DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NIJMEGEN The Netherlands

THE AUTOMORPHISM GROUP OVER FINITE FIELDS

Stefan Maubach

Report No. 0128 (November 2001)

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NIJMEGEN
Toernooiveld
6525 ED Nijmegen
The Netherlands

The automorphism group over finite fields

Stefan Maubach

Abstract

It is shown that the invertible polynomial maps over a finite field $\mathbb{F}_q$, if looked at as bijections $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, give all possible bijections in case $q = 2$, or $q = p^r$ where $p > 2$. In case $q = 2^r$ where $r > 1$ it is shown that the tame subgroup of the invertible polynomial maps give only the even bijections, i.e. only half the bijections. As a consequence it is shown that a set $S \subset \mathbb{F}_q^n$ can be a zero set of a coordinate if and only if $\#S = q^{n-1}$.

1 Introduction

Though many theorems about polynomial maps are true for an arbitrary field, or an arbitrary algebraically closed field, these theorems are mostly used for the characteristic zero case, or more specifically, the complex numbers. However, it might be interesting to study polynomial maps over characteristic $p > 0$, or even over finite fields. Some research in this direction has been done, see for example [5], [3], [4], [6] (chapter 10 paragraph 3). The case that we are considering, the automorphism group, or the tame automorphism group, over a finite field might be very useful, as can be seen in the paper [2]. In fact, it might be one of the few useful applications of polynomial mappings in the "real" world of "money, economics and data travel" : in [2] a method is given on how to encrypt data using the tame automorphism group over a finite field. Therefore, a theoretical approach of the automorphism group or tame automorphism group over a finite field can give a good foundation for similar applications. Also it might induce some ideas on already standing conjectures over the complex numbers, like the tame generators conjecture.

2 Bijections induced by automorphisms over $\mathbb{F}_{p^n}$

Definition 2.1. Let k be a field, $A_n := k[X_1, \ldots, X_n]$. Then

$End_k(A_n) := A_n^n$.
$\mathcal{P}(k^n)$ is the set of all maps $k^n \longrightarrow k^n$.
$\mathcal{B}(k^n) \subset \mathcal{P}(k^n)$ is the set of all bijections $k^n \longrightarrow k^n$.

$\mathcal{E} : End_k(A_n) \longrightarrow \mathcal{P}(k^n)$ is the functor sending $e \in End_k(A_n)$ ($e = (e_1, \ldots, e_n) \in A_n^n$) to the map $\mathcal{E}(e) : k^n \longrightarrow k^n$ defined by

$$\mathcal{E}(e)(\alpha_1, \ldots, \alpha_n) := (e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n)).$$

$Aut(k,n) := \{e \in End_k(A_n) \mid \mathcal{E}(e) \in \mathcal{B}(k^n)\}$.
$Aut_k(A_n) := \{e \in End_k(A_n) \mid$ there exists $e' \in End_k(A_n)$ such that $ee' = e'e = Id\}$ where $Id \in A_n^n$ equals $(X_1, \ldots, X_n)$.
$T(k,n)$ is the tame automorphism subgroup of $Aut_k(A_n)$ (generated by $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$ all $f \in k[X_2, \ldots, X_n]$ and all linear maps).

Remark: $Aut(k,n)$ is in general larger than $Aut_k(A_n)$: in case k is a finite field of p^n elements, let $\varphi := (X_1^{p^n}, X_2, \ldots, X_n)$. Then the map $\mathcal{E}(X_1^{p^n}, X_2, \ldots, X_n)$ is a bijection $k^n \longrightarrow k^n$ but φ is not an invertible element of $End_k(A_n)$.

In this article we will try to answer the question whether $\mathcal{E}(Aut_k(A_n)) = \mathcal{B}(k^n)$. The case that k is infinite is easy:

Lemma 2.2. *If k is not a finite field then $\mathcal{E}(Aut(k,n))$ (and hence $\mathcal{E}(Aut_k(A_n))$) is smaller than $\mathcal{B}(k^n)$.*

Proof. Suppose $F = (F_1, \ldots, F_n)$ is a polynomial map $k^n \longrightarrow k^n$ interchanging 0 and $A := (1, 0, \ldots, 0)$, and the identity anywhere else. Then $F_i - X_i$ is a polynomial map $k^n \longrightarrow k$ which is zero everywhere in case $i \geq 2$ or zero almost everywhere in case $i = 1$; over an infinite field this implies $F_i - X_i = 0$. □

The case that k is a finite field has some surprising result:

Theorem 2.3. *Let k be a finite field.*

(i). $\#\mathcal{E}(T(k,1)) = \#\mathcal{B}(k)/(\#k - 2)!$, so only if $k = F_2, F_3$ then $\mathcal{E}(T(k,1)) = \mathcal{B}(k)$.

(ii). If $n \geq 2$ and $kar(k) \neq 2$ or $k = \mathbb{F}_2$ then $\mathcal{E}(T(k,n)) = \mathcal{B}(k^n)$.

(iii). If $n \geq 2$ and $k = \mathbb{F}_{2^m}$ where $m \geq 2$ then $\#\mathcal{E}(T(k,n)) = \#\mathcal{B}(k^n)/2$. In fact, $\mathcal{E}(T(k,n))$ is the alternating subgroup A_l of the symmetric group $S_l \cong \mathcal{B}(k^n)$ where $l = \#k^n$.

The proof will go in several steps. It will involve the fact that $\mathcal{B}(k^n)$, with as operation composition of maps, is isomorphic to the symmetic group S_l where $l = (\#k^n)$, since every bijection $\sigma \in \mathcal{B}(k^n)$ can be seen as a permutation of elements in k^n. This enables us to use a theorem of Jordan:

Definition 2.4. Let G be a transitive subgroup of S_n. G is called a *primitive* subgroup if there exist no two elements $i, j \in \{1, \ldots, n\}$ such that for any $g \in G$ we have either $\{g(i), g(j)\} = \{i, j\}$ or $\{g(i), g(j)\} \cap \{i, j\} = \{\}$.

Theorem 2.5. *Let G be a primitive subgroup of S_n. Suppose G contains a 3-cycle. Then G contains the alternating subgroup A_n.*

For a proof, see [1].

Definition 2.6. Let k be a finite field, and let $\alpha = (\alpha_1, \ldots, \alpha_n) \in k^n, b \in k$. Let

$$f_i := \prod_{\substack{a \in k \\ a \neq \alpha_i}} (X_i - a) \in k[X_i].$$

Let $\lambda := f_1(\alpha_1)\cdots f_n(\alpha_n)$. Then define

$$f_{(\alpha,b)} := b\lambda^{-1}\prod_{i=1}^{n} f_i(X_i).$$

Notice $f_{(\alpha,b)}(\alpha) = b$ and $f_{(\alpha,b)}(\beta) = 0$ for all $\beta \in k^n\backslash\{\alpha\}$.

Definition 2.7. Let k be a finite field.

(i). Let $\alpha \in k^{n-1}, b \in k$. Then define

$$\sigma_{(\alpha,b)} := \big(X_1 + f_{(\alpha,b)}(X_2,\ldots,X_n), X_2,\ldots,X_n\big).$$

(ii). Let $i \in \{2,\ldots,n\}$. Define

$$\sigma_i := \big(X_i, X_2,\ldots,X_{i-1},X_1,X_{i+1},\ldots,X_n\big),$$

the map interchanging X_i and X_1.

(iii). Choose some $a \in k^*$ such that $\{1,a,a^2,\ldots\} = k^*$. Let

$$\tau := (aX_1, X_2,\ldots,X_n).$$

(iv). Let G be the subgroup of $T(k,n)$ generated by the $\sigma_{(\alpha,b)}$, the σ_i, and τ.

Lemma 2.8. $\mathcal{E}(G) = \mathcal{E}(T(k,n))$.

Proof. We need to show that (1) for any $f \in k[X_2,\ldots,X_n]$ we have $\sigma \in G$ such that $\mathcal{E}(\sigma) = \mathcal{E}(X_1+f, X_2,\ldots,X_n)$, and that (2) for each linear map L we have some $\sigma \in G$ such that $\mathcal{E}(\sigma) = \mathcal{E}(L)$.
Part (1): Let $\zeta := (X_1 + f, X_2,\ldots,X_n)$ for some $f \in k[X_2,\ldots,X_n]$. Notice that $\sigma_{(\alpha_1,b_1)}\sigma_{(\alpha_2,b_2)} = \sigma_{(\alpha_2,b_2)}\sigma_{(\alpha_1,b_1)} = (X_1 + g, X_2,\ldots,X_n)$ where $g \in k[X_2,\ldots,X_n]$ satisfies (in case $\alpha_1 \neq \alpha_2$) $g(\alpha_1) = b_1$, $g(\alpha_2) = b_2$. In the same way we see that if we define σ to be the composition of all $\sigma_{(\alpha,f(\alpha))}$, where α runs through k^{n-1} that $\sigma = (X_1 + g, X_2,\ldots,X_n)$ and $g(\alpha) = f(\alpha)$ for all $\alpha \in k^{n-1}$. Thus $\mathcal{E}(\sigma) = \mathcal{E}(\zeta)$.
Part (2): Since $\sigma_i\tau^m\sigma_i = (X_1,\ldots,X_{i-1},a^mX_i,X_{i+1},\ldots,X_n)$ and $\{1,a,a^2,\ldots\} = k^*$ we can get any map $L_{i,\lambda} := (X_1,\ldots,X_{i-1},\lambda X_i,X_{i+1},\ldots,X_n)$ where $\lambda \in k^*$ is arbitrary. It is well-known that these maps, together with the maps $\sigma_\gamma := (X_1 + \gamma_2X_2 + \ldots + \gamma_nX_n, X_2,\ldots,X_n)$ where $\gamma := (\gamma_2,\ldots,\gamma_n) \in k^{n-1}$, generate the linear maps. By part (1) there exists for each $\gamma \in k^{n-1}$ a map $\mu_\gamma \in G$ such that $\mathcal{E}\sigma_\gamma = \mathcal{E}\mu_\gamma$, and that suffices to prove (2). □

Lemma 2.9. *Let k be a finite field. Let G be as in definition 2.7*(iv). *Then*

(i). $\mathcal{E}(G)$ is a primitive group,

(ii). $\mathcal{E}(G)$ contains a 3-cycle.

Proof.
(i): The fact that $\mathcal{E}(G)$ is transitive follows from the fact that G contains all linear bijections $k^n \longrightarrow k^n$. So we need to show that for arbitrary $r = (r_1, \ldots, r_n), s = (s_1, \ldots, s_n) \in k^n$, $r \neq s$ there exists some $\sigma \in G$ such that $\sigma(r) \neq r$, $\sigma(s) = s$. Let $i \in \{1, \ldots, n\}$ such that $r_i \neq s_i$. If $i \geq 2$ then we take the map $\sigma_{(\alpha,1)}$ where $\alpha \in k^{n-1}$ the last $n-1$ elements of $r = (r_1, \alpha) \in k^n$. Then $\sigma_{(\alpha,1)}(r) = (r_1 + 1, \alpha)$ and $\sigma_{(\alpha,1)}(s) = s$. In case $i = 1$ we can take $\sigma_2\sigma_{(\alpha,s)}\sigma_2$ for some other appropriate r, s.
(ii): Let o:$= (0, \ldots, 0) \in k^{n-1}$ and let

$$\sigma := \sigma_{(o,1)} = \big(X_1 + f_{(o,1)}(X_2, \ldots, X_n), X_2, \ldots, X_n\big),$$
$$\mu := \sigma_2\sigma\sigma_2 = \big(X_1, X_2 + f_{(o,1)}(X_1, X_3, \ldots, X_n), X_3, \ldots, X_n\big).$$

Then σ permutes only the set $V_1 := \{(a, 0, \ldots, 0) \mid a \in k\}$ and μ permutes only the set $V_2 := \{(0, a, 0, \ldots, 0) \mid a \in k\}$. Both σ and μ are cyclic of order kar(k) on V_1 resp. V_2. Let $\zeta := \sigma^{-1}\mu^{-1}\sigma\mu$. Then ζ acts on a subset of $V_1 \cup V_2$. Now if $\alpha \notin V_2, \sigma(\alpha) \notin V_2$ then one can easily check (using the fact that μ only works on elements of V_2) that $\zeta(\alpha) = \alpha$. Also if $\alpha \notin V_1, \mu(\alpha) \notin V_1$ then one can easily check (using the fact that σ only works on elements of V_1) that $\zeta(\alpha) = \alpha$. Thus we have left the cases:
1) $\alpha \notin V_2, \sigma(\alpha) \in V_2$ (the element $A := (-1, 0, \ldots, 0)$),
2) $\alpha \notin V_1, \mu(\alpha) \in V_1$ (the element $B := (0, -1, 0, \ldots, 0)$),
3) $\alpha \in V_1$, $\alpha \in V_2$ (the element $O := 0$).
Notice $\sigma(A) = O, \sigma(B) = B, \mu(B) = O, \mu(A) = A, \sigma(O) \notin V_2, \mu(O) \notin V_1$. Using this we see that $\zeta(A) = B$, $\zeta(B) = O$, $\zeta(O) = A$ hence ζ is a 3-cycle. □

Now we are ready for:

Proof. (of theorem 2.3) We will use notations as in definition 2.7. We will see $\mathcal{B}(k^n)$ as a subgroup of S_{q^n} where $q = \#k$. By theorem 2.5, lemma 2.8 and lemma 2.9 we see that A_{q^n} is a subgroup of $\mathcal{E}(G) = \mathcal{E}(T(k, n))$.
(i) Case $n = 1$: $T(k, 1)$ consists only of the linear maps $x \longrightarrow ax + b$ where $a \in k^*, b \in k$. So these are $\#k^* \times \#k = (q-1)q$ different maps. Since $\#\mathcal{B}(k) = (\#k)!$ the result follows.
(ii) Case $n \geq 2$, kar$(k) \neq 2$: If we can find $\sigma \in G$ such that $\mathcal{E}(\sigma) \notin A_{q^n}$, then $\mathcal{E}(G) = S_{q^n}$; in other words, find $\sigma \in G$ such that the sign of $\mathcal{E}(\sigma)$ is -1. Our claim is: τ is such an element. τ (or $\mathcal{E}(\tau)$) has order $q-1$ and consists of a number of seprate $(q-1)$-cycles: for each $\alpha \in k^{n-1}$ a seprate cycle in the set $V_\alpha := \{(a, \alpha) \mid a \in k^*\}$. Hence q^{n-1} cycles of order $q-1$. Now a cycle of order $q-1$ has sign -1 since $q-1$ is even. Since q is odd, q^{n-1} is odd too, hence the sign of τ is -1
Case $n \geq 2$, $k = \mathbb{F}_2$: In this case we can find another element of sign -1, namely $\sigma_{(0,1)}$. This map works only on $(0, \ldots, 0)$ and $(1, 0, \ldots, 0)$; it interchanges them. Hence the sign is -1. The rest is the same as the previous case.
(iii) Case $n \geq 2$, $k = \mathbb{F}_q = \mathbb{F}_{2^r}$, $r \geq 2$: We will show that every generator of G has sign 1, so $\mathcal{E}(G) = A_{q^n}$.
1) $\sigma^2_{(\alpha,b)} = (X_1 + 2f_{(\alpha,b)}, X_2, \ldots, X_n) = Id.$ (since $2 \equiv 0$). Hence $\sigma_{(\alpha,b)}$ consists only of 2-cycles. If we count the number of elements which stay invariant, then we know how many 2-cycles. The set of non-invariant elements is $V := \{(a, \alpha) \mid a \in k\}$. hence

we have $\#V/2 = 2^r/2 = 2^{r-1}$ 2-cycles. Since 2^{r-1} is even (for $r \geq 2$), the sign is 1.
2) $\sigma_i^2 = Id.$ hence consists of only 2-cycles too. Let us look at σ_2. This map leaves $V := \{(a, a, \alpha) \mid a \in k, \alpha \in k^{n-2}\}$ invariant. Hence we have $(\#k^n - \#V)/2 = ((2^r)^n - (2^r)^{n-1})/2 = 2^{rn-r-1}(2^r - 1)$ 2-cycles. This number is also even (since $rn - r - 1 \geq 2$ for $n, r \geq 2$) hence the sign is 1.
3) τ has order $2^r - 1$ and consists of a number of $(2^r - 1)$-cycles. These cycles have sign 1, hence τ has sign 1. □

3 Conclusions

Using theorem 2.3 we can also completely define all zero sets of coordinates over finite fields. $Z(F)$ will be the zero set of F, and k a finite field of q elements. A coordinate is an element $F \in k[X_1, \ldots, X_n]$ such that there exist $F_2, \ldots, F_n \in k[X_1, \ldots, X_n]$ satisfying $k[F, F_2, \ldots, F_n] = k[X_1, \ldots, X_n]$.

Corollary 3.1. *A set $S \subseteq k^n$ is a zero set of a coordinate $F \in k[X_1, \ldots, X_n]$ if and only if $\#S = q^{n-1}$.*

Proof. The case $n = 1$ is trivial, since every coordinate is of the form $aX_1 + b$ where $a \in k^*$. So let $n \geq 2$ and define $V_0 := \{(0, \alpha) \mid \alpha \in k^{n-1}\}$. S being the zero set of a coordinate is equivalent to having an automorphism φ satisfying $\varphi(S) = V_0$ (the first component of φ will be the coordinate). The "only if"-part of corollary 3.1 follows from the fact that φ induces a bijection $k^n \longrightarrow k^n$, and thus $\#S = \#\varphi(S) = \#V_0$. Conversely we need to find an invertible polynomial map φ satisfying $\varphi(S) = V_0$. In other words, we need to find a bijection B which sends S to V_0 and is induced by an invertible polynomial map φ (i.e. $B := \mathcal{E}(\varphi)$). Using theorem 2.3, in case $q = 2$ or $q = p^r$ where $p > 2$ we can find such a bijection B. In case $q = 2^r, r \geq 2$ we show that there exists an even bijection which sends S to V_0. We can achieve this by taking two elements $a, b \in k^n \backslash (S \cup V_0)$, $a \neq b$ (this is possible since $q > 2$, $n > 1$) and then taking a bijection B sending S to V_0 and the identity on $k^n \backslash (S \cup V_0 \cup \{a, b\})$ and then either interchanging a and b or sending a to a and b to b. □

Notice that the first two results of theorem 2.3 are also true if we replace $T(k, n)$ by $Aut_k(A_n)$; however, the third one is unclear. However, if that wouldn't be the case, it would imply strange things for the following conjecture:

Conjecture 3.2. (Tame conjecture, TC(k,n)) Let k be a field and $n \in \mathbb{N}^*$. Then $Aut_k(A_n) = T(k, n)$.

Corollary 3.3. *(of theorem2.3) Suppose $k = \mathbb{F}_{2^r}$ where $r \geq 2$ and $F \in Aut_k(A_n)$ such that $\mathcal{E}(F) \in S_l \backslash A_l$, $l = \#k$. Then $TC(k, n)$ is not true.*

Such a counterexample over $\mathbb{F}_{2^r}$ might induce a counterexample over $\mathbb{C}$, but that's not clear.

References

[1] I.M. Isaacs and Thilo Zieschang, *Generating Symmetric Groups*, Amer. Math. Monthly, **102** 734-739 (1995)

[2] T.Moh, *A Public key system and master key functions*, Comm. in Algebra, 27(5), 2207-2222 (1999)

[3] K. Adjamagbo, *On seperable algebras over a U.F.D. and the Jacobian Conjecture in any characteristic*, Proceedings of the conference 'Invertible Polynomial Maps', 89-104

[4] K. Adjamagbo, H. Derksen, A. van den Essen, On polynomial maps in positive characteristic and the jacobian Conjecture, report 9208, Univ. of Nijmegen, (1992)

[5] P. Nousiainen, *On the Jacobian problem in positive characteristic*, Pennsylvania State Univ. , preprint (1981)

[6] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Birkhäuser, Verlag (2000).