Pacific Journal of Mathematics

CONGRUENCE OF TWO-DIMENSIONAL SUBSPACES IN $M_2(K)$ (CHARACTERISTIC 2)

B. Corbas and G.D. Williams

Volume 188 No. 2 April 1999

PACIFIC JOURNAL OF MATHEMATICS
Vol. 188, No. 2, 1999

CONGRUENCE OF TWO-DIMENSIONAL SUBSPACES IN $M_2(K)$ (CHARACTERISTIC 2)

B. Corbas and G.D. Williams

Two-dimensional subspaces of $M_2(K)$ are here classified up to congruence, K being any field of characteristic 2. This complements the authors' earlier solution of the problem over fields of characteristic $\neq 2$. There is again a corresponding conclusion for the structure of a certain class of local rings.

1. Introduction.

This is a sequel to [2] and shares motivation, notation and preliminaries with that paper. To recall, the problem is to classify ordered pairs (A, B) of (2×2) matrices over a field K up to *equivalence*, where (A, B) is equivalent to (A', B') if there exist invertible matrices P and $Q = (q_{ij})$ such that

$$\begin{cases} P^tAP = q_{11}A' + q_{12}B' \\ P^tBP = q_{21}A' + q_{22}B' \end{cases}.$$

If $\langle A, B\rangle$ is the subspace of $M_2(K)$ spanned by A and B, we may equally speak of $\langle A, B\rangle$ and $\langle A', B'\rangle$ being *congruent* via P. Recall also that if X is the set of all the pairs (A, B), then GL_2 acts on the right on X by (A, B). $P = (P^tAP, P^tBP)$ and on the left by $Q\cdot(A, B) = (q_{11}A+q_{12}B, q_{21}A+q_{22}B)$, and that thereby $G = GL_2 \times GL_2$ acts on the left via $(P, Q) \cdot (A, B) = Q \cdot (A, B) \cdot P^{-1}$.

One motivation for this problem is that its solution enables us to classify up to isomorphism a certain naturally arising class of local rings, namely those of the form $R = K \oplus J$, where the Jacobson radical J is such that $J^3 = 0$ and both J/J^2 and J^2 have dimension two over K. Such rings have been considered by, among others, Chikunji [1], at least when K is finite.

In the companion paper to the present we have solved the classification problem over any field of characteristic $\neq 2$, and we turn our attention here to the case where char $K = 2$, which we assume henceforth. Our earlier strategy (that of splitting a pair into the sum of a symmetric and an antisymmetric pair) is thus not viable anymore and we have to follow a different approach. We remark that we deal here with an arbitrary field. If we confine ourselves to finite or, more generally, perfect fields then a number of subtleties in the ensuing discussion disappear, and the treatment is correspondingly shorter. In the final section we apply our results to the case $K = \mathbf{F}_q$ (q even).

We dispense first with the simple case in which A and B are *linearly dependent*, or in other words $\dim\langle A, B\rangle \leq 1$. Here we may take $A = 0$ and it is clear that $(0, B)$ is equivalent to $(0, B')$ if and only if there exist $P \in GL_2(K)$ and $\lambda \in K^*$ such that $P^tBP = \lambda B'$. We shall say that B and B' are *projectively congruent* in this case.

Here and throughout we will write $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\Delta = \det P$. If $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then $P^tAP = \begin{pmatrix} a^2\alpha + ac(\beta+\gamma) + c^2\delta & ab\alpha + ad\beta + bc\gamma + cd\delta \\ ab\alpha + ad\gamma + bc\beta + cd\delta & b^2\alpha + bd(\beta+\gamma) + d^2\delta \end{pmatrix}$. Let $D_{\text{off}}(A) = \beta - \gamma$ be the difference (or sum) of the off-diagonal entries in A. The following evident lemma will often be used in the sequel:

Lemma 1. $\det(P^tAP) = \Delta^2 \det(A)$ *and* $D_{\text{off}}(P^tAP) = \Delta D_{\text{off}}(A)$.

We now classify matrices up to projective congruence:

Proposition 1. *The distinct projective congruence classes are represented by:* $\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}$, $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & \\ & \xi \end{pmatrix}$ *and* $\begin{pmatrix} 1 & 1 \\ & \delta \end{pmatrix}$ *with* $\xi \in K^*/K^{*2}$ *and* $\delta \in K$.

[We use $\xi \in K^*/K^{*2}$ to mean that ξ runs over a complete set of representatives for the cosets of K^{*2} in K^*, and will use similar abbreviations throughout.]

Proof. If the bilinear form represented by A is alternating, then A is congruent to $\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}$ or $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. Otherwise, by congruence, we may assume that A is of the form $\begin{pmatrix} \alpha & \beta \\ & \delta \end{pmatrix}$ with $\alpha \neq 0$. Since we are only interested in projective congruence we may take $\alpha = 1$. But if $\beta \neq 0$, then A is now congruent to $\begin{pmatrix} 1 & 1 \\ & \delta/\beta^2 \end{pmatrix}$. So we may assume that $A = \begin{pmatrix} 1 & \beta \\ & \delta \end{pmatrix}$, with $\beta = 0$ or 1. These two cases are not equivalent, since one is symmetric and the other not.

Consider now $P^t \begin{pmatrix} 1 & \beta \\ & \delta \end{pmatrix} P = \lambda \begin{pmatrix} 1 & \beta \\ & \delta' \end{pmatrix}$. From Lemma 1, $\Delta^2\delta = \lambda^2\delta'$, so that δ and δ' are in the same multiplicative square-class, and moreover $\Delta\beta = \lambda\beta$. If $\beta = 1$, then $\Delta = \lambda$ and so $\delta = \delta'$. If $\beta = 0$ and conversely δ, δ' are in the same square-class, say $\delta' = d^2\delta$ ($d \neq 0$), then $\begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$ is congruent to $\begin{pmatrix} 1 & \\ & \delta' \end{pmatrix}$ via $P = \begin{pmatrix} 1 & \\ & d \end{pmatrix}$. □

We turn now to the main case of pairs (A, B) with A and B linearly independent. Although there is not the same necessity as in [2] to deal with the case of A and B symmetric first, we still find it convenient to do so here, since there are some differences in the detail of how we treat the symmetric and asymmetric cases.

2. The Symmetric Case.

In this section we classify linearly independent pairs (A, B) in which both matrices are symmetric. Observe first that such a pair is equivalent to one in which $A = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ or $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}$. For if $W = \langle A, B \rangle$ equals the space of diagonal matrices, then it contains the identity, and this is congruent over $\mathbf{F}_2$ to $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}$, via $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. If not, then since $\dim W = 2$ and the space of all symmetric matrices has dimension 3, W is spanned by a diagonal matrix D and a non-diagonal matrix $\begin{pmatrix} \alpha & \beta \\ \beta & \delta \end{pmatrix}$. Since $D \neq 0$ we may assume that one of α, δ is zero and indeed, by congruence, that $\alpha = 0$. Now we may take $\beta = 1$. But $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}$ is projectively congruent to $\begin{pmatrix} & 1 \\ 1 & \delta \end{pmatrix}$ (for any $\delta \neq 0$), via $P = \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$. So we may assume that $\delta = 0$ or 1, establishing our claim.

In order to classify symmetric pairs we need two groups. The first is the usual additive subgroup of K in characteristic 2, namely $\Gamma = \{x^2 + x : x \in K\}$. The other is the group $\mathcal{K}$ of all bijective functions $K \to K$, $x \mapsto \lambda x + \mu$ where μ belongs to the subfield F of squares in K and $\lambda \in F^*$. Thus $\mathcal{K}$ acts naturally on K. It is, of course, the semidirect product of F^* by F.

We now classify the symmetric pairs, or in other words the orbits of G on the subset S of X consisting of symmetric pairs.

Theorem 1. *The following table gives a complete set of representatives for the orbits of G on S:*

1. $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$ $(\delta \in \mathcal{K}\backslash K)$	2. $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$ $(\delta \in K/\Gamma)$
3. $\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 0 & \\ & 0 \end{pmatrix}$	4. $\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$
5. $\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$	6. $\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & \\ & \xi \end{pmatrix}$ $(\xi \in K^*/K^{*2})$

Proof. The dependent pairs 3) to 6) have been dealt with in Section 1. For the independent pairs there are two cases to consider, as explained above.

1) $A = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$: We may take $B = \begin{pmatrix} \alpha & \\ & \delta \end{pmatrix}$. At least one of α, δ is non-zero. Via P we may assume that $\alpha \neq 0$, and then that $\alpha = 1$. Consider now equivalence between $\Pi = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$ and $\Pi' = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} 1 & \\ & \delta' \end{pmatrix}$. Suppose δ and δ' are in the same $\mathcal{K}$-orbit, say $\delta' = x^2 + y^2\delta$ $(y \neq 0)$. With $P = \begin{pmatrix} 1 & x \\ & y \end{pmatrix}$ and $Q = \begin{pmatrix} y & \\ x & 1 \end{pmatrix}$ one immediately checks that $\Pi \cdot P = Q \cdot \Pi'$, whence the pairs are equivalent.

Conversely, if the pairs are equivalent via $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $Q = \begin{pmatrix} k & l \\ m & n \end{pmatrix}$ (which notation we will take as standard henceforth), then in particular $P^t \begin{pmatrix} 1 & \\ & \delta \end{pmatrix} P = \begin{pmatrix} n & m \\ m & n\delta' \end{pmatrix}$ and taking determinants shows that $\Delta^2\delta = m^2 + n^2\delta'$. Note that $n \neq 0$, for example by Prop. 1, and thus δ, δ' are in the same $\mathcal{K}$-orbit.

2) $A = \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}$: As before, we may take $B = \begin{pmatrix} \alpha & \\ & \delta \end{pmatrix}$ and further assume that $\alpha \neq 0$ and then that $\alpha = 1$. For $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}$ is equivalent to $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}$ and hence to $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$, which appears above. Consider equivalence between $\Pi = \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & \delta \end{pmatrix}$ and $\Pi' = \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix},$

$\begin{pmatrix}1 & \\ & \delta'\end{pmatrix}$. Suppose that $\delta' - \delta = x^2 + x \in \Gamma$. Taking $P = \begin{pmatrix}1 & x \\ & 1\end{pmatrix}$ and $Q = \begin{pmatrix}1 & \\ x & 1\end{pmatrix}$, we find that $\Pi \cdot P = Q \cdot \Pi'$.

If, conversely, Π and Π' are equivalent via a general P and Q, then

$$\begin{aligned}(1)\qquad & \begin{pmatrix}c^2 & \Delta + cd \\ \Delta + cd & d^2\end{pmatrix}, \begin{pmatrix}a^2 + c^2\delta & ab + cd\delta \\ ab + cd\delta & b^2 + d^2\delta\end{pmatrix} \\ &= \begin{pmatrix}l & k \\ k & k + l\delta'\end{pmatrix}, \begin{pmatrix}n & m \\ m & m + n\delta'\end{pmatrix},\end{aligned}$$

from which we deduce the equations $\begin{cases}\Delta + cd + d^2 = \delta' c^2 \\ ab + cd\delta + b^2 + d^2\delta = \delta'(a^2 + c^2\delta)\end{cases}$.

If $c = 0$, the first equation gives $a = d$, and then the second implies that

$$(2) \qquad \delta' - \delta = x^2 + x \in \Gamma, \qquad \text{with } x = b/a.$$

If $c \neq 0$, then

$$(3) \qquad \delta' = \frac{\Delta + cd + d^2}{c^2}.$$

By symmetry, replacing P by $P^{-1} = \frac{1}{\Delta}\begin{pmatrix}d & b \\ c & a\end{pmatrix}$, we also have

$$\delta = \frac{\Delta^{-1} + ac\Delta^{-2} + a^2\Delta^{-2}}{c^2\Delta^{-2}} = \frac{\Delta + ac + a^2}{c^2}.$$

Thus

$$(4) \qquad \delta' - \delta = y^2 + y, \quad \text{with } y = \frac{a + d}{c}.$$

Hence again $\delta' - \delta \in \Gamma$.

Finally, types 1) and 2) above do not overlap, since clearly the space $\left\langle \begin{pmatrix} & 1 \\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & \\ & \delta\end{pmatrix} \right\rangle$ contains no non-zero alternating matrix, whereas type 1) spaces do. □

3. The Asymmetric Case.

We now consider the orbits of G on the set $X - S$ of asymmetric pairs. If such a pair (A, B) is linearly independent, then the two-dimensional space $\langle A, B\rangle$ has non-trivial intersection with the three-dimensional space of symmetric matrices in $M_2(K)$. Hence we may assume that A is *symmetric* and B is *not*. Equivalence of such pairs clearly determines A up to projective congruence and so we may take A to be $\begin{pmatrix}1 & \\ & 0\end{pmatrix}$, $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ or $\begin{pmatrix}1 & \\ & \xi\end{pmatrix}$ $(\xi \in K^*/K^{*2})$. These cases do not overlap and we will treat them in turn. When it comes to the last type, however, it turns out that the analysis proceeds in a more streamlined way if we replace $\begin{pmatrix} 1 & \\ & \xi \end{pmatrix}$ by the matrix $\begin{pmatrix} \eta & 1 \\ 1 & 1 \end{pmatrix}$, with $\eta = 1+\xi$, to which it is congruent via $P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. If $\begin{pmatrix} 1 & \\ & \xi' \end{pmatrix}$ similarly corresponds to $\begin{pmatrix} \eta' & 1 \\ 1 & 1 \end{pmatrix}$, then by Prop. 1 $\begin{pmatrix} 1 & \\ & \xi \end{pmatrix}$ is projectively congruent to $\begin{pmatrix} 1 & \\ & \xi' \end{pmatrix} \Leftrightarrow$ there exists $\nu \neq 0$ such that $\xi' = \nu^2\xi$, or equivalently $\eta' = (1+\nu^2) + \nu^2\eta$. If $\mathcal{H}$ denotes the subgroup of the group $\mathcal{K}$ of Section 1 consisting of just those functions for which $\mu = 1 + \lambda$, we have proved:

Proposition 2. $\begin{pmatrix} 1 & \\ & \xi \end{pmatrix}$ *is congruent to* $\begin{pmatrix} \eta & 1 \\ 1 & 1 \end{pmatrix}$, *with* $\eta = 1+\xi$. *Moreover* $\begin{pmatrix} \eta & 1 \\ 1 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} \eta' & 1 \\ 1 & 1 \end{pmatrix}$ *are projectively congruent if and only if* η *and* η' *are in the same* $\mathcal{H}$*-orbit.*

In addition to the various groups already introduced we need one more class of additive subgroups of K. Namely, for any t, $\eta \in K$ let $x_\lambda = \frac{\lambda(t+1)+t+\eta}{\lambda^2+\eta}$ and let $\mathcal{R}(t,\eta) = \{x_\lambda : \lambda \in K,\ \lambda^2 \neq \eta\} \cup \{0\}$. If $\lambda \neq \mu$, one easily verifies that $x_\lambda + x_\mu = x_\nu$ with $\nu = \frac{\lambda\mu+\eta}{\lambda+\mu}$, and it follows that $\mathcal{R}(t,\eta)$ is an additive subgroup of K. We will assume that $\eta \neq 1$.

Remark. For $t = 1$ we have

$$\mathcal{R}(1,\eta) = \left\{ \frac{1+\eta}{\lambda^2+\eta} : \lambda^2 \neq \eta \right\} \cup \{0\} = \left\{ \frac{\xi}{\mu^2+\xi} : \mu^2 \neq \xi \right\} \cup \{0\},$$

where $\xi = 1+\eta$. For $t \neq 1$ we may describe $\mathcal{R}(t,\eta)$ in an alternative, more natural way as follows. Namely, it is the inverse image under the additive homomorphism $K \to K$, $a \mapsto a^2 + a$ of the subgroup $\theta\Gamma$ of K, where $\theta = \frac{1+t^2}{1+\eta}$. To see this, the reader is invited to verify firstly that if $y_\lambda = \frac{(\lambda+t)(1+\eta)}{(1+t)(\lambda^2+\eta)}$ then $x_\lambda^2 + x_\lambda = \theta(y_\lambda^2 + y_\lambda)$, and secondly that if $x^2 + x = \theta(y^2+y)$ (some x, y), then $x = x_\lambda$ where $\lambda = \frac{xt(1+\eta)+y(t+\eta)(1+t)}{x(1+\eta)+y(1+t^2)}$. We shall not need this in the sequel.

We are now in a position to classify the asymmetric pairs.

Theorem 2. *The following table gives a complete set of representatives for the orbits of* G *on* $X - S$*:*

7. $\begin{pmatrix}1 & \\ & 0\end{pmatrix}, \begin{pmatrix} & 0\\ 1 & \end{pmatrix}$	8. $\begin{pmatrix}1 & \\ & 0\end{pmatrix}, \begin{pmatrix} & 1\\ \gamma & \end{pmatrix}$ $(\gamma \neq 1)$
9. $\begin{pmatrix}1 & \\ & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ & 1\end{pmatrix}$	10. $\begin{pmatrix} & 1\\ 1 & \end{pmatrix}, \begin{pmatrix}1 & 1\\ & \delta\end{pmatrix}$ $(\delta \in K/\Gamma)$
11. $\begin{pmatrix}\eta & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}t+\eta\delta & 1\\ & \delta\end{pmatrix}$ $(\eta \in \mathcal{H}\backslash(K-\{1\}),\ t \in K,\ \delta \in K/\mathcal{R}(t,\eta))$	
12. $\begin{pmatrix}0 & \\ & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\ & \delta\end{pmatrix}$ $(\delta \in K)$	

Proof. The dependent pairs 12) have been discussed in Section 1, so we now consider independent pairs $\Pi = (A, B)$ in which A is symmetric and B is not. If $\Pi' = (A, B')$ is a second such pair (with the same A) and $\Pi \cdot P = Q \cdot \Pi'$, then, with the usual notation, $P^tAP = kA + lB'$ and $P^tBP = mA + nB'$. Since A is symmetric and B' is not, we have $l = 0$. Moreover, from Lemma 1 we have the following facts:

$$k = \Delta \quad \textit{if } A \textit{ is nonsingular} \quad \text{and} \tag{5}$$

$$\Delta D_{\text{off}}(B) = nD_{\text{off}}(B'). \tag{6}$$

We now analyze the three types for A alluded to at the start of the section.

7)-9) $A = \begin{pmatrix}1 & \\ & 0\end{pmatrix}$: We may take $B = \begin{pmatrix}0 & \beta\\ \gamma & \delta\end{pmatrix}$. There are two cases: (a) $\delta = 0$, (b) $\delta = 1$.

(a) If $B = \begin{pmatrix} & \beta\\ \gamma & \end{pmatrix}$, $B' = \begin{pmatrix} & \beta'\\ \gamma' & \end{pmatrix}$ and $\Pi \cdot P = Q \cdot \Pi'$, then $P^tAP = kA$ implies that $b = 0$. Then $P^tBP = mA + nB'$ gives $\begin{pmatrix}ac(\beta+\gamma) & ad\beta\\ ad\gamma & 0\end{pmatrix} = \begin{pmatrix}m & n\beta'\\ n\gamma' & 0\end{pmatrix}$ and in particular:

$$\begin{cases} ad\beta = n\beta' \\ ad\gamma = n\gamma' \end{cases}. \tag{7}$$

Since ad and n are non-zero, $\beta = 0 \Leftrightarrow \beta' = 0$. If $\beta = 0$, we may assume that $\gamma = 1$. If not, we may assume that $\beta = 1$. If now $\beta = \beta' = 1$, then (7) gives $\gamma = \gamma'$.

(b) Any pair $\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$, $\begin{pmatrix} & \beta \\ \gamma & 1 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ & 1 \end{pmatrix}$ via $P = \begin{pmatrix} 1 & 0 \\ \gamma & \beta+\gamma \end{pmatrix}$, $Q = \begin{pmatrix} 1 & 0 \\ \beta\gamma & \beta^2+\gamma^2 \end{pmatrix}$.

Finally, cases (a) and (b) do not overlap. For if the P-transform of this last pair equals the Q-transform of a type (a) pair, for a general P, Q, it follows easily that $b = d = 0$, contradicting nonsingularity of P. This deals with types 7)-9) in the table.

10) $A = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$: We may clearly take $B = \begin{pmatrix} \alpha & 1 \\ & \delta \end{pmatrix}$. Moreover, we may assume $\alpha = 1$. For if $\alpha \neq 0$, (A, B) is equivalent to $\left(A, \begin{pmatrix} 1 & 1 \\ & \alpha\delta \end{pmatrix}\right)$ via $P = \begin{pmatrix} 1 & \\ & \alpha \end{pmatrix}$, $Q = \begin{pmatrix} \alpha & \\ & \alpha \end{pmatrix}$; and if $\alpha = 0$, it is equivalent to $\left(A, \begin{pmatrix} 1 & 1 \\ & 0 \end{pmatrix}\right)$ via $P = \begin{pmatrix} 1+\delta & 1 \\ 1 & 0 \end{pmatrix}$, $Q = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Consider now equivalence between $\Pi = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ & \delta \end{pmatrix}$ and $\Pi' = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ & \delta' \end{pmatrix}$. If $\delta' - \delta = x^2 + x \in \Gamma$, then $\Pi \cdot P = Q \cdot \Pi'$, where $P = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $Q = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$. If, conversely, Π is equivalent to Π' by means of a general P, Q, then from (6) $\Delta = n$. But also $\det(P^tBP) = \det(mA + nB')$, giving $\Delta^2\delta = n^2\delta' + m^2 + mn$, and then

$$\delta' - \delta = x^2 + x, \quad \text{with } \ x = m/n. \tag{8}$$

We have accounted for type 10).

11) $A = \begin{pmatrix} \eta & 1 \\ 1 & 1 \end{pmatrix}$: Here $\eta \neq 1$ is fixed and we may again take $B = \begin{pmatrix} \alpha & 1 \\ & \delta \end{pmatrix}$. Suppose that for some P, Q we have $\Pi \cdot P = Q \cdot \Pi'$, where $\Pi = (A, B)$, $\Pi' = (A, B')$ and $B' = \begin{pmatrix} \alpha' & 1 \\ & \delta' \end{pmatrix}$. From (5) and (6) we have $k = n = \Delta$. Moreover $P^tAP = kA$, so that $P^tA = kAP^{-1}$, i.e. $\begin{pmatrix} \eta a + c & a + c \\ \eta b + d & b + d \end{pmatrix} = \begin{pmatrix} \eta d + c & \eta b + a \\ c + d & a + b \end{pmatrix}$. Thus $d = a$, $c = \eta b$ and $P = \begin{pmatrix} a & b \\ \eta b & a \end{pmatrix}$. Now $P^tBP = mA + nB'$ becomes:

$$\begin{pmatrix} a^2\alpha + \eta ab + \eta^2 b^2\delta & ab\alpha + a^2 + \eta ab\delta \\ ab\alpha + \eta b^2 + \eta ab\delta & b^2\alpha + ab + a^2\delta \end{pmatrix} = \begin{pmatrix} m\eta + n\alpha' & m + n \\ m & m + n\delta' \end{pmatrix}. \tag{9}$$

Adding the $(1,1)$-entry to η times the $(2,2)$-entry gives $\Delta(\alpha+\eta\delta) = n(\alpha'+\eta\delta')$ and, since $\Delta = n$, $\alpha+\eta\delta = \alpha'+\eta\delta'$. Thus $t = \alpha+\eta\delta$ is an *invariant.*

Adding the bottom entries in (9) and using $n = a^2+\eta b^2$ leads to $n(\delta'-\delta) = ab\alpha+\eta b^2+\eta ab\delta+b^2\alpha+ab+\eta b^2\delta = ab(t+1)+b^2(t+\eta)$. Either $b=0$, and then $\delta'=\delta$, or $b\neq 0$, in which case $\delta'-\delta = \frac{\lambda(t+1)+t+\eta}{\lambda^2+\eta}$, where $\lambda = a/b$. This is the typical element x_λ of the group $\mathcal{R}(t,\eta)$ defined earlier. Conversely, if $\alpha+\eta\delta = \alpha'+\eta\delta' = t$ and $\delta'-\delta = x_\lambda$ (some λ), then Π and Π' are equivalent via $P = \begin{pmatrix}\lambda & 1\\ \eta & \lambda\end{pmatrix}$, $Q = \begin{pmatrix}\Delta & 0\\ \lambda t+\eta & \Delta\end{pmatrix}$. This deals with type 11) and the theorem is proved. □

4. Finite Fields.

In this section we apply our results to the finite field $K = \mathbf{F}_q$ (q even) and determine the number of equivalence classes and the class sizes. We begin by determining the stabilizers of the various representatives 1)-12) of Theorems 1, 2. Since all elements of K are squares, it follows that $\mathcal{K}$ acts transitively on K and $\mathcal{H}$ acts transitively on $K-\{1\}$. Thus in 1) we need only consider $\delta = 0$, and in 11) we may take $\eta = 0$. In 6) we take $\xi = 1$. The homomorphism $K \to K$, $x \mapsto x^2+x$ has kernel $\{0,1\}$, so that Γ is of index two in K and in 2) and 10) we may take δ to be 0 or a fixed element $\varepsilon \notin \Gamma$. As for 11), we have $\mathcal{R}(0,0) = \mathcal{R}(1,0) = K$. If $t \neq 0,1$ then $\mathcal{R}(t,0) = \{tx^2+(t+1)x : x \in K\}$ has index two in K and we take δ to be 0 or a fixed element $\varepsilon_t \notin \mathcal{R}(t,0)$. Equivalently $tX^2+(t+1)X+\varepsilon_t$ is a fixed irreducible polynomial.

We now have:

Theorem 3. *The stabilizers of the various representatives are given as follows:*

Representative	Stabilizing elements (P,Q)
1. $\begin{pmatrix} & 1\\ 1 & \end{pmatrix}, \begin{pmatrix}1 & \\ & 0\end{pmatrix}$	$\begin{pmatrix}a & 0\\ c & d\end{pmatrix}, \begin{pmatrix}ad & \\ & a^2\end{pmatrix}$
2. $\begin{pmatrix} & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & \\ & \delta\end{pmatrix}$ $(\delta = 0,\varepsilon)$	$\begin{pmatrix}a & a+c\delta\\ c & a\end{pmatrix}, \begin{pmatrix}a^2+c^2\delta & c^2\\ a^2 & a^2+c^2\delta\end{pmatrix}$ and $\begin{pmatrix}a & c\delta\\ c & a+c\end{pmatrix}, \begin{pmatrix}a^2+c^2+c^2\delta & c^2\\ c^2\delta & a^2+c^2\delta\end{pmatrix}$
3. $\begin{pmatrix}0 & \\ & 0\end{pmatrix}, \begin{pmatrix}0 & \\ & 0\end{pmatrix}$	All

4. $\begin{pmatrix}0 & \\ & 0\end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$	$\begin{pmatrix}a & b \\ c & d\end{pmatrix}, \begin{pmatrix}k & 0 \\ m & \Delta\end{pmatrix}$
5. $\begin{pmatrix}0 & \\ & 0\end{pmatrix}, \begin{pmatrix}1 & \\ & 0\end{pmatrix}$	$\begin{pmatrix}a & 0 \\ c & d\end{pmatrix}, \begin{pmatrix}k & 0 \\ m & a^2\end{pmatrix}$
6. $\begin{pmatrix}0 & \\ & 0\end{pmatrix}, \begin{pmatrix}1 & \\ & 1\end{pmatrix}$	$\begin{pmatrix}a & c \\ c & a\end{pmatrix}, \begin{pmatrix}k & 0 \\ m & \Delta\end{pmatrix}$
7. $\begin{pmatrix}1 & \\ & 0\end{pmatrix}, \begin{pmatrix} & 0 \\ 1 & \end{pmatrix}$	$\begin{pmatrix}a & 0 \\ c & d\end{pmatrix}, \begin{pmatrix}a^2 & 0 \\ ac & ad\end{pmatrix}$
8. $\begin{pmatrix}1 & \\ & 0\end{pmatrix}, \begin{pmatrix} & 1 \\ \gamma & \end{pmatrix}$ $(\gamma \neq 1)$	$\begin{pmatrix}a & 0 \\ c & d\end{pmatrix}, \begin{pmatrix}a^2 & 0 \\ ac(1+\gamma) & ad\end{pmatrix}$
9. $\begin{pmatrix}1 & \\ & 0\end{pmatrix}, \begin{pmatrix}0 & 1 \\ & 1\end{pmatrix}$	$\begin{pmatrix}a & \\ & a\end{pmatrix}, \begin{pmatrix}a^2 & \\ & a^2\end{pmatrix}$
10. $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix}1 & 1 \\ & \delta\end{pmatrix}$ $(\delta = 0, \varepsilon)$	$\begin{pmatrix}a & a+c\delta \\ c & a\end{pmatrix}, \begin{pmatrix}\Delta & 0 \\ \Delta & \Delta\end{pmatrix}$ and $\begin{pmatrix}a & c\delta \\ c & a+c\end{pmatrix}, \begin{pmatrix}\Delta & 0 \\ 0 & \Delta\end{pmatrix}$
11a. $\begin{pmatrix} & 1 \\ 1 & 1\end{pmatrix}, \begin{pmatrix}t & 1 \\ & 0\end{pmatrix}$ $(t = 0, 1)$	$\begin{pmatrix}a & \\ & a\end{pmatrix}, \begin{pmatrix}a^2 & \\ & a^2\end{pmatrix}$
11b. $\begin{pmatrix} & 1 \\ 1 & 1\end{pmatrix}, \begin{pmatrix}t & 1 \\ & \delta\end{pmatrix}$ $(t \neq 0, 1;\ \delta = 0, \varepsilon_t)$	$\begin{pmatrix}a & a(1+t^{-1}) \\ 0 & a\end{pmatrix}, \begin{pmatrix}a^2 & 0 \\ a^2(t+1) & a^2\end{pmatrix}$ and the above
12. $\begin{pmatrix}0 & \\ & 0\end{pmatrix}, \begin{pmatrix}1 & 1 \\ & \delta\end{pmatrix}$ $(\delta \in K)$	$\begin{pmatrix}a & c\delta \\ c & a+c\end{pmatrix}, \begin{pmatrix}k & 0 \\ m & \Delta\end{pmatrix}$

Proof. Most of this is very easily extracted from the proofs of Theorems 1, 2. Only lines 2, 6, 10 and 12 require explanation, and we deal with these in turn.

2) If $\Pi \cdot P = Q \cdot \Pi$, then Equation (1) in the proof of Theorem 1 holds, with $\delta = \delta'$. There are two cases:

i) $c = 0$: Then $a = d$ and from (2) $x = 0$ or 1, i.e. $b = 0$ or a.

ii) $c \neq 0$: From (4) $y = 0$ or 1, i.e. $d = a$ or $a + c$. If $d = a$, then (3) gives $\delta = \frac{a+b}{c}$, so that $b = a + c\delta$. If $d = a + c$, (3) gives $\delta = \frac{b}{c}$ and so $b = c\delta$.

Thus in either case $P = \begin{pmatrix} a & a + c\delta \\ c & a \end{pmatrix}$ or $\begin{pmatrix} a & c\delta \\ c & a + c \end{pmatrix}$, and the form of Q results at once from (1).

6) The equation $P^t BP = nB$ here gives $P^t = nP^{-1}$. By determinants we have $n = \Delta$, and so $\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$, whence $d = a$, $b = c$.

10) From (8) in the proof of Theorem 2 we have $x = 0$ or 1, and thus $P^t B = (mA + nB)P^{-1}$, with $m = 0$ or n. Recall that $n = \Delta$. We deal with the cases:

i) $m = 0$: The matrix equation becomes $\begin{pmatrix} a & a + c\delta \\ b & b + d\delta \end{pmatrix} = \begin{pmatrix} d + c & b + a \\ c\delta & a\delta \end{pmatrix}$, and so $b = c\delta$, $d = a + c$.

ii) $m = n$: This time $\begin{pmatrix} a & a + c\delta \\ b & b + d\delta \end{pmatrix} = \begin{pmatrix} d & b \\ d + c\delta & b + a\delta \end{pmatrix}$, and thus $b = a + c\delta$, $d = a$.

12) The reasoning is similar to the previous two cases and we omit it. □

We may now determine the number of equivalence classes over $\mathbf{F}_q$ and their sizes. Note that $|G| = q^2(q-1)^2(q^2-1)^2$, $|X| = q^8$ and $|S| = q^6$. It is convenient to introduce the additive character $\psi : \mathbf{F}_q \to \{\pm 1\}$ given by $\psi(x) = 1$ $(x \in \Gamma)$, -1 $(x \notin \Gamma)$.

Theorem 4. *The following table gives, for each type of representative, the sizes of the stabilizer and equivalence class and the number of classes:*

Rep.	|Stabilizer|	|Class|	Number of classes
1	$q(q-1)^2$	$q(q^2-1)^2$	1
2	$2(q-1)(q-\psi(\delta))$	$\frac{1}{2}q^2(q-1)(q^2-1)(q+\psi(\delta))$	2
3	$\|G\|$	1	1
4	$q^2(q-1)^2(q^2-1)$	q^2-1	1
5	$q^2(q-1)^3$	$(q+1)(q^2-1)$	1
6	$q^2(q-1)^2$	$(q^2-1)^2$	1
7	$q(q-1)^2$	$q(q^2-1)^2$	1
8	$q(q-1)^2$	$q(q^2-1)^2$	$q-1$
9	$q-1$	$q^2(q-1)(q^2-1)^2$	1
10	$2(q-1)(q-\psi(\delta))$	$\frac{1}{2}q^2(q-1)(q^2-1)(q+\psi(\delta))$	2
11a	$q-1$	$q^2(q-1)(q^2-1)^2$	2
11b	$2(q-1)$	$\frac{1}{2}q^2(q-1)(q^2-1)^2$	$2q-4$
12	$q(q-1)^2(q-\psi(\delta))$	$q(q^2-1)(q+\psi(\delta))$	q

In all there are $4q+8$ classes, of which 7 are symmetric. For the linearly independent pairs, the number of classes is $3q+4$, and 3 of these are symmetric.

Proof. We count the number of solutions (a, c) of the equation $a^2+ac+c^2\delta = 0$, for a given δ. If $c = 0$, then $a = 0$. If $c \neq 0$, then $\delta = \left(\frac{a}{c}\right)^2 + \frac{a}{c}$ and there are two solutions for a if $\delta \in \Gamma$, and none otherwise. So the total number of solutions is $1 + 2(q-1) = 2q-1$ $(\delta \in \Gamma)$, 1 $(\delta \notin \Gamma)$.

It follows that the number of solutions of $a^2+ac+c^2\delta \neq 0$ is $q^2-2q+1 = (q-1)^2$ $(\delta \in \Gamma)$, q^2-1 $(\delta \notin \Gamma)$. In either case this equals $(q-1)(q-\psi(\delta))$. This explains lines 2, 10 and 12, and the rest is clear. □

Note that a simple check shows that the sum of all the class sizes is $q^8 = |X|$, as should be, and that the sum of the symmetric class sizes is $q^6 = |S|$.

Corollary. *For the finite local rings of the Introduction, there are $3q+4$ isomorphism classes (q even). Of these, 3 are commutative.*

This agrees with the result for $q = 2$ in [**1**], found by computer search.

References

[1] C.J. Chikunji, *On the Classification of Finite Rings*, Ph.D. Thesis, University of Reading, 1996.

[2] B. Corbas and G.D. Williams, *Congruence of Two-Dimensional Subspaces in $M_2(K)$ (characteristic $\neq 2$)*, Pacific J. of Math., **188**(**2**) (1999), 225-235.

Received August 11, 1997.

University of Reading
Reading RG6 6AX
England

University of Reading
Reading RG6 6AX
England
E-mail address: G.D.Williams@reading.ac.uk