Automorphisms of Unitary Block Designs*

MICHAEL E. O'NAN

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903

Received February 25, 1971

TO PROFESSOR RICHARD BRAUER, TO COMMEMORATE HIS SEVENTIETH BIRTHDAY, FEBRUARY 10, 1971

INTRODUCTION

In this paper, we discuss the geometry and determine the automorphism group of the unital or unitary block design associated with the three-dimensional unitary group.

If $V$ is a three-dimensional vector space over the field with $q^3$ elements and $b$ is a nondegenerate Hermitian bilinear form on $V$, we let $X$ denote the family of isotropic one-dimensional subspaces of $V$ with respect to $b$. Then $X$ has $1 + q^3$ points, and the three-dimensional projective unitary groups, PSU$(3, q)$ and PGU$(3, q)$, act on $X$ as doubly-transitive permutation groups. There is a naturally arising family of subsets of $X$, $\mathcal{A}$, forming a unitary block design on $X$. Each member of $\mathcal{A}$ is the set of isotropic one-dimensional subspaces contained in a fixed nonisotropic two-dimensional subspace of $V$. Our principal result is:

**Theorem.** $\text{aut}(\mathcal{A}) = \text{PGU}(3, q)$.

In another paper this result is used to implement a characterization of PSU$(3, q)$ as a doubly-transitive permutation group. It is primarily with this characterization in mind that the material herein is developed.

The paper is divided into five sections. In the first section we discuss various properties of the three-dimensional unitary groups for the purpose of establishing notations and certain preliminary lemmas. In the second are discussed properties of the unitary block design $\mathcal{A}$. In the succeeding section we develop a relationship between $\mathcal{A}$ and a natural geometry of circles in an affine plane and study this circle geometry. In the fourth section we determine the automorphism group of the circle geometry and in the last the automorphism group of $\mathcal{A}$.

* The material herein was presented to Princeton University in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

495

© 1972 by Academic Press, Inc.
1. Properties of $U_3(q)$

Let $F$ be a field with $q$ elements, where $q = p^n > 2$ and $p$ is some prime. Let $E$ be a quadratic extension of $F$. Then $E$ has $q^2$ elements and an automorphism $x \mapsto x^q$, which we write as $x^q = \bar{x}$. $F$ is the subfield of fixed elements of this automorphism. Let $V$ be a three-dimensional vector space over $E$ and $b$ a nondegenerate Hermitian bilinear form on $V$.

As usual $GU(3, q)$ is the group of linear transformations on $V$ leaving $b$ invariant. By Dickson [2, p. 134], the order of $GU(3, q)$ is $(1 + q^3)q^3(q^2 - 1)(q + 1)$. The center of $GU(3, q)$ is of order $1 + q$. The center consists of the transformations $\alpha \cdot I$, where $I$ is the identity and $\alpha \in E$ and $\alpha \bar{x} = x$. $SU(3, q)$ is the subgroup of $GU(3, q)$ consisting of linear transformations with determinant unity. Its order is $(1 + q^3)q^3(q^2 - 1)$. Its center is of order $(1 + q, 3)$. The central factor group of $SU(3, q)$ is denoted by $PSU(3, q)$, or simply $U_3(q)$. $U_3(q)$ is then a simple group of order $(1 + q^3)q^3(q^2 - 1)/(q + 1, 3)$ [2, pp. 131-144].

If $W$ is a subspace of $V$, $W^*$, as usual, denotes the orthogonal complement of $W$ with respect to the bilinear form $b$. Since $b$ is nondegenerate, $\dim W + \dim W^* = 3$. If $W \cap W^* \neq 0$, $W$ is said to be isotropic. Otherwise $W$ is said to be nonisotropic. A vector $x$ is isotropic if $b(x, x) = 0$, nonisotropic if $b(x, x) \neq 0$. In other words, $x$ is isotropic or nonisotropic according as the subspace it spans is isotropic or nonisotropic. We note the following:

**Lemma 1.1.** Let $\alpha \in F$, $\alpha \neq 0$. Then there exists a $\beta \in E$ such that $\beta \bar{\alpha} = \alpha$. There are in fact exactly $1 + q$ such $\beta$.

**Lemma 1.2.** There are $1 + q^3$ isotropic one-dimensional subspaces in $V$, $q^4 - q^3 + q^2$ nonisotropic one-dimensional subspaces. See Dickson [2, p. 134].

**Lemma 1.3.** Let $x$ and $y$ be linearly independent isotropic vectors of $V$. Then $b(x, y) \neq 0$, and the subspace spanned by $x$ and $y$ is nonisotropic.

**Proof.** Let $W$ be the subspace of $V$ spanned by $x$ and $y$. If $b(x, y) = 0$, then $W \subseteq W^*$. Then, $\dim W + \dim W^* \geq 4$, a contradiction.

If $\alpha x + \beta y \in W \cap W^*$, from $b(x, \alpha x + \beta y) = b(y, \alpha x + \beta y) = 0$, it follows quickly that $\alpha = \beta = 0$. Thus, $W$ is nonisotropic.

**Lemma 1.4.** Let $x$ and $y$ be linearly independent isotropic vectors of $V$. Replacing $y$ by $\alpha y$, if necessary, we may obtain a basis $x, y, z$ for $V$ such that $b(x, x) = b(y, y) = 0$; $b(x, z) = 1$; $b(x, y) = 1$; $b(x, z) = b(y, z) = 0$.

This follows from Lemmas 1.1 and 1.3.
Since GU(3, q) preserves b, it induces a permutation group on the isotropic one-dimensional subspaces. Since the center of GU(3, q) fixes all subspaces, the induced representation of GU(3, q) on X affords permutation representations of PGU(3, q) and U₃(q) on X. It is a consequence of Lemma 1.4 that these representations are doubly-transitive.

We fix a basis of the sort whose existence is guaranteed by Lemma 1.4. We call the vectors of this basis x, y, z, where x, y, z enjoy the properties of x, y, z in Lemma 1.4. Henceforth, ∞ ∈ X denotes the subspace spanned by x and 0 ∈ X, the subspace spanned by y. H is defined to be the subgroup of U₃(q) which fixes ∞. Next we determine H.

All matrices are exhibited with respect to the ordered basis x, z, y.

We consider the matrices:

\[
\begin{vmatrix}
1 & \alpha & \beta \\
0 & 1 & -\bar{\alpha} \\
0 & 0 & 1
\end{vmatrix}, \quad \text{with } \alpha, \beta \in E \text{ and } \beta + \bar{\beta} + \alpha \bar{\alpha} = 0,
\]

\[
\begin{vmatrix}
\lambda & 0 & 0 \\
0 & \lambda/\lambda & 0 \\
0 & 0 & 1/\lambda
\end{vmatrix}, \quad \text{with } \lambda \in E \text{ and } \lambda \neq 0.
\]

One checks by direct verification:

**Lemma 1.5.** (\(x, \beta\)) and \(k_\lambda\) preserve b.

Since det((\(x, \beta\))) = 1 and det(\(k_\lambda\)) = 1, it follows from Lemma 1.5 that (\(x, \beta\)) ∈ SU(3, q) and \(k_\lambda\) ∈ SU(3, q). We take Q to be the homomorphic image in U₃(q) of the family of matrices (\(x, \beta\)), K the homomorphic image in U₃(q) of the family of matrices \(k_\lambda\). Again direct calculation shows:

**Lemma 1.6.** (i) Q is a group.

(ii) \((x_1, \beta_1) \cdot (x_2, \beta_2) = (x_1 + \alpha x_2, \beta_1 + \beta_2 - \alpha \bar{x}_2)\).

(iii) \(|Q| = q^3\).

Note that a matrix \(k_\lambda\) is central in SU(3, q) if and only if \(\lambda = \bar{\lambda}/\lambda = 1/\bar{\lambda}\). Equivalently, \(\lambda \bar{\lambda} = 1\) and \(\lambda^q = 1\). Thus, the intersection of the set of matrices \(k_\lambda\) with the center of SU(3, q) has \((1 + q, 3)\) elements. Then it follows readily:

**Lemma 1.7.** (i) \(k_{\lambda_1} \cdot k_{\lambda_2} = k_{\lambda_1 \lambda_2}\).

(ii) K is cyclic.

(iii) \(|K| = (q^2 - 1)/(q + 1, 3)\).

It also follows by direct calculation:
LEMMA 1.8. (i) \( K \) normalizes \( Q \).

(ii) \( k_\lambda \cdot (\alpha, \beta) \cdot k_\lambda^{-1} = ((\lambda^3/\bar{\lambda})\alpha, \lambda\bar{\lambda}\beta) \).

LEMMA 1.9. \( Q \) is regular and transitive on \( X - \infty \).

Proof. Let \( \lambda x + \eta y + \zeta z \) span some subspace of \( X - \infty \). Since \( \lambda x + \eta y + \zeta z \) is isotropic, \( \lambda \bar{\eta} + \bar{\lambda} \eta + \bar{\zeta} \zeta = 0 \). If \( \eta = 0 \), then also \( \zeta = 0 \), and \( \lambda x + \eta y + \zeta z = \lambda x \) spans \( \infty \). Thus, \( \eta \neq 0 \). We may then assume \( \eta = 1 \) and \( \lambda x + y + \zeta z \) spans the same subspace. Since \( \lambda x + y + \zeta z \) is isotropic, \( \lambda + \bar{\lambda} + \bar{\zeta} \zeta = 0 \).

Thus, \( (-\frac{\bar{\eta}}{\eta}, \lambda) \in Q \) and \( (-\frac{\bar{\zeta}}{\zeta}, \lambda) y = \lambda x + y + \zeta z \). Therefore, \( Q \) is transitive on \( X - \infty \), and since \( |Q| = |X - \infty| = q^2 \), \( Q \) is regular on \( X - \infty \).

LEMMA 1.10. \( H = KQ \).

Proof. Clearly, \( K \cdot Q \subseteq H \). By Lemmas 1.6 and 1.7,

\[ |KQ| = q^2(q^2 - 1)/(q + 1, 3). \]

Since \( U_3(q) \) is transitive on \( X \),

\[ |X| = 1 + q^3, \quad |U_3(q)| = (1 + q^3)q^2(q^2 - 1)/(q + 1, 3), \]

it follows that \( |H| = |KQ| \).

We define \( P \) to be the subgroup of \( Q \) consisting of elements of first co-ordinate 0, i.e., \( P = \{(0, \beta) : \beta \in E \text{ and } \beta + \bar{\beta} = 0\} \). Regarding \( E \) as an additive group, there is a homomorphism \( \sigma : Q \to E \) defined by \( \sigma((\alpha, \beta)) = \alpha \). Clearly, \( P = \ker \sigma, |P| = q \). The following are easily verified.

LEMMA 1.11. (i) \( P \) is invariant under \( K \).

(ii) \( k_\lambda \) induces on \( P \) the automorphism \( (0, \beta) \mapsto (0, \lambda\bar{\lambda}\beta) \).

(iii) \( k_\lambda \) induces on \( Q/P = E \), the automorphism \( z \mapsto (\lambda^3/\bar{\lambda})z, z \in E \).

LEMMA 1.12. (i) \( K \) is transitive on \( P = 1 \).

(ii) \( K \) is irreducible on \( Q/P \).

LEMMA 1.13. (i) \( P \) is a maximal characteristic subgroup of \( Q \).

(ii) \( P = Z_1(Q) = [Q, Q] \).

Since \( Q \) is regular and transitive on \( X - \infty \), we identify \( Q \) and \( X - \infty \). Under the identification we assume \( 1 = (0, 0) \in Q \) corresponds to \( 0 \in X \).

\( K \) fixes the points 0 and \( \infty \). From Lemma 1.10 it follows that \( K \) is precisely
the subgroup of $U_3(q)$ fixing 0 and $\infty$. By the identification of the previous paragraph the action of $K$ on $X - \infty$ corresponds to its action on $Q$ as a group of automorphisms. Since $K$ is cyclic of order $(q^3 - 1)/(q + 1, 3)$, it has a unique subgroup, which we call $W$, of order $(q + 1)/(q + 1, 3)$. Note that $W$ is the homomorphic image of $\langle k_\lambda \mid \lambda \in E \text{ and } \lambda \bar{\lambda} = 1 \rangle$. Next we determine the action of $K$ on $X$.

**Lemma 1.14.** (i) If $f \in K$ and $f$ fixes three or more points then $f \in W$.

(ii) If $f \in W$, $f \neq 1$, the fixed point set of $f$ is $\infty \cup P$.

**Proof.** Suppose $k_\lambda \in SU(3, q)$ induces $f \in U_3(q)$. Since $f$ fixes more than three points, $f$ fixes some $(\alpha, \beta) \neq (0, 0)$. Since $\alpha \bar{x} + \beta + \bar{\beta} = 0$ and $(\alpha, \beta) \neq (0, 0), \beta \neq 0$. Now $(\alpha, \beta) \rightarrow ((\lambda^2/\bar{\lambda}) \alpha, \lambda \bar{\lambda} \beta)$. Thus, $\lambda \bar{\lambda} = 1$ and $f \in W$.

Next we determine the fixed point set of $f$, assuming $f \neq 1$. Since $\lambda \bar{\lambda} = 1$ and $P = \{(0, \beta) : \beta + \bar{\beta} = 0 \text{ and } \beta \in E\}$, $f$ fixes all points of $\infty \cup P$. If $f$ fixes $(\alpha, \beta)$ with $\alpha \neq 0$, then $\lambda^2 = \bar{\lambda}$ and $\lambda \bar{\lambda} = 1$. Therefore, $k_\lambda$ is central and $f = 1$.

(ii) follows from this.

In summary then, the action of $K$ on $X$ may be described as follows: $K$ fixes 0 and $\infty$, $K$ has one orbit, $P - 1$, of length $q - 1$, $K$ is regular and faithful on all remaining orbits of length $|K|$.

We note also that $U_3(q)$, represented on $X$, has the properties:

1. $U_3(q)$ is doubly-transitive on $X$, $|X| = 1 + q^3$, with $q$ a prime power.

2. The subgroup $H$ which fixes a point $\infty$ of $X$ has a normal subgroup $Q$, regular on $X - \infty$.

3. The subgroup $K$ fixing two points 0, $\infty$ in $X$ is cyclic of order $(q^3 - 1)/(q + 1, 3)$.

In another paper we shall show that, if $q$ is odd, any group having these three properties is isomorphic to $U_3(q)$. If $q$ is even, the same conclusion is implied by results of Suzuki [3]. Likewise, if $q + 1 \equiv 0 \pmod{3}$, the same conclusion has been obtained by Suzuki [4].

**2. The Unitary Block Design of $U_3(q)$**

Let $Y$ be a set with $1 + q^3$ elements. Let $\mathscr{B}$ be a family of subsets of $Y$ with the properties:

(i) If $A \in \mathscr{B} \mid A \mid = 1 + q$.

(ii) Every two element subset of $Y$ is contained in precisely one member of $\mathscr{B}$. 
We then say that $\mathcal{B}$ is a unital or unitary block design on $Y$ and call the elements of $\mathcal{B}$ blocks. If $\mathcal{B}$ is a unital on $Y$ and $a \in Y$, by $\mathcal{B}_a$ we mean the family of blocks of $\mathcal{B}$ which contain $a$. $\mathcal{B}_a'$ denotes the family of blocks of $\mathcal{B}$ which do not contain $a$.

Isomorphisms and automorphisms of block designs are defined in the usual way as one-one maps carrying blocks to blocks. We denote the full automorphism group of $\mathcal{B}$ as $\text{aut}(\mathcal{B})$.

The following are standard and follow quickly from the definitions.

**Lemma 2.1.** Let $\mathcal{B}$ be a unitary block design on $Y$. Then $\mathcal{B}$ has $q^4 - q^3 + q^2$ blocks.

**Lemma 2.2.** Let $\mathcal{B}$ be a unitary block design on $Y$. Then each point of $Y$ is contained in exactly $q^2$ blocks of $\mathcal{B}$, i.e., if $a \in Y$, $|\mathcal{B}_a| = q^2$. Also, $|\mathcal{B}_a'| = q^4 - q^3$.

As in section one, $X$ is the family of isotropic one-dimensional subspaces of the vector space $V$. We now consider a unitary block design on $X$. We define the unitary block design $\mathcal{A}$ on $X$ as follows: $B \in \mathcal{A}$ if and only if $B$ is the family of isotropic one-dimensional subspaces of some two-dimensional nonisotropic subspace $W$ of $V$. Conditions (i) and (ii) in the definition of a unitary block design follow from:

**Lemma 2.3.** Each two-dimensional nonisotropic subspace of $V$ has $1 + q$ isotropic one-dimensional subspaces. See Dickson, [2, p. 134].

**Lemma 2.4.** Two distinct isotropic one-dimensional subspaces of $V$ lie in a unique nonisotropic two-dimensional subspace of $V$.

**Proof.** Since two distinct isotropic one-dimensional subspaces of $V$ lie in a unique two-dimensional subspace $W$ of $V$, it suffices to show that $W$ is nonisotropic. This, however, is immediate from Lemma 1.3.

Now the group $\text{GU}(3, q)$ is linear and preserves the bilinear form $b$. It follows that elements of $\text{GU}(3, q)$ carry blocks to blocks and so $\text{PGU}(3, q) \subseteq \text{aut}(\mathcal{A})$. Since $U_3(q)$ is doubly-transitive on $X$ and since every two element subset of $X$ belongs to a unique block, it follows that $U_3(q)$ is transitive on the blocks of $\mathcal{A}$.

In the following all blocks are understood to belong to $\mathcal{A}$. Recall also that $H$ is the subgroup of $U_3(q)$ fixing $\infty$. We show next how the blocks containing $\infty$ are determined by the elements of $H$.

**Lemma 2.5.** The following are equivalent:
(i) $B$ is a block containing $\infty$.

(ii) $B = \infty \cup hP$, $h \in Q$.

(iii) $B$ is the union of $\infty$ and an orbit of $P$.

**Proof.** One block containing $\infty$ consists of the isotropic one-dimensional subspaces lying in the subspace spanned by $x$ and $y$. Since $b(x, x) = 0$, $b(y, y) = 0$, and $b(x, y) = 1$, the $1 + q$ isotropic one-dimensional subspaces of the subspace spanned by $x$ and $y$ are represented by the vectors $x$, $y + \beta x$, with $\beta + \overline{\beta} = 0$.

Now $(0, \beta) \in P$ if $\beta + \overline{\beta} = 0$, by definition of $P$. Also, $(0, \beta)y = y + \beta x$. Thus $\infty \cup P$ is a block. Since $Q$ fixes $\infty$ and is transitive on $X - \infty$, $Q$ is transitive on the blocks of $A_\infty$. It follows that the blocks containing $\infty$ are of the form $\infty \cup hP$, $h \in Q$, and so (i) and (ii) are equivalent.

Since $P$ is central in $Q$, if $h \in Q$, $hP = Ph$. Thus, the union of $\infty$ and an orbit of $P$ is a block, and conversely all blocks are of this form. Lemma 2.5 follows.

**Lemma 2.6.** If $M \subseteq H$, $M \neq 1$, and $M$ fixes three or more points, the fixed point set of $M$ is a block containing $\infty$. Moreover, $M$ is conjugate in $H$ to some subgroup of $W$.

**Proof.** Since $H$ is transitive on $X - \infty$ and $M$ fixes $\infty$, conjugating by elements of $H$, we may assume $M$ fixes 0 and $\infty$. By Lemma 1.14, $M \subseteq W$. Moreover, the fixed point set of $M$ is $\infty \cup P$, a block by Lemma 2.5 (i). The result follows.

Next we study the action of $H$ on $A$.

**Lemma 2.7.** $H$ has two orbits on $A$. One consists of the blocks of $A_\infty$, the other of the blocks of $A_\infty'$. The former is of length $q^2$, the latter of length $q^4 - q^2$.

**Proof.** It follows from Lemma 2.5 that the blocks of $A_\infty$ are an orbit of $H$ of length $q^2$.

Let $B \in A_\infty'$ and suppose $T \subseteq H$ is the subgroup fixing $B$. We claim: if $t \in T - 1$, then $t$ fixes no point of $B$.

It suffices to prove this when $t$ is of prime order $r$. If $t$ fixes exactly one point of $B$, then $r = p$. It follows that $t \in Q$. But the only fixed point of an element of $Q - 1$ is $\infty$ and $\infty \notin B$. Thus, if $t$ fixes one point of $B$, it fixes more than one point of $B$. If $t$ fixes exactly two points, $\infty$ is one of its fixed points and if $t$ fixes two points of $B$, $\infty \in B$, contrary to hypothesis. Thus, we may assume $t$ fixes at least two points of $B$ and more than two points. By Lemma 2.6 the fixed point set of $t$ is a block containing $\infty$. Since $B$ has at least two points of the block of fixed points of $t$, $\infty \in B$, contrary to hypothesis. It follows that $t$ fixes no point of $B$. 

It follows that \(| T | = (q + 1). Since
\[ | T | = \frac{(q^9(q^2 - 1)/(q + 1, 3)), }{ | T | = (q + 1)/(q + 1, 3)}. \]
It follows that the orbit of \( B \) is of length greater than or equal to \( q^4 - q^3. \)
By Lemma 2.2, \(| A_w' | = q^4 - q^3. \) Thus, the orbit of \( B \) is of length less than or equal to \( q^4 - q^3. \) Thus, the orbit of \( B \) is of length \( q^4 - q^3 \) and is, in fact, \( A_w'. \)

So far we have thoroughly related the blocks containing \( 00 \) to the elements of \( H. \) By the previous result all blocks not containing \( \infty \) are a single orbit under \( H. \) It is appropriate, therefore, to exhibit such a block.

Let \( \omega \) be a primitive \((q + 1) - st \) root of unity. Take \( u \in E \) such that \( u + \bar{u} = -1. \) If \( q \) is odd, of course, we may take \( u = -1/2. \) Then, \( \omega^{q+1} = \omega \bar{\omega} = 1 \) and \( (\omega^i, u) \in Q. \)

**Lemma 2.8.** \( A = \{(\omega^i, u) : 0 \leq i \leq q\} \) is a block of \( A_w'. \)

**Proof.** Clearly \( A \subseteq X - \infty \) and \(| A | = 1 + q. \) We show that \( A \) is a block. The elements of \( A \) correspond to the isotropic one-dimensional subspaces spanned by the vectors \( y + \omega^i z + ux \) in \( V. \) These vectors represent the \( 1 + q \) isotropic one-dimensional subspaces of the two-dimensional nonisotropic subspace spanned \( y + ux \) and \( x. \) The lemma follows.

Henceforth, we let \( \Delta \) be the block containing \( 0 \) and \( \infty, \Delta = \infty \cup P. \) We let \( L \) be the subgroup of \( U_3(q) \) fixing \( \Delta. \) Relative to the ordered basis \( z, x, y, \) \( L \) consists of the matrices
\[
\begin{bmatrix}
(d \det M)^{-1} & 0 & 0 \\
0 & M \\
0 & 0
\end{bmatrix}
\]
with \( M \) a \( 2 \times 2 \) matrix inducing a linear operator which preserves the restriction of the bilinear form \( b \) to the subspace spanned by \( x \) and \( y. \) \( L \) then is a homomorphic image of \( GU(2, q). \) The kernel of the homomorphism is the central element of \( GU(2, q) \) of order \( (q + 1, 3). \) The commutator subgroup of \( L \) is \( SL(2, q) \) and the restriction of \( L \) to \( \Delta \) is \( PGL(2, q). \) Dickson [2, p. 132].

We have already noted that \( PGU(3, q) \subseteq \text{Aut}(A) \) and \([PGU(3, q) : U_3(q)] = (q + 1, 3). \) The subgroup of \( PGU(3, q) \) stabilizing the points \( 0 \) and \( \infty \) in \( X \) consists of the permutations inducing on \( Q \) the mappings \((\alpha, \beta) \rightarrow (\mu \alpha, \mu \beta),\) where \( \mu \) is an arbitrary nonzero element of \( E. \)

We now describe another subgroup of \( \text{Aut}(A). \)

Let \( \theta \) be an automorphism of the field \( E \) and define \( \bar{\theta} \) on \( V \) by
\[
\bar{\theta}(\alpha x + \beta y + \nu z) = \theta(\alpha)x + \theta(\beta)y + \theta(\nu)z.
\]

\( \bar{\theta} \) has the properties:
(i) \( \theta(\alpha u + \beta v) = \theta(\alpha) \theta(u) + \theta(\beta) \theta(v) \).
(ii) \( b(\theta(u), \theta(v)) = \theta(b(u, v)) \), for all \( u, v \in V, \alpha, \beta \in E \).

From these two properties of \( \theta \) it follows that \( \theta \) induces on \( X \) a function \( \theta^* \in \text{aut}(\mathcal{A}) \). The mapping \( \theta \to \theta^* \) embeds \( \text{aut}(E) \) into \( \text{aut}(\mathcal{A}) \). We let \( \theta \) be the group \( \langle \theta^* \rangle \). \( \theta \) is, of course, cyclic of order \( 2n \). From the definition of \( \theta \) it follows readily:

**Lemma 2.9.** \( \theta \) normalizes \( \text{PGU}(3, q) \), \( \text{U}_q(q) \), and its subgroups \( H, Q, P, K, \) and \( L \).

**Corollary 2.9a.** On \( Q \), \( \theta^* \in \theta \) induces the mapping \( (\alpha, \beta) \to (\theta(\alpha), \theta(\beta)) \).

**Corollary 2.9b.** \( L \) is normalized by \( \theta \) and on \( P \), \( \theta^* \in \theta \) induces the mapping \( (0, \beta) \to (0, \theta(\beta)) \). On \( K \), \( \theta^* \) induces the mapping \( k_\lambda \to k_{\theta(\lambda)} \).

As usual we let \( \text{PGU}(3, q) = \text{PGU}(3, q) \cdot \theta \).

### 3. The Geometry of Circles

Our ultimate goal is to prove that \( \text{aut}(\mathcal{A}) = \text{PGU}(3, q) \). To obtain this result it is clearly sufficient to show that \( \text{aut}(\mathcal{A})_{\infty} = \text{PGU}(3, q)_{\infty} \). Accordingly we consider \( \text{aut}(\mathcal{A})_{\infty} \).

Suppose therefore that \( f \in \text{aut}(\mathcal{A})_{\infty} \). Recall the mapping \( \sigma: Q \to E \) of section 1 defined by \( \sigma((\alpha, \beta)) = \alpha \). Since \( f \in \text{aut}(\mathcal{A})_{\infty} \), \( f \) carries blocks containing \( \infty \) into blocks containing \( \infty \). By Lemma 2.5 all blocks of \( \mathcal{A}_{\infty} \) are sets of the form \( \infty \cup hP, h \in Q \). \( f \) therefore induces a permutation on the cosets of \( P \) in \( Q \). Since \( \ker \sigma = P \), by means of the mapping \( \sigma \) the cosets of \( P \) in \( Q \) may be identified with the elements of \( E \). Thus \( f \) induces a function \( \tau(f) \) on \( E \) such that the following diagram is commutative.

\[
\begin{array}{ccc}
Q & \xrightarrow{\sigma} & E \\
\downarrow f & & \downarrow \tau(f) \\
Q & \xrightarrow{\sigma} & E
\end{array}
\]

We thereby obtain a homomorphism \( f \to \tau(f) \) from \( \text{aut}(\mathcal{A})_{\infty} \) into the symmetric group on \( E \). We prove that \( \text{aut}(\mathcal{A})_{\infty} = \text{PGU}(3, q)_{\infty} \) by showing \( \tau(\text{aut}(\mathcal{A})_{\infty}) = \tau(\text{PGU}(3, q)_{\infty}) \) and \( \ker \tau \subseteq \text{PGU}(3, q)_{\infty} \).

If \( B \) is a block of \( \mathcal{A}_{\infty} \), \( B \to \infty \) is a coset of \( P \) in \( Q \), and is collapsed by \( \sigma \) to a point in \( E \). Central to the subsequent discussion will be our description of the \( \sigma \)-images of the blocks of \( \mathcal{A}_{\infty}' \). We call the image in \( E \) of a block in \( \mathcal{A}_{\infty}' \).
a circle and denote the collection of all circles by \( \mathcal{C} \). Thus \( \mathcal{C} = \{ \sigma(B) : B \in \mathcal{A}_x \} \).

We say a permutation \( f \) of \( E \) is circle-preserving if \( f(C) \in \mathcal{C} \) whenever \( C \in \mathcal{C} \). From the definition of \( \mathcal{C} \) it follows immediately:

**Lemma 3.1.** The group \( \tau(\text{aut}(\mathcal{A}_x)) \) is circle-preserving.

We denote the family of all circle-preserving maps by \( \text{aut}(\mathcal{C}) \). We have

\[
\tau(\text{PΓU}(3, q)_x) \subseteq \tau(\text{aut}(\mathcal{A}_x)) \subseteq \text{aut}(\mathcal{C}).
\]

In the next section we show that \( \text{aut}(\mathcal{C}) = \tau(\text{PΓU}(3, q)_x) \). In this section we study the family \( \mathcal{C} \).

**Lemma 3.2.** The set \( C = \{ \omega^i : 0 \leq i \leq q \} \) is a circle.

**Proof.** Note that \( C \) is the \( \sigma \)-image of the block \( A \) of Lemma 2.8.

**Lemma 3.3.** \( \tau(\text{PΓU}(3, q)_x) \) consists of the transformations on \( E \) of the form \( z \to \mu \theta(z) + a \), where \( a, \mu \in E, \mu \neq 0 \), and \( \theta \) is an automorphism of the field \( E \).

**Lemma 3.4.** The family of circles \( \mathcal{C} \) consists precisely of the sets of the form \( \mu C + a, \mu, a \in E, \mu \neq 0 \), \( C = \{ \omega^i : 0 \leq i \leq q \} \).

**Proof.** Since \( \omega \) is a primitive \( (q + 1) - st \) root of unity, \( C \) is precisely the set of solutions to the equation \( z \overline{z} = 1 \). Thus, if \( \theta \in \text{aut}(E) \), \( \theta(C) = C \). It follows from Lemma 3.3 that all sets of the form \( \mu C + a, \mu, a \in E, \mu \neq 0 \) are circles. Now by Lemma 2.7, \( H \subseteq \text{PΓU}(3, q)_x \) is transitive on the blocks of \( \mathcal{A}_x \). Therefore, all circles are of the form \( \mu C + a, \mu, a \in E, \mu \neq 0 \).

Among the other consequences of Lemma 3.4 we note that all circles have \( 1 + q \) points.

Now the circle \( C = \{ \omega^i \}_{0 \leq i \leq q} \) may be described as the set of solutions to the equation \( z \overline{z} = 1 \). Applying the transformations \( z \to \lambda z + a \), we see that the remaining circles may be described as \( \{ z : (z - a)(\overline{z} - \overline{a}) = \mu \} \) for \( a \in E, \mu \in F, \mu \neq 0 \). Circles containing 0 are determined by equations of the form \( \overline{z} - \overline{a} z - a \overline{z} = 0, a \neq 0 \).

**Definition.** If \( D \) is a circle, the center of \( D \) is the sum of the points on \( D \).

**Lemma 3.5.** Let \( D \) be a circle, \( D = \{ z : (z - a)(\overline{z} - \overline{a}) = \mu \}, a \in E, \mu \in F, \mu \neq 0 \). Then the point \( a \) is the center of \( D \).

**Proof.** \( D = \lambda C + a \) for some \( \lambda \in E \) satisfying \( \lambda \overline{\lambda} = \mu \). (such a \( \lambda \) exists by Lemma 1.1). Now

\[
\sum_{i=0}^{q} \omega^i = \frac{\omega^{q+1} - 1}{\omega - 1} = 0,
\]

and so \( \sum_{z \in D} z = (q + 1)a = a \).
Lemma 3.6. If \( a_1, a_2 \in E, \mu_1, \mu_2 \in F, \mu_1, \mu_2 \neq 0 \), and
\[
\{ z : (z - a_1)(\bar{z} - \bar{a}_1) = \mu_1 \} = \{ z : (z - a_2)(\bar{z} - \bar{a}_2) = \mu_2 \},
\]
then \( a_1 = a_2, \mu_1 = \mu_2 \).

Proof. Each set is a circle and by Lemma 3.5., \( a_1 = a_2 \). Choosing \( b \) any point on the circle it follows
\[
\mu_1 = (b - a_1)(\bar{b} - \bar{a}_1) = (b - a_2)(\bar{b} - \bar{a}_2) = \mu_2.
\]

Thus, there exists a one-one correspondence between the circles of \( \mathcal{C} \) and equations of the form \( (z - a)(\bar{z} - \bar{a}) = \mu, a \in E, \mu \in F, \mu \neq 0 \). We note that the proof of Lemma 3.6 yields:

Lemma 3.7. Any two circles with a common center and a common boundary point are equal.

The following are easily proved:

Lemma 3.8. Let \( c \in E, c \neq 0 \). There is an \( a \in E, a \neq 0 \), such that \( \bar{a}|a = c \) if and only if \( cc = 1 \).

Lemma 3.9. Let \( a, b \in E, a, b \neq 0 \). Then \( a \) and \( b \) are linearly independent over \( F \) if and only if \( \bar{a}|a = b|b \).

Definition. Let \( C_1 \) and \( C_2 \) be two circles having a common point \( a \). We say that \( C_1 \) and \( C_2 \) are tangent at \( a \) if \( C_1 = C_2 \) or if \( C_1 \) and \( C_2 \) have no common point other than \( a \).

We discuss the tangency of circles having 0 in common.

Lemma 3.10. Let \( zz = \bar{a}z - a\bar{z} = 0 \) and \( zz = \bar{b}z - b\bar{z} = 0, a, b \neq 0 \), be two distinct circles containing 0. (Hence, \( a \neq b \)). These circles are tangent if and only if \( a \) and \( b \) are linearly dependent over \( F \).

Proof. It will suffice to show that the equations representing the circles have nonzero solution if and only if \( a \) and \( b \) are linearly independent over \( F \).

The two equations are equivalent to the system: \( zz = \bar{a}z - a\bar{z} = 0 \) and \( (b - a)\bar{z} + (\bar{b} - \bar{a})z = 0 \).

Note that the function \( z \to (b - a)\bar{z} + (\bar{b} - \bar{a})z \) is a nonzero \( F \)-linear function from \( E \) to \( F \). Thus, there is a \( c \in E, c \neq 0 \), such that the solutions \( z \) to the equation \( (b - a)\bar{z} + (\bar{b} - \bar{a})z = 0 \) consist of the points \( \{\lambda c\}_{\lambda \in F} \).

Now \( \lambda c \), with \( \lambda \in F \), is a solution to the equation \( zz = \bar{a}z - a\bar{z} = 0 \) if and only if \( \lambda \bar{c} = \lambda (\bar{a}c + a\bar{c}) = 0 \). Thus, \( \lambda = 0 \) or \( \lambda = (\bar{a}c + a\bar{c})/\bar{c} \). Thus, the given pair of equations admits a common nonzero solution if and only if
\[ \overline{ac} + a\overline{c} \neq 0. \] Equivalently, \( \overline{c}/c + \overline{a}/a \neq 0. \) Since \( \overline{c}/c = -(\overline{b} - \overline{a})(\overline{b} - a) \), this is equivalent to \( \overline{a}/a \neq (\overline{b} - \overline{a})(\overline{b} - a) \) or \( \overline{a}/a \neq b/b. \) By Lemma 3.9 the result follows.

**Corollary 3.10a.** Tangency is an equivalence relation on the family of circles which contain a given point.

**Corollary 3.10b.** There are \( 1 + q \) tangency classes of circles through a given point. Each tangency class has \( q - 1 \) circles.

**Corollary 3.10c.** If \( S \) is a circle containing 0, the tangency class of \( S \) consists precisely of the \( q - 1 \) distinct circles \( \lambda S, \lambda \in F, \lambda \neq 0. \)

**Corollary 3.10d.** Let \( S \) be a circle containing 0. Then the points of \( S - 0 \) determine distinct subspaces of \( E \) regarded as a vector space over \( F. \)

**Corollary 3.10e.** The transformations \( z \mapsto \lambda z, \lambda \in F, \lambda \neq 0, \) fix each tangency class at 0, while permuting the members of a given tangency class transitively among themselves.

**Lemma 3.11.** No distinct pair of circles have three common points.

**Proof.** We may assume both circles contain the origin and are determined by the equations

\[
\begin{align*}
zz - \overline{a}z - a\overline{z} &= 0, \quad a \neq 0, \\
zz - \overline{b}z - b\overline{z} &= 0, \quad b \neq 0.
\end{align*}
\]

If this system of equations has two nonzero solutions, so too has

\[
\begin{align*}
zz - \overline{a}z - a\overline{z} &= 0, \\
(b - a)\overline{z} + (\overline{b} - \overline{a})z &= 0.
\end{align*}
\]

If \( b \neq a, \) the solutions to the latter system all lie in a line, in contradiction to Corollary 3.10d.

It follows from Corollary 3.10d that if \( S \) is a circle through a point \( a, \) there is a unique line \( \ell \) through \( a \) such that \( \ell \) and \( S \) intersect exactly at \( a. \) We call this line the tangent line of \( S \) at \( a. \)

**Lemma 3.12.** The tangent line through 0 of the circle \( zz - \overline{a}z - a\overline{z} = 0, \ a \neq 0, \) is the line \( \{va : v \in E \text{ and } v + \overline{v} = 0\}. \)

**Proof.** We consider the intersection of the line and the circle. If \( va \) lies on both the line and the circle, \( v\overline{w}a\overline{a} = (v + \overline{v}) a\overline{a}. \) Since \( a \neq 0, \) \( v\overline{v} = v + \overline{v}. \) Since \( v + \overline{v} = 0, \) \( v\overline{v} = 0 \) and so \( v = 0. \) The result follows.
COROLLARY 3.12a. Tangent circles have the same tangent line at their point of tangency.

COROLLARY 3.12b. Each line through a point a is the tangent line of some tangency class of circles at a.

LEMMA 3.13. Let $S_1, S_2, \ldots, S_{q-1}$ be a tangency class of circles through a point a. Then the complement of the set $\bigcup_{i=1}^{q-1} (S_i - a)$ is the tangent line $\ell$ of the tangency class.

Proof. By definition $(S_i - a) \cap (S_j - a) = \emptyset$ if $i \neq j$. Since $|S_i - a| = q$, $|\bigcup_{i=1}^{q-1} (S_i - a)| = q(q - 1)$. Thus the complement of $\bigcup_{i=1}^{q-1} (S_i - a)$ has $q$ points. Since $\ell \cap (S_i - a) = \emptyset$ and $|\ell| = q$, the result follows.

The next lemmas will be useful in what follows.

LEMMA 3.14. Let $C$ be a circle containing a point a of E. Suppose $x \in X - \infty$ and $o(x) = a$. Then there is a block $B \in \mathcal{A}$ such that $x \in B$ and $o(B) = C$.

Proof. There is a block $B' \in \mathcal{A}$ such that $o(B') = C$, since $C \in \mathcal{C}$. Then, there is a point $x' \in B'$ such that $o(x') = o(x)$. Thus, $hx' = x$ for some $h \in P$. Therefore, $o(hB') = o(h) o(B') = o(B') = C$. Letting $B = hB'$, the result follows.

LEMMA 3.15. Let $B_1$ and $B_2$ be two blocks of $\mathcal{A}$ containing a common point a. If $o(B_1) = o(B_2)$, then $B_1 = B_2$.

Proof. Let $\mathcal{A}$ be the family of blocks of $\mathcal{A}$ which contain a and $\mathcal{C}(a)$ the family of circles of $\mathcal{C}$ which contain $o(a)$. By Lemma 2.2, exactly $q^2$ blocks of $\mathcal{A}$ contain a. Only one of these blocks contains $\infty$ as well. Thus $\mathcal{A}$ has $q^2 - 1$ blocks. By Corollary 3.10b, there are $q^2 - 1$ circles of $\mathcal{C}$ containing $o(a)$. Thus $\mathcal{C}(a)$ has $q^2 - 1$ circles. By Lemma 3.14 the mapping $B \rightarrow o(B)$ carries $\mathcal{A}$ onto $\mathcal{C}(a)$. Since $|\mathcal{A}| = |\mathcal{C}(a)|$, the mapping is one-one as well, and the result follows.

Lemmas 3.11 and 3.15 together have the following interesting consequence.

PROPOSITION. There are in the geometry of $\mathcal{A}$ on X no configurations of the following type:

where a, b, c, d, e, and f are distinct points and A, B, C, and D distinct blocks.
Proof. If such a configuration exists, we may assume by the transitivity of $U_3(q)$ that $a = \infty$. Now $\infty \notin C$. For if $\infty \in C$, $A$ and $C$ would have in common the distinct points $b$ and $a = \infty$. Then, $A = C$ contrary to hypothesis. Likewise, $\infty \notin D$. Thus, $C, D \in \mathcal{A}'$ and $\sigma(C)$ and $\sigma(D)$ are circles. Since $A, B \in \mathcal{A}'$, $\sigma(A - \infty)$ and $\sigma(B - \infty)$ are points in $E$. Since $A \neq B$, $\sigma(A - \infty) \neq \sigma(B - \infty)$. Since $A$ and $D$ are distinct, $f \notin A$ and $\sigma(f) \neq \sigma(A - \infty)$. Likewise, $\sigma(f) \neq \sigma(B - \infty)$. Therefore, the circles $\sigma(C)$ and $\sigma(D)$ have in common the three distinct points $\sigma(f), \sigma(A - \infty)$, and $\sigma(B - \infty)$. By Lemma 3.11 $\sigma(C) = \sigma(D)$. By Lemma 3.15 $C = D$, a contradiction.

4. Determination of $\text{aut}(\mathcal{E})$

In this section we show that $\text{aut}(\mathcal{E}) = \tau(\text{PGU}(3, q)_\infty)$. A first step in the proper direction is:

**Lemma 4.1.** Any transformation of $\text{aut}(\mathcal{E})$ carries lines to lines.

**Proof.** Let $\ell$ be a line and $a$ a point on $\ell$. By Corollary 3.12b, $\ell$ is the tangent line of some tangency class at $a$, $S_1, S_2, \ldots, S_{q-1}$. If $f \in \text{aut}(\mathcal{E})$, $f(S_1), f(S_2), \ldots, f(S_{q-1})$ is a tangency class at $f(a)$. By Lemma 3.13, $\ell$ is the complement of $\bigcup_{i=1}^{q-1} (S_i - a)$. As $f(\ell)$ is the complement of $\bigcup_{i=1}^{q-1} (f(S_i) - f(a))$, by Lemma 3.13, $f(\ell)$ is the tangent to the class $f(S_1), f(S_2), \ldots, f(S_{q-1})$. Thus, $f(\ell)$ is a line.

It is known that all transformations of $E$ which carry lines to lines are of the form $z \rightarrow A\theta(z) + a$, where $a \in E$, $\theta$ is a field automorphism of $E$, and $A$ is an $F$-linear transformation of $E$ into itself. See Dembowski [1, p. 32]. It follows then that all transformations of $\text{aut}(\mathcal{E})$ are of this form.

**Lemma 4.2.** If $f \in \text{aut}(\mathcal{E})$ carries the circle $S_1$ to the circle $S_2$, $f$ carries the center of $S_1$ to the center of $S_2$.

**Proof.** We may write $f(z) = T(z) + a$, where $T$ is an additive transformation. Then the center of $S_1$ is, by definition, $\sum_{z \in S_1} z$. Then

$$f \left( \sum_{z \in S_1} z \right) = T \left( \sum_{z \in S_1} z \right) + a = \sum_{z \in S_1} T(z) + a = \sum_{z \in S_1} (T(z) + a)$$

$$= \sum_{z \in S_1} f(z) = \sum_{z \in f(S_1)} z.$$

The last quantity is, by definition, the center of $S_2$. 
LEMMA 4.3. If $|F| \neq 3$, there is a $z \in E, z \notin F$, such that $zz = 1$ and $z + \bar{z} \neq 0$.

Proof. The equation $zz = 1$ has exactly $1 + q$ solutions in $E$. We count those solutions to $zz = 1$ such that either $z \in F$ or $z + \bar{z} = 0$.

First suppose that $F$ is of characteristic two. Then $z \in F$ and $z + \bar{z} = 0$ are equivalent. If in addition $zz = 1$, then $z^2 = 1$ and $z = 1$. Thus, there is precisely one solution of $zz = 1$ such that either $z \in F$ or $z + \bar{z} = 0$. Since there are $q + 1 > 1$ solutions of $zz = 1$, there is a $z \in E, z \notin F$, such that $zz = 1$ and $z + \bar{z} \neq 0$.

Next suppose $F$ is of odd characteristic. If $zz = 1$ and $z + \bar{z} = 0$, then $z = -z$ and $z^4 = 1$. If $z^2 = 1$ and $z \in F$, then $\bar{z} = z$ and $z^2 = 1$. Thus if $zz = 1$ and either $z + \bar{z} = 0$ or $z \in F$, we must have $z^2 = 1$. Since there are $1 + q$ solutions to $zz = 1$, if $1 + q > 4$, there is a $z \in E, z \notin F$, such that $zz = 1$ and $z + \bar{z} \neq 0$.

LEMMA 4.4. If $|F| \neq 3$, it is possible to choose $A \in E, A \neq 0$, such that the system of equations $zz = 1$ and $zz - \lambda(z + \bar{z}) = 0$ has exactly two solutions $z_1, z_I$ with $z_1 \neq z_I$.

Proof. By Lemma 4.3, we can choose $z_1 \in E, z_1 \notin F$, such that $z_1 \bar{z}_1 = 1$ and $z_1 + \bar{z}_1 \neq 0$. Let $\lambda = 1/(z_1 + \bar{z}_1)$. Since $z_1 \notin F, z_1 \neq \bar{z}_1$ and the system of equations $zz = 1$ and $zz - \lambda(z + \bar{z}) = 0$ has two distinct solutions $z_1, \bar{z}_1$. Since each equation represents a circle, by Lemma 3.11, $z_1$ and $\bar{z}_1$ are the only solutions to both equations.

LEMMA 4.5. Suppose the $F$-linear transformation of $E, z \rightarrow T(z)$ belongs to $\text{aut}(\mathcal{C})$. Then either $T(z) = \lambda z$, for some $\lambda \in E, \lambda \neq 0$, or $T(z) = \bar{\lambda}z$, for some $\lambda \in E, \lambda \neq 0$.

Proof. If $T(1) = \lambda$, replacing $T$ by $\lambda^{-1}T$, it suffices to prove that if $T$ is $F$-linear, $T(1) = 1$, and $T$ belongs to $\text{aut}(\mathcal{C})$, then $T(z) = z$ or $T(z) = \bar{z}$.

Since $T(0) = 0$, $T$ carries circles centered at 0 into circles centered at 0, by Lemma 4.2. Since $T(1) = 1$, by Lemma 3.7, $T$ fixes the circle $zz = 1$. Since $T$ if $F$-linear and $T(1) = 1$, $T$ fixes all $\mu \in F$.

If $|F| = 3$, of the four points on the circle $zz = 1$, $T$ fixes $\pm 1$ and fixes or interchanges the remaining pair. In the former case $T$ fixes two linearly independent vectors, so $T = I$. In the latter case, $T$ agrees with $z \rightarrow \bar{z}$ on two linearly independent vectors, so $T(z) = \bar{z}$.

If $|F| \neq 3$, by Lemma 4.4, there is a $\lambda \in F, \lambda \neq 0$, such that the circles $zz = 1$ and $zz - \lambda(z + \bar{z}) = 0$ intersect in the points $z_1, \bar{z}_1$, with $z_1 \neq \bar{z}_1$. Since $T$ fixes all points $\mu, \mu \in F$, $T$ fixes the center of $zz - \lambda(z + \bar{z}) = 0$. Since $T$ also fixes a boundary point of this circle, it fixes the circle
$z\bar{z} - \lambda(z + \bar{z}) = 0$. Since $T$ also fixes $z\bar{z} = 1$, $T$ fixes or interchanges the points $z_1, \bar{z}_1$. It follows then that either $T(z) = z$ or $T(z) = \bar{z}$.

Recall from Lemma 3.3 that $\tau(\text{PGU}(3, q)_\infty)$ consists of the transformations $z \mapsto \mu \theta(z) + a, a, \mu \in E, \mu \neq 0, \theta$ a field automorphism of $E$. We have also seen (following Lemma 4.1) that all transformations of $\text{aut}(\mathcal{C})$ are of the form $z \mapsto A \theta(z) + a$, where $a \in E, \theta$ is a field automorphism, and $A$ is an $F$-linear transformation of $E$. Using Lemma 4.5, it now follows:

**Proposition.** $\text{Aut}(\mathcal{C}) = \tau(\text{PGU}(3, q)_\infty)$.

5. Determination of $\text{Aut}(\mathcal{A})$

In this section, we prove that $\text{aut}(\mathcal{A}) = \text{PGU}(3, q)$. It suffices to show that $\text{aut}(\mathcal{A})_\infty = \text{PGU}(3, q)_\infty$. Applying the mapping $\tau : \text{aut}(\mathcal{A})_\infty \to \text{aut}(\mathcal{C})$ and using the fact that $\tau(\text{PGU}(3, q)_\infty) = \text{aut}(\mathcal{C})$, it suffices to show that $\ker \tau \subseteq \text{PGU}(3, q)$.

**Lemma 5.1.** If $g \in \text{aut}(\mathcal{C})$, $g$ fixes 0 and all circles containing 0, then $g$ is the identity.

**Proof.** Since $g$ fixes all circles containing 0, $g$ fixes all tangency classes at 0 and therefore all lines containing 0. Since every point is the intersection of a line through 0 and a circle through 0, $g$ is the identity.

**Lemma 5.2.** If $g \in \text{aut}(\mathcal{A})$, $g$ fixes $a, b \in X$, $a \neq b$, and $g$ fixes all blocks containing $b$, $g$ is the identity.

**Proof.** By the double-transitivity of $\text{aut}(\mathcal{A})$ we may assume $a = \infty$ and $b = 0$. Then $g \in \text{aut}(\mathcal{A})_\infty$. By Lemma 3.14, $\tau(g)$ fixes all circles containing 0. By Lemma 5.1, $\tau(g) = 1$. Therefore, $g$ fixes all blocks containing $\infty$, as well as, all blocks containing 0.

Now every point off $\mathcal{A}$ (the block containing 0 and $\infty$) is the intersection of a block containing 0 and a block containing $\infty$. Since $g$ fixes all blocks containing $\infty$ and all blocks containing 0, $g$ fixes all points off $\mathcal{A}$.

Thus, $g$ fixes all blocks having two points off $\mathcal{A}$, i.e., all blocks not equal to $\mathcal{A}$. Since each point of $\mathcal{A}$ is the intersection of $\mathcal{A}$ and a block not equal to $\mathcal{A}$, $g$ fixes all points off $\mathcal{A}$.

**Proposition.** $\ker \tau = P \subseteq \text{PGU}(3, q)$.

**Proof.** If $f \in \ker \tau$, $f$ fixes $\infty$ and all blocks containing $\infty$. By Lemma 2.5, $P \subseteq \ker \tau$ and $P$ is transitive on $B - \infty$ if $B \in \mathcal{A}_\infty$. Thus, there is an $h \in P$
such that $h \cdot f \in \ker \tau$, $h \cdot f$ fixes $\infty$ and some point $a \neq \infty$. By Lemma 5.2, $h \cdot f = 1$, and so $f \in P$.

It then follows:

**Theorem.** $\text{aut}(\mathcal{A}) = \text{PGU}(3, q)$.

**Lemma 5.3.** Let $N$ be a subgroup of $\text{PGL}(2, q)$ and suppose $N$ is doubly-transitive in the usual representation of $\text{PGL}(2, q)$ of degree $1 + q$. Then, $\text{PSL}(2, q) \subseteq N$ ($q$ odd).

**Proof.** Let $\Delta$ be the set of $1 + q$ elements on which $\text{PGL}(2, q)$ operates. If $\alpha \in \Delta$, let $P_\alpha$ be the regular normal subgroup of $\text{PGL}(2, q)_\alpha$. Let $M = \text{PSL}(2, q) \cap N$.

Since $M \triangleleft N$ and $N$ is doubly-transitive on $\Delta$, $M$ is transitive on $\Delta$. If $q = p^n$, $|\text{PGL}(2, q)| = (1 + p^n) p^n (p^n - 1)n$. Since $N$ is doubly-transitive, $p^n \mid |N|$, so $N \cap P_\alpha \neq 1$, for each $\alpha \in \Delta$.

By Dickson’s theorem [5, p. 44], either $M = \text{PSL}(2, q)$, or $q = 9$ and $M = A_3$. In the latter case, however, the normalizer of $M$ is not doubly-transitive. Thus, $M = \text{PSL}(2, q)$; so $N \supseteq \text{PSL}(2, q)$.

**Corollary to Theorem.** If $G \subseteq \text{aut}(\mathcal{A})$ and $G$ is doubly-transitive on $X$, $U_3(q) \subseteq G$. If $|G| = |U_3(q)|$, $G = U_3(q)$ ($q$ odd).

**Proof.** If $N$ is the subgroup of $G$ fixing the block $\Delta$, $N$ is doubly-transitive on $\Delta$. By Lemma 5.3 $P \subseteq N$. Since $G$ is transitive, it follows that all conjugates of $P$ are contained in $G$. Since $U_3(q)$ is simple, $U_3(q)$ is generated by conjugates of $P$, so $U_3(q) \subseteq G$.

**Acknowledgment**

The author wishes to extend his thanks to his advisor Professor Daniel Gorenstein.

**References**