Which finite simple groups are unit groups?

Davis, Christopher James; Occhipinti, Tommy

Published in:
Journal of Pure and Applied Algebra

DOI:
10.1016/j.jpaa.2013.08.013

Publication date:
2014

Document Version
Early version, also known as pre-print

Citation for published version (APA):
WHICH FINITE SIMPLE GROUPS ARE UNIT GROUPS?

CHRISTOPHER DAVIS AND TOMMY OCCHIPINTI

Abstract. We prove that if $G$ is a finite simple group which is the unit group of a ring, then $G$ is isomorphic to either (a) a cyclic group of order 2; (b) a cyclic group of prime order $2^k - 1$ for some $k$; or (c) a projective special linear group $\text{PSL}_n(\mathbb{F}_2)$ for some $n \geq 3$. Moreover, these groups do all occur as unit groups. We deduce this classification from a more general result, which holds for groups $G$ with no non-trivial normal 2-subgroup.

Throughout this paper, rings will be assumed to be unital, but not necessarily commutative, and ring homomorphisms send 1 to 1. The finite groups $G$ of odd order which occur as unit groups of rings were determined in [3]. We will prove similar results for a more general class of groups; the description of this class of groups uses the following.

Definition 1. For a finite group $G$, the $p$-core of $G$ is the largest normal $p$-subgroup of $G$. We denote this subgroup by $O_p(G)$. It is the intersection of all Sylow $p$-subgroups of $G$.

We now state the main result. The authors are most grateful to the anonymous referee for our earlier paper [2], who recognized that one of the results proved in that paper could be strengthened into the following.

Theorem 2. Let $G$ denote a finite group such that $O_2(G) = \{1\}$ and such that $G$ is isomorphic to the unit group of a ring $R$. Then

$$G \cong \text{GL}_{n_1}(\mathbb{F}_{2^{k_1}}) \times \cdots \times \text{GL}_{n_r}(\mathbb{F}_{2^{k_r}}).$$

Before proving Theorem 2, we record the following corollary.

Corollary 3. The finite simple groups which occur as unit groups of rings are precisely the groups

(a) $\mathbb{Z}/2\mathbb{Z}$,

(b) $\mathbb{Z}/p\mathbb{Z}$ for a Mersenne prime $p = 2^k - 1$,

(c) $\text{PSL}_n(\mathbb{F}_2)$ for $n \geq 3$.

Proof. If $G$ is a finite simple group, then either $O_2(G) = \{1\}$ or $O_2(G) = G$. If $O_2(G) = G$, then $G$ is a 2-group, and because we are assuming $G$ is simple, we must have $G \cong \mathbb{Z}/2\mathbb{Z}$, which for instance is isomorphic to the unit group of $\mathbb{Z}$.

Hence assume $G$ is a finite simple group which is isomorphic to the unit group of a ring and further assume $O_2(G) = \{1\}$. By Theorem 2 we know

$$G \cong \text{GL}_{n_1}(\mathbb{F}_{2^{k_1}}) \times \cdots \times \text{GL}_{n_r}(\mathbb{F}_{2^{k_r}}).$$

These groups all occur as unit groups of the corresponding products of matrix rings, so we are reduced to determining which of them are simple; this forces

$$G \cong \text{GL}_n(\mathbb{F}_{2^k}).$$

If $n > 1$ and $k > 1$, then the subgroup of invertible scalar matrices forms a nontrivial normal subgroup. Hence two possibilities remain. If $n = 1$, then $\text{GL}_1(\mathbb{F}_{2^k})$ is cyclic of order $2^k - 1$; such a group is simple if and only if its order is prime. If $k = 1$, then $\text{GL}_n(\mathbb{F}_2) = \text{PSL}_n(\mathbb{F}_2)$. For the case $k = 1, n = 2$, we have $\text{PSL}_2(\mathbb{F}_2) \cong S_3$ (see for example [4, Section 3.3.1]); this group is not simple. For the cases $k = 1, n \geq 3$, it is well-known that $\text{PSL}_n(\mathbb{F}_2)$ is simple (see for example [4, Section 3.3.2]). This completes the proof.

1The authors also thank Colin Adams, John F. Dillon, Dennis Eichhorn, Noam Elkies, Kiran Kedlaya, Charles Toll, and Ryan Vinroot for many useful discussions.

Date: August 6, 2013.
Remark 4. The simple groups $A_8$ and $\text{PSL}_2(\mathbb{F}_7)$ also occur as unit groups. This follows immediately from the exceptional isomorphisms

$$A_8 \cong \text{PSL}_4(\mathbb{F}_2) \text{ and } \text{PSL}_2(\mathbb{F}_7) \cong \text{PSL}_3(\mathbb{F}_2).$$


Having recorded the above consequences of the main result, we now gather the preliminary results used in its proof. We begin with the following observation.

Lemma 5. Let $G$ denote a finite group with $O_2(G) = \{1\}$, and let $R$ denote a ring with $R^\times \cong G$. 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 $R^\times$. By the assumption $O_2(G) = \{1\}$, the center of $G$ cannot contain any elements of order 2. Hence $1 = -1$. □

Lemma 6. Keep notation as in Lemma 5, and fix an isomorphism $R^\times \cong G$. Because $R$ has characteristic 2, we have a natural map

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

extending the fixed embedding of $G$ into $R$. The image of $\varphi$ is a ring with unit group isomorphic to $G$.

Proof. Write $S$ for the image of $\varphi$. On one hand, we have that $S^\times \subseteq R^\times \cong G$. On the other hand, the induced map $\varphi : G \to S^\times \to R^\times$ is surjective. This shows that the unit group of $S$ is isomorphic to $G$. □

Lemma 7. Let $R$ denote a finite ring of characteristic 2. If $J \subseteq R$ is a two-sided ideal such that $J^2 = 0$, then $1 + J$ is a normal elementary abelian 2-subgroup of $R^\times$.

Proof. Note that for any $j, k \in J$ and $r \in R^\times$, we have

- $(1 + j)^2 = 1 + j^2 = 1$;
- $(1 + j)(1 + k) = 1 + j + k + jk = 1 + j + k = (1 + k)(1 + j)$;
- $r(1 + j)r^{-1} = 1 + rjr^{-1} \in 1 + J$.

The first of these calculations shows that $1 + J$ is a subset of $R^\times$, and the three calculations together show that it is a normal elementary abelian 2-group. □

We now use these preliminary results to prove our main theorem.

Proof of Theorem 2. By Lemma 6 we may assume $R$ is a finite ring (and is in particular artinian) and has characteristic 2. Let $J$ denote a two-sided ideal of $R$ such that $J^2 = 0$. By Lemma 7, the set $1 + J$ is a normal 2-subgroup of $R^\times$, and so by the assumption $O_2(G) = \{1\}$, we have $J = \{0\}$. Thus the ring $R$ has no non-zero two-sided ideals $J$ with $J^2 = 0$, and hence $R$ has no non-zero two-sided nilpotent ideals. By [11] Theorem 5.4.5, the artinian ring $R$ is semisimple. By Wedderburn’s Theorem [11] Theorem 5.3.4, we have

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for some $n_1, \ldots, n_r \geq 1$ and some division algebras $D_1, \ldots, D_r$. Our ring $R$ is finite and hence each $D_i$ is finite. By another theorem of Wedderburn [11] Theorem 3.8.6], we have that each $D_i$ is a finite field. Finally, because the ring $R$ has characteristic 2, each field $D_i$ has characteristic 2. This completes the proof. □

References


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