WHICH ALTERNATING AND SYMMETRIC GROUPS ARE UNIT GROUPS?

CHRISTOPHER DAVIS AND TOMMY OCCHIPINTI

ABSTRACT. We prove there is no ring with unit group isomorphic to S_n for $n \geq 5$ and that there is no ring with unit group isomorphic to A_n for $n \geq 5$, $n \neq 8$. To prove the non-existence of such a ring, we prove the non-existence of a certain ideal in the group algebra $\mathbb{F}_2[G]$, with G an alternating or symmetric group as above. We also give examples of rings with unit groups isomorphic to S_1, S_2, S_3, S_4, A_1, A_2, A_3, A_4, and A_8. Most of our existence results are well-known, and we recall them only briefly; however, we expect the construction of a ring with unit group isomorphic to S_4 to be new, and so we treat it in detail.

1. INTRODUCTION

Throughout this paper, our rings are assumed associative and to have identity element 1. We will consider a special case of the general question: For what finite groups G is there a ring with unit group isomorphic to G? We shall see in the following example that this is a nontrivial condition.

Example 1.1. *There does not exist a ring whose unit group is cyclic of order 5. The proof is by contradiction. A ring R such that $R^\times \cong C_5$ would have no units of order 2, and hence $1 = -1$ in R. Thus R is an $\mathbb{F}_2$-algebra. By considering the ring homomorphism*

$$\mathbb{F}_2[x]/(x^5 - 1) \to R$$

which sends x to a generator of $R^\times$, and by identifying $\mathbb{F}_2[x]/(x^5-1)$ with $\mathbb{F}_2 \times \mathbb{F}_{2^4}$, we find that R must contain an isomorphic copy of $\mathbb{F}_{2^4}$. Hence R has at least 15 units, and this is a contradiction.

Remark 1.2. *The finite groups of odd order which occur as the unit group of a ring were determined in* [2].

In the present paper, we determine which symmetric groups and alternating groups are unit groups. Our proofs are similar in several ways to the above proof. For example, although our groups do have elements of order 2 (except in trivial cases), we exploit the fact that our groups have no *central* elements of order 2 (except in trivial cases).

The main result proved in this paper is the following.

Theorem 1.3. *The only finite symmetric groups and alternating groups which are unit groups of rings are the groups*

$$S_1, S_2, S_3, S_4, A_1, A_2, A_3, A_4, A_8.$$

Date: July 16, 2013.

Proof. The trivial abelian cases of S_1, S_2 and A_1, A_2, A_3 are treated in Section 7.1. The well-known case of S_3 is discussed in Section 3. An example of a ring with unit group isomorphic to S_4 is given in Theorem 6.3. The fact that S_n does not occur as the unit group of a ring for any $n \geq 5$ is given in Theorem 4.1. The fact that A_n does not occur as the unit group of a ring for any $n \geq 5, n \neq 8$ is given in Theorem 5.1. Two examples of rings with unit group isomorphic to A_4 are given in Section 7.2. The classical result that $M_{4\times 4}(\mathbb{F}_2)$ has unit group isomorphic to A_8 is recalled in Theorem 7.6. □

Remark 1.4. *Let G denote a finite group with no non-trivial normal 2-subgroup. It is possible to reduce the task of finding a ring with unit group G to the task of finding an isomorphism between G and a finite direct product of groups $GL_n(\mathbb{F})$, where $\mathbb{F}$ is a finite field of characteristic 2. In particular, this method can reproduce our results for S_n and A_n with $n \geq 5$, albeit in a less elementary way. We plan to describe this result in subsequent work.*

Notation and conventions. Our rings are assumed unital but not necessarily commutative, and ring homomorphisms send 1 to 1. Also, when we say S is a subring of R, we include the assumption that 1 is the same in both rings. For a ring R, we let $R^\times$ denote the unit group of R. The groups G considered in this paper will be finite. For a group G we let $Z(G)$ denote its center. Following the convention in [5], for a group ring $R[G]$ and for T a subset of G, we set

$$\hat{T} := \sum_{t \in T} t \in R[G].$$

(Here R will be understood from context; for us, R is typically $\mathbb{F}_2$.) We also write $\langle T \rangle$ for the subgroup of G generated by T. We write ι for the identity element of A_n or S_n. When we discuss a normalizer $N_G(T)$ or a centralizer $Z_G(T)$, we do not necessarily assume that T is a subgroup. For example, $N_G(T)$ is the set of $g \in G$ such that $gTg^{-1} = T$; in particular, it is not necessarily the same as the normalizer of $\langle T \rangle$. We write D_n for the dihedral group of order $2n$.

2. Unit groups with trivial center

In this section, we describe some general results which will be applied to the special cases of alternating groups and symmetric groups in the following sections. Our motivating question is the following.

Question 2.1. *Let G denote a group with trivial center. Does there exist a ring with unit group isomorphic to G?*

We begin with an easy exercise.

Proposition 2.2. *Let G denote a finite group with trivial center, and let R denote a ring with unit group $R^\times \cong G$. Then R has characteristic 2.*

Proof. The elements 1 and -1 are units in R and are in the center of R, hence are in the center of $R^\times$. Hence $1 = -1$. □

The following reduces our Question 2.1 into a question about finite rings.

Proposition 2.3. *Let G denote a finite group with trivial center. If there exists a ring with unit group isomorphic to G, then there exists a two-sided ideal $I \subseteq \mathbb{F}_2[G]$*

such that the quotient $\mathbb{F}_2[G]/I$ has unit group isomorphic to G, and furthermore such that the natural composition

$$G \subseteq \mathbb{F}_2[G]^\times \to (\mathbb{F}_2[G]/I)^\times \cong G$$

is the identity map.

Proof. Let R denote a ring with unit group isomorphic to G, and fix an isomorphism $R^\times \cong G$. There exists a unique homomorphism

$$\varphi : \mathbb{Z}[G] \to R,$$

such that the induced map

$$\varphi : G \to \mathbb{Z}[G]^\times \to R^\times \cong G$$

is the identity map. Because G has trivial center, by Proposition 2.2, we know R has characteristic 2. Hence our homomorphism φ factors through a homomorphism

$$\varphi : \mathbb{F}_2[G] \to R.$$

Let R' denote the image of φ. Because R' is a subring of R, we know that the unit group of R' is a subgroup of G. On the other hand, we checked above that the image of φ contains G. Hence the unit group of R' is equal to G. Taking I to be the kernel of φ completes the proof. □

Our approach to Question 2.1 will be to consider the restrictions on an ideal $I \subseteq \mathbb{F}_2[G]$ as described in Proposition 2.3.

Hypothesis 2.4. *Throughout this section, let G denote a finite group with trivial center and let I denote an ideal as in Proposition 2.3. We also write φ for the natural map $\mathbb{F}_2[G] \to \mathbb{F}_2[G]/I$.*

Definition 2.5. *The* weight *of an element $x \in \mathbb{F}_2[G]$ is the number of non-zero coefficients that appear in the expression*

$$x = \sum_{g \in G} a_g g \qquad (a_g \in \mathbb{F}_2).$$

Lemma 2.6. *The ideal I contains no elements of weight 2.*

Proof. We prove that if $g+h \in I$, then $g = h$; this implies that I contains no weight 2 elements. If $g + h \in I$, then $\varphi(g) = -\varphi(h)$. Because our ring is characteristic 2, this implies $\varphi(g) = \varphi(h)$. Because we have assumed that the restriction of φ to G is injective, this can only happen if $g = h$. □

Lemma 2.7. *Let $x \in \mathbb{F}_2[G]$ denote a unit. Then there exists $\sigma_x \in G$ such that $x + \sigma_x \in I$.*

Proof. This follows from the following remarks:

- $\varphi(x)$ is a unit and so $\varphi(x) = \varphi(\sigma_x)$ for some $\sigma_x \in G$;
- $x \equiv \sigma_x \bmod I$ for some $\sigma_x \in G$;
- $x + \sigma_x = x - \sigma_x$ because our ring is characteristic 2.

□

Proposition 2.8. *Let $\hat{T} \in \mathbb{F}_2[G]$ denote a unit, which we view as arising from a subset $T \subseteq G$. The element $\sigma_{\hat{T}}$ described in Lemma 2.7 is in the centralizer of $N_G(T)$ in G, where $N_G(T)$ is the normalizer of T in G.*

Proof. Because I is a two-sided ideal, for any $g \in G$ we have

$$g(\hat{T} + \sigma_{\hat{T}}) \in I$$
$$(\hat{T} + \sigma_{\hat{T}})g \in I.$$

In particular, taking $g \in N_G(T)$ and adding these last two elements, we find

$$g\hat{T} + \hat{T}g + g\sigma_{\hat{T}} + \sigma_{\hat{T}}g \in I$$
$$g\sigma_{\hat{T}} + \sigma_{\hat{T}}g \in I.$$

By Lemma 2.6, the elements $g\sigma_{\hat{T}}$ and $\sigma_{\hat{T}}g$ cannot be distinct elements of G. Hence g and $\sigma_{\hat{T}}$ commute. Because $g \in N_G(T)$ was arbitrary, we deduce that $\sigma_{\hat{T}}$ is in the centralizer of $N_G(T)$ in G, as required. □

We are now ready to apply these general results to some specific groups.

3. An example: unit group S_3

There is a well-known ring with unit group isomorphic to S_3, namely, the matrix ring $M_{2\times 2}(\mathbb{F}_2)$. In this section, we apply the general techniques of the previous section to the group S_3 as a way of illustrating our approach.

The symmetric group S_3 has trivial center, and so the results of Section 2 all apply in the case $G \cong S_3$. We consider the restrictions on an ideal $I \subseteq \mathbb{F}_2[S_3]$ such that

$$(\mathbb{F}_2[S_3]/I)^\times \cong S_3,$$

and such that furthermore the induced map

$$S_3 \to \mathbb{F}_2[S_3]^\times \to (\mathbb{F}_2[S_3]/I)^\times \cong S_3$$

is the identity map.

Consider the element

$$H_1 := \sum_{\sigma \in S_3} \sigma \in \mathbb{F}_2[S_3]$$

corresponding to the full subgroup S_3. It is easy to check that $H_1^2 = 0$ and that $(H_1 + \iota)^2 = \iota$. Hence $H_1 + \iota$ is a unit in $\mathbb{F}_2[S_3]$. If we write $T = S_3 \setminus \{\iota\}$, then we can abbreviate this unit by $\hat{T}$. By Lemma 2.7, there must exist an element $\sigma_{\hat{T}} \in S_3$ such that $\hat{T} + \sigma_{\hat{T}} \in I$. Because the normalizer of $T = S_3 \setminus \{\iota\}$ in S_3 is the full group S_3, by Proposition 2.8, we must have $\sigma_{\hat{T}} = \iota$, and hence $\hat{T} + \iota \in I$, and hence $H_1 \in I$. The reader may check that the 32-element ring $\mathbb{F}_2[S_3]/(H_1)$ has unit group isomorphic to S_3.

Let $\tau \in S_3$ denote a 3-cycle, and let $H_2 := \iota + \tau + \tau^2$. Then $(H_2) = (H_1, H_2)$, and the reader may check that the 16-element ring $\mathbb{F}_2[S_3]/(H_2)$ is isomorphic to $M_{2\times 2}(\mathbb{F}_2)$. Hence $\mathbb{F}_2[S_3]/(H_2)$ is another example of a ring with unit group isomorphic to S_3.

4. Unit group S_n

Having analyzed the case of S_3 in the previous section, we postpone the case of S_4 and turn our attention to S_n for $n \geq 5$. These groups have trivial center, so again the results of Section 2 apply. Our goal is to prove the following theorem.

Theorem 4.1. *There does not exist a ring with unit group isomorphic to S_n for any $n \geq 5$.*

Proof. By way of contradiction, we suppose that we have a ring with unit group isomorphic to S_n. Let $I \subseteq \mathbb{F}_2[S_n]$ denote an ideal satisfying the hypotheses of Proposition 2.3. Our goal is to produce an element of weight 2 in the ideal I and thus reach a contradiction.

Let $\tau = (12345)$ and consider the element $T := \iota+\tau^2+\tau^3 \in \mathbb{F}_2[S_n]$. The fact that T is a unit of order 3 and with inverse $1+\tau+\tau^4$ is readily verified[1]. By Lemma 2.7, there exists some $\sigma \in S_n$ such that $\iota + \tau^2 + \tau^3 + \sigma \in I$. By Proposition 2.8, the element σ must be in the centralizer of the normalizer of $\{\iota, \tau^2, \tau^3\}$ in S_n. One may check that the normalizer of $\{\iota, \tau^2, \tau^3\}$ in S_n is $D_5 \times S_{n-5}$ and that the centralizer of $D_5 \times S_{n-5}$ is $Z(S_{n-5})$.

Thus $\sigma \in Z(S_{n-5})$. If $\sigma = \iota$, then $\iota + \tau^2 + \tau^3 + \iota = \tau^2 + \tau^3 \in I$ is a weight 2 element in I, which is not allowed. The only remaining case is $n = 7$ and $\sigma = (67)$. Let $T = \iota + \tau^2 + \tau^3 + \sigma \in I$. Raising both sides to the 16-th power, we find that

$$T^{16} = \iota^{16} + (\tau^2)^{16} + (\tau^3)^{16} + \sigma^{16} \in I.$$

(We used here that τ and σ commute, and that our base ring has characteristic 2.) Because τ has order five and σ has order two, we find

$$T^{16} = \iota + \tau^2 + \tau^3 + \iota = \tau^2 + \tau^3 \in I,$$

which is a contradiction. This completes the proof that there are no rings with unit group isomorphic to S_n, for $n \geq 5$. □

5. Unit group A_n

The methods of the previous section carry over directly to the case of the alternating groups A_n. The only substantive difference is that our proof breaks down in the case A_8, essentially because $A_{8-5} = A_3$ is abelian. This is to be expected, though, because as we will see in Theorem 7.6, the ring $M_{4\times4}(\mathbb{F}_2)$ has unit group isomorphic to A_8.

Theorem 5.1. *There does not exist a ring with unit group isomorphic to A_n for any $n \geq 5, n \neq 8$.*

Proof. The proof is very similar to the proof of Theorem 4.1, so we focus only on the main steps. Let $I \subseteq \mathbb{F}_2[A_n]$ denote an ideal satisfying the hypotheses of Proposition 2.3. Because the 5-cycle $\tau = (12345)$ is in A_n for any $n \geq 5$, we again have a unit $\iota + \tau^2 + \tau^3$, and we again wish to consider possible values of $\sigma \in A_n$ such that $\iota + \tau^2 + \tau^3 + \sigma \in I$. One may check that the normalizer of $\{\iota, \tau^2, \tau^3\}$ in A_n is $D_5 \times A_{n-5}$. If $n \geq 5, n \neq 8$, then the centralizer of this subgroup in A_n is trivial, and hence $\sigma = \iota$, and we are finished as before. □

Remark 5.2. *If $n = 8$, then the element σ described in the previous proof should be in the centralizer of $D_5 \times A_3$; this centralizer is a cyclic group of order 3. In the proof of Theorem 4.1, we at one point considered σ^{16}. In the S_n case, we were able to prove that σ^{16} was always trivial. In the A_8 case, σ may have order 3, and so the proof breaks down, as it should because $(M_{4\times4}(\mathbb{F}_2))^\times \cong A_8$; see Theorem 7.6 below.*

[1]The existence of such an order 3 unit T is explained as follows. By the Chinese Remainder Theorem, $\mathbb{F}_2[\tau] \cong \mathbb{F}_2 \times \mathbb{F}_{2^4}$. The unit group of $\mathbb{F}_{2^4}$ is cyclic of order 15 and hence $\mathbb{F}_2[\tau]^\times$ has a cyclic subgroup of order 3.

6. Unit group S_4

The only remaining nonabelian symmetric group to consider is S_4. We describe rings with unit group isomorphic to S_4 in this section. We first need some results similar to the results in Section 2.

Lemma 6.1. *Let $H \subseteq S_n$ denote a subgroup of even order. Then $\hat{H}^2 = 0 \in \mathbb{F}_2[S_n]$ and $\hat{H} + \iota$ is a unit in $\mathbb{F}_2[S_n]$. (Recall our convention that we write $\hat{H}$ for the element $\sum_{h \in H} h \in \mathbb{F}_2[S_n]$.)*

Proof. For the first assertion, we have

$$\hat{H}^2 = |H| \cdot \hat{H} = 0,$$

because $|H|$ is even. For the second assertion, one checks that $(\hat{H} + \iota)^2 = \iota$. □

Proposition 6.2. *Let R denote a ring with unit group isomorphic to S_4, and let $I \subseteq \mathbb{F}_2[S_4]$ denote an ideal as in Proposition 2.3.*

1. *The ideal I contains $\hat{H}$, for H an isomorphic copy of S_3 (and hence for H any isomorphic copy of S_3) inside of S_4.*
2. *The ideal I contains either*

$$\iota + (24) + (12)(34) + (1234)$$

or

$$\iota + (24) + (12)(34) + (1432).$$

Proof. To prove (1), let H denote an isomorphic copy of S_3 contained inside of S_4, and view $\hat{H}$ as an element of $\mathbb{F}_2[S_4]$ as usual. Then by Lemma 6.1, $\hat{H} + \iota$ is a unit in $\mathbb{F}_2[S_4]$. Then by Proposition 2.8, we find that

$$\hat{H} + \iota + \sigma \in I$$

for some σ in the centralizer of H in S_4. The only possibility is $\sigma = \iota$, which completes the proof of (1).

To prove (2), we again find a unit $T \in \mathbb{F}_2[S_4]$ and consider the possible values of σ such that $T + \sigma \in I$. Let $T = \iota + (24) + (12)(34)$. The fact that T is a unit of order 4 with inverse

$$\iota + (1234) + (1432) + (14)(23) + (13)$$

is readily verified[2]. Using Magma, it was verified that $\sigma = (1234)$ and $\sigma = (1432)$ were the only choices for which the two-sided ideal generated by $T + \sigma$ did not contain an element of weight 2. □

Theorem 6.3. *Let J_1 (respectively, J_2) denote the two-sided ideal in $\mathbb{F}_2[S_4]$ generated by the two elements*

$$\iota + (24) + (12)(34) + (1234) \qquad \textit{(respectively, } \iota + (24) + (12)(34) + (1432)\textit{)}$$

and

$$\iota + (12) + (23) + (13) + (123) + (132).$$

Let $R_1 := \mathbb{F}_2[S_4]/J_1$ and let $R_2 := \mathbb{F}_2[S_4]/J_2$.

[2]The unit T was found using [4, Theorem 1.2], which shows that $(24) + (12)(34)$ is nilpotent, because it is an even weight element consisting of elements in a copy of the 2-group $D_4 \subset S_4$.

The rings R_1 and R_2 are nonisomorphic rings with 128 *elements and with unit group isomorphic to S_4. Every ring with unit group isomorphic to S_4 contains a subring isomorphic to either R_1 or R_2.*

Proof. It can be verified in Magma that R_1 is a ring with 128 elements and with exactly 24 distinct units corresponding to the cosets $\sigma + J_1$, for $\sigma \in S_4$. (Sample Magma code which verifies this claim is given in Appendix A.) The same can be done for R_2, or it can be checked that $R_2 \cong R_1^{\mathrm{op}}$, from which the claim that $R_2^\times \cong R_1^\times$ follows.

We next check that R_1 and R_2 are not isomorphic. An isomorphism $\psi : R_1 \to R_2$ would induce an isomorphism $\psi : R_1^\times \to R_2^\times$. Because the only automorphisms of S_4 are inner automorphisms, the restriction of ψ to S_4 would have to correspond to conjugation by some element $\tau \in S_4$. Consider the image of an arbitrary element $x := \sigma_1 + \cdots + \sigma_n \in J_1$ under the composition

$$\mathbb{F}_2[S_4] \to \mathbb{F}_2[S_4]/J_1 \xrightarrow{\psi} \mathbb{F}_2[S_4]/J_2.$$

On one hand, x must map to the coset J_2. On the other hand, x must map to

$$\tau\sigma_1\tau^{-1} + \cdots + \tau\sigma_n\tau^{-1} + J_2.$$

Thus we have shown that if there is an isomorphism $\psi : R_1 \to R_2$, then there exsts an element $\tau \in S_4$ such that $\tau J_1 \tau^{-1} \subseteq J_2$ and thus $J_1 \subseteq \tau^{-1} J_2 \tau$. Because J_2 is a two-sided ideal, this would imply

$$J_1 \subseteq \tau^{-1} J_2 \tau \subseteq J_2.$$

However, $J_1 \subseteq J_2$ implies that both the elements

$$\iota + (24) + (12)(34) + (1234) \qquad \text{and} \qquad \iota + (24) + (12)(34) + (1432)$$

are in J_2, and hence so is their sum $(1234) + (1432)$. This contradicts the fact that the cosets $(1234) + J_2$ and $(1432) + J_2$ are distinct.

We now prove the final assertion, that any ring R with unit group isomorphic to S_4 contains a subring isomorphic to R_1 or R_2. We know that such a ring R contains as a subring $\mathbb{F}_2[S_4]/I$, where I is an ideal as in Proposition 2.3. So it suffices to show that if I is an ideal as in Proposition 2.3, then $I = J_1$ or J_2. It was proven in Proposition 6.2 that I must contain either J_1 or J_2. So it remains only to show that the ideal I cannot be strictly larger than J_1 or J_2. It was verified in Magma that for each nonzero principal ideal (x) in R_1, the ring $R_1/(x)$ has at most 6 units, and hence cannot have unit group isomorphic to S_4. □

7. The remaining cases

7.1. **The abelian cases.** These cases are trivial, but we include them for the sake of completeness.

Proposition 7.1. *For each group G in the list*

$$S_1, S_2, A_1, A_2, A_3,$$

there exists a ring with unit group isomorphic to G.

Proof. The groups S_1, S_2, A_1, A_2, A_3 are cyclic groups of order $1, 2, 1, 1, 3$, respectively. Hence, they are isomorphic to the unit groups of the fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_2, \mathbb{F}_2, \mathbb{F}_4$, respectively. □

7.2. **Unit group A_4.** In this section we give two different rings with unit group isomorphic to A_4. We describe the first ring as an explicit quotient of $\mathbb{F}_2[A_4]$. We describe the second ring as a quotient of the ring of Hurwitz quaternions.

Theorem 7.2. *Let $J \subseteq \mathbb{F}_2[A_4]$ denote the two-sided ideal generated by the elements*

$$\iota + (12)(34) + (13)(24) + (14)(23)$$

and

$$\iota + (132) + (12)(34) + (143).$$

Then the quotient $\mathbb{F}_2[A_4]/J$ is a ring with 32 elements and with unit group isomorphic to A_4.

Proof. By adapting the Magma code in Appendix A, this assertion is readily verified. □

We next use quaternions to give a second example of a ring with unit group isomorphic to A_4. First we set some notation.

Definition 7.3. *Let B denote the division algebra $\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where i, j, k are defined as in the Hamilton quaternions. Let $\omega = \frac{1+i+j+k}{2}$ and let $\mathcal{O} \subset B$ denote*

$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\omega \subseteq B;$$

then $\mathcal{O}$ is a subring of B known as the Hurwitz quaternions*.*

The authors thank Noam Elkies for the following example.

Theorem 7.4. *Let $\mathcal{O}$ denote the ring of Hurwitz quaternions, as in Definition 7.3. The quotient ring $\mathcal{O}/2\mathcal{O}$ is a ring with 16 elements and with unit group isomorphic to A_4.*

Proof. By [3, Proposition 3], the unit group $\mathcal{O}^\times$ is isomorphic to the binary tetrahedral group; in particular, there is a short exact sequence

$$1 \to \{\pm 1\} \to \mathcal{O}^\times \to A_4 \to 1.$$

The kernel of the induced map

$$\mathcal{O}^\times \to (\mathcal{O}/2\mathcal{O})^\times$$

is exactly $\mathcal{O}^\times \cap (1 + 2\mathcal{O}) = \{\pm 1\}$. Hence $(\mathcal{O}/2\mathcal{O})^\times$ contains a subgroup isomorphic to A_4. On the other hand, $\mathcal{O}/2\mathcal{O}$ is a ring with 16 elements. Hence its unit group must be precisely A_4. □

Remark 7.5. *The ring $\mathcal{O}/2\mathcal{O}$ from Theorem 7.4 is isomorphic to $\mathbb{F}_2[A_4]/J$, where J is the ideal generated by $\iota + (123) + (132)$.*

7.3. **Unit group A_8.** The only remaining case is A_8, which we recall in the following theorem.

Theorem 7.6. *The unit group of $M_{4\times 4}(\mathbb{F}_2)$ is isomorphic to A_8.*

Proof. We have

$$M_{4\times 4}(\mathbb{F}_2)^\times = GL_4(\mathbb{F}_2) = PSL_4(\mathbb{F}_2) \cong A_8.$$

For this last isomorphism, see [7, Section 3.12.1]. □

Acknowledgments. The question studied in this paper was first posed to the second author by Charles Toll. Special thanks to him, and to Colin Adams, John F. Dillon, Dennis Eichhorn, Noam Elkies, Kiran Kedlaya, and Ryan Vinroot for many useful conversations. The authors made frequent use of both Magma [1] and Sage [6] while investigating this question. The free Magma online calculator `http://magma.maths.usyd.edu.au/calc/` was especially helpful.

Appendix A. Sample Magma code

To find a ring with unit group isomorphic to S_4, we explicitly computed the unit group of a certain quotient of $\mathbb{F}_2[S_4]$. The computation was done in Magma, and we next provide sample code which performs this computation.

Example A.1. *The following was used at the beginning of the proof of Theorem 6.3. It first creates the ring R_1 and counts its total number of elements as well as its number of units. It then ensures that no elements $\sigma_1 \neq \sigma_2$ become equal in $R_1 \cong \mathbb{F}_2[S_4]/I$.*

```
G:=SymmetricGroup(4);
F2G:=GroupAlgebra(GF(2), G);

x1:= F2G!G!1+F2G!G!(2,4)+F2G!G!(1,2)(3,4)+F2G!G!(1,2,3,4);

x2:=F2G!0;
H1:=sub<G|(1,2),(1,2,3)>;
for h in H1 do
    x2:=x2+F2G!h;
end for;

I:=ideal<F2G|x1, x2>;
R1:= F2G/I;

numunits:=0;
for x in R1 do
    if IsUnit(x) then
        numunits:=numunits+1;
    end if;
end for;

#(F2G/I);
numunits;

for y1 in G do
    for y2 in G do
        if F2G!y1 + F2G!y2 in I then
            if y1 ne y2 then
                y1;
                y2;
            end if;
        end if;
```

```
    end for;
end for;
```

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] S. Z. Ditor. On the group of units of a ring. *Amer. Math. Monthly*, 78:522–523, 1971.

[3] Emmanuel Hallouin and Christian Maire. Cancellation in totally definite quaternion algebras. *J. Reine Angew. Math.*, 595:189–213, 2006.

[4] S. A. Jennings. The structure of the group ring of a p-group over a modular field. *Trans. Amer. Math. Soc.*, 50:175–185, 1941.

[5] César Polcino Milies and Sudarshan K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications*. Kluwer Academic Publishers, Dordrecht, 2002.

[6] W. A. Stein et al. *Sage Mathematics Software (Version 5.3)*. The Sage Development Team, 2012. `http://www.sagemath.org`.

[7] R. Wilson. *The Finite Simple Groups*. Graduate Texts in Mathematics. Springer, 2009.

University of California, Irvine, Dept of Mathematics, Irvine, CA 92697
Current address: University of Copenhagen, Dept of Mathematical Sciences, Universitetsparken 5, 2100 København Ø, Denmark
E-mail address: `davis@math.ku.dk`

University of California, Irvine, Dept of Mathematics, Irvine, CA 92697
Current address: Carleton College, Dept of Mathematics, Northfield, MN 55057
E-mail address: `tocchipinti@carleton.edu`