CUBIC SURFACES IN AG(3, q) AND PROJECTIVE PLANES OF ORDER $q^3$

ABSTRACT. Spread sets of projective planes of order $q^3$ are represented as sets of $q^3$ points in $\mathcal{A} \cong \text{AG}(3, q^3)$. A line through the origin in $\mathcal{A}$ can be interpreted as a space $\mathcal{A}_0 \cong \text{AG}(3, q)$, and the spread set induces a cubic surface $\mathcal{S}$ in $\mathcal{A}_0$. If the projective plane is a semifield plane of dimension 3 over its kernel, then $\mathcal{S}$ has the property that it misses a plane of $\mathcal{A}_0$. Determining all such surfaces $\mathcal{S}$ leads to a complete classification of the semifield planes of order $q^3$, whose spread sets are division algebras of dimension 3.

An alternative proof of a result due to Menichetti, that finite division algebras of dimension 3 are associative or are twisted fields, follows with the classification.

1. INTRODUCTION

In a recent paper [10] we studied $\text{GF}(q^3)$ ($q = p^r$, $p$ prime) by interpreting its elements as points of the affine 3-space $\mathcal{A}_0 \cong \text{AG}(3, q)$. The purpose of the present paper is to extend and apply these results.

We examined in [10] a class $\mathcal{S}$ of surfaces in $\mathcal{A}_0$ which is invariant under a group of mappings analogous to linear fractional transformations. $\mathcal{S}$ contains cubic surfaces, quadric surfaces, and planes. In the course of investigating the nature of these surfaces, a question on cubic surfaces with exterior planes was left open. That question is answered here in Section 3 (Theorem 3.2). An application of Theorem 3.2 to spread sets of finite projective planes is exploited in Section 5 and becomes the key to our subsequent classification (in Section 6) of semifield planes of order $q^3$, whose spread sets are division algebras of dimension 3.

In Section 2 we follow an earlier study [9] and consider $\mathcal{A} \cong \text{AG}(3, q^3)$, where the points of $\mathcal{A}$ are identified with $3 \times 3$ matrices over $\text{GF}(q)$. In particular we isolate a line $OI$ in $\mathcal{A}$, and identify it with $\mathcal{A}_0 \cong \text{AG}(3, q)$, thus making a connection with the geometry on $\mathcal{A}_0$ developed in [10]. Using the notion of compatibility of points in $\mathcal{A}$ (which is the geometrical equivalent of the necessary condition for matrices to lie in the same spread set), we find the points of line $OI$ that are incompatible with a point $P$ of $\mathcal{A}$. Such a set of points is seen to be a cubic surface of the type studied in [10]; this observation allows fruitful application of some of the results in [10], and of the new result (Theorem 3.2) proved in Section 3.

We are thus led to a study of indicator sets (spread sets) in the context of the results of [10]. In Sections 4 and 5 we concentrate on indicator sets which contain a set $\{\lambda P + \mu Q\}$ of $q^2$ points. The only known indicator sets of this
type are those which define semifield planes. Accordingly, semifield planes are studied in Section 6, resulting in a list of all semifield planes of order $q^3$ whose spread sets are division algebras of dimension 3 (Theorem 6.5).

Also in Section 6 we note that the foregoing results provide a new proof of the result of Menichetti [7] that any finite division algebra of dimension 3 over a field is associative, or is a twisted field (Theorem 6.6).

We introduce here some definitions, notations and conventions which will be used in subsequent sections. Let $K$ denote a field isomorphic to $GF(q^3)$, and let $F$ be the subfield of $K$ isomorphic to $GF(q)$. We denote elements of $K$ and $F$ by capital Latin and small Greek letters respectively. The unit element will be denoted either by $I$ or by $1$.

The cardinality of a finite set $S$ will be denoted by $|S|$; occasionally the same symbol, $|\cdot|$, will be used to denote a determinant over $K$. A group generated by $A, B, C, \ldots$ will be denoted by $<A, B, C, \ldots>$, while the remainder of a set $S$ when a subset $T$ has been removed is given as $S \setminus T$ or $S \backslash T$.

Any mapping $X \to X^p^n$ ($X \in K, 0 \leq n < q^3$) is an automorphism of $K$, and any automorphism of $K$ is so expressed. Two well-known mappings from $K$ to $F$ will be used:

(i) The norm of $X$: $N(X) = X^{1+q+q^2}$. It is immediate that $N(0) = 0$, and that if $N(X) = \lambda \neq 0$, then there are exactly $q^2 + q + 1$ elements of $K$ with norm $\lambda$.

(ii) The trace of $X$: $tr(X) = X + X^q + X^{q^2}$. There are exactly $q^2$ elements of $K$ with trace $\alpha \in F$. In [10], any plane of $\mathcal{A}_0 \cong AG(3, q)$ was seen to have equation $tr(AX) + \alpha = 0$ ($A \in K, A \neq 0, \alpha \in F$).

The author is grateful to the referee for a number of helpful comments, which have greatly improved the manuscript.

2. $AG(3, q^3)$ and its subspaces

The space $\mathcal{A} = AG(3, q^3)$ [4, pp. 27, 28] is simply the three-dimensional vector space over the field $K \cong GF(q^3)$. Points of $\mathcal{A}$ are vectors, while lines and planes are respectively one- and two-dimensional subspaces, with their translates, and incidence is inclusion. As explained in [9, pp. 212, 213], the points of $\mathcal{A}$ can be identified with the $3 \times 3$ matrices over the subfield $F \cong GF(q)$. Thus $\mathcal{A}$ contains points $O$ and $I$, corresponding to the zero and identity matrices respectively. In terms of coordinates, $O$ is $(0, 0, 0)$ and $I$ is $(1, t, t^2)$, where $\{1, t, t^2\}$ is a basis for $K$ as a vector space over $F$. Any point $M$ has coordinates $(1 t t^2)M$ (thinking of $M$ as a matrix over $F$). In particular, we have points $(1 t^q t^{2q}) = (1 t^2)T$ and $(1 t^{q^2} t^{2q^2}) = (1 t^2)T^2$ which define a