Finite simple groups with short Galois orbits on conjugacy classes

Victor Bovdi, Thomas Breuer, Attila Maróti

PII: S0021-8693(19)30574-5
DOI: https://doi.org/10.1016/j.jalgebra.2019.10.024
Reference: YJABR 17405

To appear in: *Journal of Algebra*

Received date: 16 May 2019

Please cite this article as: V. Bovdi et al., Finite simple groups with short Galois orbits on conjugacy classes, *J. Algebra* (2020), doi: https://doi.org/10.1016/j.jalgebra.2019.10.024.

FINITE SIMPLE GROUPS WITH SHORT GALOIS ORBITS ON CONJUGACY CLASSES

VICTOR BOVDI, THOMAS BREUER, AND ATTILA MARÓTI

Abstract. All finite simple groups are determined with the property that every Galois orbit on conjugacy classes has size at most 4. From this we list all finite simple groups G for which the normalized group of central units of the integral group ring $\mathbb{Z}G$ is an infinite cyclic group.

Dedicated to Professors Ágnes Szendrei and Mária B. Szendrei on the occasion of their birthdays.

1. Introduction

According to [23, Hilfssatz V 14.7], the group of units of the ring of integers of the center of the rational group algebra $\mathbb{Q}G$ of a finite group G is isomorphic to the direct product of the groups of units of the rings of integers of the fields $\mathbb{Q}(\chi)$ where χ runs over a set of representatives of the orbits of algebraically conjugate irreducible complex characters of G.

Moreover, for a finite group G, the group of central units of the integral group ring $\mathbb{Z}G$ is isomorphic, by the theorem of Berman and Higman (see [31, Theorem 10], [8, 1.1, p. 5], and [16, Theorem 2.2, p. 23]), to $\langle -1\rangle \times Z(G) \times R(G)$ where $R(G) = 1$ or $R(G)$ is a finitely generated torsion-free abelian subgroup of the units of $\mathbb{Z}G$ with elements of augmentation 1. A systematic study of central units was launched by A. Bovdi and his PhD student Patay, see [16, Chapter 8].

In particular, [16, Lemma 8.1, p. 81] describes the basic situation when $R(G) = 1$. For a finite group G we have $R(G) = 1$ if and only if the character field $\mathbb{Q}(\chi)$ of each complex irreducible character χ of G is either $\mathbb{Q}$ or imaginary quadratic (of the form

2010 *Mathematics Subject Classification.* 16U60; 16S34; 20E45; 20K15; 20D05.

Key words and phrases. integral group ring, finite simple group.

The work of the first author was supported by UAEU UPAR grant G00002160. The second author gratefully acknowledges support by the German Research Foundation (DFG) within the SFB-TRR 195 "Symbolic Tools in Mathematics and their Application". The work of the third author on the project leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 741420), was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and also by the National Research, Development and Innovation Office (NKFIH) Grant No. K115799.

$\mathbb{Q}(\sqrt{d})$ for some $d < 0$ in $\mathbb{R}$). This happens if and only if every generator of every cyclic group $\langle g \mid g \in G\rangle$ is conjugate in G to g or to g^{-1}. We give a generalization of this statement in Proposition 2.2.

Following A. Bovdi (see also [12] for infinite groups), a not necessarily finite group G is called a *cut*-group if all central units of $\mathbb{Z}G$ are trivial (of the form $\pm g$ where $g \in Z(G)$). Early results on *cut*-groups were obtained by A. Bovdi and Patay. Recent results and references on this topic can be found in [10, 12] and [13].

The description of finite nilpotent *cut*-groups of class 2 was obtained by Patay (see [8, 3.10] and [16, Theorem 8.2, p. 83]). Bächle [10, Theorem 1.2] proved that any prime divisor of the order of a finite solvable *cut*-group is 2, 3, 5, or 7.

In the 1970's, Patay studied the question of when a finite simple group is a *cut*-group, see [29] and [30]. Afterwards, several people continued to investigate this question and for a long time the most extensive results on this topic were obtained by Aleev and his students (see [2, 3, 4, 5, 6, 7, 28]). The (finite) list of finite simple *cut*-groups was deduced in [11, Theorem 5.1] from a longer list of groups obtained in [1]. Note that in part (ii) of our Theorem 1.3 we give a corrected list of groups presented in [1]. Recently, Trefethen [32] determined all non-abelian finite simple groups which can occur as composition factors of finite *cut*-groups.

For a finite group G we denote the rank of $R(G)$ by $\mathfrak{r}_{\mathbb{Z}}(G)$ or simply by $\mathfrak{r}_{\mathbb{Z}}$.

An aim of this paper is to determine all finite simple groups G for which $\mathfrak{r}_{\mathbb{Z}}(G) = 1$.

Theorem 1.1. *A finite simple group G satisfies $\mathfrak{r}_{\mathbb{Z}}(G) = 1$ if and only if it is listed in Table 1.*

TABLE 1. Finite simple groups G with $\mathfrak{r}_{\mathbb{Z}}(G) = 1$

C_5,
A_n with $n \in \{5, 6, 10, 11, 13, 16, 17, 21, 25\}$,
$\mathrm{PSL}(2, 11), \mathrm{PSL}(3, 3), \mathrm{PSL}(3, 4), \mathrm{PSL}(4, 3)$,
$\mathrm{PSp}(6, 3), \mathrm{PSp}(8, 2)$,
$\mathrm{P\Omega}(7, 3), \mathrm{P\Omega}^+(8, 3)$,
$\mathrm{G}_2(3), \mathrm{F}_4(2), {}^2\mathrm{E}_6(2)$,
Fi_{22}

Theorem 1.1 in the special case of alternating groups was obtained in [6]. All non-abelian, non-alternating groups G listed in Theorem 1.1 were shown to satisfy $\mathfrak{r}_{\mathbb{Z}}(G) = 1$ in [4, p. 328-329].

In general, the following asymptotic statement holds.

Theorem 1.2. *There exists a universal constant $c > 0$ such that whenever G is a finite simple group then $k(G)^c < \mathfrak{r}_{\mathbb{Z}}(G) < k(G)$ provided that $\mathfrak{r}_{\mathbb{Z}}(G) > 1$ where $k(G)$*

denotes the number of conjugacy classes of G. In particular, $\mathfrak{r}_{\mathbb{Z}}(G) \to \infty$ as the orders of the finite simple groups G tend to infinity.

We deduce Theorem 1.1 from a more general result, Theorem 1.3.

Let G be a finite group and e its exponent. Let ϵ be a primitive e-th root of unity. The Galois group $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}[\epsilon] : \mathbb{Q})$, isomorphic to the unit group of $\mathbb{Z}/e\mathbb{Z}$, acts naturally on the set $\mathrm{Irr}(G)$ of complex irreducible characters of G and on the set $\mathcal{C}$ of conjugacy classes of G. Since for every element α in $\mathcal{G}$ the number of fixed points of α on $\mathcal{C}$ and on $\mathrm{Irr}(G)$ coincide (see [25, Thm. 6.32]), the number of $\mathcal{G}$-orbits on $\mathcal{C}$ and on $\mathrm{Irr}(G)$ are the same, by [25, Cor. 6.33]). We keep the notation $\mathcal{G}$ and $\mathcal{C}$ throughout this paper.

For a finite group G let $f(G)$ denote the maximal length of an orbit of $\mathcal{G}$ on $\mathcal{C}$. The group G is rational if and only if $f(G) = 1$. Another goal of the present paper is to classify finite simple groups G for which $f(G) \leq 4$.

Feit and Seitz [18] proved that the only rational non-abelian finite simple groups are $\mathrm{PSp}(6,2)$ and $\mathrm{P}\Omega^+(8,2)$. In [1] a list of groups for which $f(G) \leq 2$ is given. Since this list contains errors, we reproduce it in Table 2. (Note that the groups ${}^3\mathrm{D}_4(2)$, ${}^3\mathrm{D}_4(3)$, ${}^2\mathrm{B}_2(8)$, ${}^2\mathrm{B}_2(32)$, ${}^2\mathrm{G}_2(27)$, ${}^2\mathrm{F}_4(2)'$ appear incorrectly in [1, Table 1] and $\mathrm{G}_4(2)$ is not displayed.)

Theorem 1.3. *Let G be a finite simple group. Then $f(G) \leq 4$ if and only if G is listed in Table 2.*

Our strategy for classifying the finite simple groups G with a given value $f(G)$ is to use upper bounds for certain parameters to get a list of candidates, and to check each of these candidates explicitly. Thus this last step is the problem to determine simple groups G with given value $f(G)$.

In Section 2 we explain the technical background of the paper. Proposition 2.2 is a generalization of an old result of A. Bovdi. These ideas are used to deduce a key tool of the work, Lemma 2.3. Section 3 introduces two functions with which computations are performed using known character tables of finite simple groups. These results as well as Proposition 3.1 are later used in Sections 5 and 6. After a short section on reductions, classical simple groups are treated in Section 5 and exceptional simple groups of Lie type in Section 6. Section 7 is on alternating groups. In Section 8 we establish Theorem 1.2.

2. Background

In this section we present some background concerning the invariant $\mathfrak{r}_{\mathbb{Z}}$. In particular, we prove Proposition 2.2 which is a generalization of [16, Lemma 8.1, p. 81].

The following formula was well-known in the 1970's, see Patay [30].

$$\mathfrak{r}_{\mathbb{Z}} = h_{\mathbb{R}} + \tfrac{1}{2} h_{\mathbb{C}} - n_G. \tag{1}$$

TABLE 2. Finite simple groups G with $f(G) \leq 4$

$f(G)$	G
1	C_2, $\mathrm{PSp}(6,2)$, $\mathrm{P\Omega}^+(8,2)$
2	C_3, A_n for $n \geq 5$ $\mathrm{PSL}(2,7), \mathrm{PSL}(2,11), \mathrm{PSL}(3,4)$, $\mathrm{PSp}(6,3), \mathrm{PSp}(8,2)$, $\mathrm{PSU}(3,3), \mathrm{PSU}(3,5), \mathrm{PSU}(4,2) \cong \mathrm{PSp}(4,3), \mathrm{PSU}(4,3), \mathrm{PSU}(5,2), \mathrm{PSU}(6,2)$, $\mathrm{P\Omega}(7,3), \mathrm{P\Omega}^+(8,3)$, $\mathrm{F}_4(2), \mathrm{G}_2(3), \mathrm{G}_2(4), {}^2\mathrm{E}_6(2)$, $\mathrm{B}, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}'_{24}24, \mathrm{He}, \mathrm{HN}, \mathrm{HS}, \mathrm{J}_2, \mathrm{M}, \mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}$, $\mathrm{McL}, \mathrm{Suz}, \mathrm{Th}$
3	$\mathrm{PSL}(2,8), \mathrm{PSL}(2,13), \mathrm{PSL}(2,17), \mathrm{PSL}(2,19)$, $\mathrm{PSp}(10,2), \mathrm{PSp}(4,5)$, ${}^3\mathrm{D}_4(2), {}^2\mathrm{B}_2(8)$, $\mathrm{J}_1, \mathrm{J}_3, \mathrm{J}_4, \mathrm{O'N}, \mathrm{Ru}$
4	C_5, $\mathrm{PSL}(2,29), \mathrm{PSL}(2,31), \mathrm{PSL}(3,3), \mathrm{PSL}(4,3)$, $\mathrm{PSp}(12,2), \mathrm{PSp}(4,4)$, $\mathrm{PSU}(3,4)$, $\mathrm{P\Omega}^-(8,2), \mathrm{P\Omega}^-(10,2), \mathrm{P\Omega}^+(12,2)$, ${}^2\mathrm{F}_4(2)'$

Here $h_{\mathbb{R}}$ denotes the number of real-valued complex irreducible characters of G, $h_{\mathbb{C}} = |\mathrm{Irr}(G)| - h_{\mathbb{R}}$, and n_G is the number of $\mathcal{G}$-orbits on $\mathcal{C}$ and on $\mathrm{Irr}(G)$.

For $a \in G$ let $|a|$ denote the order of a and let a^G be the conjugacy class of a. The $\mathbb{Q}$-class $\{a^G\}_{\mathbb{Q}}$ of a is defined to be the set $\cup_{s=1,\,(s,|G|)=1}^{|a|-1}(a^s)^G$. The number $n_{\mathbb{Q}}$ of $\mathbb{Q}$-classes in G is equal to n_G. The $\mathbb{R}$-class $\{a^G\}_{\mathbb{R}}$ of $a \in G$ is defined to be $a^G \cup (a^{-1})^G$. Let $n_{\mathbb{R}}$ be the number of $\mathbb{R}$-classes of G.

From these we obtain the following.

Proposition 2.1. *If G is a finite group, then $\mathfrak{r}_{\mathbb{Z}} = n_{\mathbb{R}} - n_{\mathbb{Q}}$.*

Proof. It is sufficient to see by (1) that $\frac{1}{2}\Big(|\mathrm{Irr}(G)| + h_{\mathbb{R}}\Big) = n_{\mathbb{R}}$. This is clear since $|\mathrm{Irr}(G)| = |\mathcal{C}|$ and $h_{\mathbb{R}}$ is equal to the number of real conjugacy classes in G by [25, Thm. 6.23]. □

We emphasize that Proposition 2.1 was well known for decades.

Let $\mathcal{A}$ be the set of conjugacy classes g^G of G such that some generator of $\langle g\rangle$ is conjugate in G neither to g nor to g^{-1}. The group $\mathcal{G}$ acts on $\mathcal{A}$ in a natural way according to its action on $\mathcal{C}$. Let a_2 denote the number of orbits in this specified action. Let $\sigma \in \mathcal{G}$ be complex conjugation. It acts as inversion on $\mathcal{C}$ (which action may be trivial). Let a_1 be the number of orbits of $\langle\sigma\rangle$ on $\mathcal{A}$. Analogously, let $\mathcal{B}$ be the set of complex irreducible characters χ of G such that $\mathbb{Q}(\chi)$ is neither rational nor imaginary quadratic. The group $\mathcal{G}$ acts on $\mathcal{B}$ in a natural way. Let the number of orbits of $\mathcal{G}$ in this specified action be b_2. The element σ in $\mathcal{G}$ acts as complex conjugation on $\mathrm{Irr}(G)$. Let the number of orbits of $\langle\sigma\rangle$ on $\mathcal{B}$ be denoted by b_1.

The following is a generalization of the result of A. Bovdi [16, Lemma 8.1, p. 81] already mentioned in the Introduction.

Proposition 2.2. *Let G be a finite group. Let a_1, a_2, b_1, b_2 be as above. Then $2a_2 \le a_1$ and $2b_2 \le b_1$. Moreover, $\mathfrak{r}_{\mathbb{Z}}(G) = a_1 - a_2 = b_1 - b_2$.*

Proof. Let $\mathcal{G}$ denote the Galois group that acts on the sets $\mathcal{C}$ and $\mathrm{Irr}(G)$ of conjugacy classes and irreducible characters of G. Let $\sigma \in \mathcal{G}$ be complex conjugation on $\mathrm{Irr}(G)$. It acts as inversion on $\mathcal{C}$. Let r denote the rank of $R(G)$. Then Proposition 2.1 says $r = |\mathcal{C}/\langle\sigma\rangle| - |\mathcal{C}/\mathcal{G}|$, the difference of orbit numbers of $\langle\sigma\rangle$ and $\mathcal{G}$ on $\mathcal{C}$, respectively. By Brauer's Permutation Lemma and the Orbit Counting Lemma (see [25, Thm. 6.32, Cor. 6.33]), we have $|\mathcal{C}/\langle\sigma\rangle| = |\mathrm{Irr}(G)/\langle\sigma\rangle|$ and $|\mathcal{C}/\mathcal{G}| = |\mathrm{Irr}(G)/\mathcal{G}|$ and therefore $r = |\mathrm{Irr}(G)/\langle\sigma\rangle| - |\mathrm{Irr}(G)/\mathcal{G}|$.

Now we can consider the Galois action on the set $\mathcal{A} = \{c \in \mathcal{C} \ : \ c^{\langle\sigma\rangle} \neq c^{\mathcal{G}}\}$, and immediately get $r = |\mathcal{A}/\langle\sigma\rangle| - |\mathcal{A}/\mathcal{G}|$. Analogously, the $\mathcal{G}$-action on the set $\mathcal{B} = \{\chi \in \mathrm{Irr}(G) \ : \ \chi^{\langle\sigma\rangle} \neq \chi^{\mathcal{G}}\}$ yields $r = |\mathcal{B}/\langle\sigma\rangle| - |\mathcal{B}/\mathcal{G}|$.

Since $\mathcal{G}$ joins at least two $\langle\sigma\rangle$-orbits on $\mathcal{A}$ and $\mathcal{B}$, respectively, we also have $|\mathcal{A}/\langle\sigma\rangle| \ge 2|\mathcal{A}/\mathcal{G}|$ and $|\mathcal{B}/\langle\sigma\rangle| \ge 2|\mathcal{B}/\mathcal{G}|$. □

Observe that $\mathfrak{r}_{\mathbb{Z}}(G) = \sum_C (|C/\langle\sigma\rangle| - 1)$, where the summation runs over the $\mathcal{G}$-orbits C on the classes of G (and where $|C/\mathcal{G}| = 1$ holds). This follows by applying the idea of Proposition 2.2 to single orbits. One gets $\mathfrak{r}_{\mathbb{Z}}(G) \ge |C/\langle\sigma\rangle| - 1$ for each orbit. In particular, $\mathfrak{r}_{\mathbb{Z}}(G) \ge f(G)/2 - 1$.

We denote Euler's totient function by φ. Note that for any $g \in G$, the product of $|N_G(\langle g\rangle)/C_G(g)|$ and the length of the $\mathcal{G}$-orbit of the G-conjugacy class of g is equal to $\varphi(|g|)$. For a positive integer $m = p_1^{k_1} \cdots p_t^{k_t}$ where $p_1, \ldots, p_t$ are distinct primes and $k_1, \ldots, k_t$ are positive integers the value of $\varphi(m)$ is $\prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i-1})$. It is easy to see that $\varphi(m) \ge \sqrt{m}/2$.

Thus we have shown the following.

Lemma 2.3. *Let H be a cyclic subgroup in a finite group G. If $n = |N_G(H)/C_G(H)|$, then*

(i) $f(G) \ge \frac{\varphi(|H|)}{n} \ge \frac{\sqrt{|H|}}{2n}$ *and*

(ii) $\mathfrak{r}_{\mathbb{Z}}(G) \geq \frac{\varphi(|H|)}{2n} - 1 \geq \frac{\sqrt{|H|}}{4n} - 1$.

In particular, if $f(G) \leq 4$, *then* $\varphi(|H|) \leq 4n$.

3. Computational results

In this section we collect the computational results needed to prove Theorems 1.1 and 1.3. We use the computer system GAP [21]. Such computations are shown already in [4].

We present a function for computing $\mathfrak{r}_{\mathbb{Z}}(G)$ for a finite group G. When applied to the character table of the group G, say, it returns the value $h_{\mathbb{R}}+(|\mathrm{Irr}(G)|-h_{\mathbb{R}})/2-n_{\mathbb{Q}}$.

```
RankOfCentralUnits:= function( tbl )
    local X, real;
    X:= Irr( tbl );
    real:= Number( X, chi -> chi = ComplexConjugate( chi ) );
    return real + ( Length( X ) - real ) / 2 - Length( RationalizedMat( X ) );
end;;
```

We use this function to determine all non-abelian finite simple groups G in the character table library [17] with $\mathfrak{r}_{\mathbb{Z}}(G)$ equal to 0 or 1. (The output may differ from the one shown here, depending on the version of the table library and on the availability of other GAP packages.) We provide the inputs and outputs for the reader's convenience.

```
gap> AllCharacterTableNames( IsSimple, true, IsAbelian, false,
>       IsDuplicateTable, false, RankOfCentralUnits, 0 );
[ "A12", "A7", "A8", "A9", "Co1", "Co2", "Co3", "HS", "L3(2)", "M", "M11",
  "M12", "M22", "M23", "M24", "McL", "O8+(2)", "S6(2)", "Th", "U3(3)",
  "U3(5)", "U4(2)", "U4(3)", "U5(2)", "U6(2)" ]
gap> AllCharacterTableNames( IsSimple, true, IsAbelian, false,
>       IsDuplicateTable, false, RankOfCentralUnits, 1 );
[ "2E6(2)", "A10", "A11", "A13", "A16", "A17", "A5", "A6", "F4(2)", "Fi22",
  "G2(3)", "L2(11)", "L3(3)", "L3(4)", "L4(3)", "O7(3)", "O8+(3)", "S6(3)",
  "S8(2)" ]
```

We now present a function for computing the maximal length of Galois orbits on the set of conjugacy classes of a finite group. When applied to the character table of the group G, say, it returns 1 if all conjugacy classes of G are rational, and the maximum of the lengths of Galois orbits on classes of G otherwise.

```
MaximalGaloisOrbitLength:= function( tbl )
local fams;
fams:= Filtered( GaloisMat( TransposedMat( Irr( tbl ) ) ).galoisfams, IsList );
return MaximumList( List( fams, l -> Length( l[1] ) ), 1 );
```

```
end;;
```

We use this function to determine all non-abelian finite simple groups G in the character table library [17] with maximal Galois orbit length at most 4 on the set of conjugacy classes of G. The computations shown below/above take altogether only a few seconds; note that they use stored character tables and no table has to be computed.

```
gap> AllCharacterTableNames( IsSimple, true, IsAbelian, false,
> IsDuplicateTable, false, MaximalGaloisOrbitLength, x -> x = 1 );
[ "O8+(2)", "S6(2)" ]
gap> AllCharacterTableNames( IsSimple, true, IsAbelian, false,
> IsDuplicateTable, false, MaximalGaloisOrbitLength, x -> x = 2 );
[ "2E6(2)", "A10", "A11", "A12", "A13", "A14", "A15", "A16", "A17", "A18",
  "A19", "A5", "A6", "A7", "A8", "A9", "B", "Co1", "Co2", "Co3", "F3+",
  "F4(2)", "Fi22", "Fi23", "G2(3)", "G2(4)", "HN", "HS", "He", "J2",
  "L2(11)", "L3(2)", "L3(4)", "M", "M11", "M12", "M22", "M23", "M24", "McL",
  "O7(3)", "O8+(3)", "S6(3)", "S8(2)", "Suz", "Th", "U3(3)", "U3(5)",
  "U4(2)", "U4(3)", "U5(2)", "U6(2)" ]
gap> AllCharacterTableNames( IsSimple, true, IsAbelian, false,
> IsDuplicateTable, false, MaximalGaloisOrbitLength, x -> x = 3 );
[ "3D4(2)", "J1", "J3", "J4", "L2(13)", "L2(17)", "L2(19)", "L2(8)", "ON",
  "Ru", "S10(2)", "S4(5)", "Sz(8)" ]
gap> AllCharacterTableNames( IsSimple, true, IsAbelian, false,
> IsDuplicateTable, false, MaximalGaloisOrbitLength, x -> x = 4 );
[ "2F4(2)'", "L2(29)", "L2(31)", "L3(3)", "L4(3)", "O10-(2)", "O8-(2)",
  "S12(2)", "S4(4)", "U3(4)" ]
```

We next deal with a few groups individually.

Proposition 3.1. *If G is any of the simple groups* $\mathrm{PSL}(2,23)$, $\mathrm{PSL}(2,27)$, $\mathrm{PSL}(2,47)$, $\mathrm{PSL}(2,59)$, Ly, $\mathrm{PSU}(9,2)$, $\mathrm{P\Omega}^-(12,2)$, $\mathrm{P\Omega}(7,5)$, $\mathrm{P\Omega}(9,3)$, $\mathrm{P\Omega}(11,3)$, $\mathrm{P\Omega}^+(8,4)$, $\mathrm{P\Omega}^+(8,5)$, $\mathrm{P\Omega}^+(10,2)$, $\mathrm{P\Omega}^+(10,3)$, $\mathrm{P\Omega}^+(12,3)$, $\mathrm{P\Omega}^+(14,2)$, $\mathrm{P\Omega}^+(16,2)$, *then* $f(G) > 4$. *We also have* $f(\mathrm{P\Omega}^+(12,2)) = 4$ *and* $\mathfrak{r}_{\mathbb{Z}}(\mathrm{P\Omega}^+(12,2)) = 17$.

Proof. For $G \in \{\mathrm{PSL}(2,23), \mathrm{PSL}(2,27), \mathrm{PSL}(2,47), \mathrm{PSL}(2,59), \mathrm{P\Omega}^+(10,2), \mathrm{Ly}\}$, the character table is available in [17], and the GAP function `MaximalGaloisOrbitLength` gives $f(G) > 4$.

For $G \in \{\ \mathrm{P\Omega}^+(12,2),\ \mathrm{P\Omega}^-(12,2),\ \mathrm{P\Omega}^+(12,3),\ \mathrm{P\Omega}(7,5)\ \}$, the character tables have been computed with [15]. We have

$$f(\mathrm{P\Omega}^+(12,2)) = 4,\ f(\mathrm{P\Omega}^-(12,2)) = 8,\ f(\mathrm{P\Omega}^+(12,3)) = 11,\ f(\mathrm{P\Omega}(7,5)) = 6.$$

Moreover, the GAP function `RankOfCentralUnits` gives $\mathfrak{r}_{\mathbb{Z}}(\mathrm{P\Omega}^+(12,2)) = 17$.

TABLE 3. Some elements in matrix groups

G	$\overline{G}$	$\lvert g\rvert$	$\#\chi_{g^i}$	$\lvert Z(G)\rvert$
$\mathrm{SU}(9,2)$	$\mathrm{PSU}(9,2)$	255	16	3
$\Omega(9,3)$	G	41	6	1
$\Omega(11,3)$	G	164	5	1
$\Omega^+(8,4)$	G	255	8	1
$\Omega^+(8,5)$	$\mathrm{P}\Omega^+(8,5)$	312	12	2
$\Omega^+(10,3)$	G	164	5	1
$\Omega^+(14,2)$	G	127	9	1
$\Omega^+(16,2)$	G	255	8	1

In the remaining cases, we use the fact that two elements in a matrix group cannot be conjugate if their characteristic polynomials differ. Table 3 shows the relevant data.

In all these cases, we found an element g of the order in question by taking a few (about a hundred) pseudo random elements from the matrix group G, and computed the set of characteristic polynomials of the powers g^i, with i coprime to $|g|$. The number n, say, of these polynomials is a lower bound for the number of those conjugacy classes in G that contain generators of $\langle g\rangle$. If G is itself not simple then the factor group $\overline{G} = G/Z(G)$ is simple, and the preimage of each class of $\overline{G}$ under the natural epimorphism from G consists of at most $|Z(G)|$ classes of G. Thus $n/|Z(G)|$ is a lower bound for the number of conjugacy classes in $\overline{G}$ that contain generators of $\langle gZ(G)\rangle$.

For example, consider $G = \mathrm{SU}(9,2)$.

```
gap> g:= SU(9,2);;  ord:= 255;;
gap> repeat x:= PseudoRandom( g ); until Order( x ) = 255;
gap> Length( Set( List( PrimeResidues( ord ),
>                  i -> CharacteristicPolynomial( x^i ) ) ) );
16
```

There are at least 16 classes in G that contain the generators of a cyclic subgroup $\langle g\rangle$ of order 255, since these elements have 16 different characteristic polynomials. The simple group $\overline{G} = \mathrm{PSU}(9,2)$ arises from G by factoring out $Z(G)$, which has order 3. The preimage of each class of $\mathrm{PSU}(9,2)$ under the natural epimorphism from $\mathrm{SU}(9,2)$ consists of either 1 or 3 classes of $\mathrm{SU}(9,2)$. Thus $\overline{G}$ has at least $[16/3] = 5$ conjugacy classes that contain the images of the generators of $\langle g\rangle$ under the natural epimorphism from G. Hence in particular $f(\mathrm{PSU}(9,2)) > 4$. □

4. Some reductions

We begin our considerations of Theorem 1.3 and Theorem 1.1.

Let $G = C_p$ for some prime p. We have $f(G) = \varphi(p) = p - 1$, which is at most 4 if and only if $p \leq 5$. Furthermore, $\mathfrak{r}_{\mathbb{Z}}(G) = 1$ if and only if $p = 5$ (see Proposition 2.1).

Let $G = A_n$ for some $n \geq 5$. Since G has index 2 in the symmetric group of degree n, whose character table is integral, each Galois orbit on conjugacy classes or irreducible characters of G has length at most 2, hence $f(G) \leq 2$. (In fact we have equality, because the character tables of A_n for $n \geq 3$ are not integral.) Moreover, $\mathfrak{r}_{\mathbb{Z}}(G) = 1$ if and only if $n \in \{5, 6, 10, 11, 13, 16, 17, 21, 25\}$ by [6].

Theorems 1.3 and 1.1 follow from the previous section and also by results of Molodorich [28] in case G is a sporadic simple group. Thus, in order to prove Theorem 1.3 and Theorem 1.1, we may assume that G is a finite simple group of Lie type.

The computations in Section 3 are that the finite simple groups of Lie type listed in Theorem 1.1 or Theorem 1.3 have the claimed properties. Thus it remains to show that no other simple group of Lie type satisfies the conditions of these theorems.

5. Classical simple groups

In this section we prove Theorems 1.1 and 1.3, as well as the asymptotics stated in Theorem 1.2, for finite simple classical groups different from alternating groups. Our approach below is similar to the approach of Babai, Pálfy, Saxl [9, Section 4]. Namely, sufficiently large groups are eliminated by exposing elements g of large order such that the normalizer of the cyclic group $\langle g \rangle$ only induces few automorphisms.

First we deal with Theorem 1.2 and one direction of Theorem 1.3 (the other direction was established in Section 3) for finite simple classical groups.

The general linear group $\mathrm{GL}(n, q)$ contains elements of order $q^n - 1$. These elements are called Singer elements and the cyclic subgroups generated by them are the Singer subgroups. A Singer subgroup in $\mathrm{SL}(n, q)$ is the intersection of $\mathrm{SL}(n, q)$ with a Singer subgroup of $\mathrm{GL}(n, q)$. Singer subgroups can be defined also in other classical subgroups of $\mathrm{GL}(n, q)$ as cyclic subgroups of maximal possible orders that act irreducibly on the natural module for $\mathrm{GL}(n, q)$. These are intersections of the classical groups with the Singer subgroups of $\mathrm{GL}(n, q)$. As it was described by Huppert [24], there are Singer subgroups in all symplectic groups, in the odd-dimensional unitary groups, and in the minus type orthogonal groups. The other classical groups do not contain irreducible cyclic subgroups.

5.1. **Classical simple groups containing irreducible cyclic subgroups.** According to [24] (see also [14, Table 1]), the group $\mathrm{SL}(n, q)$ has Singer subgroups of order $(q^n - 1)/(q - 1)$, the group $\mathrm{GU}(n/2, q)$ where n is even and $n/2$ is odd has Singer subgroups of order $q^{n/2} + 1$, the group $\mathrm{SU}(n/2, q)$ where n is even and $n/2$ is odd has Singer subgroups of order $(q^{n/2} + 1)/(q + 1)$, the group $\mathrm{Sp}(n, q)$ where n is even has

Singer subgroups of order $q^{n/2}+1$, the groups $\mathrm{GO}^-(n,q)$ and $\mathrm{SO}^-(n,q)$ where n is even have Singer subgroups of order $q^{n/2}+1$, and the group $\Omega^-(n,q)$ where n is even has Singer subgroups of order $\frac{1}{d}(q^{n/2}+1)$ where d is the greatest common divisor of 2 and $q+1$.

Let $G \le \mathrm{GL}(n,q)$ be any of the above classical groups with a Singer subgroup $C = G \cap S$ where S is a Singer subgroup of $\mathrm{GL}(n,q)$. Since C acts irreducibly on the natural module, $C \le S$ and S is cyclic of order q^n-1, we have $C_{\mathrm{GL}(n,q)}(C) = S$ and so $C_G(C) = C$ and $Z(G) \le C$ by Schur's lemma and Wedderburn's theorem. Any element of G normalizing C also normalizes $C_{\mathrm{GL}(n,q)}(C) = S$. Since $N_{\mathrm{GL}(n,q)}(S)/S$ is cyclic of order n, the group $N_G(C)/C$ must be cyclic of order dividing n.

We continue with the following.

Proposition 5.1. *Let S be a non-solvable group from the following list.*

(i) $\mathrm{SL}(n,q)$;
(ii) $\mathrm{GU}(n/2,q)$, $\mathrm{SU}(n/2,q)$ *with n even and $n/2$ odd;*
(iii) $\mathrm{Sp}(n,q)$, $\mathrm{GO}^-(n,q)$, $\mathrm{SO}^-(n,q)$, $\Omega^-(n,q)$ *with n even.*

There exists a universal constant $c > 0$ such that both $f(S)+1$ and $\mathfrak{r}_{\mathbb{Z}}(S)+2$ are larger than q^{cn}. In particular, $f(S) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(S) \to \infty$ as $|S| \to \infty$.

Proof. The group S can naturally be embedded in $G = \mathrm{GL}(n,q)$. Let C be a Singer subgroup in G. The group $H = S \cap C$ acts irreducibly on the underlying vector space by [24]. We have $C_G(H) = C$. On the other hand,

$$|N_S(H)/C_S(H)| \le |N_G(C)/C_G(C)| \le n.$$

We want to apply the inequality $f(S) \ge \sqrt{|H|}/(2n)$ from Lemma 2.3. For $n > 56$, we have $2n \le 2^{n/8}$ and $|H| \ge (q^{n/2}+1)/(q+1) \ge q^{n/2-2}$, thus $f(S) \ge q^{n/8-1} > q^{n/10}$. For $4 < n < 56$, the inequality $1 + bq^a \ge q^{ab}$ for $q > 1$, $a > 0$, and $0 < b < 1$ yields

$$f(S) + 1 \ge 1 + \frac{1}{112} q^{n/4-1} \ge 1 + \frac{1}{112} q^{n/20} \ge q^{n/2240}.$$

Finally, for $2 \le n \le 4$, we have (since case (ii) does not appear) $\sqrt{|H|}/(2n) \ge \sqrt{(q^{n/2}+1)/2}/8 > q^{n/4}/12$ and thus

$$f(S) + 1 \ge 1 + q^{n/4}/12 \ge q^{n/48}.$$

It follows by Lemma 2.3 that there exists a constant $c > 0$ such that both $f(S)+1$ and $\mathfrak{r}_{\mathbb{Z}}(S)+2$ are larger than q^{cn}. It also follows that $f(S) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(S) \to \infty$ as $|S| \to \infty$. □

We next pass from groups S to $\bar{S} = S/Z$ where Z denotes the center of S.

Lemma 5.2. *Let H be a cyclic subgroup in a finite group S. Assume that the center Z of S is contained in H. Let $\bar{H}$ and $\bar{S}$ denote the groups H/Z and S/Z. Then $N_{\bar{S}}(\bar{H})/C_{\bar{S}}(\bar{H})$ is isomorphic to a section of $N_S(H)/C_S(H)$.*

Proof. If $s \in C_S(H)$, then $sZ \in C_{\bar{S}}(\bar{H})$ and so $C_S(H)/Z$ is a subgroup of $C_{\bar{S}}(\bar{H})$. Let $sZ \in N_{\bar{S}}(\bar{H})$ and let h be a generator of H. Clearly,

$$(sZ)(hZ) = (h^m Z)(sZ)$$

for some $m \in \mathbb{Z}$. It follows that $s \in N_S(H)$ and so $N_{\bar{S}}(\bar{H})$ is a subgroup of $N_S(H)/Z$. The lemma follows. □

We continue with the following.

Proposition 5.3. *Let $\bar{S}$ be a non-abelian simple group from the following list.*

(i) $\mathrm{PSL}(n,q)$;
(ii) $\mathrm{PSU}(n/2,q)$ *with n even and $n/2$ odd;*
(iii) $\mathrm{PSp}(n,q)$, $\mathrm{P\Omega}^-(n,q)$ *with n even.*

There exists a universal constant $c > 0$ such that $f(\bar{S}) + 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) + 2$ are larger than q^{cn}. In particular, $f(\bar{S}) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \to \infty$ as $|\bar{S}| \to \infty$.

Proof. Let S be a non-solvable group from the list: $\mathrm{SL}(n,q)$, $\mathrm{SU}(n/2,q)$ with n even and $n/2$ odd, $\mathrm{Sp}(n,q)$ and $\Omega^-(n,q)$ with n even. Let H be as in the proof of Proposition 5.1.

The center Z of S is contained in H. Let $\bar{H} = H/Z$ and $\bar{S} = S/Z$. Now

$$|N_{\bar{S}}(\bar{H})/C_{\bar{S}}(\bar{H})| \leq |N_S(H)/C_S(H)|$$

by Lemma 5.2. Thus $|N_{\bar{S}}(\bar{H})/C_{\bar{S}}(\bar{H})| \leq n$ again by the proof of Proposition 5.1.

If $\bar{S} \neq \mathrm{PSU}(n/2,q)$, then $\frac{1}{4n}(q^{n/2}+1) \leq |H/Z|$.

If $\bar{S} = \mathrm{PSU}(n/2,q)$, then $(q^{n/2}+1)/(d(q+1)) \leq |H/Z|$ where d is the greatest common divisor of $n/2$ and $q+1$.

These two lower bounds and Lemma 2.3 imply that there exists a constant $c > 0$ such that $f(\bar{S}) + 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) + 2$ are larger than q^{cn}. It also follows that $f(\bar{S}) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \to \infty$ as $|\bar{S}| \to \infty$. □

Now we apply Lemma 2.3 to the groups $\bar{S}$ listed in the statement of Proposition 5.3, w. r. t. Singer subgroups H, in order to compute the parameters (n,q) for which $f(\bar{S}) \leq 4$ can hold.

If $\bar{S} = \mathrm{PSL}(n,q)$ is (non-abelian) simple and different from an alternating group, then $4n < \varphi\big((q^n-1)/(d(q-1))\big)$ where $d = (n, q-1)$ unless (n,q) is in

$$\{\ (2,7),(2,8),(2,11),(2,13),(2,17),(2,19),(2,23),(2,27),(2,29),(2,31),$$
$$(2,47),(2,59),(3,2),(3,3),(3,4),(4,3)\ \}.$$

All projective special linear groups with such exceptional parameters appear in the list of Theorem 1.3 (and thus all Galois orbits on the set of conjugacy classes have size at most 4 by Section 3), apart from $\bar{S} = \mathrm{PSL}(2,23)$, $\mathrm{PSL}(2,27)$, $\mathrm{PSL}(2,47)$, $\mathrm{PSL}(2,59)$ in which cases $f(\bar{S}) > 4$ by Proposition 3.1.

Let $\bar{S} = \mathrm{PSp}(n,q)$ be simple with $n \geq 4$ even. This group contains a cyclic subgroup of order $\frac{1}{d}(q^{n/2}+1)$ where $d = (2, q-1)$. We have $\varphi(\frac{1}{d}(q^{n/2}+1)) > 4n$ unless

$$(n,q) \in \{(4,3),(4,4),(4,5),(6,2),(6,3),(8,2),(10,2),(12,2)\}.$$

All arising exceptional groups appear in the list of Theorem 1.3 and all Galois orbits on the set of conjugacy classes have size at most 4 by Section 3.

Let $\bar{S} = \mathrm{PSU}(n/2,q)$ be simple with $n/2 \geq 3$ odd. This group contains a cyclic subgroup of order $\frac{q^{n/2}+1}{d(q+1)}$ where $d = (n/2, q+1)$. We have $\varphi(\frac{q^{n/2}+1}{d(q+1)}) > 2n$ unless

$$(n,q) \in \{\ (6,3),(6,4),(6,5),(10,2),(18,2)\ \}.$$

The first four groups arising appear in the list of Theorem 1.3 and the corresponding values for f are at most 4 by Section 3. The group $\mathrm{PSU}(9,2)$ satisfies $f(\mathrm{PSU}(9,2)) > 4$ by Proposition 3.1.

Let $\bar{S} = \mathrm{P\Omega}^-(n,q)$ be simple with $n \geq 8$ even. There is a cyclic subgroup of order $\frac{1}{d}(q^{n/2}+1)$ where $d = (2, q+1)$ in $\bar{S}$. We have $\varphi(\frac{1}{d}(q^{n/2}+1)) > 4n$ unless $(n,q) \in \{(8,2),(10,2),(12,2)\}$. The first two groups arising appear in the list of Theorem 1.3 and all Galois orbits on the set of conjugacy classes have size at most 4 by Section 3. The group $\mathrm{SO}^-(12,2)$ satisfies $f(\mathrm{SO}^-(12,2)) > 4$ by Proposition 3.1.

5.2. **Classical simple groups not containing irreducible cyclic subgroups.** In order to deal with the remaining simple classical groups, we need a lemma.

Lemma 5.4. *Let V be a vector space of dimension $n \geq 4$ defined over a finite field F. Let g be an element in $\mathrm{GL}(V)$ such that the $F\langle g\rangle$-module V may be decomposed as $V = U \oplus W$ where U and W are irreducible $F\langle g\rangle$-modules with the property that*

$$(\dim(U), \dim(W)) \in \{\ (n-1,1),\ (n-2,2)\ \}.$$

Then $|N_S(\langle g\rangle)/C_S(\langle g\rangle)| \leq 2n$ for any subgroup S of $\mathrm{GL}(V)$ with $g \in S$.

Proof. Let $C = \langle g\rangle$ and $G = \mathrm{GL}(V)$. We may assume that $S = G$. Let $h \in N_G(C)$. Since

$$Uh = (UC)h = U(Ch) = U(hC) = (Uh)C,$$

the vector space Uh is an FC-submodule of V. Similarly, Wh is also an FC-submodule of V.

Since C acts irreducibly on U and W, the induced actions are subgroups of Singer subgroups of $\mathrm{GL}(U)$ and $\mathrm{GL}(W)$. In particular, $|C|$ is coprime to $|F|$, hence the FC-module V is completely reducible and so

$$\{Uh,\ Wh\} = \{U,\ W\}.$$

It follows that the group $N_G(C)$ has a subgroup N of index at most 2 such that both U and W are FN-submodules of V. Let

$$(\dim(U), \dim(W)) \in \{\ (n-1,1),\ (n-2,2)\ \}$$

with $n > 4$. In this case $N_G(C) = N$. Let g_1 and g_2 be the projections of g on $\mathrm{GL}(U)$ and $\mathrm{GL}(W)$ respectively. The groups $C_{\mathrm{GL}(U)}(g_1)$ and $C_{\mathrm{GL}(W)}(g_2)$ are multiplicative groups of finite fields by Schur's lemma and Wedderburn's theorem. We have

$$|N_G(C)/C_G(C)| \leq |N_{\mathrm{GL}(U)}(\langle g_1\rangle)/C_{\mathrm{GL}(U)}(g_1)| \cdot |N_{\mathrm{GL}(W)}(\langle g_2\rangle)/C_{\mathrm{GL}(W)}(g_2)| \leq$$

$$\leq \max\{(n-1)\cdot 1\ ,\ (n-2)\cdot 2\} = 2(n-2).$$

If $\dim(U) = \dim(W) = 2$, then $|N/C_G(C)| \leq 4$ and so $|N_G(C)/C_G(C)| \leq 8$. □

Proposition 5.5. *Let $\bar{S}$ be a non-abelian simple group from the following list.*

(i) $\mathrm{PSU}(n/2, q)$ *with n divisible by 4;*
(ii) $\mathrm{P}\Omega(n, q)$ *with n odd;*
(iii) $\mathrm{P}\Omega^+(n, q)$ *with n even.*

There exists a universal constant $c > 0$ such that $f(\bar{S}) + 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) + 2$ are larger than q^{cn}. In particular, $f(\bar{S}) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \to \infty$ as $|\bar{S}| \to \infty$.

Proof. Let S be the group $\mathrm{SU}(n/2, q) \leq \mathrm{GL}(V)$ where n is divisible by 4 and V is the vector space of dimension $n/2$ defined over the field of size q^2 equipped with a non-singular conjugate-symmetric sesquilinear form. There is a non-singular subspace U of V of dimension $(n/2) - 1$. The vector space $W = U^{\perp}$ is a non-singular subspace of dimension 1 and $V = U \oplus W$ as vector spaces. Since $\dim(U)$ and $\dim(W)$ are both odd, there is an element $g \in S$ of maximal possible order by [24] such that $H = \langle g\rangle$ acts irreducibly on both U and W. Moreover we may choose g in such a way that H contains the center Z of S. Let $\bar{S} = S/Z$ and $\bar{H} = H/Z$. It follows that

$$|N_{\bar{S}}(\bar{H})/C_{\bar{S}}(\bar{H})| \leq |N_S(H)/C_S(H)| \leq n$$

by Lemmas 5.2 and 5.4. Now $\frac{1}{d}\left(q^{(n/2)-1} + 1\right) = |\bar{H}|$ where d denotes the greatest common divisor of the numbers $n/2$ and $q + 1$. There exists a constant $c_1 > 0$ such that $q^{c_1 n} < \frac{1}{2n}\varphi(|\bar{H}|) - 1$, by the paragraph preceding Lemma 2.3, provided that the right-hand side is larger than 1. Thus $f(\bar{S}) + 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) + 2$ are larger than $q^{c_1 n}$ by Lemma 2.3. In particular, $f(\bar{S}) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \to \infty$ as $|\bar{S}| \to \infty$.

Now we view V as a vector space of dimension n defined over the field of size q. Let V be equipped with a non-singular quadratic form. Let S be $\Omega(n, q) \leq \mathrm{GL}(V)$ with n and q odd, or let S be $\Omega^+(n, q) \leq \mathrm{GL}(V)$ with n even. As described in [33, p. 75], there are subgroups $\Omega^-(n-1, q) \times \Omega(1, q)$ and $\Omega^-(n-2, q) \times \Omega^-(2, q)$ in S, in the respective cases, preserving a decomposition $V = U \oplus W$ where U and W are non-singular subspaces of V with

$$(\dim(U), \dim(W)) \in \{\,(n-1, 1),\ (n-2, 2)\,\}.$$

Let S be any of the orthogonal groups considered in this proof. Let $\bar{S} = S/Z$ where Z is the center of S. As in the previous paragraph, there is a cyclic group H with

$Z \leq H \leq S$ such that H acts irreducibly on both subspaces U and W and

$$|N_{\bar{S}}(\bar{H})/C_{\bar{S}}(\bar{H})| \leq 2n$$

where $\bar{H} = H/Z$. We have $\frac{1}{4}\left(q^{(n-2)/2}+1\right) \leq |\bar{H}|$. There exists a constant $c_2 > 0$ such that $q^{c_2 n} < \frac{1}{4n}\varphi(|\bar{H}|) - 1$, by the paragraph preceding Lemma 2.3, provided that the right-hand side is larger than 1. Thus $f(\bar{S}) + 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) + 2$ are larger than $q^{c_2 n}$ by Lemma 2.3. In particular, $f(\bar{S}) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \to \infty$ as $|\bar{S}| \to \infty$.

Finally, let c be the minimum of c_1 and c_2. □

Now we apply Lemma 2.3 to the groups $\bar{S}$ listed in the statement of Proposition 5.5, w. r. t. the subgroups H that were chosen in the proof of that proposition, in order to compute the parameters (n, q) for which $f(\bar{S}) \leq 4$ can hold.

Let $\bar{S}$ be as in the statement of Proposition 5.5.

Let $\bar{S} = \mathrm{PSU}(n/2, q)$ with $n \geq 8$ divisible by 4. This group contains a cyclic subgroup of order divisible by $\frac{1}{d}(q^{(n/2)-1} + 1)$ where $d = (n/2, q+1)$. We have

$$\varphi\left(\tfrac{1}{d}(q^{(n/2)-1} + 1)\right) > 4n$$

unless $(n, q) \in \{(8, 2), (8, 3), (12, 2)\}$. Since $\mathrm{PSU}(4, 2) \cong \mathrm{PSp}(4, 3)$, all three arising exceptional groups $\bar{S}$ satisfy $f(\bar{S}) \leq 4$ by Section 3 and appear in the list of Theorem 1.3.

Let $\bar{S} = \mathrm{P}\Omega(n, q)$ be simple with $n \geq 7$ and q both odd. This group contains a cyclic subgroup of order divisible by $\frac{1}{2}(q^{(n-1)/2} + 1)$. We have

$$\varphi\left(\tfrac{1}{2}(q^{(n-1)/2} + 1)\right) > 8n$$

unless $(n, q) \in \{(7, 3), (7, 5), (9, 3), (11, 3)\}$. We have $f(\mathrm{P}\Omega(7, 3)) \leq 4$ by Section 3. The remaining three groups $\bar{S}$ satisfy $f(\bar{S}) > 4$ by Proposition 3.1.

Finally, let $\bar{S} = \mathrm{P}\Omega^+(n, q)$ with $n \geq 8$ even. This group contains a cyclic subgroup of order divisible by $\frac{1}{d}(q^{(n-2)/2} + 1)$. We have

$$\varphi\left(\tfrac{1}{d}(q^{(n-2)/2} + 1)\right) > 8(n-2)$$

by the proof of Lemma 5.4, where $d = (2, q+1)$ unless

$$(n, q) \in \{(8, 2), (8, 3), (8, 4), (8, 5), (10, 2), (10, 3), (12, 2), (12, 3), (14, 2), (16, 2)\}.$$

The first two groups $\bar{S}$ arising, together with $\bar{S} = \Omega^+(12, 2)$, satisfy $f(\bar{S}) \leq 4$ by Section 3 and appear in the list of Theorem 1.3. All other arising groups $\bar{S}$, apart from $\Omega^+(12, 2)$, satisfy $f(\bar{S}) > 4$ by Proposition 3.1.

This finishes the proof of the asymptotic part of Theorem 1.2 and the proof of Theorem 1.3 in case G is a classical group.

It remains to show Theorem 1.1 for classical groups. The content of Section 3 shows that if G is a simple classical group appearing in the list of the statement of Theorem 1.1 or in the list of the statement of Theorem 1.3 then Theorem 1.1 is true

for the group G. Let G be a simple classical group not appearing in these lists. We must show that $\mathfrak{r}_{\mathbb{Z}}(G) > 1$. We have $f(G) > 4$ by Theorem 1.3. We conclude that $\mathfrak{r}_{\mathbb{Z}}(G) \geq f(G)/2 - 1 > 1$ by the paragraph after Proposition 2.2.

6. Simple groups of Lie type

An aim of this section is to complete the proofs of Theorems 1.3 and 1.1 by dealing with the remaining class of finite simple groups, the exceptional simple groups of Lie type.

The next proposition is a consequence of Tables I and II in the paper [9] of Babai, Pálfy and Saxl.

Proposition 6.1. *Let $\bar{S}$ be an exceptional simple group of Lie type defined over the field of size q or the Tits group ${}^2\mathrm{F}_4(2)'$. Then $f(\bar{S}) \leq 4$ if and only if*

$$\bar{S} \in \{\ {}^3\mathrm{D}_4(2),\ {}^2\mathrm{E}_6(2),\ \mathrm{F}_4(2),\ \mathrm{G}_2(3),\ \mathrm{G}_2(4),\ {}^2\mathrm{B}_2(8),\ {}^2\mathrm{F}_4(2)'\ \}.$$

It follows that $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \geq 2$ unless $\bar{S} \in \{{}^2\mathrm{E}_6(2), \mathrm{F}_4(2), \mathrm{G}_2(3)\}$ when $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) = 1$. Moreover, $f(\bar{S}) + 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) + 2$ are larger than q^c for some universal constant $c > 0$. In particular, if $|\bar{S}| \to \infty$, then $f(\bar{S}) \to \infty$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \to \infty$.

Proof. Tables I and II in [9] give information about cyclic tori T in exceptional groups $\bar{S}$ of Lie type including the Tits group $\bar{S} = {}^2\mathrm{F}_4(2)'$. The groups T satisfy $C_{\bar{S}}(T) = T$ and the middle columns in the tables provide $|T|$. The $|T|$ are polynomials in q where q is the size of the field of definition for $\bar{S}$. The exact values of $|N_{\bar{S}}(T)/T|$ are also provided in [9, Tables I and II]. All such entries are at most 30. The third and fourth statements of the proposition follow from Lemma 2.3.

Also, [9, Tables I and II] shows that for every $\bar{S}$ there is a T such that $4|N_{\bar{S}}(T)/T| < \varphi(|T|)$ unless

$$\bar{S} \in \{\ {}^3\mathrm{D}_4(2),\ {}^2\mathrm{E}_6(2),\ \mathrm{F}_4(2),\ \mathrm{G}_2(3),\ \mathrm{G}_2(4),\ {}^2\mathrm{B}_2(8),\ {}^2\mathrm{F}_4(2)'\ \}.$$

These seven groups $\bar{S}$ satisfy $f(\bar{S}) \leq 4$ by Section 3. The first statement now follows from Lemma 2.3. Moreover, among these seven groups only ${}^2\mathrm{E}_6(2)$, $\mathrm{F}_4(2)$ and $\mathrm{G}_2(3)$ satisfy $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) = 1$ and $\mathfrak{r}_{\mathbb{Z}}(\bar{S}) \geq 2$ for the others, by Section 3. The second statement follows. □

The other aim of this section is to summarize some of our results on simple groups of Lie type.

Proposition 6.2. *There exists a universal constant $c > 0$ such that whenever G is a finite simple group of Lie type of Lie rank r defined over the field of size q then $\mathfrak{r}_{\mathbb{Z}}(G) > q^{cr}$ provided that $\mathfrak{r}_{\mathbb{Z}}(G) > 1$.*

Proof. This follows from Propositions 5.3, 5.5 and 6.1. □

7. Alternating groups

As a continuation of [26], Patay, in his unpublished master's thesis written around 1975 at Uzhgorod University, was first to consider the structure of central units of $\mathbb{Z}A_n$ in the case when A_n is the alternating group of degree n.

By results of Frobenius [19] and formula (1), the number $\mathfrak{r}_{\mathbb{Z}}(A_n)$ is equal to the number of partitions $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n that satisfy the following conditions: (a) λ_i is odd, $1 \le i \le k$; (b) the λ_i are pairwise distinct; (c) $n \equiv k \pmod 4$; (d) $\prod_{i=1}^{k} \lambda_i$ is not a square. This fact was well-known in the 1970's and it was used by Patay to classify groups A_n with $\mathfrak{r}_{\mathbb{Z}}(A_n) = 0$.

There is an "experimental formula" in [6, p. 166] for the behavior of $\mathfrak{r}_{\mathbb{Z}}(A_n)$ for large n. Here we prove a weaker statement.

Proposition 7.1. *If $n \ge 26$, then $\mathfrak{r}_{\mathbb{Z}}(A_n) > c^{\sqrt{n}}$ for some universal constant $c > 1$.*

Proof. Let n be an integer at least 26. Then $\mathfrak{r}_{\mathbb{Z}}(A_n) > 1$ by [6]. In order to prove the claim, we may assume that n is sufficiently large. Let i be the integer such that $0 \le i \le 5$ and $n + i$ is divisible by 6. By [22, Lemma 2], there is a prime p between $3\frac{n+i}{6}$ and $4\frac{n+i}{6}$. Thus $n/2 < p < 2n/3 + 4$. Choose an integer k that is congruent to n modulo 4 such that $|k - (\sqrt{p}/10)|$ is as small as possible. Let m be the integer satisfying

$$2m + k^2 - 1 = n - p.$$

By our condition $p < 2n/3 + 4$ and the definition of k, we have $m > n/10$ provided that n is sufficiently large.

The number of $(k-1)$-tuples $(x_1, \ldots, x_{k-1})$ of positive integers $x_1, \ldots, x_{k-1}$ such that $m = x_1 + \cdots + x_{k-1}$ is $\binom{m-1}{k-2}$. There are at most $(k-1)!$ ways to order the x_i. Thus the number of partitions of m into exactly $k-1$ parts is at least

$$\tfrac{1}{(k-1)!}\binom{m-1}{k-2} \ge \left(\tfrac{1}{k-1}\right)^{k-2}\left(\tfrac{m-1}{k-2}\right)^{k-2}.$$

This is at least $c^{\sqrt{n}}$ for some constant $c > 1$, provided that n is sufficiently large, by the following estimations.

We have $k - \sqrt{p}/10 < 4$ and thus $10(k-4) < \sqrt{p} < \sqrt{2n/3 + 4}$, which implies $n > 150(k-4)^2 - 6$. We get $m > n/10 > 15(k-4)^2 - 3/5$ and thus $\frac{m-1}{(k-1)(k-2)} > \frac{15(k-4)^2 - 8/5}{(k-1)(k-2)}$, which is larger than 2 if $k > 5$ holds. A lower bound of the form $c^{\sqrt{n}}$ for 2^{k-2} arises from the fact that $k \ge \sqrt{p}/10 - 4 > \sqrt{n/2}/10 - 4$ holds.

We claim that $\mathfrak{r}_{\mathbb{Z}}(A_n)$ is at least the number of partitions of m into exactly $k-1$ parts. For this we use the description of certain partitions found before the statement of this proposition.

Let π be a partition of m into exactly $k-1$ parts. For each i with $1 \le i \le k-1$, add i to the i-th smallest part in π. Let the resulting partition be π'. Now multiply

each part of π' by 2 and add 1. Let the resulting partition be π''. Finally, add a part equal to p to π'' to obtain the partition π'''. This is a partition of $p+2m+k^2-1=n$ into exactly k parts each of distinct odd lengths such that the product of the parts is not a square (since p divides this number but p^2 does not). Finally, if π_1 and π_2 are partitions of m into exactly $k-1$ parts providing the partition π''' in the described way, then $\pi_1=\pi_2$. □

8. Proof of Theorem 1.2

Let $k(G)$ denote the number of conjugacy classes of the finite group G. This is equal to the number of complex irreducible characters of G. For any finite group G we have $\mathfrak{r}_{\mathbb{Z}}(G) < k(G)$ by (1). The theorem is true for G a cyclic group of prime order, again by (1).

In order to prove our statement, we may assume that G is a sufficiently large non-abelian finite simple group. In particular, we may assume that G is not a sporadic simple group. Thus G is an alternating group or a simple group of Lie type. The last statement follows from Propositions 7.1 and 6.2 (together with [11, Theorem 5.1] and Theorem 1.1).

We have $k(A_n) < d^{\sqrt{n}}$ for some universal constant $d > 1$ by classical results on the number of partitions of n. If G is a finite simple group of Lie type of Lie rank r defined over the field of size q, then $k(G) \leq (6q)^r < q^{4r}$ by [27, Theorem 1]. (For an improvement of this latter bound see [20].) From these and Propositions 7.1 and 6.2 it follows that there exists a universal constant $c' > 0$ such that $k(G)^{c'} < \mathfrak{r}_{\mathbb{Z}}(G)$ for any finite simple group G with $\mathfrak{r}_{\mathbb{Z}}(G) > 1$.

Acknowledgement

We thank Rifkhat Z. Aleev for some discussions on this topic especially during the preparation of the first version of this paper.

References

[1] Alavi, S. H.; Daneshkhah, A. On semi-rational finite simple groups. *Monatsh. Math.* **184** (2017), no. 2, 175–184.

[2] Aleev, R. Z. Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers. *Internat. J. Algebra Comput.* **4** (1994), no. 3, 309–358.

[3] Aleev, R. Zh. Central units of integral group rings of finite groups. (Russian) *Dokl. Akad. Nauk.* **369** (1999), no. 2, 151–152.

[4] Aleev, R. Z. Central units of integral group rings of finite groups. *Thesis of Doctor of Sciences*, Chelyabinsk:355, 2000.

[5] Aleev, R. Z.; Ishechkina, N. B. A theory of central unit groups of integral group rings of groups $Sz(q)$. *Proc. Steklov Inst. Math.* 2001, Algebra. Topology, suppl. 2, S1–S15.

[6] Aleev, R. Z.; Kargapolov, A. V.; Sokolov, V. V. The ranks of central unit groups of integral group rings of alternating groups. *J. Math. Sci.* **164** (2010), no. 2, 163–167.

[7] Aleev, R. Zh.; Panina, G. A. The units of cyclic groups of orders 7 and 9. (Russian) *Izv. Vyssh. Uchebn. Zaved. Mat.* 1999, no. 11, 81–84.
[8] Artamonov, V. A.; Bovdi, A. A. Integral group rings: groups of invertible elements and classical K-theory. Translated in *J. Soviet Math.* **57** (1991), no. 2, 2931–2958. *Itogi Nauki i Tekhniki, Algebra.* Topology. Geometry, Vol. 27, 3–43, **232**, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989.
[9] Babai, L.; Pálfy, P. P.; Saxl, J. On the number of p-regular elements in finite simple groups. *LMS J. Comput. Math.*, **12** (2009), 82–119.
[10] Bächle, A. Integral group rings of solvable groups with trivial central units. *Forum Math.* **30** (2018), no. 4, 845–855.
[11] Bächle, A.; Caicedo, M.; Jespers, E.; Maheshwary, S. Global and local properties of finite groups with only finitely many central units in their integral group ring. ArXiv:1808.03546.
[12] Bakshi, G. K.; Maheshwary, S.; Passi, I. B. S. Integral group rings with all central units trivial. *J. Pure Appl. Algebra* **221** (2017), no. 8, 1955–1965.
[13] Bakshi, G. K.; Maheshwary, S.; Passi, I. B. S. Group rings and the RS property. *Comm. Algebra* **47** (2019), no. 3, 969–977.
[14] Bereczky, Á. Maximal overgroups of Singer elements in classical groups. *J. Algebra*, **234** (2000), no. 1, 187–206.
[15] Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.
[16] Bovdi, A. A. The multiplicative group of an integral group ring. (Mul'tiplikativnaya gruppa tselochislennogo gruppovogo kol'tsa.) Uzhgorod: Uzhgorodskij Gosudarstvennyj Universitet. Kod GASNTI 27.17.19, 1987, pages 210.
[17] Breuer, T. The GAP Character Table Library, Version 1.2.2, (http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib), Mar 2013, GAP package.
[18] Feit, W.; Seitz, G. M. On finite rational groups and related topics. *Illinois J. Math.* **33** (1989), no. 1, 103–131.
[19] Frobenius, G. Über die Charactere der alternierenden Gruppe. Sitzungsberichte der Berl. Ak, 1901, S. 303–315.
[20] Fulman, J.; Guralnick, R. M. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023–3070.
[21] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.0*; 2018, (https://www.gap-system.org).
[22] Hanson, D. On a theorem of Sylvester and Schur. *Canad. Math. Bull.* **16** (1973), 195–199.
[23] Huppert, B. Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967.
[24] Huppert, B. Singer-Zyklen in klassischen Gruppen. *Math. Z.* **117** (1970), 141–150.
[25] Isaacs, I. M. Character theory of finite groups. Pure and Applied Mathematics, No. 69, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976.
[26] Jucys, A. A. A. Symmetric polynomials and the center of the symmetric group ring. *Rep. Mathematical Phys.* **5** (1974), no. 1, 107–112.
[27] Liebeck, M. W.; Pyber, L. Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997), no. 2, 538–562.
[28] Molodorich, M. I. Class character rings of sporadic groups. *Sib. Elektronic Math. Rep.* **11** (2014), 878–886.

[29] Patay, Z. F. On the center of the multiplicative group of an integral group ring. Material of young mathematicians. Note of the Scientific Center of *Akad. Nauk Ukrain. SSR*, Uzhgorod University, 35–41, 1975. *Dep. VINITI, 18.05.76* N: 1734-76 DEP.
[30] Patay, Z. F. The multiplicative group of a group ring. Studies in the qualitative theory of differential equations and its applications, pp. 47–48, **75**, *Akad. Nauk Ukrain. SSR*, Inst. Mat., Kiev, 1978.
[31] Sandling, R. Graham Higman's thesis "Units in Group Rings". 93–116 in Integral representations and applications (Oberwolfach, 1980), Springer Lecture Notes 882, Springer Berlin-New York, 1981.
[32] Trefethen, S. Non-Abelian composition factors of finite groups with the CUT-property. *J. Algebra* **522** (2019), 236–242.
[33] Wilson, R. A. The finite simple groups. Graduate Texts in Mathematics, 251. Springer-Verlag London, Ltd., London, 2009.

Department of Mathematical Sciences, UAEU, Al-Ain, United Arab Emirates
E-mail address: vbovdi@gmail.com

Lehrstuhl D für Mathematik, RWTH Aachen University, 52065 Aachen, Germany
E-mail address: sam@math.rwth-aachen.de

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
E-mail address: maroti.attila@renyi.mta.hu