Serdica
Mathematical Journal
Сердика
Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **27** (2001), 343-350

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

POLYNOMIAL AUTOMORPHISMS OVER FINITE FIELDS

Stefan Maubach

Communicated by V. Drensky

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 the case $q = 2$, or $q = p^r$ where $p > 2$. In the case $q = 2^r$ where $r > 1$ it is shown that the tame subgroup of the invertible polynomial maps gives 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, for 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

2000 *Mathematics Subject Classification:* 14R10, 14R15, 11C08, 20B27, 20B25, 20B15, 20B99.

Key words: polynomial automorphisms, tame automorphisms, affine spaces over finite fields, primitive groups.

has been done, see for example in [6], [1], [2] and [3] (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 [5]. 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 [5] 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 the 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, $A_n := k[X_1, \ldots, X_n]$. Following the tradition, and since the endomorphisms of A_n are determined by the images of the variables $X_1, \ldots, X_n$, we identify the endomorphisms with the n-tuples in 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 $k^n \longrightarrow k^n$.

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

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

$\mathrm{Aut}(k, n) := \{e \in \mathrm{End}_k(A_n) \mid \mathcal{E}(e) \in \mathcal{B}(k^n)\}$.
$\mathrm{Aut}_k(A_n) :=$ *the group of automorphisms of the k-algebra A_n, (i.e. $\mathrm{Aut}_k(A_n)$ is the set of invertible elements of $\mathrm{End}_k(A_n)$).*
$T(k, n)$ is the tame automorphism subgroup of $\mathrm{Aut}_k(A_n)$, generated by $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$ for all $f \in k[X_2, \ldots, X_n]$ and by all linear maps.

As usual, "$\#S$" will denote the number of elements in a finite set S.

Remark. $\mathrm{Aut}(k, n)$ is in general larger than $\mathrm{Aut}_k(A_n)$: when k is the finite field with 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 $\mathrm{End}_k(A_n)$.

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

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

P r o o f. 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 if $i \geq 2$ or zero almost everywhere if $i = 1$. Over an infinite field this implies $F_i - X_i = 0$. □

In the case when k is a finite field we have a surprising result:

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

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

(ii) *If* $n \geq 2$ *and* $\mathrm{char}(k) \neq 2$ *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* $\mathcal{A}_l$ *of the symmetric group* $\mathcal{S}_l \cong \mathcal{B}(k^n)$ *where* $l = \#k^n$.

The proof will go in several steps. It will involve the fact that $\mathcal{B}(k^n)$, with composition of maps as operation, is isomorphic to the symmetic group $\mathcal{S}_l$ where $l = (\#k^n)$, because 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 $\mathcal{S}_n$. 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 $\{g(i), g(j)\} \cap \{i, j\} = \emptyset$.*

Theorem 2.5. *Let G be a primitive subgroup of $\mathcal{S}_n$. Suppose G contains a 3-cycle. Then G contains the alternating subgroup $\mathcal{A}_n$.*

For a proof, see [4].

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 that $f_{(\alpha,b)}(\alpha) = b$ 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 $\{1, a, a^2, \ldots\} = k^*$. Define*

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

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

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

P r o o f. We need to show that (1) for any $f \in k[X_2, \ldots, X_n]$ there exists $\sigma \in G$ 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 $\sigma_{(\alpha',b')}\sigma_{(\alpha'',b'')} = \sigma_{(\alpha'',b'')}\sigma_{(\alpha',b')} = (X_1 + g, X_2, \ldots, X_n)$, where $g \in k[X_2, \ldots, X_n]$ satisfies (in case $\alpha' \neq \alpha''$) $g(\alpha') = b'$, $g(\alpha'') = b''$. 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}, then $\sigma = (X_1 + g, X_2, \ldots, X_n)$ and $g(\alpha) = f(\alpha)$ for all $\alpha \in k^{n-1}$. Thus $\mathcal{E}(\sigma) = \mathcal{E}(\zeta)$.
Part (2): Since $\sigma_i \tau^m \sigma_i = (X_1, \ldots, X_{i-1}, a^m X_i, X_{i+1}, \ldots, X_n)$ 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 $\sigma_\gamma := (X_1 + \gamma_2 X_2 + \ldots + \gamma_n X_n, X_2, \ldots, X_n)$ where $\gamma := (\gamma_2, \ldots, \gamma_n) \in k^{n-1}$, generate the group of linear maps. By part (1) for each $\gamma \in k^{n-1}$ there exists 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 $i \in \{1, \ldots, n\}$ be such that $r_i \neq s_i$. If $i \geq 2$, then we take the map $\sigma_{(\alpha,1)}$, where $\alpha \in k^{n-1}$ is the $n-1$-tuple of the last $n-1$ coordinates of $r = (r_1, \alpha) \in k^n$. Then $\sigma_{(\alpha,1)}(r) = (r_1 + 1, \alpha)$ and $\sigma_{(\alpha,1)}(s) = s$. In the 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

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

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 $\mathrm{char}(k)$ on V_1, respectively on V_2. Let $\zeta := \sigma^{-1}\mu^{-1}\sigma\mu$. Then ζ acts trivially on $k^n \backslash (V_1 \cup V_2)$ and nontrivially only 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 works only 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 works only on elements of V_1) that $\zeta(\alpha) = \alpha$. Thus the only cases left are:
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 that $\sigma(A) = O, \sigma(B) = B, \mu(B) = O, \mu(A) = A, \sigma(O) \notin V_2, \mu(O) \notin V_1$. Using this we see that $\zeta(A) = B$, $\zeta(B) = O$, $\zeta(O) = A$, and hence ζ is a 3-cycle. □

Now we are ready for the proof of the main result:

Proof of Theorem 2.3. We will use notations as in Definition 2.7. We will consider $\mathcal{B}(k^n)$ as a subgroup of $\mathcal{S}_{q^n}$ where $q = \#k$. By Theorem 2.5, Lemma 2.8 and Lemma 2.9 we see that $\mathcal{A}_{q^n}$ 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 $a \in k^*, b \in k$. These maps are all different bijections, so these are $\#k^* \times \#k = (q-1)q$ different maps. Since $\#\mathcal{B}(k) = (\#k)!$ the result follows.
(ii) Case $n \geq 2$, $\mathrm{char}(k) \neq 2$: If we can find $\sigma \in G$ such that $\mathcal{E}(\sigma) \notin \mathcal{A}_{q^n}$, then

$\mathcal{E}(G) = \mathcal{S}_{q^n}$; 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 separate $(q-1)$-cycles: there is a separate cycle in the set $V_\alpha := \{(a, \alpha) \mid a \in k^*\}$ for each $\alpha \in k^{n-1}$. Hence τ has 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 $\sigma_{(\mathrm{o},1)}$ where $\mathrm{o} = (0, \ldots, 0) \in k^{n-1}$. This map acts nontrivially only on $(0, \ldots, 0)$ and $(1, 0, \ldots, 0)$; it interchanges them. Hence the sign is -1. The rest is the same as in 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 $\mathcal{E}(G) = \mathcal{A}_{q^n}$.
1) $\sigma^2_{(\alpha,b)} = (X_1 + 2f_{(\alpha,b)}, X_2, \ldots, X_n) = Id$, (since $2 \equiv 0 \mod (2)$). Hence $\sigma_{(\alpha,b)}$ consists only of 2-cycles. If we count the number of elements which stay invariant, then we will know how many 2-cycles contains it. 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 of $\sigma_{(\alpha,b)}$ is 1.
2) $\sigma_i^2 = Id$, hence σ_i consists only of 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 also has sign 1. $\square$

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. Recall that 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 the cases $q = 2$ or $q = p^r$ where $p > 2$ we can find such a bijection B. In the case $q = 2^r, r \geq 2$, we will 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. $\square$

Notice that the first two results of Theorem 2.3 are also true if we replace $T(k, n)$ by $\mathrm{Aut}_k(A_n)$; however, the third one is unclear. However, if that would not 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 a positive integer. Then* $\mathrm{Aut}_k(A_n) = T(k, n)$.

Corollary 3.3 (of Theorem 2.3)**.** *Suppose $k = \mathbb{F}_{2^r}$ where $r \geq 2$ and $F \in \mathrm{Aut}_k(A_n)$ 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 this is not clear.

REFERENCES

[1] K. Adjamagbo. On separable algebras over a U.F.D. and the Jacobian Conjecture in any characteristic. In: Automorphisms of affine spaces (Ed. Arno van den Essen). Proceedings of the international conference on invertible polynomial maps, Curaçao, Netherlands Antilles, July 4–8, 1994. Dordrecht: Kluwer Academic Publishers, 1995, 89–103.

[2] K. Adjamagbo, H. Derksen, A. van den Essen. On polynomial maps in positive characteristic and the Jacobian Conjecture. Unpublished, report 9208, Univ. of Nijmegen, 1992.

[3] A. van den Essen. Polynomial Automorphisms and the Jacobian Conjecture. Progress in Mathematics, Birkhäuser Verlag, Basel-Boston-Berlin, 2000.

[4] I. M. Isaacs, T. Zieschang. Generating symmetric groups. *Amer. Math. Monthly* **102** (1995), 734–739.

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

[6] P. Nousiainen. On the Jacobian Problem in positive characteristic. Pennsylvania State Univ., preprint, 1981.

University of Nijmegen
Toernooiveld 1
The Netherlands
E-mail: stefanm@sci.kun.nl

Received November 21, 2001
Revised December 12, 2001