JOURNAL OF NUMBER THEORY **34**, 33–40 (1990)

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 $\phi: F^* \to E$ 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 σ 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 σ of F for which there exists a permutation κ 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 $\phi: F^* \to E$ 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 σ of F satisfying

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

Denote by D the kernel of ϕ.

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

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

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

0022-314X/90 $3.00

implies an affirmative answer to the following question, which was asked by F. Rivero [6]: let σ be an automorphism of the additive group of a finite field F of odd characteristic, and suppose that σ maps the set of squares to itself and satisfies $\sigma 1 = 1$; does it follow that σ 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 σ of F for which there exists a permutation κ of E such that

$$\phi(\sigma x - \sigma y) = \kappa\phi(x - y) \qquad \text{for all} \quad x, y \in F \text{ with } x \neq y. \tag{3}$$

Denote by K the subfield of F generated by D. A *K-semilinear automorphism* of F is an automorphism β of the additive group of F for which there exists a field automorphism γ 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 σ is a permutation of F, then σ belongs to G if and only if there exist a K-semilinear automorphism β of F and an element $b \in F$, such that*

$$\sigma x = \beta x + b \qquad \textit{for all} \quad x \in F. \tag{4}$$

The proof of Theorem 2 is given in Section 3.

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

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

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

$$\sigma x = a \cdot \alpha x + b \qquad \textit{for all} \quad x \in F.$$

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 Grundhöfer [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 Grundhöfer 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 $\mathcal{N}_i$: $M_i \to L$ denote the norm map, for $i = 1, 2$. Let further σ: $M_1 \to M_2$ be a surjective L-linear map. Then we have $\mathcal{N}_2\sigma = \mathcal{N}_1$ if and only if there exist an element $a \in M_2$ with $\mathcal{N}_2 a = 1$ and a field isomorphism α: $M_1 \to M_2$ that is the identity on L, such that*

$$\sigma x = a \cdot \alpha x \qquad \textit{for all} \quad x \in M_1.$$

The proof of Theorem 4 is given in Section 5.

If L has cardinality two, then clearly σ satisfies $\mathcal{N}_2\sigma = \mathcal{N}_1$ 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 $N_0 = \{\sigma \in N : \sigma 0 = 0\}$; this is a subgroup of N. For $b \in F$, let τ_b be the permutation of F that sends each $x \in F$ to $x + b$, and let $T = \{\tau_b : b \in F\}$. Clearly, T is a subgroup of N that is isomorphic to the additive group of F. Since T acts transitively on F we have $N = TN_0 = N_0T$.

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

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

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

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

$$\deg f \leqslant d, \qquad g = f(z).$$

Also, z and z^{d-1} 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

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

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 $f_1 f_2 - X^d$ is divisible by $X^q - X$. But from $2d \leqslant (\# E)d = q-1$ it follows that the degree of $f_1 f_2 - X^d$ is less than q. Therefore $f_1 f_2 = X^d$, so there exist $a \in F^*$ and $u \in \mathbf{Z}$, $0 \leqslant u \leqslant d$, such that $f_1 = aX^u$, i.e.,

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

Since ρ acts bijectively on F^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 $\tau_{-y}\rho z = \tau_{-y}(az^u) = a(z+y)^u$. On the other hand, $\tau_{-y}\rho = \rho'\tau_b$ for some $\rho' \in N_0$ and $b \in F$. Applying to ρ' what we just proved for ρ we find that $\rho' z = a' z^{u'}$ for some $a' \in F^*$ and $u' \in \mathbf{Z}$, $0 < u' \leqslant d$. Then $\tau_{-y}\rho z = \rho'\tau_b z = \rho'(z-b) = a'z^{u'} - b$, 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 α is a field automorphism of F.

Let now σ 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

$\sigma^{-1}z = az^u + b$. This means precisely that $\sigma x = ax^u + b = a \cdot \alpha x + b$ for all $x \in F$, with α 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 α 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 β of F and each $b \in F$, the permutation σ of F given by (4) belongs to G;

(ii) $G \subset J$;

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

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

Proof of (ii). The surjectivity of ϕ implies that the permutation κ in (3) is uniquely determined by σ. Also, the map sending σ to κ 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 $G \subset J$. 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 α 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 τ by a conjugate (which is allowed, since T is normal in N), we may assume that $\tau \in U$. Let the automorphism α of F and the element $b \in F$ be such that for all $x \in F$ one has $\tau x = \alpha x + b$. If α is the identity, then $\tau = \tau_b \in T$, and we are done. Suppose therefore that α is not the identity. Since the order of α divides the order of τ, it must be equal to p. An easy calculation shows that $\tau^p 0 = \mathrm{Tr}\, b$, where Tr denotes the trace from F to the field of invariants of α. But τ^p is the identity, so $\mathrm{Tr}\, b = 0$. 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 τ, contradicting the hypothesis.

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

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 p 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 $\sigma \in J$ there is an automorphism σ^* of the additive group of F such that for each $a \in F$ one has $\sigma\tau_a\sigma^{-1} = \tau_{\sigma^* a}$. If in addition $\sigma \in J_0$, then $\sigma^* a = \tau_{\sigma^* a} 0 = \sigma\tau_a\sigma^{-1} 0 = \sigma a$ 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 μ_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 μ_D is a characteristic subgroup of N_0, and N_0 is normal in J_0, so μ_D is normal in J_0. Hence if R' denotes the subring of R generated by μ_D, then for all $\sigma \in J_0$ and $v \in R'$ one has $\sigma v \sigma^{-1} \in R'$. But $\mu_D \subset \mu_F$, 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 γ of K such that for each $x \in K$ one has $\sigma\mu_x = \mu_{\gamma x}\sigma$; this means precisely that for every $y \in F$ one has $\sigma(xy) = (\gamma x)(\sigma y)$, so that σ 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 α of F, with μ_a as in Section 3. Replacing σ by $\mu_{\sigma 1}^{-1}\sigma$ we may assume that $\sigma 1 = 1$. From $H \subset G$ and Theorem 2 it follows that σ is additive and that there exists a field automorphism γ of K such that for all $x \in K$, $y \in F$ one has $\sigma(xy) = (\gamma x)(\sigma y)$. Extending γ to an automorphism γ^* of F and replacing σ by $\sigma\gamma^{*-1}$ we may assume that σ is K-linear. Putting $x = 1$, $y = 0$ in (3) we see that $\kappa 1 = 1$, so the affine permutation κ 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 σ 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 σy, $(\sigma x)(\sigma y)$. Therefore from

$$\begin{aligned}\sigma y + u_{x,y}(\sigma x)(\sigma y) &= \sigma y + \sigma(xy) = \sigma((1+x)y) \\ &= u_{1+x,y}(\sigma(1+x))(\sigma y) = u_{1+x,y}\sigma y + u_{1+x,y}(\sigma x)(\sigma y)\end{aligned}$$

it follows that $u_{x,y} = 1$. This proves that σ 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 σ as in (4). Since β is an F-semilinear automorphism of F, there exist $a \in F^*$ and an automorphism α 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 $\sigma\colon M_1 \to M_2$ be an L-linear map with $\mathcal{N}_2\sigma = \mathcal{N}_1$. Then the element $a = \sigma 1$ satisfies $\mathcal{N}_2 a = 1$. Replacing σ by the map sending every $x \in M_1$ to $a^{-1}\sigma x$ we may assume that $\sigma 1 = 1$. Then σ is the identity on L. We wish to prove that σ is a field isomorphism.

First let L be finite. Since 0 is the only element of M_1 of norm 0, the map σ 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 $F = M_1$, $E = L^*$, $\phi = \mathcal{N}_1$.

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 $f_x(t) = \mathcal{N}_1(t - x) = \mathcal{N}_2\sigma(t - x) = \mathcal{N}_2(t - \sigma x) = f_{\sigma x}(t)$.

Since L is infinite this implies that $f_x = f_{\sigma x}$, so x and σx 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 $M_1 = \bigcup_\tau V_\tau$. Since a vector space over an infinite field cannot be written as the union of finitely many proper subspaces, this implies that there exists τ with $M_1 = V_\tau$. This means that σ 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.
2. L. Carlitz, A theorem on permutations in a finite field, *Proc. Amer. Math. Soc.* **11** (1960), 456–459.
3. T. Grundhöfer, Über Abbildungen mit eingeschränktem Differenzenprodukt auf einem endlichem Körper, *Arch. Math.* **37** (1981), 59–62.
4. R. McConnel, Pseudo-ordered polynomials over a finite field, *Acta Arith.* **8** (1963), 127–151.
5. W. Meyer and R. Perlis, On the genus of norm forms, *Math. Ann.* **246** (1980), 117–119.
6. F. Rivero, "Group Actions on Minimal Functions over Finite Fields," Dissertation, Louisiana State University, 1987.