ be the prime subfield contained in the field $\mathbb{K}$. Remark that $\mathrm{Aut}(\mathbb{K}) = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. The general semilinear group $\Gamma\mathrm{L}_n(\mathbb{K})$ of degree n over $\mathbb{K}$ is a semidirect product of $\mathrm{GL}_n(\mathbb{K})$ with $\mathrm{Aut}(\mathbb{K})$ ($\Gamma\mathrm{L}_n(\mathbb{K}) = \mathrm{GL}_n(\mathbb{K}) \rtimes \mathrm{Aut}(\mathbb{K})$). The special semilinear group $\Sigma\mathrm{L}_n(\mathbb{K})$ of degree n over $\mathbb{K}$ is a semidirect product of $\mathrm{SL}_n(\mathbb{K})$ with $\mathrm{Aut}(\mathbb{K})$ ($\Sigma\mathrm{L}_n(\mathbb{K}) = \mathrm{SL}_n(\mathbb{K}) \rtimes \mathrm{Aut}(\mathbb{K})$), the affine semilinear group $\mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K})$ of degree n over $\mathbb{K}$ is a semidirect product of $\mathbb{K}^n$ with $\Gamma\mathrm{L}_n(\mathbb{K})$ ($\mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K}) = \mathbb{K}^n \rtimes \Gamma\mathrm{L}_n(\mathbb{K})$), and the affine special semilinear group $\mathrm{ASL}_n(\mathbb{K})$ of degree n over $\mathbb{K}$ ($\mathrm{A}\Sigma\mathrm{L}_n(\mathbb{K}) = \mathbb{K}^n \rtimes \Sigma\mathrm{L}_n(\mathbb{K})$), respectively. Each element of $\mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K})$ can be written as $\boldsymbol{x} \mapsto A\boldsymbol{x}^\sigma + b$ with $A \in \mathrm{GL}_n(\mathbb{K})$, $\boldsymbol{x}, b \in \mathbb{K}^n$, and $\sigma \in \mathrm{Aut}(\mathbb{K})$, where $\sigma \in \mathrm{Aut}(\mathbb{K})$ acts componentwise on the vector $\boldsymbol{x} = (X_1, \ldots, X_n) \in \mathbb{K}^n$ (i.e., $\boldsymbol{x}^\sigma = (X_1^\sigma, \ldots, X_n^\sigma)$). Similarly, each element of $\mathrm{A}\Sigma\mathrm{L}_n(\mathbb{K})$ (resp. $\Gamma\mathrm{L}_n(\mathbb{K})$, $\Sigma\mathrm{L}_n(\mathbb{K})$) can be written as $\boldsymbol{x} \mapsto A'\boldsymbol{x}^\sigma + b$ (resp. $\boldsymbol{x} \mapsto A\boldsymbol{x}^\sigma$, $\boldsymbol{x} \mapsto A'\boldsymbol{x}^\sigma$), respectively, where $A \in \mathrm{GL}_n(\mathbb{K})$, $A' \in \mathrm{SL}_n(\mathbb{K})$, $\boldsymbol{x}, b \in \mathbb{K}^n$, and $\sigma \in \mathrm{Aut}(\mathbb{K})$. It is well-known that

$$\mathrm{SL}_n(\mathbb{K}) \lhd \mathrm{GL}_n(\mathbb{K}) \lhd \Gamma\mathrm{L}_n(\mathbb{K}) < \mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K}), \tag{1.1}$$

$$\mathrm{SL}_n(\mathbb{K}) \lhd \Sigma\mathrm{L}_n(\mathbb{K}) \lhd \Gamma\mathrm{L}_n(\mathbb{K}) < \mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K}), \tag{1.2}$$

and

$$\mathrm{SL}_n(\mathbb{K}) \lhd \Sigma\mathrm{L}_n(\mathbb{K}) < \mathrm{A}\Sigma\mathrm{L}_n(\mathbb{K}) \leq \mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K}), \tag{1.3}$$

where $<$, $\leq$, and $\lhd$ denote proper subgroup, subgroup, and normal subgroup, respectively (see, for example, [1]). For a (possibly infinite) set $\mathcal{S}$, the cardinality of $\mathcal{S}$, the symmetric group on $\mathcal{S}$ and the alternating group on $\mathcal{S}$ are denoted by $\#\mathcal{S}$, $\mathrm{Sym}(\mathcal{S})$, and $\mathrm{Alt}(\mathcal{S})$, respectively. Let $\mathrm{sgn} : \mathrm{Sym}(\mathcal{S}) \to \{\pm 1\}$ be the sign function. The sign function sgn is a group homomorphism, and $\mathrm{Ker}(\mathrm{sgn}) = \mathrm{Alt}(\mathcal{S})$. When $\mathcal{S}$ is an n-dimensional linear space over $\mathbb{K}$ (i.e., $\mathcal{S} = \mathbb{K}^n$), there exists a natural injective group homomorphism

$$\pi : \mathrm{A}\Gamma\mathrm{L}_n(\mathbb{K}) \to \mathrm{Sym}(\mathbb{K}^n). \tag{1.4}$$

We identify any subgroup G of $\mathrm{A\Gamma L}_n(\mathbb{K})$ with its image $\pi(G)$ via the injective group homomorphism π. Define

$$\mathrm{AL}_n(\mathbb{K}) := \{A^2\boldsymbol{x} + b \mid A \in \mathrm{GL}_n(\mathbb{K}), \boldsymbol{x}, b \in \mathbb{K}^n\} < \mathrm{AGL}_n(\mathbb{K}) \leq \mathrm{A\Gamma L}_n(\mathbb{K}).$$

Let $\mathbb{F}_q$ be a finite field with q elements ($p = \mathrm{char}(\mathbb{F}_q)$, $q = p^m$, and $m \geq 1$). Throughout the paper, we assume that $\mathbb{K}/\mathbb{F}$ be a finite Galois extension with Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Moreover, we focus on the case where $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_p$. Semilinear groups over finite fields or elements of semilinear groups over finite fields are studied by many authors in combinatorial group theory, finite geometries, finite group theory, number theory, and so on (see for instance [1], [2], [3], [4], [8], [10], [19], [21]). Let $\tau_{\gamma,\delta}$ ($(\in \mathrm{AGl}_1(\mathbb{F}_q))$, $\boldsymbol{x} \mapsto \gamma\boldsymbol{x} + \delta$, and let $\phi_{\gamma,k} : \mathbb{F}_q \to \mathbb{F}_q$, $\boldsymbol{x} \mapsto \gamma\boldsymbol{x}^k$, where $\gamma \in \mathbb{F}_q^*$, $\delta \in \mathbb{F}_q$, and $k \geq 1$.

One of the most interesting results in permutation polynomials over finite fields is a theorem which proved by Carlitz [3]:

Theorem 1 ([3, Theorem]) : *Assume that* $q > 2$. *Then we have*

$$\langle \mathrm{AGL}_1(\mathbb{F}_q), \phi_{1,q-2} \rangle = \mathrm{Sym}(\mathbb{F}_q).$$

Theorem 1 ([3, Theorem]) was generalized by Fryer in [12, Theorem] when q is a prime (see also [11]).

Theorem 2 ([3, Theorem]) : *If* γ *is a square of* $\mathbb{F}_p$ *and* $p = 4n+1$, *or* γ *is a nonsquare of* $\mathbb{F}_p$ *and* $p = 4n+3$, *then*

$$\langle \tau_{1,1}, \phi_{\gamma,p-2} \rangle = \mathrm{Sym}(\mathbb{F}_p).$$

If γ *is a square of* $\mathbb{F}_p$ *and* $p = 4n+3$, *or* γ *is a nonsquare of* $\mathbb{F}_p$ *and* $p = 4n+1$, *then*

$$\langle \tau_{1,1}, \phi_{\gamma,p-2} \rangle = \mathrm{Alt}(\mathbb{F}_p).$$

Berger proved the following result ([2, Theorem 1]) for the case $m \geq 2$, and Stafford proved the following result ([21, Theorem 2]) for the case $m \geq 1$. [21, Theorem 2] is a slightly stronger version of [2, Theorem 1].

Theorem 3 ([21, Theorem 2]) : *Let* $\mathcal{G} \leq \mathrm{Sym}(\mathbb{F}_q)$ *be a permutation group. If* $\mathcal{G}$ *contains the affine group* $\mathrm{AGL}_1(\mathbb{F}_q)$ *then either* $\mathcal{G}$ *is a subgroup of* $\mathrm{AGL}_m(\mathbb{F}_p)$, *or*

(i) *if p is odd,* $\mathcal{G} = \mathrm{Sym}(\mathbb{F}_q)$.

(ii) *if* $p = 2$, $\mathcal{G} = \mathrm{Sym}(\mathbb{F}_q)$ *or* $\mathcal{G} = \mathrm{Alt}(\mathbb{F}_q)$.

Stafford also proved the following result ([21, Theorem 1]).

Theorem 4 ([21, Theorem 1]) : *Assume that* $q > 2$. *Let* $1 < k < q-2$ *be an integer relatively prime to* $q-1$. *Define* $\mathcal{G}_k := \langle \tau_{\gamma,\delta}, \phi_{1,k} \mid \gamma \in \mathbb{F}_q^*, \delta \in \mathbb{F}_q \rangle$. *Then*

(i) *If* $k = p^i$ *and* $d = \gcd(m, i)$, *then* $\mathcal{G}_k$ *is the semidirect product of* $\mathrm{AGL}_1(\mathbb{F}_q)$ *and the subgroup of order* m/d *generated by the semilinear map* ϕ_{1,p^d}.

(ii) *If p is odd and k is not a power of p, then* $\mathcal{G}_k = \mathrm{Sym}(\mathbb{F}_q)$.

(iii) *If* $p = 2$ *and k is not a power of 2, then* $\mathcal{G}_k \geq \mathrm{Alt}(\mathbb{F}_q)$. *Moreover,* $\mathcal{G}_k = \mathrm{Sym}(\mathbb{F}_q)$ *if and only if* $\phi_{1,k}$ *is an odd permutation.*

Wells found several sets of generators for the alternating group $\mathrm{Alt}(\mathbb{F}_q)$ ([22, Theorem 4.7] and [22, Theorem 4.8]).

Theorem 5 ([22, Theorem 4.7]) : *The following equation holds* :

$$\mathrm{Alt}(\mathbb{F}_q) = \langle \mathrm{AL}_n(\mathbb{F}_q), \phi_{1,q-2} \circ \tau_{1,\delta} \circ \phi_{1,q-2} \mid \delta \in \mathbb{F}_q \rangle.$$

Theorem 6 ([22, Theorem 4.8]) : *The alternating group* $\mathrm{Alt}(\mathbb{F}_q)$ *is generated by* $\tau_{\rho^2,0}$, $\tau_{1,1}$, *and any one of the elements in the following list:*

(i) $\phi_{1,q-2} \circ \tau_{1,1} \circ \phi_{1,q-2}$ (all q),

(ii) $\phi_{1,q-2}$ ($q \equiv 3 \bmod 4$),

(iii) $\phi_{\gamma,q-2}$ ($q \equiv 1 \bmod 4$, γ not square; or $q \equiv 3 \bmod 4$, γ square).

For other results on permutation polynomials over $\mathbb{F}_q$, see, for example, [4], [5], [6], [7], [9], [11], [13], [14], [15], [16], [22], and [23]. Permutation polynomials have applications in coding theory and cryptography (cf. [18]).

On the other hand, Mortimer consider permutation groups on the n-dimensional linear space $\mathbb{F}_q^n$ over $\mathbb{F}_q$ with $n \geq 2$.

Theorem 7 ([19, Main Theorem]) : *If* $\mathrm{AGL}_n(\mathbb{F}_q) \leq \mathcal{G} \leq \mathrm{Sym}(\mathbb{F}_q^n)$ *with* $n \geq 2$, *then either*

(i) $\mathcal{G} = \mathrm{Alt}(\mathbb{F}_q^n)$ *or* $\mathcal{G} = \mathrm{Sym}(\mathbb{F}_q^n)$ *or*

(ii) there exist integers r and b with $q = r^b$ *such that*

$$\mathrm{ASL}_{bn}(\mathbb{F}_r) \leq \mathcal{G} \leq \mathrm{A\Gamma L}_{bn}(\mathbb{F}_r)$$

or

(iii) $\mathrm{AGL}_2(\mathbb{F}_4) < \mathcal{G} < \mathrm{AGL}_4(\mathbb{F}_2)$ *and* $\mathcal{G}_\alpha \cong \mathrm{Alt}(\mathbb{F}_7)$ ($\mathcal{G}_\alpha$ *is the stabilizer of a point* α *of* $\mathbb{F}_q^n$).

The results [19, Main Theorem], [21, Theorem 1], and [22, Theorem 4.8] lead us to raise to the following question:

Question : Suppose that $n \geq 2$. Set

$$\mathcal{G}_1 := \Gamma\mathrm{L}_n(\mathbb{F}_q), \mathcal{G}_2 := \mathrm{A}\Gamma\mathrm{L}_n(\mathbb{F}_q), \mathcal{G}_3 := \Sigma\mathrm{L}_n(\mathbb{F}_q), \mathcal{G}_4 := \mathrm{A}\Sigma\mathrm{L}_n(\mathbb{F}_q) \leq \mathrm{Sym}(\mathbb{F}_q^n).$$

Under which condition $\mathcal{G}_i < \mathrm{Alt}(\mathbb{F}_q^n)$ holds for each $i\,(1 \leq i \leq 4)$?

The paper answers the above question. The main result of this paper is as follows:

Main Theorem : *Suppose that n is a positive integer with* $n \geq 2$.

(1) If $q = 2$ and $n \geq 3$, or $p = 2$ and $n \geq 2$, then

$$\Gamma\mathrm{L}_n(\mathbb{F}_q) < \mathrm{Alt}(\mathbb{F}_q^n). \tag{1.5}$$

(2) If $q = 2$ and $n \geq 3$, or $p = 2$ and $n \geq 2$, then

$$\mathrm{A}\Gamma\mathrm{L}_n(\mathbb{F}_q) \leq \mathrm{Alt}(\mathbb{F}_q^n). \tag{1.6}$$

(3) We assume that one of the following five conditions holds :

(i) $q = 2$ and $n \geq 3$, (ii) $p = 2$ and $n \geq 2$, (iii) $p \equiv 1 \bmod 4$ and $n \geq 3$, (iv) $p \equiv 3 \bmod 4$ and m : odd, (v) $p \equiv 3 \bmod 4$, m, n : even.

Then we have

$$\mathrm{SL}_n(\mathbb{F}_q) < \mathrm{Alt}(\mathbb{F}_q^n). \tag{1.7}$$

(4) We assume that one of the following five conditions holds :

(i) $q = 2$ and $n \geq 3$, (ii) $p = 2$ and $n \geq 2$, (iii) $p \equiv 1 \bmod 4$ and $n \geq 3$, (iv) $p \equiv 3 \bmod 4$ and m : odd, (v) $p \equiv 3 \bmod 4$, m, n : even.

Then we have

$$\mathrm{A}\Sigma\mathrm{L}_n(\mathbb{F}_q) \leq \mathrm{Alt}(\mathbb{F}_q^n). \tag{1.8}$$

2. Intermediate Results

Let $\sigma : \mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto x^p$ be the p-th Frobenius map on $\mathbb{F}_q = \mathbb{F}_{p^m}$. In Proposition 1, we derive the formula of the sign of the permutation induced by the Frobenius maps $\sigma^k : \mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto x^{p^k}\ (1 \le k \le m)$ over the finite field $\mathbb{F}_{p^m}$.

Proposition 1 (Sign of Frobenius maps) : Let k be a positive integer satisfying $1 \le k \le m$. Then the sign of the p^k-th Frobenius map $\sigma^k : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^{p^k}$ is as follows:

$$\operatorname{sgn}(\sigma^k) = \begin{cases} -1, & (p,m,k) = (2,2,1) \text{ or} \\ & \qquad p \equiv 3 \bmod 4, m : \text{even}, k : \text{odd}, \\ 1, & \text{otherwise.} \end{cases} \tag{2.1}$$

In other words, we have

$$\sigma^k \in \begin{cases} \operatorname{Sym}(\mathbb{F}_q) \setminus \operatorname{Alt}(\mathbb{F}_q), & (p,m,k) = (2,2,1) \text{ or} \\ & \qquad p \equiv 3 \bmod 4, m \text{m} : \text{even}, k : \text{odd}, \\ \operatorname{Alt}(\mathbb{F}_q), & \text{otherwise.} \end{cases} \tag{2.2}$$

Proof : For any prime p and for any integer $m \ge 1$, $\mathbb{F}_q = \mathbb{F}_{p^m}$ and $\mathbb{F}_p^m$ are $\mathbb{F}_p$-linear isomorphc to each other. Let $\{\beta_1, \ldots, \beta_m\}$ be an $\mathbb{F}_p$-basis of the m-dimensional $\mathbb{F}_p$-linear space $\mathbb{F}_q$. Then there always exists a normal basis (cf. [17, Theorem 2.35]). If $\{\beta_1, \ldots, \beta_m\}$ is a normal basis, there exists $\alpha \in \mathbb{F}_q$ such that $\beta_i = \alpha^{p^{i-1}}$ for all i $(1 \le i \le m)$. Assume that $\{\alpha^{p^0}, \alpha^{p^1}, \ldots, \alpha^{p^{m-1}}\}$ is an $\mathbb{F}_p$-normal basis of the m-dimensional $\mathbb{F}_p$-linear space $\mathbb{F}_q$. We define the $\mathbb{F}_p$-linear isomorphism $\psi : \mathbb{F}_p^m \to \mathbb{F}_{p^m}$ as follows:

$$\psi : \mathbb{F}_p^m \to \mathbb{F}_{p^m},\quad (a_1, \ldots, a_m) \mapsto a_1 \alpha^{p^0} + \cdots + a_m \alpha^{p^{m-1}},$$

where $a_i \in \mathbb{F}_p$ for each i $(1 \le i \le m)$. Then the map ψ is obviously bijective, and the inverse of the map ψ is given by

$$\psi^{-1} : \mathbb{F}_{p^m} \to \mathbb{F}_p^m,\quad a_1 \alpha^{p^0} + \cdots + a_m \alpha^{p^{m-1}} \mapsto (a_1, \ldots, a_m).$$

Set

$$T_{i,j}^{(m)} := (X_1, \ldots, X_{i-1}, X_j, X_{i+1}, \ldots, X_{j-1}, X_i, X_{j+1}, \ldots, X_m) \in \mathrm{AGL}_m(\mathbb{F}_p)$$

for each $1 \le i, j \le m$ with $i \ne j$. Since $\{\alpha^{p^0}, \alpha^{p^1}, \ldots, \alpha^{p^{m-1}}\}$ is the $\mathbb{F}_p$-normal basis of $\mathbb{F}_q$, the equation

$$(\psi^{-1}\circ\sigma\circ\psi)(a_1,\dots,a_m)=(a_m,a_1,\dots,a_{m-1})$$

holds for each $(a_1,\dots,a_m)\in\mathbb{F}_p^m$. Therefore, we have

$$\psi^{-1}\circ\sigma\circ\psi = T_{1,m}^{(m)}\circ T_{1,m-1}^{(m)}\circ\cdots\circ T_{1,3}^{(m)}\circ T_{1,2}^{(m)}. \tag{2.3}$$

By taking sign of both sides of Equation (2.3), we obtain

$$\begin{aligned}\operatorname{sgn}(\sigma) &= \operatorname{sgn}(\psi^{-1}\circ\sigma\circ\psi)\\ &= \operatorname{sgn}(T_{1,m}^{(m)}\circ T_{1,m-1}^{(m)}\circ\cdots\circ T_{1,3}^{(m)}\circ T_{1,2}^{(m)})\\ &= \operatorname{sgn}(T_{1,m}^{(m)})\operatorname{sgn}(T_{1,m-1}^{(m)})\cdots\operatorname{sgn}(T_{1,3}^{(m)})\operatorname{sgn}(T_{1,2}^{(m)})\\ &= \prod_{i=2}^{m}\operatorname{sgn}(T_{1,i}^{(m)}).\end{aligned} \tag{2.4}$$

From [14, Lemma 1], $\operatorname{sgn}(T_{1,i}^{(m)})$ is given by the following formula:

$$\operatorname{sgn}(T_{1,i}^{(m)})=\begin{cases}1, & p=2 \text{ and } m\geq 3,\\ -1, & p=2 \text{ and } m=2,\\ (-1)^{\frac{p-1}{2}}, & p:\text{odd},\end{cases} \tag{2.5}$$

for each i $(2\leq i\leq m)$. Substituting Equation (2.5) into Equation (2.4) yields

$$\operatorname{sgn}(\sigma)=\begin{cases}1, & p=2 \text{ and } m\geq 3,\\ (-1)^{m-1}, & p=2 \text{ and } m=2,\\ (-1)^{\frac{p-1}{2}(m-1)}, & p:\text{odd}.\end{cases} \tag{2.6}$$

By rewriting Equation (2.6), we get

$$\operatorname{sgn}(\sigma)=\begin{cases}-1, & (p,m)=(2,2) \text{ or } p\equiv 3 \bmod 4,\ m:\text{even},\\ 1, & \text{otherwise}.\end{cases} \tag{2.7}$$

Since the map sgn is a group homomorphism, we have

$$\operatorname{sgn}(\sigma^k)=\operatorname{sgn}(\underbrace{\sigma\circ\cdots\circ\sigma}_{k \text{ times}})=\operatorname{sgn}(\sigma)^k. \tag{2.8}$$

Hence by Equation (2.7) and Equation (2.8), we obtain Equation (2.1). This completes the proof. □

Example 1 : We demonstrate Proposition 1 on the following three examples. Let $f(T)\in\mathbb{F}_p[T]$ be an irreducible polynomial, α a root of f. We represent $\mathbb{F}_q$ as the quotient ring $\mathbb{F}_p[T]/(f(T))$, where $(f(T))$ is the ideal of $\mathbb{F}_p[T]$ generated by $f(T)$.

(1) Set $p=2,\ m=2,$ and $f(T)=T^2+T+1.$ Then we have $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$. It is easy to verify that $\sigma(0)=0,\ \sigma(1)=1,$ $\sigma(\alpha)=\alpha+1,$ and $\sigma(\alpha+1)=\alpha$. Thus, σ is a transposition, and $\sigma\in\mathrm{Sym}(\mathbb{F}_4)\setminus\mathrm{Alt}(\mathbb{F}_4)$.

(2) Set $p=3,\ m=2,$ and $f(T)=T^2+T+2.$ Then we have $\mathbb{F}_9=\{0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2\}$. It is easy to verify that $\sigma(0)=0,\ \sigma(1)=1,\ \sigma(2)=2,\ \sigma(\alpha)=2\alpha+2,\ \sigma(\alpha+1)=2\alpha,$ $\sigma(\alpha+2)=2\alpha+1,\ \sigma(2\alpha)=\alpha+1,\ \sigma(2\alpha+1)=\alpha+2,$ and $\sigma(2\alpha+2)=\alpha$. Thus, σ is a product of three transpositions, and $\sigma\in\mathrm{Sym}(\mathbb{F}_9)\setminus\mathrm{Alt}(\mathbb{F}_9)$.

(3) Set $p=2,\ m=3,$ and $f(T)=T^3+T+1.$ Then we have $\mathbb{F}_8=\{0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1\}$. It is easy to verify that $\sigma(0)=0,\ \sigma(1)=1,\ \sigma(\alpha)=\alpha^2,\ \sigma(\alpha+1)=\alpha^2+1,\ \sigma(\alpha^2)=\alpha^2+\alpha,$ $\sigma(\alpha^2+1)=\alpha^2+\alpha+1,\ \sigma(\alpha^2+\alpha)=\alpha,$ and $\sigma(\alpha^2+\alpha+1)=\alpha+1.$ Thus, σ is a product of two 3-cycles, and $\sigma\in\mathrm{Alt}(\mathbb{F}_8)$.

For a positive integer k with $1\le k\le m,$ define the polynomial map $\sigma_n^k\in\mathrm{A\Gamma L}_n(\mathbb{F}_q)$ as follows:

$$\sigma_n^k(X_1,\dots,X_n):=(X_1^{p^k},\dots,X_n^{p^k})\in\mathrm{A\Gamma L}_n(\mathbb{F}_q).$$

Remark that $\sigma_n^m=\mathrm{id}_{\mathbb{F}_q^n}$.

Proposition 2 (Sign of σ_n^k with $n\ge 2$) : Suppose that $n\ge 2$ and $1\le k\le m.$ Then the sign of the surjective polynomial map $\sigma_n^k\in\mathrm{A\Gamma L}_n(\mathbb{F}_q)$ is as follows:

$$\mathrm{sgn}(\sigma_n^k)=\begin{cases}-1, & p\equiv 3\bmod 4, m:\text{even},\ n,\ k:\text{odd},\\ 1, & \text{otherwise.}\end{cases}\tag{2.9}$$

In other words, we have

$$\sigma_n^k\in\begin{cases}\mathrm{Sym}(\mathbb{F}_q^n)\setminus\mathrm{Alt}(\mathbb{F}_q^n), & p\equiv 3\bmod 4,\ m:\text{even},\ n,\ k:\text{odd},\\ \mathrm{Alt}(\mathbb{F}_q^n), & \text{otherwise.}\end{cases}\tag{2.10}$$

Proof : We define the polynomial map $\sigma_{1,n}^k:\mathbb{F}_q\to\mathbb{F}_q$ as follows:

$$\sigma_{1,n}^k(X_1,\dots,X_n):=(X_1^{p^k},X_2,\dots,X_n).$$

Remark that $\sigma_{1,n}^k\in\mathrm{Sym}(\mathbb{F}_q^n)$. Since

$$\sigma_n^k = (T_{1,n}^{(n)} \circ \sigma_{1,n}^k \circ T_{1,n}^{(n)}) \circ \cdots \circ (T_{1,2}^{(n)} \circ \sigma_{1,n}^k \circ T_{1,2}^{(n)}) \circ \sigma_{1,n}^k$$

and the map sgn is a group homomorphism, we have

$$\begin{aligned}\operatorname{sgn}(\sigma_n^k) &= \operatorname{sgn}((T_{1,n}^{(n)} \circ \sigma_{1,n}^k \circ T_{1,n}^{(n)}) \circ \cdots \circ (T_{1,2}^{(n)} \circ \sigma_{1,n}^k \circ T_{1,2}^{(n)}) \circ \sigma_{1,n}^k) \\ &= \operatorname{sgn}(T_{1,n}^{(n)} \circ \sigma_{1,n}^k \circ T_{1,n}^{(n)}) \circ \cdots \circ \operatorname{sgn}(T_{1,2}^{(n)} \circ \sigma_{1,n}^k \circ T_{1,2}^{(n)}) \circ \operatorname{sgn}(\sigma_{1,n}^k) \\ &= \operatorname{sgn}(\sigma_{1,n}^k)^n \times \prod_{i=2}^n \operatorname{sgn}(T_{1,i}^{(n)})^2 \\ &= \operatorname{sgn}(\sigma_{1,n}^k)^n. \end{aligned} \tag{2.11}$$

By Equation (2.11) and the equation $\sigma_{1,n}^k = \underbrace{\sigma_{1,n} \circ \cdots \circ \sigma_{1,n}}_{k \text{ times}}$, we obtain

$$\operatorname{sgn}(\sigma_n^k) = \left(\operatorname{sgn}(\sigma_{1,n})\right)^{kn}. \tag{2.12}$$

We choose an arbitrary element $\mathbf{x^{(0)}} := (x_2^{(0)}, \ldots, x_n^{(0)}) \in \mathbb{F}_q^{n-1}$. For $\mathbf{x^{(0)}} := (x_2^{(0)}, \ldots, x_n^{(0)}) \in \mathbb{F}_q^{n-1}$, we define the map $\sigma_{1,n,\mathbf{x^{(0)}}}$ as follows:

$$\begin{aligned} \sigma_{1,n,\mathbf{x^{(0)}}} : \quad \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ (x_1, \ldots, x_n) &\mapsto (x_1^p, x_2, \ldots, x_n), \quad \text{if} (x_2, \ldots, x_n) = \mathbf{x^{(0)}}, \\ (x_1, \ldots, x_n) &\mapsto (x_1, x_2, \ldots, x_n), \quad \text{otherwise.} \end{aligned} \tag{2.13}$$

The map $\sigma_{1,n,\mathbf{x^{(0)}}}$ is obviously bijective, and the following equation holds:

$$\sigma_{1,n} = \prod_{\mathbf{x^{(0)}} \in \mathbb{F}_q^{n-1}} \sigma_{1,n,\mathbf{x^{(0)}}}. \tag{2.14}$$

Substituting Equation (2.14) into Equation (2.12) yields

$$\operatorname{sgn}(\sigma_n^k) = \left(\prod_{\mathbf{x^{(0)}} \in \mathbb{F}_q^{n-1}} \operatorname{sgn}(\sigma_{1,n,\mathbf{x^{(0)}}}) \right)^{kn}. \tag{2.15}$$

The right-hand side of Equation (2.14) is a composition of disjoint permutations on $\mathbb{F}_q^n$. By the definition of the map (2.13), we have

$$\operatorname{sgn}(\sigma_{1,n,\mathbf{x^{(0)}}}) = \operatorname{sgn}(\sigma) \tag{2.16}$$

for each $\mathbf{x^{(0)}} := (x_2^{(0)}, \ldots, x_n^{(0)}) \in \mathbb{F}_q^{n-1}$. Finally, combining Equation (2.15) and Equation (2.16) yields

$$\operatorname{sgn}(\sigma_n^k) = \operatorname{sgn}(\sigma)^{knq^{n-1}}. \tag{2.17}$$

Hence, by Equation (2.17) and Proposition 1, we obtain Equation (2.9). □

Example 2 : We demonstrate Proposition 2 on the three examples in Example 1.

(1) $\sigma_2, \sigma_2^2 = \mathrm{id}_{\mathbb{F}_4^2} \in \mathrm{Alt}(\mathbb{F}_4^2)$

(2) $\sigma_3 \in \mathrm{Sym}(\mathbb{F}_9^3) \setminus \mathrm{Alt}(\mathbb{F}_9^3)$, and $\sigma_3^2 = \mathrm{id}_{\mathbb{F}_9^3} \in \mathrm{Alt}(\mathbb{F}_9^3)$.

(3) $\sigma_2, \sigma_2^2, \sigma_2^3 = \mathrm{id}_{\mathbb{F}_8^2} \in \mathrm{Alt}(\mathbb{F}_8^2)$.

Proposition 3 (Sign of σ_n^k): Suppose that $n \geq 1$ and $1 \leq k \leq m$. Then the sign of the surjective polynomial map $\sigma_n^k = (X_1^{p^k}, \ldots, X_n^{p^k}) \in \mathrm{A\Gamma L}_n(\mathbb{F}_q)$ is as follows:

$$\mathrm{sgn}(\sigma_n^k) = \begin{cases} -1, & (p,m,n,k) = (2,2,1,1) \text{ or} \\ & p \equiv 3 \bmod 4,\ m : \text{even},\ n,\ k : \text{odd}, \\ 1, & \text{otherwise.} \end{cases} \tag{2.18}$$

In particular, if $p = \mathrm{char}(\mathbb{F}_q) = 2$ and $n \geq 2$, then $\sigma_n^k \in \mathrm{Alt}(\mathbb{F}_q^n)$ for each $k (1 \leq k \leq m)$.

Proof : This is a direct consequence of Proposition 1 and Proposition 2. □

3. Proof of Main Theorem

We are now in a position to prove Main Theorem.

Proof of Main Theorem.

We first remark that by [14, Main Theorem 1], the containment (1.5) follows immediately from the containment (1.6). Similarly, by [14, Main Theorem 1], the containment (1.7) can be derived from the containment (1.8). Therefore, it suffices to consider assertion (2) and assertion (4). We prove assertion (2). Assertion (2) follows immediately from [14, Corollary 2] and Proposition 2 (or Proposition 3). Next we prove assertion (4). Assertion (4) follows immediately from [20, Theorem 8.8], [14, Main Theorem 2], and Proposition 2 (or Proposition 3). This concludes the proof of Main Theorem. □

Acknowledgements

This work was partially supported by JSPS KAKENHI, Grant-in-Aid for Young Scientists (B) (Grant Number 16K16066) and Grant-in-Aid for Young Scientists (Grant Number 19K20270).

References

[1] S.S. Abhyankar, Galois theory on the line in nonzero characteristic, *Bull. Amer. Math. Soc*. 27 (1992), 68–133.

[2] T.P. Berger, On the automorphism groups of affine-invariant codes, *Des. Codes Cryptogr.* 7 (1996), 215–221.

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

[4] L. Carlitz, A theorem on permutations in a finite field, *Proc. Amer. Math. Soc.* 11 (1960), 456–459.

[5] L. Carlitz, A theorem on "ordered" polynomials in a finite field, *Acta Arith.* 7 (1962), 167–172.

[6] L. Carlitz, Some theorems on permutation polynomials, *Bull. Amer. Math. Soc.* 68 (1962), 120–122.

[7] S.R. Cavior, A note on octic permutation polynomials, *Math. Comp.* 17 (1963), 450–452.

[8] P. Dembowski, Finite Geometries, Reprint of the 1968 edition, Classics in Mathematics, Springer-Verlag, Berlin, 1997.

[9] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* 11 (1897), 65–120, 161–183.

[10] J.D. Dixon, B. Mortimer, Permutation groups, Graduate Texts in Mathematics, Vol. 163, Springer-Verlag, New York, 1996.

[11] K.D. Fryer, A class of permutation groups of prime degree, *Canad. J. Math.* 7 (1955), 24–34.

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

[13] R.M. Guralnick, Subgroups of prime power index in a simple group, *J. Algebra* 81 (1983), 304–311.

[14] K. Hakuta, On permutations induced by tame automorphisms over finite fields, *Acta Math. Vietnam.* 43 (2018), 309–324.

[15] K. Hakuta, Generalization of a counterexample to Derksen's theorem in characteristic two, Beitr. Algebra Geom. 60 (2019), 679–682.

[16] K. Hakuta, Permutation groups induced by Derksen groups in characteristic two, *Acta Math. Vietnam.* 46 (2021), 123–132.

[17] R. Lidle and H. Niederreiter, Finite Fields, Second edition, Encyclopedia of Mathematics and its applications, Vol. 20, Cambridge University Press, 1997.

[18] J. Liu, S. Mesnager, L. Chen, Partially Homomorphic Encryption Schemes over Finite Fields, In: C. Carlet, M. Hasan, V. Saraswat (eds.), Security, Privacy, and Applied Cryptography Engineering – SPACE 2016, Lecture Notes in Computer Science, vol. 10076 (2016), 109–123.

[19] B. Mortimer, Permutation groups containing affine groups of the same degree, *J. London Math. Soc*. 15 (1977), 445–455.

[20] J.J. Rotman, An Introduction to the Theory of Groups, fourth edition, Graduate Texts in Mathematics, Vol. 148, Springer-Verlag, 1995.

[21] R.M. Stafford, Groups of permutation polynomials over finite fields, *Finite Fields Appl*. 4 (1998), 450–452.

[22] C. Wells, Generators for groups of permutation polynomials over finite fields, *Acta Sci. Math*. (Szeged) 29 (1968), 167–176.

[23] M.E. Zieve, On a theorem of Carlitz, *J. Group Theory* 17 (2014), 667–669.

Received May, 2021