THE ALTERNATING GROUP A_8 AND THE GENERAL LINEAR GROUP $GL_4(2)$

JOHN MURRAY*

ABSTRACT. We give an explicit construction for the isomorphism $A_8 \cong GL_4(2)$.

The involutions of cycle type 2^3 in the symmetric group S_6, together with the null-set, can be given the structure of an elementary abelian group of order 16, in such a way that S_6 preserves the group operation. This gives an embedding ζ of S_6 into the general linear group $GL_4(2)$. Regarding S_6 as a subgroup of the alternating group A_8, we show that ζ extends to A_8. Coincidence of group orders implies that this extension is an isomorphism.

1. INTRODUCTION

Let $S(X)$ denote the group of permutations, and $A(X)$ the subgroup of even permutations, of a set X. If $n \in \mathbb{N}$, set $X_n := \{1, \ldots, n\}$. We use S_n (respectively A_n) to denote any member of the isomorphism class of groups containing $S(X_n)$ (respectively $A(X_n)$). If q is a power of a rational prime number p, then GF(q) will denote the finite field containing q elements. The general linear group $GL_n(2)$ consists of all invertible $n \times n$ matrices with entries in GF(2). Since 1 is the only non-zero element in GF(2), every invertible matrix over GF(2) has determinant 1. So $GL_n(2)$ coincides with its special linear subgroup $SL_n(2)$. There is only one scalar matrix in $SL_n(2)$, namely the identity $n \times n$ matrix. So $SL_n(2)$ can be identified with its projective special linear factor group $L_n(2)$.

C. Jordan [3] first demonstrated that the groups A_8 and $L_4(2)$ are isomorphic. W. Edge gives some interesting historical background and references in [2]. The definitive modern proof is due to J. Conway [1]. His proof relies on properties of the Cayley embeddings of an elementary group of order 8 in A_8. There are two classes of such subgroups, which he calls the even and odd subgroups. It turns out that the even subgroups, together with an abstract identity symbol, can be given the structure of an elementary abelian group of order 16, with the group operation compatible with the conjugation action of A_8 on even subgroups. This gives an injective homomorphism $A_8 \hookrightarrow L_4(2)$, which, by coincidence of group orders, is an isomorphism.

In this paper, we explore the combinatorial background to Conway's proof. Suppose that n is a positive integer. We call a product of n disjoint transpositions an n-involution. Using a simple set-theoretic construction, we show that the transpositions (1-involutions) of S_6, together with an abstract identity element ϕ, can be given the structure of an elementary abelian group of order 16. As S_6 has an outer automorphism which interchanges 1-involutions and 3-involutions, this gives a natural construction for an elementary abelian group whose non-trivial elements

Date: October 28, 1998.

1991 *Mathematics Subject Classification.* 20C.

*The author was supported by a Forbairt Fellowship while writing this paper.

are the 3-involutions in S_6. Next, we define the signature of an even (or an odd) subgroup of A_8 as a certain 3-involution in S_6. Proposition 4.2 shows that the intersection of an even with an odd subgroup is governed by the commutativity of their signatures. Using this fact, we show that the conjugation action of A_8 on its even subgroups is compatible with the group operation defined on their signatures. This provides an explicit, and we hope well-motivated, account of Conway's construction.

We note that our 3-involutions correspond to J. J. Sylvester's *synthemes.* The set of 5 transpositions in S_6 moving a given numeral correspond, via Proposition 3.3, to the set of five synthemes which he calls a *pentad.* See [6, 7.11] or [4] for an account of the combinatorial properties of the outer automorphisms of S_6.

Our interest in the topics in this paper arose from a study [5] of aspects of the representation theory of the sporadic finite simple group *McL*. This group is the unique finite simple group in which the centralizer of an involution is isomorphic to the universal covering group $\hat{A}_8 \cong 2.A_8$ of A_8. It has two classes of subgroups $2^4 : A_7$, where the A_7 acts flag transitively on the 2^4, and the 2^4 is conjugate to the inverse image in $\hat{A}_8$ of a Cayley embedding of 2^3 in A_8. As the referee kindly informed me, the sporadic finite simple group M_{24} actually has a subgroup of type $2^4 : A_8$, where the complement A_8 acts faithfully on the 2^4.

2. The transpositions of S_6

Let X be a set. We use ϕ to denote the empty subset of X. If A and B are subsets of X, their *symmetric difference* $A \triangle B$ is defined by:

$$A \triangle B := (A \cup B) \backslash (A \cap B).$$

Symmetric difference gives a commutative binary operation on the powerset $\mathbb{P}(X)$ of X. In fact, we have the following well-known result:

Lemma 2.1. *$(\mathbb{P}(X), \triangle)$ is an elementary abelian 2-group of order $2^{|X|}$, with the empty set as identity.*

Proof. Using Venn diagrams, it is easy to show that $\triangle$ is an associative operation. Also

$$A \triangle A = A \backslash A = \phi,$$
$$A \triangle \phi = \phi \triangle A = A \backslash \phi = A,$$

The lemma follows. □

As $(\mathbb{P}(X), \triangle)$ is an abelian group, $< X > := \{\phi, X\}$ is a normal subgroup. Let $\overline{\mathbb{P}}(X)$ denote the quotient group $\mathbb{P}(X)/ < X >$. Then $\overline{\mathbb{P}}(X)$ is elementary abelian of order $2^{|X|-1}$. If $A \in \mathbb{P}(X)$, then $A^{\perp} := A \triangle X$ is the complement of A in X. So the elements of $\overline{\mathbb{P}}(X)$ are the 2-part partitions $\{A, A^{\perp}\}$ of X. Let $\triangle$ denote the group operation in $\overline{\mathbb{P}}(X)$. Then for $A, B \subseteq X$, we have

$$\{A, A^{\perp}\} \triangle \{B, B^{\perp}\} = \{A \triangle B, (A \triangle B)^{\perp}\}$$
$$= \{A \triangle B^{\perp}, (A \triangle B^{\perp})^{\perp}\}.$$

Suppose now that $|X|$ is even. We say that $\{A, A^{\perp}\} \in \overline{\mathbb{P}}(X)$ is *even* if $|A|$ is even. Since

$$|A \triangle B| = |A| + |B| - 2|A \cap B|,$$

it follows that the product of any two even elements of $\overline{\mathbb{P}}(X)$ is even. So the set, $\mathbb{E}(X)$, of even elements forms a subgroup of index 2 in $\overline{\mathbb{P}}(X)$.

Lemma 2.2. *Suppose that* $n \geq 2$. *Then* $(\mathbb{E}(X_n), \triangle)$ *is an elementary abelian group of order* 2^{n-2}.

It is a coincidence of small numbers that every non-trivial even 2-part partition of $X_6 := \{1, \ldots, 6\}$ contains exactly one part of size 2. So the non-trivial elements of $\mathbb{E}(X_6)$ can be identified with the transpositions (i, j) of $S(X_6) \cong S_6$. This allows us to define the operation $\triangle$ on the set consisting of ϕ together with the transpositions of $S(X_6)$. For example

$$\begin{aligned}(1,2) \triangle (3,4) &= (5,6),\\ (1,2) \triangle (2,3) &= (1,3),\\ (1,2) \triangle (1,2) &= \phi,\\ (1,2) \triangle \phi &= (1,2).\end{aligned}$$

Lemma 2.3. *Let* $s \neq t$ *be transpositions in* $S(X_6)$. *Then there is the unique transposition,* $u \neq s, t$, *in* $S(X_6)$, *with the property that* u *commutes with all transpositions in* $S(X_6)$ *which commute with both* s *and* t. *Moreover,* $s \triangle t = u$. *Thus* $S(X_6)$ *acts on the group* $(\mathbb{E}(X_6), \triangle)$.

Proof. Suppose that $st = ts$. Without loss of generality $s = (1, 2)$ and $t = (3, 4)$. Any transposition which commutes with all transpositions of $S(X_6)$ which commute with both s and t necessarily commutes with s and t. So it is one of $(1, 2)$,$(3, 4)$ or $(5, 6)$. Thus $u = (5, 6)$. Also $(1, 2) \triangle (3, 4) = (5, 6)$,

Suppose that $st \neq ts$. Without loss of generality $s = (1, 2)$ and $t = (1, 3)$. The transpositions of S_6 which commute with both s and t are precisely those which fix the symbols $1, 2, 3$. So the transpositions which commute with these are $(1, 2)$,$(1, 3)$ and $(2, 3)$. Thus $u = (2, 3)$. Also $(1, 2) \triangle (1, 3) = (2, 3)$.

The group $S(X_6)$ acts by conjugation on its transpositions, and hence on the non-trivial elements of $\mathbb{E}(X_6)$. We can make $S(X_6)$ to act on $\mathbb{E}(X_6)$ by setting $\phi^\sigma := \phi$, for all $\sigma \in S(X_6)$. Then $S(X_6)$ preserves the group operation of $\mathbb{E}(X_6)$, since it preserves the commutation relations between its own elements. □

No element of $S(X_6)$ centralizes every transposition. So the previous lemma gives an embedding:

$$\zeta : S(X_6) \hookrightarrow \mathrm{Aut}(\mathbb{E}(X_6)) \cong L_4(2).$$

R. Gow has pointed out the following consequence of this fact.

Corollary 2.4. $S_6 \cong \mathrm{Sp}_4(2)$.

Proof. Suppose that X is a finite set of even cardinality. Set

$$\begin{aligned}&\lambda : \mathbb{E}(X) \times \mathbb{E}(X) \to \mathrm{GF}(2),\\ &\lambda(\{A, A^\perp\}, \{B, B^\perp\}) = |A \cap B| 1_{\mathrm{GF}(2)}, \quad \text{for } A, B \subseteq X.\end{aligned}$$

It is readily verified that λ endows $\mathbb{E}(X)$ with an alternating bilinear form. The elements of $\mathrm{Aut}(\mathbb{E}(X)) \cong L_{2^{n-2}}(2)$ which preserve λ form a group isomorphic to the symplectic group $\mathrm{Sp}_{2^{n-2}}(2)$.

We now specialize to $X = X_6$. If (i, j) and (k, l) are transpositions in $S(X_6)$, then $\lambda((i, j), (k, l)) = 0$ if and only if (i, j) commutes with (k, l). In particular, the action of $S(X_6)$ on $\mathbb{E}(X_6)$ preserves λ. So $\zeta(S(X_6))$ is isomorphic to a subgroup of $\mathrm{Sp}_4(2)$. However,

$$|S(X_6)| = 2^4 \cdot 3^2 \cdot 5 = 2^{2\cdot 2}(2^{2\cdot 2} - 1)(2^2 - 1) = |\,\mathrm{Sp}_4(2)|.$$

We conclude that $\zeta(S(X_6))$, and hence S_6, is isomorphic to $\mathrm{Sp}_4(2)$. $\square$

We need the following lemma:

Lemma 2.5. *Let x and y be transpositions in $S(X_6)$. Then $xy = yx \iff y = x^t$, for some involution t of cycle type 2^3.*

Proof. Suppose that $xy = yx$. If $x = y$, then we may take t to be any involution of cycle type 2^3 which commutes with x. If $x \neq y$, then without loss of generality $x = (1, 2)$ and $y = (3, 4)$, and $t = (1, 3)(2, 4)(5, 6)$ will do.

Suppose that $y = x^t$, for some involution t. If t commutes with x, then $x = y$. Otherwise, we may assume that $x = (1, 2)$ and $t = (1, 3)(2, 4)(5, 6)$. Then $y = x^t = (3, 4)$ commutes with x. $\square$

3. The 3-involutions of S_6

As is well known, S_6 possesses outer automorphisms i.e. automorphisms which do not arise from the conjugation action of the group on itself. In the spirit of the paper, we provide an elementary proof of this fact, and in Proposition 3.3 we establish a property of the outer automorphisms which we will need.

Let X be a finite set. A *transposition of* X is a permutation of X which swaps two elements and fixes all other elements. We call a product of n disjoint transpositions an *n-involution*. Suppose that s and t are each products of disjoint transpositions of X. We say that *s is contained in t*, or *t contains s*, if each transposition which occurs in s also occurs in t. So, for example, the 2-involution $(1, 2)(3, 4)$ is contained in the 3-involution $(1, 2)(3, 4)(5, 6)$.

Consider the subgroup $H = <(1, 2, 3, 4, 5)> \rtimes <(2, 3, 5, 4)>$ of $S(X_5)$. We have $[S(X_5) : H] = 6$ and it is easy to show that

$$\mathrm{Core}(H) := \bigcap_{\sigma \in S(X_5)} H^\sigma = \{1\}.$$

So the permutation representation of $S(X_5)$ on the left cosets $H\backslash S(X_5)$ of H in $S(X_5)$ induces an embedding

$$\iota\colon S(X_5) \hookrightarrow S(X_6),$$

via some fixed identification $S(H\backslash S(X_5)) \cong S(X_6)$. The image $K := \iota(S(X_5))$ is necessarily a transitive subgroup of $S(X_6))$. In particular, it is not conjugate to the stabilizer, $S(X_5)$, of the numeral 6 in $S(X_6)$. Now $[S(X_6) : K] = 6$. Also, it is well known that $A(X_6)$ is the only proper non-trivial normal subgroup of $S(X_6)$, from which we deduce that $\mathrm{Core}(K) = \{1\}$. So the permutation representation of $S(X_6)$ on the left cosets $K\backslash S(X_6)$ of K in $S(X_6)$ induces an automorphism

$$\tau\colon S(X_6) \hookrightarrow S(X_6),$$

via some fixed identification $S(K\backslash S(X_6)) \cong S(X_6)$. We claim that τ is an outer automorphism of S_6. To prove this, we will show that τ interchanges the 1-involutions and the 3-involutions of S_6.

Note that the involutions in $S(X_5)$ are 1 or 2-involutions, while those of $S(X_6)$ are 1, 2 or 3-involutions.

Lemma 3.1. *The conjugacy classes of $S(X_5)$ which have non-trivial intersection with H are those of cycle type $1^5, 5, 1.4, 1.2^2$. So if $\iota(\sigma)$ fixes a point of X_6, for $\sigma \in S(X_5)$, then σ is a member of one of these classes.*

Proof. The first statement can be verified directly. Suppose that σ is an element of $S(X_5)$ and $\iota(\sigma)$ fixes a point of X_6. Then $\sigma\mu H = \mu H$, for some $\mu \in S(X_5)$. Hence $\sigma^\mu \in H$. This completes the proof. □

Corollary 3.2. *Let t be an involution in $S(X_5)$. If t is a 1-involution then $\iota(t)$ is a 3-involution. If t is a 2-involution then $\iota(t)$ is a 2-involution. In particular K contains no 1-involutions.*

Proof. It is clear that $\iota(A(X_5)) = K \cap A(X_6)$ (for instance because $A(X_5)$ is the unique subgroup of index 2 in $S(X_5)$).

Suppose that t is a 1-involution. Then $\iota(t) \in K \backslash A(X_6)$ is either a 1-involution or a 3-involution. A 1-involution has fixed points in X_6. So the former case is impossible, using Lemma 3.1.

Suppose that t is a 2-involution. Then $\iota(t)$ is an even involution. So it must be a 2-involution. □

We now prove the following:

Proposition 3.3. *τ interchanges the classes of 1-involutions and 3-involutions. In particular τ is an outer automorphism of $S(X_6)$.*

Proof. The 1-involutions and the 3-involutions are the only classes of odd involutions in $S(X_6)$. So τ either normalizes both classes or interchanges them.

Let t be a 1-involution in $S(X_6)$. Since K contains no involutions, $\tau(t)$ is a fixed point free permutation of X_6. So $\tau(t)$ must be a 3-involution. The result follows. □

Corollary 3.4. *Let x and y be 3-involutions in $S(X_6)$. Then $xy = yx \iff y = x^t$, for some 1-involution t in $S(X_6)$.*

Proof. This follows immediately from Lemma 2.5 and Proposition 3.3. □

We have previously identified the non-trivial elements of $\mathbb{E}(X_6)$ with the 1-involutions of $S(X_6)$. So we can use τ to identify the the non-trivial elements of $\mathbb{E}(X_6)$ with the 3-involutions of $S(X_6)$. This allows us to define the operation $\triangle$ on the set consisting of the 3-involutions of $S(X_6)$, together with the symbol ϕ. Notice that τ is not uniquely defined: it depends on the way in which $S(K\backslash S(X_6))$ is identified with $S(X_6)$. However, the operation $\triangle$ does not depend on the choice of τ, as the following result shows.

Corollary 3.5. *Let $s \neq t$ be 3-involutions in $S(X_6)$. There is the unique 3-involution, $u \neq s, t$, in $S(X_6)$, with the property that it commutes with all 3-involutions in $S(X_6)$ which commute with both s and t. Moreover $s \triangle t = u$. In particular, the element u does not depend on the choice of outer automorphism τ.*

Proof. This follows immediately from Lemma 2.3 and Proposition 3.3. □

Using this result, it is easy to see that

$$\begin{aligned}(1,2)(3,4)(5,6) \triangle (1,2)(3,5)(4,6) &= (1,2)(3,6)(4,5),\\ (1,2)(3,4)(5,6) \triangle (1,3)(2,5)(4,6) &= (1,2)(3,4)(5,6)^{(1,3)(2,5)(4,6)}\\ &= (1,6)(2,4)(3,5).\end{aligned}$$

Also, by definition

$$\begin{aligned}(1,2)(3,4)(5,6) \triangle (1,2)(3,4)(5,6) &= \phi,\\ (1,2)(3,4)(5,6) \triangle \phi &= (1,2)(3,4)(5,6).\end{aligned}$$

Let n be a positive integer. The map

$$\begin{aligned}S(X_n) \to & A(X_{n+2}),\\ \sigma \to & \begin{cases} \sigma, & \text{if } \sigma \in A(X_n)\\ \sigma \circ (n+1, n+2), & \text{if } \sigma \in S(X_n) \setminus A(X_n)\end{cases}\end{aligned}$$

is an injective homomorphism. We use $\mathbb{S}(X_n)$ to denote its image. The action of $S(X_6)$ on the set consisting of ϕ and the class of 3-involutions induces a map

$$\zeta : \mathbb{S}(X_6) \to \mathrm{Aut}(\mathbb{E}(X_6)) \cong L_4(2).$$

It remains to show that ζ extends to $A(X_8)$.

4. The odd and even subgroups of A_8

We now describe the odd and even subgroups of A_8, objects first introduced by Conway [1].

Suppose that G is a finite group. Its *holomorph* is the group

$$\mathrm{Hol}(G) := G \rtimes \mathrm{Aut}(G).$$

So the elements of $\mathrm{Hol}(G)$ are pairs (g, f), with $g \in G$ and $f \in \mathrm{Aut}(G)$, and multiplication $*$ is defined by

$$(g_1, f_1) * (g_2, f_2) = (g_1 f_1(g_2), f_1 \circ f_2), \quad \text{for } g_1, g_2 \in G \text{ and } f_1, f_2 \in \mathrm{Aut}(G).$$

The map

$$\begin{aligned}\mathrm{Cy} : \mathrm{Hol}(G) \to & S(G),\\ \mathrm{Cy}(g, f)(x) = & gf(x), \quad \text{for } (g, f) \in \mathrm{Hol}(G) \text{ and } x \in G,\end{aligned}$$

is an injective homomorphism, which we shall call the *Cayley embedding*. Moreover, $\mathrm{Cy}(\mathrm{Hol}(G))$ is a self-centralising subgroup of $S(G)$, $\mathrm{Cy}(G)$ acts regularly and transitively on G and the normalizer of $\mathrm{Cy}(G)$ in $S(G)$ coincides with $\mathrm{Cy}(\mathrm{Hol}(G))$.

Let $\mathcal{E}(X_8)$ be the image in $S(X_8)$ of the Cayley embedding of an elementary abelian group $\mathbb{Z}_2^3$ of order 8, where the elements of $\mathbb{Z}_2^3$ are identified in some manner with the numerals of X_8.

Lemma 4.1. *All non-trivial elements of $\mathcal{E}(X_8)$ are 4-involutions, and each transposition of $S(X_8)$ is contained in exactly one 4-involution of $\mathcal{E}(X_8)$. The normalizer $\mathcal{N}(X_8)$ of $\mathcal{E}(X_8)$ in $S(X_8)$ is contained in $A(X_8)$ and is isomorphic to the holomorph $\mathbb{Z}_2^3 \rtimes L_3(2)$ of $\mathbb{Z}_2^3$. Therefore, there are exactly two conjugacy classes of such Cayley embeddings in $A(X_8)$, but only one class in $S(X_8)$. Also, any two distinct $A(X_8)$-conjugates of $\mathcal{E}(X_8)$ intersect in the trivial group.*

Proof. The non-trivial elements of $\mathcal{E}(X_8)$ are 4-involutions, since they are involutions of $S(X_8)$ which have no fixed points in X_8.

Suppose that x, y are 4-involutions in $\mathcal{E}(X_8)$ which both contain the same transposition t. Then xy fixes the numerals in X_8 transposed by t. Hence $xy = 1$, and so $x = y$. This shows that each transposition t of $S(X_8)$ is contained in at most one 4-involutions of $\mathcal{E}(X_8)$. The seven 4-involutions in $\mathcal{E}(X_8)$ account for $7 \times 4 = 28$ transpositions of S_8. But $S(X_8)$ has $\binom{8}{2} = 28$ transpositions. So each transposition of S_8 is contained in exactly one 4-involution of $\mathcal{E}(X_8)$.

The structure of $\mathcal{N}(X_8)$ comes from discussion prior to this lemma. Let $\mathcal{K}(X_8)$ be a complement to $\mathcal{E}(X_8)$ in $\mathcal{N}(X_8)$. It is clear that

$$\mathcal{N}(X_8) \cap A(X_8) = \mathcal{E}(X_8)(\mathcal{K}(X_8) \cap A(X_8)),$$

since $\mathcal{E}(X_8)$ is contained in $A(X_8)$. But $\mathcal{K}(X_8)$ is isomorphic to the simple group $L_3(2)$, of order 168. So $\mathcal{K}(X_8) \cap A(X_8) = \mathcal{K}(X_8)$ and hence $\mathcal{N}(X_8)$ is contained in $A(X_8)$. We conclude that there are two classes of Cayley embeddings $\mathcal{E}(X_8)$ in $A(X_8)$, while $S(X_8)$ contains only one such class.

The centralizer of a 4-involution in S_8 is isomorphic to $\mathbb{Z}_2 \wr S_4$, and is clearly not contained in $A(X_8)$. So the 4-involutions form a single conjugacy class of size $8!/(2^4 \times 24) = 105$ in $A(X_8)$. Each 4-involution is contained in some $A(X_8)$-conjugate of $\mathcal{E}(X_8)$. From the structure of $\mathcal{N}(X_8)$, there are $(8!/2)/(2^3 \times 168) = 15$ distinct conjugates of $\mathcal{E}(X_8)$ in $A(X_8)$. So these conjugates contain at most $7 \times 15 = 105$ non-trivial elements. We conclude that every 4-involution is contained in exactly one conjugate of $\mathcal{E}(X_8)$, and hence that any two distinct $A(X_8)$-conjugates of $\mathcal{E}(X_8)$ intersect in the identity group. □

Let $\mathcal{E}$ and $\mathcal{O}$ be representatives of the two classes of Cayley embeddings of $\mathbb{Z}_2^3$ in $A(X_8)$. We call the class containing $\mathcal{E}$ the *even subgroups of* $A(X_8)$, and the class containing $\mathcal{O}$ the *odd subgroups of* $A(X_8)$. We say that $\mathcal{E}$ *meets* $\mathcal{O}$ if their intersection is not the trivial group.

By Lemma 4.1, exactly one 4-involution $t \in \mathcal{E}$ contains the involution $(7, 8)$. The product of the other three involutions contained in t is a 3-involution s in $S(X_6)$. We call s the *signature of* $\mathcal{E}$, and denote it by $\mathfrak{sig}(\mathcal{E})$. Clearly $\mathfrak{sig}$ establishes a bijection between the even subgroups of $A(X_8)$ and the 3-involutions in $S(X_6)$. Similar remarks apply to $\mathcal{O}$ and to the odd subgroups of $A(X_8)$.

The following result is vital:

Proposition 4.2. *$\mathcal{E}$ meets $\mathcal{O}$ if and only if $\mathfrak{sig}(\mathcal{E})\,\mathfrak{sig}(\mathcal{O}) = \mathfrak{sig}(\mathcal{O})\,\mathfrak{sig}(\mathcal{E})$.*

Proof. Suppose that $\mathcal{E}$ meets $\mathcal{O}$. Let x be a 4-involution in $\mathcal{E} \cap \mathcal{O}$. Then x contains at least one transposition t in $S(X_6)$. Since $x \in \mathcal{E} \cap \mathcal{E}^t \cap \mathcal{O}$, Lemma 4.1 implies that either $\mathcal{E} = \mathcal{E}^t$ or $\mathcal{E}^t = \mathcal{O}$. The first case is impossible, since the normalizer of $\mathcal{E}$ in $S(X_8)$ is contained in $A(X_8)$. So $\mathcal{E}^t = \mathcal{O}$. Since $t \in S(X_6)$, it follows that $\mathfrak{sig}(\mathcal{E})^t = \mathfrak{sig}(\mathcal{E}^t) = \mathfrak{sig}(\mathcal{O})$. We conclude from Lemma 3.4 that $\mathfrak{sig}(\mathcal{E})$ commutes with $\mathfrak{sig}(\mathcal{O})$.

Conversely, suppose that $\mathfrak{sig}(\mathcal{E})\,\mathfrak{sig}(\mathcal{O}) = \mathfrak{sig}(\mathcal{O})\,\mathfrak{sig}(\mathcal{E})$. We can reverse the argument of the previous paragraph to show that $\mathcal{E}$ meets $\mathcal{O}$. □

Notice that the definition of $\mathfrak{sig}$ depended on an arbitrary choice of 6 numerals, namely X_6, from the set X_8. However, the criterion for an even and odd subgroup to meet does not depend on this choice.

Suppose that $\mathcal{E}_1$ and $\mathcal{E}_2$ are distinct even subgroups of $A(X_8)$. Set

$$\mathcal{E}_1 \triangle \mathcal{E}_2 := \mathcal{E}_3,$$

where $\mathcal{E}_3$ be the unique even subgroup satisfying

$$\mathfrak{sig}(\mathcal{E}_1) \triangle \mathfrak{sig}(\mathcal{E}_2) = \mathfrak{sig}(\mathcal{E}_3).$$

Let $\mathbb{E}(X_8)$ be the set consisting of the even subgroups of $A(X_8)$ and the symbol ϕ. If $\mathcal{E}$ is an even subgroup set

$$\mathcal{E} \triangle \mathcal{E} := \phi, \quad \mathcal{E} \triangle \phi := \mathcal{E}, \quad \phi \triangle \mathcal{E} := \mathcal{E}.$$

The group $A(X_8)$ acts on its class of even subgroups by conjugation. If $\sigma \in A(X_8)$, set $\phi^\sigma := \phi$. This makes $\mathbb{E}(X_8)$ into an $A(X_8)$-set. We have the following proposition:

Proposition 4.3. *The set $\mathbb{E}(X_8)$ forms an elementary abelian group of order 16, under the operation $\triangle$. The action of $A(X_8)$ on $\mathbb{E}(X_8)$ preserves the group operation, and hence induces an injective homomorphism $\hat{\zeta}\colon A_8 \hookrightarrow \mathrm{Aut}(\mathbb{E}(X_8)) \cong L_4(2)$.*

Proof. The first statement is obvious, given the fact that $\mathfrak{sig}$ establishes a bijection between the nontrivial elements of $\mathbb{E}(X_8)$ and those of $\mathbb{E}(X_6)$.

Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be even subgroups of $A(X_8)$. It follows from Propositions 3.5 and 4.2 that $\mathcal{E}_1 \triangle \mathcal{E}_2$ is the unique even subgroup of $A(X_8)$, distinct from $\mathcal{E}_1$ and $\mathcal{E}_2$, with the property that it meets every odd subgroup which meets both $\mathcal{E}_1$ and $\mathcal{E}_2$. Since $A(X_8)$ preserves intersections between even and odd subgroups, we have

$$(\mathcal{E}_1 \triangle \mathcal{E}_2)^\sigma = \mathcal{E}_1^\sigma \triangle \mathcal{E}_2^\sigma,$$

for each σ in $A(X_8)$. Thus $A(X_8)$ acts on the group $\mathbb{E}(X_8)$.

It is clear that no non-trivial element of $A(X_8)$ normalizes all fifteen even subgroups of A_8. So the action of $A(X_8)$ on $\mathbb{E}(X_8)$ is faithful. The rest of the lemma follows immediately. □

We note that $\hat{\zeta}$ extends ζ, in the sense that

$$\mathfrak{sig}(\mathcal{E}^{\hat{\zeta}(\sigma)}) = \mathfrak{sig}(\mathcal{E})^{\zeta(\sigma)}, \quad \text{for all } \sigma \in \mathbb{S}(X_6) \text{ and all even subgroups } \mathcal{E}.$$

Theorem 4.4. $A_8 \cong L_4(2)$.

Proof. We know from Proposition 4.3 that $A(X_8)$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathbb{E}(X_8)) \cong L_4(2)$. The coincidence of group orders

$$|A(X_8)| = \frac{8!}{2} = 2^6 \cdot 3^2 \cdot 5 \cdot 7 = 2^{(4)(4-1)/2}(2^4-1)(2^3-1)(2^2-1)(2-1) = |\,\mathrm{Aut}(\mathbb{E}(X_8))|,$$

establishes that the two groups are in fact isomorphic. □

References

[1] J. H. Conway, *Three lectures on exceptional groups*, in Finite Simple Groups, M.B. Powell, G. Higman, Academic Press, London and New York,1971.

[2] W. L. Edge, *The geometry of the linear fractional group* $LF(4, 2)$, Proceedings of the London Mathematical Society (3) 4, 317–342 (1953).

[3] C. Jordan, *Traité des substitutions et des équations algébriques*, (Paris, 1870).

[4] T. Y. Lam, D. B. Leep, *Combinatorial structure on the automorphism group of* S_6, Expositiones Mathematicae 11 (1993), no. 4, 289–308.

[5] John C. Murray, *Dade's Conjecture for the McLaughlin Simple Group*, Ph.D. Thesis, University of Illinois at Urbana-Champaign (1997).

[6] J. Rotman, *An introduction to the Theory of Groups*, Graduate Texts in Math. (148), Fourth Edition, Springer-Verlag,New York etc. 1991.

MATHEMATICS DEPARTMENT, UNIVERSITY COLLEGE DUBLIN.
E-mail address: jcmurray@tinet.ie