The affine preservers of non-singular matrices

Clément de Seguins Pazzis∗†

June 2, 2010

Abstract

When \( K \) is an arbitrary field, we study the affine automorphisms of \( M_n(K) \) that stabilize \( GL_n(K) \). Using a theorem of Dieudonné on maximal affine subspaces of singular matrices, this is easily reduced to the known case of linear preservers when \( n > 2 \) or \( \# K > 2 \). We include a short new proof of the more general Flanders’ theorem for affine subspaces of \( M_{p,q}(K) \) with bounded rank. We also find that the group of affine transformations of \( M_2(F_2) \) that stabilize \( GL_2(F_2) \) does not consist solely of linear maps. Using the theory of quadratic forms over \( F_2 \), we construct explicit isomorphisms between it, the symplectic group \( Sp_4(F_2) \) and the symmetric group \( S_6 \).

AMS Classification: 15A86; 15A63, 11E57.

Keywords: linear preservers, general linear group, singular subspaces, affine group, rank, linear subspaces, symplectic group, Arf invariant, quadratic forms, symmetric group.

1 Introduction

Here, \( K \) will denote an arbitrary field and \( n \) a positive integer. By an affine transformation of an affine space, we will always mean an affine bijective map. We let \( M_{n,p}(K) \) denote the set of matrices with \( n \) rows, \( p \) columns and entries in \( K \), and \( GL_n(K) \) the set of non-singular matrices in the algebra \( M_n(K) \) of square matrices of order \( n \).

∗Professor of Mathematics at Lycée Privé Sainte-Geneviève, 2, rue de l’École des Postes, 78029 Versailles Cedex, FRANCE.
†e-mail address: dsp.prof@gmail.com
For \((i,j) \in \llbracket 1, n \rrbracket \times \llbracket 1, p \rrbracket\), we let \(E_{i,j}\) denote the elementary matrix of \(M_{n,p}(K)\) with entry 1 at the \((i,j)\) spot and zero elsewhere.

We make the group \(GL_n(K) \times GL_p(K)\) act on the set of linear subspaces of \(M_{n,p}(K)\) by

\[(P,Q).V := PVQ^{-1}.
\]

Two linear subspaces of the same orbit will be called equivalent (this means that they represent the same set of linear transformations from a \(p\)-dimensional vector space to an \(n\)-dimensional vector space).

For non-singular matrices \(P\) and \(Q\) in \(GL_n(K)\), we define

\[u_{P,Q} : \begin{cases} M_n(K) &\rightarrow M_n(K) \\ M &\mapsto PMQ \end{cases} \quad \text{and} \quad v_{P,Q} : \begin{cases} M_n(K) &\rightarrow M_n(K) \\ M &\mapsto PM^tQ. \end{cases}\]

Clearly, these are non-singular endomorphisms of the vector space \(M_n(K)\) which map \(GL_n(K)\) onto itself, and the subset

\[G_n(K) := \{ u_{P,Q} \mid (P,Q) \in GL_n(K)^2 \} \cup \{ v_{P,Q} \mid (P,Q) \in GL_n(K)^2 \}\]

is a subgroup of \(GL(M_n(K))\), which we will call the Frobenius group.

One of the earliest result on linear preservers problems is the following one of Dieudonné [2] following a classical work of Frobenius [4]:

**Theorem 1.** The group \(G_n(K)\) consists of all the automorphisms of the vector space \(M_n(K)\) which stabilize \(GL_n(K)\).

To prove this, Dieudonné established a major result on singular subspaces of \(M_n(K)\) (i.e. linear or affine subspaces which contain only singular matrices):

**Theorem 2.** Let \(V\) be a singular affine subspace of \(M_n(K)\). Then \(\dim V \leq n(n-1)\).

If \(\dim V = n(n-1)\), then either \(V\) or \(V^t\) is equivalent to the linear subspace \(\{ [M \ 0] \mid M \in M_{n-1}(K) \}\) unless \(n = 2, \ #K = 2\) and \(V\) is not a linear subspace of \(M_n(K)\).

Notice that all matrices in the plane \(\left\{ \begin{bmatrix} x & y \\ 0 & x+1 \end{bmatrix} \mid (x,y) \in F_2^2 \right\}\) are singular, hence the exceptional case mentioned in the theorem.

Dieudonné initially restricted his study to linear transformations because he wanted to generalize the classical description for the orthogonal group of the
quadratic space \((M_2(\mathbb{K}), \det)\). As we shall see, the generalization to affine transformations is extremely easy except for the exceptional case of \(n = 2\) and \(\mathbb{K} \cong \mathbb{F}_2\), but it is very intriguing that Dieudonné, at the time the best specialist in the theory of classical groups, completely overlooked the connection between this exceptional case, the symplectic group \(\text{Sp}_4(\mathbb{F}_2)\) and the theory of quadratic forms over \(\mathbb{F}_2\). It is our main goal to fill this bizarre hole in Dieudonné’s celebrated paper.

In Section 2, we will quickly determine the affine transformations of \(M_n(\mathbb{K})\) which stabilize \(\text{GL}_n(\mathbb{K})\) when \(n > 2\) or \(#\mathbb{K} > 2\), and show briefly that we cannot expect to obtain results of the type of [8] for singular affine endomorphisms of \(M_n(\mathbb{K})\). Our (very short) proof will involve Theorems 1 and 2. We will use this opportunity to give a brand new proof of Theorem 2 in the more general formulation of Flanders with no restriction on the field (except for the case where an explicit counter-example exists). This is, to our knowledge, the shortest proof of this theorem, appealing only to basic linear algebra. In the last section, we will investigate the case \(n = 2\) and \(\mathbb{K} \cong \mathbb{F}_2\), which will involve the theory of quadratic forms over \(\mathbb{F}_2\) (the reader will find proofs of the more basic statements in section 10.4 of [7]).

Let us finish this introductory section by stating our main theorem:

**Theorem 3.** Let \(n\) be an integer and \(\mathbb{K}\) an arbitrary field. Let \(\mathcal{A}G_n(\mathbb{K})\) denote the group of affine automorphisms of \(M_n(\mathbb{K})\) which stabilize \(\text{GL}_n(\mathbb{K})\).

(a) If \(n > 2\) or \(#\mathbb{K} > 2\), then all affine automorphisms of \(M_n(\mathbb{K})\) which stabilize \(\text{GL}_n(\mathbb{K})\) are linear, hence \(\mathcal{A}G_n(\mathbb{K}) = \mathcal{G}_n(\mathbb{K})\).

(b) Not all elements of \(\mathcal{A}G_2(\mathbb{F}_2)\) are linear maps.

(c) The natural action of \(\mathcal{A}G_2(\mathbb{F}_2)\) on \(\text{GL}_2(\mathbb{F}_2)\) induces a group isomorphism from \(\mathcal{A}G_2(\mathbb{F}_2)\) to the symmetric group \(\mathcal{S}(\text{GL}_2(\mathbb{F}_2))\). Assigning its linear part to every transformation in \(\mathcal{A}G_2(\mathbb{F}_2)\) induces a group isomorphism from \(\mathcal{A}G_2(\mathbb{F}_2)\) to the symplectic group of the form \((A, B) \mapsto \det(A + B) - \det(A) - \det(B)\).

2 The case \(n > 2\) or \(#\mathbb{K} > 2\)

We start by a quick proof of statement (a) in Theorem 3. Let \(u\) be an affine automorphism of \(M_n(\mathbb{K})\) such that \(u(P)\) is non-singular for every \(P \in \text{GL}_n(\mathbb{K})\).
We assume $n > 2$ or $\# \mathbb{K} > 2$. For $i \in [1, n]$, let $V_i$ denote the set of all matrices of $M_n(\mathbb{K})$ with a zero $i$-th column. Then $V_i$ is a $(n^2 - n)$-dimensional affine subspace of $M_n(\mathbb{K})$ consisting only of non-singular matrices. It follows that the same is true of $u^{-1}(W_i)$. By Theorem 2, we deduce that $u^{-1}(W_i)$ is a linear subspace of $M_n(\mathbb{K})$. Consequently,

$$u^{-1}\{0\} = \bigcap_{i=1}^{n} u^{-1}(W_i)$$

is a linear subspace of $W$, hence it contains 0, which proves $u$ is linear. Using Theorem 1 we conclude that $u \in \mathcal{G}_n(\mathbb{K})$, which essentially finishes the proof of statement (a).

Let us now give a corollary for this part of Theorem 3.

**Corollary 4.** Let $n$ be an integer. Assume $n \neq 2$ or $\# \mathbb{K} > 2$. Then:

(i) The group $\mathcal{G}_n(\mathbb{K})$ consists of all the affine endomorphisms $u$ of $M_n(\mathbb{K})$ such that $u^{-1}(GL_n(\mathbb{K})) = GL_n(\mathbb{K})$.

(ii) If $n > 1$ or $\# \mathbb{K} > 2$, then $\mathcal{G}_n(\mathbb{K})$ consists of all the affine endomorphisms $u$ of $M_n(\mathbb{K})$ such that $u(GL_n(\mathbb{K})) = GL_n(\mathbb{K})$.

Notice that $u : \lambda \mapsto 1$ is a non-linear affine endomorphism of $M_1(\mathbb{F}_2)$ such that $u(GL_1(\mathbb{F}_2)) = GL_1(\mathbb{F}_2)$.

**Proof.** Statement (i) derives from Theorem 3 in the very same way that statement (ii) in Theorem 1 of [8] derived from statement (iii) of that same theorem (i.e. we show that the kernel of the linear part of $u$ is trivial).

Assume now $n > 1$ or $\# \mathbb{K} > 2$, and let $u$ be an affine endomorphism of $M_n(\mathbb{K})$ such that $u(GL_n(\mathbb{K})) = GL_n(\mathbb{K})$. It then suffices to show that $u$ is onto, which comes from the following lemma.

**Lemma 5.** Assume $n > 1$ or $\# \mathbb{K} > 2$. Then no strict affine subspace of $M_n(\mathbb{K})$ may contain $GL_n(\mathbb{K})$.

**Proof.** The case $n = 1$ is trivial so we assume $n \geq 2$. Assume there is a linear hyperplane of $M_n(\mathbb{K})$ which contains $GL_n(\mathbb{K})$. Then there would be a non-zero matrix $A \in M_n(\mathbb{K})$ and an integer $a$ such that $\forall P \in GL_n(\mathbb{K})$, $\text{tr}(AP) = a$.

It would follow that $\text{tr}(QAP) = \text{tr}(APQ) = a$ for every $(P, Q) \in GL_n(\mathbb{K})^2$,
hence every matrix with rank $r := \text{rk} A$ would have trace $a$. If $r \geq 2$, the two rank $r$ matrices $\sum_{i=1}^{r} E_{i,i}$ and $E_{1,2} + E_{2,1} + \sum_{i=2}^{r} E_{i,i}$ have different traces. If $r = 1$, then the rank 1 matrices $E_{1,1}$ and $E_{1,2}$ have different traces. In any case, we have a contradiction.

The reader should not expect any neat description of the singular affine endomorphisms stabilizing $\text{GL}_n(\mathbb{K})$ (unlike our results on linear endomorphisms, cf. [8]). It is indeed very easy to build large affine subspaces consisting solely of non-singular matrices, a good example being the subspace $I_n + T_n^{++}(\mathbb{K})$, where $T_n^{++}(\mathbb{K})$ denotes the subset of strictly upper triangular matrices in $M_n(\mathbb{K})$ (more generally, we can take a linear subspace $V$ of nilpotent matrices and consider the affine subspace $I_n + V$). Any affine map $u : M_n(\mathbb{K}) \to I_n + T_n^{++}(\mathbb{K})$ then stabilizes $\text{GL}_n(\mathbb{K})$.

3 A Flanders theorem for affine subspaces

This section is devoted to a generalization of Theorem 2. Prior to this, such a generalization had been proven by Flanders [3] for linear subspaces with a large enough field, and Meshulam [6] for linear subspaces with an arbitrary field. Our starting point will resemble a lot to that of Flanders, but we will be very careful to avoid multiplying by scalars as much as possible.

**Notation 1.** For $p \in [0,n]$, we set $C_p := \left\{ \begin{bmatrix} M & 0 \end{bmatrix} | M \in M_{n,p}(\mathbb{K}) \right\} \subset M_n(\mathbb{K})$.

**Theorem 6.**

Let $\mathcal{V}$ be an affine subspace of $M_n(\mathbb{K})$, and set $r := \max\{\text{rk} A | A \in \mathcal{F}\}$.

Then $\dim \mathcal{V} \leq nr$. If in addition $\dim \mathcal{V} = nr$, then $\mathcal{V}$ is equivalent to either $C_r$ or $\bar{C}_r$ except when $n = 2$, $\# \mathbb{K} = 2$, $r = 1$ and $0 \notin \mathcal{V}$.

The proof will involve the following lemma, which we will prove right away:

**Lemma 7.** Let $H$ be a $pq$-dimensional linear subspace of $M_{p,q}(\mathbb{K}) \times M_{q,p}(\mathbb{K})$ with:

(i) $\forall ((L,C), (L',C')) \in H^2$, $\forall P \in \text{GL}_q(\mathbb{K})$, $LPC' + L'PC = 0$;

(ii) if $\# \mathbb{K} > 2$ and $p = q = 1$, then $\forall (L,C) \in H$, $\forall P \in \text{GL}_q(\mathbb{K})$, $LPC = 0$.

Then either $H = M_{p,q}(\mathbb{K}) \times \{0\}$ or $H = \{0\} \times M_{q,p}(\mathbb{K})$, or $p = q = 1$ and $\mathbb{K} \simeq \mathbb{F}_2$. 5
Proof. It suffices to show that $H \subset \text{M}_{p,q}(\mathbb{K}) \times \{0\}$ or $H \subset \{0\} \times \text{M}_{q,p}(\mathbb{K})$ except in the exceptional case mentioned above. We will make great use of the following easy fact: for any $C \in \text{M}_{q,p}(\mathbb{K}) \setminus \{0\}$, one has $\sum_{P \in \text{GL}_q(\mathbb{K})} \text{Im} PC = \mathbb{K}^q$.

Assume $(L, C) \mapsto L$ is not one-to-one from $H$ and choose a non-zero $(0, C)$ in its kernel. Let $(L', C') \in H$. Then (i) shows $\forall P \in \text{GL}_q(\mathbb{K})$, $L'PC = 0$ hence $L' = 0$ by the preliminary remark, and $(L', C') \mapsto C'$ is then one-to-one from $H$. In any case, replacing $H$ with $\{(B^t, A^t) \mid (A, B) \in H\}$ shows we can assume $(L, C) \mapsto L$ is one-to-one on $H$, hence a linear isomorphism from $H$ to $\text{M}_{p,q}(\mathbb{K})$, which entails that $H = \{(L, \alpha(L)) \mid L \in \text{M}_{p,q}(\mathbb{K})\}$ for some linear map $\alpha$.

Assume $\# \mathbb{K} > 2$ and $p = q = 1$. Let $L \in \text{M}_{p,q}(\mathbb{K}) \setminus \{0\}$. Then $LP \alpha(L) = 0$ for every $P \in \text{GL}_q(\mathbb{K})$, hence $\alpha(L) = 0$ using the preliminary remark, and we deduce that $H \subset \text{M}_{p,q}(\mathbb{K}) \times \{0\}$.

Assume now $(p, q) \neq (1, 1)$ and $\alpha$ is non-zero. Assume there exists $L \in \text{M}_{p,q}(\mathbb{K}) \setminus \{0\}$ such that $\alpha(L) = 0$. For every $L' \in \text{M}_{p,q}(\mathbb{K})$, we then have $\forall P \in \text{GL}_n(\mathbb{K})$, $LP \alpha(L') = 0$ hence $\alpha(L') = 0$ (using the preliminary remark again). This contradicts a previous assumption so $\alpha$ is actually one-to-one.

Let $L \in \text{M}_{p,q}(\mathbb{K}) \setminus \{0\}$. Then $\alpha(L) \neq 0$, so the identity $\forall P \in \text{GL}_q(\mathbb{K})$, $L' P \alpha(L) = -LP \alpha(L')$ and the preliminary remark entail that $\text{Im} L' \subset \text{Im} L$ for every $L' \in \text{M}_{p,q}(\mathbb{K})$. This shows $p = 1$ since $L$ can be chosen with rank 1. Then $q > 1$, we can choose linearly independent $L$ and $L'$ in $\text{M}_{1,q}(\mathbb{K})$, so $\alpha(L)$ and $\alpha(L')$ are linearly independent; we can also choose $Y_1 \in \text{Ker} L \setminus \{0\}$ and $Y_2 \in \mathbb{K}^q \setminus \langle \text{Ker} L \cup \text{Ker} L' \rangle$, and there exists then some $P \in \text{GL}_q(\mathbb{K})$ such that $P \alpha(L') = Y_1$ and $P \alpha(L) = Y_2$. This yields $LP \alpha(L') + L' P \alpha(L) = L'Y_2 \neq 0$, contradicting (i).

Proof of Theorem 6. The case $n = 2$, $\mathbb{K} \simeq \mathbb{F}_2$ and $V$ is a linear subspace is straightforward with the help of the following easy lemma: given two rank 1 matrices $M$ and $N$ of $\text{M}_n(\mathbb{K})$, if $M + N$ has rank 1, then $\text{Ker} M = \text{Ker} N$ or $\text{Im} M = \text{Im} N$.

We now discard the case $n = 2$ and $\# \mathbb{K} = 2$, and let $V$ denote the translation vector space of $\mathcal{V}$.

Let $A = \begin{bmatrix} P_1 & C_1 \\ L_1 & \alpha_1 \end{bmatrix} \in \mathcal{V}$, with blocks $P_1$, $L_1$, $C_1$ and $\alpha_1$ respectively of size $(r, r)$, $(n - r, r)$, $(r, n - r)$ and $(n - r, n - r)$ (in the rest of the proof, all the block decompositions will have the same configuration). We assume $\text{rk} P_1 = r$. 

6
Gaussian elimination shows $A$ is equivalent to 
\[
\begin{bmatrix}
P_1 & C_1 \\
0 & \alpha_1 - L_1 P_1^{-1} C_1
\end{bmatrix}
\], hence
\[
L_1 P_1^{-1} C_1 - \alpha_1 = 0. \tag{1}
\]

Write every $M \in V$ as 
\[
M = \begin{bmatrix}
K(M) & C(M) \\
L(M) & \alpha(M)
\end{bmatrix},
\]
set $W := \text{Ker } K$ i.e. $W$ is the linear subspace of matrices of $V$ having the form
\[
\begin{bmatrix}
0 & \ast \\
? & ?
\end{bmatrix}.
\]
Set also $E := \text{M}_{n-r,r}(\mathbb{K}) \times \text{M}_{r,n-r}(\mathbb{K})$ and $\varphi(M) := (L(M), C(M)) \in E$ for any $M \in W$.

For every $M \in W$, the matrix $A + M$ belongs to $V$ and has $P_1$ as left-upper block, hence (1) shows:
\[
(L(M) + L_1) P_1^{-1} (C(M) + C_1) - \alpha_1 - \alpha(M) = 0.
\]

Subtracting (1), we deduce:
\[
\forall M \in W, \quad L(M) P_1^{-1} C(M) = \alpha(M) - L(M) P_1^{-1} C_1 - L_1 P_1^{-1} C(M). \tag{2}
\]

Notice that the left-hand side of the equality is a quadratic form $q$ of $M$ on $V$, whilst the right-hand side is a linear form. We deduce:

(i) if $\# K > 2$, then $\forall M \in W$, $L(M) P_1^{-1} C(M) = 0$;

(ii) in any case, $\forall (M, N) \in W^2$, $L(M) P_1^{-1} C(N) + L(N) P_1^{-1} C(M) = 0$.

Using an equivalence, we lose no generality assuming that $V$ contains $J_r := \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.

Applying (2) to $A = J_r$ shows $\varphi$ is one-to-one\(^2\) and $\varphi(W)$ is a totally singular subspace for the non-degenerate symmetric bilinear form $b : ((L, C), (L', C')) \mapsto \text{tr}(LC' + L'C)$ on $E$. Hence $\text{rk } \varphi \leq (\dim E)/2 = r(n - r)$ and the rank theorem shows:
\[
dim V = \text{rk } K + \dim W = \text{rk } K + \text{rk } \varphi \leq r^2 + r(n - r) = nr.
\]

Assume now $\dim V = nr$. Then $K$ is onto and $\varphi(W)$ has dimension $r(n - r)$.

For every $P \in \text{GL}_r(\mathbb{K})$, we can then find some $A \in V$ with $P^{-1}$ as first block.

\(^1\)For (ii), compute the polar form of $q$ as defined by $b_q(M, N) := q(M + N) - q(M) - q(N)$.

\(^2\)Indeed, $(L(M), C(M)) = (0, 0)$ entails $\alpha(M) = L(M) C(M) = 0$. 

7
Lemma 7 thus applies to $\varphi(W)$. By transposing $V$ if necessary, we lose no generality assuming $\varphi(W) = M_{n-r,r}(K) \times \{0\}$, in which case $W$ consists of all matrices of the form $\begin{bmatrix} 0 & 0 \\ ? & 0 \end{bmatrix}$. The factorization lemma for affine maps helps us then recover affine maps $\tilde{C}$ and $\tilde{\alpha}$ such that

$$V = \left\{ \begin{bmatrix} A & \tilde{C}(A) \\ B & \tilde{\alpha}(A) \end{bmatrix} \mid A \in M_r(K), \ B \in M_{n-r,r}(K) \right\}$$

and we have seen that $\tilde{C}(0) = 0$ and $\tilde{\alpha}(0) = 0$, hence $\tilde{C}$ and $\tilde{\alpha}$ are linear!

Let $P \in \text{GL}_r(K)$. Then identity (1) shows $\forall B \in M_{n-r,r}(K), \ BP^{-1}\tilde{C}(P) = \alpha(P)$. Taking $B = 0$ shows $\alpha(P) = 0$, then taking all possible $B$’s shows $\tilde{C}(P) = 0$. The classical result span$(\text{GL}_r(K)) = M_r(K)$ (use Lemma 5 or more simply Lemma 3 of [8]) then entails $\tilde{\alpha} = 0, \tilde{C} = 0$ and $V = C_r$. \hfill \Box

The next corollary will easily follow with a standard line of reasoning.

**Corollary 8.** Given positive integers $n > p$, let $V$ be an affine subspace of $M_{n,p}(K)$ and set $r := \max\{\text{rk } A \mid A \in F\}$. Then $\dim V \leq nr$. If in addition $\dim V = nr$, then $V$ is equivalent to $\{ \begin{bmatrix} M & 0 \end{bmatrix} \mid M \in M_{n,r}(K) \}$.

**Proof.** We embed $V$ into $M_n(K)$ as an affine subspace $V'$ by mapping any $M \in V$ to $\begin{bmatrix} M & 0 \end{bmatrix}$. Then Theorem 6 applies to $V'$ (notice that the exceptional case $n = 2$ and $r = 1$ does not occur), hence $\dim V = \dim V' \leq nr$.

Assume now $\dim V' = nr$. Notice that $V'$ cannot be equivalent to $tC_r$ (the intersection of kernels of matrices of $V'$ would be $\{0\}$, which is not the case). Hence $V'$ is equivalent to $C_r$, which shows there is a $(n-r)$-dimensional subspace $F$ of $K^n$ on which every $M' \in V'$ vanishes. Then every $M \in V$ vanishes on $G := F \cap (K^p \times \{0\})$, with $\dim G \geq p - r$. Since $\dim V = nr$, we deduce that $\dim G = p - r$ and $V$ is the set of matrices of $M_{n,p}(K)$ vanishing on $G$. Hence $V$ is clearly equivalent to the linear subspace $\left\{ \begin{bmatrix} M & 0 \end{bmatrix} \mid M \in M_{n,r}(K) \right\}$ of $M_{n,p}(K)$.

\hfill \Box

\footnote{Using again $L(M)C(M) = \alpha(M)$ for every $M \in V$.}
4 The case of $M_2(\mathbb{F}_2)$

4.1 A quick review of quadratic forms in characteristic 2

Let $K$ be a field of characteristic 2 and $V$ an $n$-dimensional vector space over $K$. A quadratic form on $V$ is a map of the type $q : x \mapsto b(x,x)$ for some (a priori non-symmetric) bilinear form $b : V \times V \to K$. To such a quadratic form $q$ is assigned a polar form $b_q : (x,y) \mapsto q(x+y) - q(x) - q(y)$, which is always an alternate bilinear form. We say that $q$ is regular (or non-degenerate) when its polar form is non-degenerate, i.e. symplectic (notice this implies that $n$ is even).

Two quadratic forms $q_1$ and $q_2$ on $V$ are called equivalent when there exists a linear automorphism $u$ of $V$ such that $q_2 = q_1 \circ u$.

Given a basis $B$ of $V$, a representing matrix for $q$ in $B$ is a matrix $A \in M_n(K)$ such that $q(x) = X^tAX$ for every $x \in V$ with associated column matrix $X$ in $B$. In particular, $q$ is represented in $B$ by a unique upper triangular matrix $T$, the “alternate part” $T + T^t$ of which represents $b_q$ in $B$.

Assume now $q$ is regular, and let $B$ denote a symplectic basis for $b_q$. Then there exist two diagonal matrices $D_1$ and $D_2$ such that $\begin{bmatrix} D_1 & I_n \\ 0 & D_2 \end{bmatrix}$ represents $q$ in $B$. Setting $\mathcal{P}(K) := \{ x^2 + x \mid x \in K \}$, which is a subgroup of $(K,+)$, it can then be proven that the class $\Delta(q)$ of $\text{tr}(D_1D_2)$ in the quotient group $K/\mathcal{P}(K)$ is independent on the choice of $B$: this is called the Arf invariant of $q$. Two equivalent regular quadratic forms have the same Arf invariant, and the converse is true if $K$ is perfect, in particular when $K$ is finite. Notice that $\mathcal{P}(K) = \{0\}$ when $K = \mathbb{F}_2$, in which case the Arf invariant is naturally considered as an element of $\mathbb{F}_2$.

4.2 From $\text{Sp}_4(\mathbb{F}_2)$ to affine automorphisms of $M_2(\mathbb{F}_2)$ ...

We set here $V = \mathbb{F}_2^4$ which we equip with the canonical symplectic form $b$ (for which the canonical basis $B$ is symplectic). The set $Q(b)$ of all quadratic forms on $V$ with polar form $b$ is an affine subspace of $\mathbb{F}_2^V$ with the dual space $V^*$ as translation vector space. Given $u \in \text{Sp}(b)$ and $q \in Q(b)$, the quadratic form $q \circ u$ has polar form $b$, hence $(q,u) \mapsto q \circ u^{-1}$ defines a left-action of $\text{Sp}(b)$ on $Q(b)$. We set $\psi : \text{Sp}(b) \to \mathcal{S}(Q(b))$.
as the associated homomorphism and notice that, for every \( u \in \text{Sp}(b) \), the map \( \psi(u) \) is an affine transformation which preserves the Arf invariant.

Let \( q \in \mathbb{Q}(b) \). Since \( B \) is a symplectic basis, there is a unique \( M(q) = \begin{bmatrix} a & d \\ b & c \end{bmatrix} \) such that \( q \) is represented in \( B \) by the upper triangular matrix

\[
\begin{bmatrix}
  a & 0 & 1 & 0 \\
  0 & b & 0 & 1 \\
  0 & 0 & c & 0 \\
  0 & 0 & 0 & d
\end{bmatrix}.
\]

Notice that \( q \mapsto M(q) \) is an affine isomorphism from \( \mathbb{Q}(b) \) to \( \mathbb{M}_2(\mathbb{F}_2) \) and \( \forall q \in \mathbb{Q}(b), \ \det M(q) = \Delta(q) \). In particular, the set \( \mathbb{Q}_1(b) \) of elements \( q \in \mathbb{Q}(b) \) with \( \Delta(q) = 1 \) has six elements.

**Proposition 9.** The homomorphism \( \overline{\psi} : \text{Sp}(b) \mapsto \mathfrak{S}(\mathbb{Q}_1(b)) \) induced by \( \psi \) is an isomorphism.

**Remark 1.** It can easily deduced from there that \( O(q) \simeq \mathfrak{S}_5 \) for any \( q \in \mathbb{Q}_1(b) \).

**Proof.** Notice that both groups \( \text{Sp}(b) \) and \( \mathfrak{S}(\mathbb{Q}_1(b)) \) have order 6! (see page 147 paragraph III.6 of [1]). It will then suffice to show that \( \overline{\psi} \) is one-to-one. Let \( u \in \text{Sp}(b) \setminus \{\text{id}_V\} \). We will exhibit a quadratic form \( q \) in \( \mathbb{Q}_1(b) \) for which \( u \) is not an orthogonal automorphism, so that \( \psi(u)[q] \neq q \). We choose a non-zero \( x \in V \) such that \( u(x) \neq x \), hence \( x \) and \( u(x) \) are not colinear. We then exhibit a quadratic form \( q \in \mathbb{Q}_1(b) \) such that \( q(x) = 0 \) and \( q(u(x)) = 1 \).

- If \( b(x, u(x)) = 0 \), then we extend \((x, u(x))\) into a symplectic basis \( B \) of \( V \), so
  \[
  \begin{bmatrix}
  0 & 0 & 1 & 0 \\
  0 & 1 & 0 & 1 \\
  0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 1
\end{bmatrix}
\]
  represents in \( B \) a quadratic form that suits our needs.

- If \( b(x, u(x)) = 1 \), then we choose a symplectic basis \((y, z)\) of \( \{x, u(x)\}^\perp \), so
  \[
  \begin{bmatrix}
  0 & 1 & 0 & 0 \\
  0 & 1 & 0 & 0 \\
  0 & 0 & 1 & 1 \\
  0 & 0 & 0 & 1
\end{bmatrix}
\]
  represents in \((x, u(x), y, z)\) a quadratic form that suits our needs.

\( \square \)
The affine isomorphism \( q \mapsto M(q) \) induces an isomorphism from the affine group of \( \mathbb{Q}(b) \) to that of \( M_2(\mathbb{F}_2) \) which maps the preservers of the Arf invariant to the preservers of \( \text{GL}_2(\mathbb{F}_2) \). Right-composing it with \( \psi \) yields then a group homomorphism \( \varphi : \text{Sp}(b) \to A\mathcal{G}_2(\mathbb{F}_2) \). Together with the homomorphism associated with the natural action of \( A\mathcal{G}_2(\mathbb{F}_2) \) on \( \text{GL}_2(\mathbb{F}_2) \), this defines a sequence:

\[
\text{Sp}(b) \overset{\varphi}{\longrightarrow} A\mathcal{G}_2(\mathbb{F}_2) \longrightarrow \mathcal{S}(\text{GL}_2(\mathbb{F}_2)).
\]

**Proposition 10.** The homomorphism \( \text{Sp}(b) \to A\mathcal{G}_2(\mathbb{F}_2) \) induced by \( \psi \) and \( M \) is an isomorphism, and so is the natural homomorphism \( A\mathcal{G}_2(\mathbb{F}_2) \to \mathcal{S}(\text{GL}_2(\mathbb{F}_2)) \).

**Proof.** By Lemma \( \text{[5]} \), every affine automorphism of \( M_2(\mathbb{F}_2) \) which fixes every non-singular matrix must be the identity, hence the second map is one-to-one. The conclusion follows then readily from Proposition \( \text{[9]} \). \( \square \)

We may now easily compute an explicit affine automorphism of \( M_2(\mathbb{F}_2) \) which is not linear. The six elements of \( \text{GL}_2(\mathbb{F}_2) \) are:

\[
\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}.
\]

Define \( u \in A\mathcal{G}_2(\mathbb{F}_2) \) as the element which permutes the first two and fixes all the others. Notice that the four last matrices form a basis of \( M_2(\mathbb{F}_2) \), hence \( u \) cannot be linear. More explicitly, a straightforward computation shows:

\[
\forall(a, b, c, d) \in \mathbb{F}_2^4, \quad u \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} b + c + d + 1 & a + b + d + 1 \\ a + c + d + 1 & a + b + c + 1 \end{bmatrix}.
\]

**4.3 . . . and back again to** \( \text{Sp}_4(\mathbb{F}_2) \)

Notice now that the determinant is a regular quadratic form on \( M_2(\mathbb{F}_2) \) (in the canonical basis \( (E_{1,1}, E_{2,2}, E_{1,2}, E_{2,1}) \) of \( M_2(\mathbb{F}_2) \), it is represented by the matrix

\[
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0
\end{bmatrix},
\]

with a non-singular alternate part). Let \( B \) denote its polar form, so that \( B(X,Y) = \det(X + Y) - \det X - \det Y \) for every \( (X,Y) \in M_2(\mathbb{F}_2)^2 \). Let \( u \in A\mathcal{G}_2(\mathbb{F}_2) \) and \( \bar{u} \) be its linear part. Then \( u \) is a determinant preserver (since

11
$u$ is bijective and stabilizes the finite set $GL_2(\mathbb{F}_2)$. For every $M \in M_2(\mathbb{F}_2)$, equating $\det(u(M))$ with $\det M$ yields:

$$\det u(0) + B(u(0), \vec{u}(M)) + \det(\vec{u}(M)) = \det 0 + B(u(0), M) + \det(M).$$

Taking the polar form on both sides then shows that $\vec{u}$ is a symplectic automorphism for $B$. From that, we deduce a group homomorphism:

$$\alpha : AGL_2(\mathbb{F}_2) \longrightarrow Sp(B)$$

which we claim is an isomorphism. Since both groups have the same order, it will suffice to show $\alpha$ is one-to-one. If not, then there would be a non-identity translation which preserves the determinant on $M_2(\mathbb{F}_2)$, hence a non-zero matrix $A$ such that $\det(A + M) = \det M$ for every $M \in M_2(\mathbb{F}_2)$. This would yield $\forall M \in M_2(\mathbb{F}_2)$, $\det A + B(A, M) = 0$, hence $\det A = 0$, and then $B(A, -) = 0$ with $A \neq 0$. This would contradict the fact that $B$ is symplectic. We conclude that $\alpha$ is an isomorphism, which was the final statement in Theorem 3.

**Acknowledgements**

This article is dedicated to Saab Abou-Jaoudé, who has, some time ago, offered me crucial help in my research on the Flanders’ theorem.

**References**

[1] E. Artin, *Geometric Algebra*, Interscience Tracts in Pure and Applied Mathematics, 3, Wiley Classics Library, Interscience Publishers, New-York, 1988.

[2] J. Dieudonné, Sur une généralisation du groupe orthogonal à quatre variables, *Arch. Math*, 1 (1949), 282-287.

[3] H. Flanders, On spaces of linear transformations with bounded rank, *J. Lond. Math. Soc*, 37 (1962), 10-16.

[4] G. Frobenius, Uber die Darstellung der endlichen Gruppen durch Lineare Substitutionen, *Sitzungsber Deutsch. Akad. Wiss. Berlin*, (1897), 994-1015.

[5] W. Greub, *Linear algebra, 3rd edition*, Grundlehren der mathematischen Wissenschaften, 97 Springer-Verlag, 1967.
[6] R. Meshulam, On the maximal rank in a subspace of matrices, *Q. J. Math.*, *Oxf. II*, 36 (1985), 225-229.

[7] W. Scharlau, *Quadratic and Hermitian Forms*, GmW, 270, Springer-Verlag, 1985.

[8] C. de Seguins Pazzis, The singular linear preservers of non-singular matrices, *Lin. Alg. Appl*, accepted, doi:10.1016/j.laa.2010.03.021