Automorphisms of Finite Fields

H. W. Lenstra, Jr.

Department of Mathematics, University of California, Berkeley, California 94720

Communicated by K. A. Ribet

Received September 29, 1988, revised March 14, 1989

Let $F$ be a finite field, and $\phi: F^* \rightarrow E$ a surjective group homomorphism from the multiplicative group $F^*$ of $F$ to a non-trivial abelian group $E$. A theorem of McConnel (Acta Arith. 8 (1963), 127-151) describes the permutations $\sigma$ of $F$ with the property that $\phi(\sigma x - \sigma y) = \phi(x - y)$ for all $x, y \in F, x \neq y$. We give a short proof of this theorem, based on an argument of Bruen and Levinger (Canad J Math. 25 (1973), 1060-1065). In addition, we describe the permutations $\sigma$ of $F$ for which there exists a permutation $\kappa$ of $E$ with the property that $\phi(\sigma x - \sigma y) = \kappa \phi(x - y)$ for all $x, y \in F, x \neq y$. Finally, we prove a result about automorphisms of the norm form of an arbitrary finite extension of fields.

1. INTRODUCTION

Let $F$ be a finite field, $F^*$ its multiplicative group, $E$ a non-trivial abelian group, and $\phi: F^* \rightarrow E$ a surjective group homomorphism. In this paper we are concerned with three permutation groups of $F$. The first group, which we denote by $N$, consists of all permutations $\sigma$ of $F$ satisfying

$$\phi(\sigma x - \sigma y) = \phi(x - y) \quad \text{for all } x, y \in F \text{ with } x \neq y. \quad (1)$$

Denote by $D$ the kernel of $\phi$.

**Theorem 1.** Let $\sigma$ be a permutation of $F$. Then $\sigma$ belongs to $N$ if and only if there exist an element $a \in D$, a field automorphism $\alpha$ of $F$ with $\phi \alpha = \phi$, and an element $b \in F$, such that

$$\sigma x = a \alpha x + b \quad \text{for all } x \in F. \quad (2)$$

This theorem was first proved by McConnel [4]. The case that $E$ is a group of order two is due to Carlitz [2]. Carlitz's result immediately
implies an affirmative answer to the following question, which was asked
by F. Rivero [6]: let $\sigma$ be an automorphism of the additive group of a
finite field $F$ of odd characteristic, and suppose that $\sigma$ maps the set of
squares to itself and satisfies $\sigma 1 = 1$, does it follow that $\sigma$ is a field
automorphism of $F$?

In Section 2 we give a short proof of Theorem 1, which is based on an
argument of Bruen and Levinger [1].

The second group that we consider, denoted by $G$, consists of all
permutations $\sigma$ of $F$ for which there exists a permutation $\kappa$ of $E$ such that

$$\phi(\sigma x - \sigma y) = \kappa \phi(x - y) \quad \text{for all } x, y \in F \text{ with } x \neq y$$

(3)

Denote by $K$ the subfield of $F$ generated by $D$. A $K$-semilinear
automorphism of $F$ is an automorphism $\beta$ of the additive group of $F$ for
which there exists a field automorphism $\gamma$ of $K$ such that for all $x \in K, y \in F$
one has $\beta(xy) = (\gamma x)(\beta y)$

Theorem 2 The group $G$ is the normalizer of $N$ in the group of all
permutations of $F$. Also, if $\sigma$ is a permutation of $F$, then $\sigma$ belongs to $G$ if
and only if there exist a $K$-semilinear automorphism $\beta$ of $F$ and an element
$b \in F$, such that

$$\sigma x = \beta x + b \quad \text{for all } x \in F$$

(4)

The proof of Theorem 2 is given in Section 3.

A permutation $\kappa$ of $E$ is called affine if there exist an element $e_0$ of $E$ and
a group automorphism $\chi$ of $E$ such that $\kappa e = e_0 \chi e$ for all $e \in E$.

The third group that we consider is the group of those permutations $\sigma$
of $F$ for which there exists an affine permutation $\kappa$ of $E$ such that (3) holds.
We denote this group by $H$. Clearly we have $N \subset H \subset G$.

Theorem 3 Let $\sigma$ be a permutation of $F$. Then $\sigma$ belongs to $H$ if and
only if there exist an element $a \in F^*$, a field automorphism $\alpha$ of $F$, and an
element $b \in F$, such that

$$\sigma x = a \alpha x + b \quad \text{for all } x \in F$$

If $K = F$ then we have $H = G$.

The proof of Theorem 3 is given in Section 4.

Theorem 3 extends results obtained by McConnel [4, Theorem 2] and
Grundhofer [3]. McConnel considers the case that there exists an element
$e_0$ of $E$ such that for each $e \in E$, one has $\kappa e = e_0 e$, and Grundhofer the case
that $\kappa e = e^{-1}$ for all $e \in E$. 

Our final result concerns arbitrary fields. It sharpens a lemma that was proved by Meyer and Perlis [5].

**Theorem 4** Let $L$ be a field having more than 2 elements, and $M_1, M_2$ field extensions of $L$ of finite degree. Let $N_i : M_i \rightarrow L$ denote the norm map, for $i = 1, 2$. Let further $\sigma : M_1 \rightarrow M_2$ be a surjective $L$-linear map. Then we have $N_2 \sigma = N_1$ if and only if there exist an element $a \in M_2$ with $N_2 a = 1$ and a field isomorphism $\alpha : M_1 \rightarrow M_2$ that is the identity on $L$, such that

$$\sigma x = a \cdot x \quad \text{for all} \quad x \in M_1.$$

The proof of Theorem 4 is given in Section 5.

If $L$ has cardinality two, then clearly $\sigma$ satisfies $N_2 \sigma = N_1$ if and only if it is bijective. It follows that in this case the conclusion of the theorem is still correct if $M_2$ has cardinality at most 4, but that it is wrong for larger $M_2$.

2 Proof of Theorem 1

The "if" part of Theorem 1 is trivial. We prove the "only if" part. Let $N_0 = \{ \sigma \in N \mid \sigma 0 = 0 \}$, this is a subgroup of $N$. For $b \in F$, let $\tau_b$ be the permutation of $F$ that sends each $x \in F$ to $x + b$, and let $T = \{ \tau_b \mid b \in F \}$. Clearly, $T$ is a subgroup of $N$ that is isomorphic to the additive group of $F$. Since $T$ acts transitively on $F$ we have $N = TN_0 = N_0 T$.

Let $q = \# F$, and let $F^d = F \times F \times \ldots \times F$ be the $q$-dimensional $F$-vector space consisting of all functions $F \rightarrow F$. We consider $F^d$ as a ring with componentwise ring operations, i.e., $(g_1 g_2) x = (g_1 x)(g_2 x)$ for $g_1, g_2 \in F^d, x \in F$. The subring of constant functions is identified with $F$. Let $z \in F^d$ be the identity map $F \rightarrow F$. The map from the polynomial ring $F[X]$ to $F^d$ that sends each $f \in F[X]$ to $f(z)$ induces a ring isomorphism $F[X]/(X^q - X) \cong F^d$.

We define a left action of $N$ on $F^r$ by $(\sigma g) x = g(\sigma^{-1} x)$, for $\sigma \in N, g \in F^r, x \in F$. For example, for each $b \in F$ we have $\tau_b z = z - b$. Each $\sigma$ acts as a ring automorphism on $F^d$. Also, the action is $F$-linear, so it makes $F^d$ into a left module over the group ring $F[N]$.

Write $d = \# D$, and let $V$ be the sub-$F[N]$-module of $F^r$ generated by $z^d$.

**Lemma** For every $g \in V$ there exists $f \in F[X]$ such that

$$\deg f \leq d, \quad g = f(z).$$

Also, $z$ and $z^{1/d}$ belong to $V$. 


**Proof of the Lemma.** Putting $y = 0$ in $(1)$ we see that, for any $\sigma \in N_0$ and $x \in F^*$, we have $\phi_\sigma x = \phi x$, so $(\sigma x)/x \in D$ and $(\sigma x)^d = x^d$; this holds for $x = 0$ as well. Therefore each $\sigma \in N_0$ fixes the function $z^d$. From $N = TN_0$ it thus follows that the orbit of $z^d$ under $N$ is the same as the orbit of $z^d$ under $T$, which is $\{ (z - b)^d : b \in F \}$.

Since $V$ is, as an $F$-vector space, spanned by the orbit of $z^d$ under $N$, we find that $V$ exactly consists of the $F$-linear combinations of the elements $(z - b)^d$, $b \in F$. This immediately implies the first statement of the lemma.

If $m$ is a positive integer, we have $\sum_{b \in F} b^m = -1$ or $0$, depending on whether $m$ is divisible by $q - 1$ or not. Combining this with the binomial theorem we obtain

$$\sum_{b \in F} b^q d(z - b)^d = (-1)^d dz,$$

$$\sum_{b \in F} b^{q-2} (z - b)^d = dz^{d-1}.$$ 

Since $d$ divides $q - 1$, we have $d \cdot 1 \in F^*$, so $z, z^{d-1}$ belong to $V$. This proves the lemma.

Let $\rho \in N_0$. By the lemma, there exist polynomials $f_1, f_2 \in F[X]$ of degree at most $d$, such that $\rho z = f_1(z)$ and $\rho(z^{d-1}) = f_2(z)$. We have

$$f_1(z)f_2(z) = \rho z \cdot \rho(z^{d-1}) = \rho(z^d) = z^d,$$

so the polynomial $f_1f_2 - X^d$ is divisible by $X^q - X$. But from $2d \leq (\#E)d = q - 1$ it follows that the degree of $f_1f_2 - X^d$ is less than $q$. Therefore $f_1f_2 = X^d$, so there exist $a \in F^*$ and $u \in \mathbb{Z}$, $0 \leq u \leq d$, such that $f_1 = aX^u$, i.e.,

$$\rho z = az^u.$$ 

Since $\rho$ acts bijectively on $F^*$, we have $u > 0$. We claim that the map $\alpha : F \to F$ sending each $x$ to $x^u$ is a field automorphism of $F$. To prove this, let $y$ be any element of $F$. Then we have $\tau_\rho \rho z = \tau_\rho (az^u) = a(z + y)^u$. On the other hand, $\tau_\rho \rho = \rho \tau_\rho$ for some $\rho' \in N_0$ and $b \in F$. Applying to $\rho'$ what we just proved for $\rho$ we find that $\rho' z = a' z^u$ for some $a' \in F^*$ and $u' \in \mathbb{Z}$, $0 < u' \leq d$. Then $\tau_\rho \rho z = \rho' \tau_\rho z = \rho'(z - b) = a' z^u - b$, which yields

$$a(z + y)^u = a' z^u - b.$$ 

Each side has degree less than $q$ in $z$, so we actually have $a(X + y)^u = a'X^u - b$, and therefore $u = u'$, $a = a'$, $ay^u = -b$. It follows that $(z + y)^u = z^u + y^u$, so $(x + y)^u = x^u + y^u$ for all $x \in F$. This implies that $\alpha$ is a field automorphism of $F$.

Let now $\sigma$ be any element of $N$. Choose $\rho \in N_0$ such that $\sigma \rho = \tau_b$ for some $b \in F$. Let $\rho z = az^u$, with $a, u$ as above. Then $\sigma(az^u) = z - b$, so
\[ \sigma^{-1}z = az^\nu + b. \] This means precisely that \( \sigma x = ax^\nu + b = a \cdot ax + b \) for all \( x \in F \), with \( \alpha \) as above. Putting \( x = 1, y = 0 \) in (1) we see that \( a \in \ker \phi = D \). Next putting \( y = 0 \) in (1) we see that \( \phi \alpha = \phi \).

This proves Theorem 1.

It follows from Theorem 1 that \( T \) is a normal subgroup of \( N \), and that \( N \) is the semidirect product of \( T \) and \( N_0 \). Likewise, \( N_0 \) is isomorphic to the semidirect product of \( D \) and the group of those automorphisms \( \alpha \) of \( F \) for which \( \phi \alpha = \phi \).

3. Proof of Theorem 2.

Denote by \( J \) the normalizer of \( N \) in the group of all permutations of \( F \). To prove Theorem 2, it suffices to prove the following three assertions:

(i) for each \( K \)-semilinear automorphism \( \beta \) of \( F \) and each \( b \in F \), the permutation \( \sigma \) of \( F \) given by (4) belongs to \( G \);

(ii) \( G \subseteq J \);

(iii) for each \( \sigma \in J \) there exist a \( K \)-semilinear automorphism \( \beta \) of \( F \) and an element \( b \in F \) such that (4) holds.

Proof of (i). Let \( \beta, b \) be as in (i). If \( x, y \in F^* \) belong to the same coset modulo \( D \), then \( \beta x = \gamma(xy^{-1})(\beta y) \) for some automorphism \( \gamma \) of \( K \), and \( \gamma(xy^{-1}) \in \gamma D = D \); so \( \beta x, \beta y \) also belong to the same coset modulo \( D \). Therefore \( \beta \) induces a permutation of \( F*/D \). But \( F*/D \cong E \), so there is a permutation \( \kappa \) of \( E \) such that \( \phi \beta x = \kappa \phi x \) for all \( x \in F^* \). This immediately implies that the permutation \( \sigma \) given by (4) satisfies (3). This proves (i).

Proof of (ii). The surjectivity of \( \phi \) implies that the permutation \( \kappa \) in (3) is uniquely determined by \( \sigma \). Also, the map sending \( \sigma \) to \( \kappa \) is a group homomorphism from \( G \) to the group of all permutations of \( E \), and the kernel is \( N \). Therefore \( N \) is normal in \( G \), so \( G \subseteq J \). This proves (ii).

Proof of (iii). We begin with two observations on \( N \). Let \( T \) be as in Section 2.

Denote by \( p \) the characteristic of \( F \). Every non-identity element of \( T \) is of order \( p \) and without fixed points on \( F \). We claim that, conversely, every element of \( N \) of order \( p \) without fixed points belongs to \( T \). To prove this, consider the set \( U \) of all \( \sigma \in N \) for which there exist an automorphism \( \alpha \) of \( p \)-power order of \( F \) and an element \( b \in F \) such that for all \( x \in F \) one has \( \sigma x = \alpha x + b \). This is a subgroup of \( N \), and the order of \( U \) is the largest power of \( p \) dividing the order of \( N \), so \( U \) is a Sylow-\( p \)-subgroup of \( N \). Let now \( \tau \in N \) be of order \( p \) and without fixed points on \( F \). We wish to prove that \( \tau \in T \). Replacing \( \tau \) by a conjugate (which is allowed, since \( T \) is normal in \( N \)), we may assume that \( \tau \in U \). Let the automorphism \( \alpha \) of \( F \) and the
element $b \in F$ be such that for all $x \in F$ one has $\tau x = ax + b$. If $\alpha$ is the identity, then $\tau = \tau_b \in T$, and we are done. Suppose therefore that $\alpha$ is not the identity. Since the order of $\alpha$ divides the order of $\tau$, it must be equal to $\rho$. An easy calculation shows that $\tau^0 = \text{Tr} b$, where $\text{Tr}$ denotes the trace from $F$ to the field of invariants of $\alpha$. But $\tau^0$ is the identity, so $\text{Tr} b = 0$. It is well known that this implies that there exists $c \in F$ with $b = c - \alpha c$. Then $c$ is a fixed point of $\tau$, contradicting the hypothesis.

For $a \in D$, let $\mu_a$ be the element of $N_0$ that sends every $x \in F$ to $ax$, and let $\mu_0$ be the subgroup $\{\mu_a : a \in D\}$ of $N_0$. Clearly $\mu_0$ is generated by an element of order $d$, where $d = \# D$. We claim that every element of $N_0$ not in $\mu_0$ has order less than $d$, so that $\mu_0$ is a characteristic subgroup of $N_0$. To prove this, let $\rho \in N_0$, $\rho \notin \mu_0$, and let the element $a \in D$ and the automorphism $\alpha$ of $F$ be such that for every $x \in F$ one has $\rho x = \alpha \cdot ax$. Let $\widetilde{h}$ be the order of $\alpha$ and $F'$ the field of invariants of $\alpha$. We write $r = \# F'$, so that $r \widetilde{h} = q$. From $\phi \alpha = \phi$ it follows that for each $x \in F^*$ we have $(\rho x)/x \in D$, so $ax/x^d = x^d$. This shows that $F^* \subset F'$. Consequently $(q - 1)/d \mid \text{ord} r - 1$, so $e(q - 1)/(r - 1) = d$ for some integer $e$. One easily checks that $\rho^* x = (\mathcal{N} a) x$ for every $x \in F$, where $\mathcal{N}$ denotes the norm from $F$ to $F'$. We have $\mathcal{N} a = a^{(q - 1)/(r - 1)}$, and since the order of $\alpha$ divides $d$ the order of $\mathcal{N} a$ divides $d$. Therefore the order of $\rho$ divides $e d$. This proves our claim, because $e d < e \sum_{i=0}^{h-1} r^i = e(q - 1)/(r - 1) = d$.

Write $J_0 = \{\sigma \in J : \sigma 0 = 0\}$. For each $\sigma \in J$, $\tau \in T$, $\tau \neq 1$, the element $\sigma \tau \sigma^{-1}$ of $N$ has order $\rho$ and acts without fixed points on $F$, so by what we proved above about $T$ we have $\sigma \tau \sigma^{-1} \in T$. This proves that $T$ is normal in $J$. Since $T$ is isomorphic to the additive group of $F$ it follows that for each $a \in J$ there is an automorphism $\sigma^*$ of the additive group of $F$ such that for each $a \in F$ one has $a \sigma^* a = \sigma^* a$. If in addition $\sigma \in J_0$, then $\sigma^* a = \tau_{a \sigma}, 0 = \sigma \tau_{a \sigma^{-1}} = a \sigma$ for each $a \in F$, so $\sigma = \sigma^*$. This proves that every $\sigma \in J_0$ acts as an automorphism of the additive group of $F$.

Denote by $R$ the endomorphism ring of the additive group of $F$. For $a \in F$, let $\mu_a$ be the element of $R$ that sends each $x \in F$ to $ax$, and let $\mu_F = \{\mu_a : a \in F\}$; this is a subring of $R$ that is isomorphic to $F$. By what we just proved, we may view $J_0$ as a subgroup of the group of units of $R$. We proved above that $\mu_0$ is a characteristic subgroup of $N_0$, and $N_0$ is normal in $J_0$, so $\mu_0$ is normal in $J_0$. Hence if $R'$ denotes the subring of $R$ generated by $\mu_0$, then for all $\sigma \in J_0$ and $v \in R'$ one has $\sigma v \sigma^{-1} \in R'$. But $\mu_0 \subset F$, so we have $R' = \{\mu_a : a \in K\}$, with $K$ as defined in the introduction, and $R' \cong K$. It follows that for each $\sigma \in J_0$ there exists a field automorphism $\gamma$ of $K$ such that for each $x \in K$ one has $\sigma x = \mu_{\gamma x} \sigma$; this means precisely that for every $y \in F$ one has $\sigma (\gamma y) = (\gamma x)(\gamma y)$, so that $\sigma$ is a $K$-semilinear automorphism of $F$. Since $J = TJ_0$, this proves (iii).

This proves Theorem 2.
4. Proof of Theorem 3.

The "if" part of Theorem 3 is trivial. We prove the "only if" part.

Write \( H_0 = \{ \sigma \in H : \sigma 0 = 0 \} \). Since we have \( H = TH_0 \) it suffices to prove that any \( \sigma \in H_0 \) can be written as \( \sigma = \mu_a \alpha \) for some \( a \in F^* \) and some field automorphism \( \alpha \) of \( F \), with \( \mu_a \) as in Section 3. Replacing \( \sigma \) by \( \mu_a^{-1} \sigma \) we may assume that \( \sigma 1 = 1 \). From \( H \subset G \) and Theorem 2 it follows that \( \sigma \) is additive and that there exists a field automorphism \( \gamma \) of \( K \) such that for all \( x \in K, y \in F \) one has \( \sigma(xy) = (\gamma x)(\sigma y) \). Extending \( \gamma \) to an automorphism \( \gamma^* \) of \( F \) and replacing \( \sigma \) by \( \sigma \gamma^* \) we may assume that \( \sigma \) is \( K \)-linear. Putting \( x = 1, y = 0 \) in (3) we see that \( \kappa 1 = 1 \), so the affine permutation \( \kappa \) of \( E \) is actually a group automorphism of \( E \). Hence for all \( x, y \in F^* \) we have \( \phi \sigma(xy) = \kappa \phi(xy) = (\kappa \phi x)(\kappa \phi y) = (\phi \sigma x)(\phi \sigma y) = \phi((\sigma x)(\sigma y)) \), so \( \sigma(xy) = u_{x,y}(\sigma x)(\sigma y) \) for some \( u_{x,y} \in D \subset K^* \). Since \( \sigma \) is \( K \)-linear, we have \( u_{x,y} = 1 \) whenever \( x \in K^* \), \( y \in F^* \). Let now \( x, y \in F^* \), \( x \notin K^* \). Then 1, \( x \) are linearly independent over \( K \), so the same is true for \( \sigma y, (\sigma x)(\sigma y) \). Therefore from

\[
\sigma y + u_{x,y}(\sigma x)(\sigma y) = \sigma y + \sigma(xy) = \sigma((1 + x)y)
\]

\[
= u_{1 + x,y}(\sigma(1 + x))(\sigma y) = u_{1 + x,y}(\sigma y) + u_{1 + x,y}(\sigma x)(\sigma y)
\]

it follows that \( u_{x,y} = 1 \). This proves that \( \sigma \) is a field automorphism of \( F \), as required.

To prove the last assertion of Theorem 3, suppose that \( K = F \), and let \( \sigma \in G \). Write \( \sigma \) as in (4). Since \( \beta \) is an \( F \)-semilinear automorphism of \( F \), there exist \( a \in F^* \) and an automorphism \( \alpha \) of \( F \) such that we have \( \beta x = a \cdot \alpha x \) for all \( x \in F \). Then \( \sigma \in H \), as required. This proves Theorem 3.

5. Proof of Theorem 4.

The "if" part of Theorem 4 is trivial. We prove the "only if" part. Let \( \sigma : M_1 \to M_2 \) be an \( L \)-linear map with \( N_2 \sigma = N_1 \). Then the element \( a = \sigma 1 \) satisfies \( N_2 a = 1 \). Replacing \( \sigma \) by the map sending every \( x \in M_1 \) to \( a^{-1} \sigma x \) we may assume that \( \sigma 1 = 1 \). Then \( \sigma \) is the identity on \( L \). We wish to prove that \( \sigma \) is a field isomorphism.

First let \( L \) be finite. Since 0 is the only element of \( M_1 \) of norm 0, the map \( \sigma \) is injective, so \( M_1 \) and \( M_2 \) have the same degree over \( L \). We may therefore assume that \( M_1 = M_2 \). Then the desired result follows from Theorem 1, with \( F = M_1, E = L^*, \phi = N_1 \).

Suppose now that \( L \) is infinite. For \( i \in \{ 1, 2 \} \) and \( x \in M_i \), let \( f_x \in L[X] \) be the characteristic polynomial of the \( L \)-linear map \( M_i \to M_i \), sending each \( y \) to \( xy \); this is a power of the irreducible polynomial of \( x \) over \( L \). For all \( x \in M_1, t \in L \) we have \( f_x(t) = N_1(t - x) = N_2(t - x) = N_2(t - \sigma x) = f_{\sigma x}(t) \).
Since $L$ is infinite this implies that $f_x = f_{\sigma x}$, so $x$ and $\sigma x$ are conjugate over $L$. Hence if $M'$ denotes an algebraic closure of $M_2$ then for each $x \in M_1$ there is an $L$-embedding $\tau: M_1 \to M'$ with $\tau x = \sigma x$. Writing $V_\tau = \{x \in M_1 : \tau x = \sigma x\}$ we find that $M_1 = \bigcup V_\tau$. Since a vector space over an infinite field cannot be written as the union of finitely many proper subspaces, this implies that there exists $\tau$ with $M_1 = V_\tau$. This means that $\sigma$ is a field isomorphism, as required. This proves Theorem 4.

ACKNOWLEDGMENT

The author was supported by NSF contract DMS 87-06176

REFERENCES

1 A BRUEN AND B LEVINGER, A theorem on permutations of a finite field, *Canad J Math* 25 (1973), 1060–1065
6 F RIVERO, “Group Actions on Minimal Functions over Finite Fields,” Dissertation, Louisiana State University, 1987

Printed by Catherine Press, Ltd., Tempelhofer 41, B-8000 Brugge, Belgium