Finite Simple Groups with Few Orbits under Automorphisms

Markus Stroppel

Mathematisches Institut B, Universität Stuttgart, D-70550 Stuttgart, Germany
E-mail: stroppel@mathematik.uni-stuttgart.de

We determine the finite simple groups whose group of automorphisms acts with at most 5 orbits: this characterizes the projective special linear groups of degree 2 over fields with at most 9 elements.

The following notes contain a characterization of the groups $\mathrm{PSL}\,(2,f)$ for $f \in \{4,5,7,8,9\}$ by the fact that they are finite simple groups whose automorphism group has at most 5 orbits. The classification of finite simple groups is not used in the proof. Using the classification, one could get a much shorter proof, cf. 4.3 below, or see [17] 4.5.

1. INTRODUCTION.

Let G be a finite simple (nonabelian) group. We denote by $\omega\,(G)$ the number of orbits under $\mathrm{Aut}\,(G)$. It has been observed in [16] 2.3 that $\omega\,(G) = 4$ characterizes the smallest example: $G \cong \mathrm{Alt}_5$. In this note, we concentrate on the case $\omega\,(G) = 5$. It turns out that this characterizes the groups $\mathrm{PSL}\,(2,7) \cong \mathrm{PSL}\,(3,2)$, $\mathrm{PSL}\,(2,8)$, and $\mathrm{PSL}\,(2,9) \cong \mathrm{Alt}_6$, see 4.2 below. The groups $\mathrm{PSL}\,(2,2)$ and $\mathrm{PSL}\,(2,3)$ are not simple, whereas $\mathrm{PSL}\,(2,4)$ and $\mathrm{PSL}\,(2,5)$ are both isomorphic to Alt_5. Thus the condition $\omega\,(G) \le 5$ singles out the groups $\mathrm{PSL}\,(2,f)$ with $4 \le f \le 9$ among the finite simple groups.

The effect of bounds on $\omega\,(G)$ has been investigated for different classes of groups; see [14] and [15].

General Assumption. Throughout, we consider a finite simple group G with $\omega\,(G) \le 5$. According to Burnside's $p^\alpha q^\beta$-Theorem (cp. [6] 4.3.3), the order of G has at least 3 prime divisors; say t, p, q, where t is chosen minimally. Picking elements of order $1, t, p$, and q, respectively, we obtain representatives for four of the five orbits. The elements in the remaining orbit all have the same order r.

Since no other orders apart from $1, t, p, q, r$ can occur, we obtain:

LEMMA 1.1. *Either r is a prime ($which\ may\ belong\ to$ $\{t,p,q\}$), or it belongs to the set $r \in \{t^2, tp, tq, p^2, pq, q^2\}$.* ∎

The different possibilities for r will be studied separately. That is, we will concentrate first on the case where r is a power of a prime (and G has no elements of mixed order), then we will study the cases where G contains elements of odd mixed order, or of even mixed order.

The Odd Order Theorem [4] asserts $t = 2$. However, parts of our considerations will be independent of that deep result. In particular, we will mostly deal with *CN*-groups; that is, groups where every nontrivial element has nilpotent centralizer. As a forerunner to the Odd Order Theorem, it has been shown by W. Feit, M. Hall and J.G. Thompson [3] that every *CN*-group of odd order is solvable; compare [6] 14.3.1. Later on, we will also need M. Suzuki's classification of simple *CN*-groups (see [18] and [19]). Another case is dealt with by an application of an old characterization of $\mathrm{SL}\,(2, 2^n)$ by Burnside [1], or alternatively, by Suzuki's results on *C*-groups (where centralizers of involutions have a normal Sylow 2-subgroup). Finally, we apply D. Gorenstein's result about groups with abelian Sylow 2-subgroups and solvable centralizers of involutions [5]. For groups that are not *CN*-groups, we need the Odd Order Theorem [4]. Of course, Gorenstein's result could also be used at an early stage, but it appears reasonable to use weaker methods where these are sufficient. The reader may also note that we deal with simple groups with abelian Sylow 2-subgroups in almost all cases. These groups were classified by J.H. Walter [22], but we do not use that classification (involving, apart from certain projective special linear groups, the Ree groups and the sporadic group J(11) discovered by Janko). Compare [6] p. 484 for a discussion of that classification.

A large part of the present paper deals with groups whose order has only three prime divisors. According to a result of M. Herzog's [8], this condition singles out the groups $\mathrm{PSL}\,(2, f)$ (with $f \in \{4, 5, 7, 8, 9, 17\}$), $\mathrm{PSL}\,(3, 3)$, $\mathrm{PSU}\,(3, 3)$, and $\mathrm{PSU}\,(4, 2)$. Herzog has only considered the finite simple groups that were known in 1968, but the classification of finite simple groups shows that his list is complete. We do not use the classification of finite simple groups in the present paper.

Recently, groups with solvable 2-local subgroups have been investigated by M. Hayashi and Y. Tanaka, see [7]. It does not come as a surprise that the class of groups characterized in [7] has large intersection with the class of groups that we have to consider. However, the results (and methods) of that paper are not used in the present investigation.

2. GROUPS WITHOUT ELEMENTS OF MIXED ORDER.

The case where r is a prime or belongs to $\{p^2, q^2\}$ is comparatively easy, it leads immediately to *CN*-groups:

LEMMA 2.1. *Let H be a finite group where every nontrivial element has prime power order. Then H is a CN-group. If there are no elements of order 4 then the Sylow 2-subgroups are elementary abelian.*

Proof. If every element of $H\setminus\{1\}$ has prime power order then commuting elements are contained in Sylow subgroups, and H is a *CN*-group. Nonexistence of elements of order 4 implies that the Sylow 2-subgroups have exponent 2 and are therefore (elementary) abelian. ∎

M. Suzuki has determined the simple *CN*-groups; see [18] and [19]. If such a group has abelian Sylow 2-subgroups, it is isomorphic to one of the groups $\mathrm{PSL}\,(2, 2^n)$, where $n \geq 2$; compare [6] 14.4.1. Here $\mathrm{PSL}\,(n, f) := \mathrm{SL}\,(n, f)\,/\mathrm{Z}(\mathrm{SL}\,(n, f))$ denotes the quotient of the group $\mathrm{SL}\,(n, f)$ of $n \times n$ matrices of determinant 1 over the field $\mathrm{GF}(f)$ with f elements by the center $\mathrm{Z}(\mathrm{SL}\,(n, f))$. The group $\mathrm{PSL}\,(n, f)$ is denoted by $L_n(f)$ in [6]. Note also that $\mathrm{PSL}\,(2, 2^n) = \mathrm{SL}\,(2, 2^n)$ because the center is trivial.

EXAMPLES 2.2. *For* $\mathrm{Alt}_5 \cong \mathrm{PSL}\,(2, 4) \cong \mathrm{PSL}\,(2, 5)$ *we have* $\omega\,(\mathrm{Alt}_5) = 4$*, and* $\mathrm{PSL}\,(2, 8)$ *satisfies* $\omega\,(\mathrm{PSL}\,(2, 8)) = 5$.

Proof. The elements of Alt_5 have orders $1, 2, 3$, and 5 respectively. It is well known that elements of the same order in Alt_5 are conjugates under Sym_5 because they have the same type. The isomorphisms $\mathrm{PSL}\,(2, 4) \cong \mathrm{Alt}_5 \cong \mathrm{PSL}\,(2, 5)$ are obtained by observing that $\mathrm{PSL}\,(2, 4)$ and $\mathrm{PSL}\,(2, 5)$ have 5 Sylow 2-subgroups, compare [9] II 6.14.

Regarding $\mathrm{PSL}\,(2, 8) = \mathrm{SL}\,(2, 8)$, we have to work a little harder. The order of that group is $2^3 \cdot 3^2 \cdot 7$. I claim that the elements have order $1, 2, 3, 9$, and 7, respectively, and that elements of the same order belong to the same conjugacy class in the group $\Gamma\mathrm{L}(2, 8) := \mathrm{Aut}\,(\mathrm{GF}(8)) \ltimes \mathrm{GL}_2 8$.

The group

$$T := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \;\middle|\; x \in \mathrm{GF}(8) \right\}$$

of transvections is a Sylow 2-subgroup of $\mathrm{SL}\,(2, 8)$. Every nontrivial element of T has order 2, and the transvections in $\mathrm{SL}\,(2, 8)$ form a single conjugacy class in $\mathrm{GL}_2 8$. Considering the rational canonical form (compare [11] pp. 194–200), we infer that each element of order 3 in $\mathrm{SL}\,(2, 8)$ is a conjugate of

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Similarly, we obtain that elements of order 9 in $\mathrm{SL}\,(2, 8)$ are conjugates of

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix},$$

where a is a root of $X^3 + X + 1$ in $\mathrm{GF}(8)$. Since the roots of that polynomial are permuted transitively by $\mathrm{Aut}\,(\mathrm{GF}(8))$, we have that the elements of order 9 in $\mathrm{SL}\,(2,8)$ form a single conjugacy class in $\Gamma\mathrm{L}(2,8)$. Finally, the elements of order 7 have rational canonical form

$$\begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix},$$

where b is a root of $X^3 + X^2 + 1$ in $\mathrm{GF}(8)$. Again, the different roots of that polynomial form an orbit under $\mathrm{Aut}\,(\mathrm{GF}(8))$.

We still have to show that each element of $\mathrm{SL}\,(2,8)$ has prime power order. Let x be any element in $\mathrm{SL}\,(2,8)$ whose order is not a power of 3. Then x centralizes an element y (a suitable power of x) of prime order $s \neq 3$. If $s = 2$ then x is contained in the centralizer of a transvection, and thus in a Sylow 2-subgroup. For $s = 7$, the element y is a conjugate of

$$A := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

where a is a generator of the multiplicative group of $\mathrm{GF}(8)$. The centralizer of A in $\mathrm{SL}\,(2,8)$ consists of diagonal matrices: that is, the centralizer is just the group generated by A, and has order 7. ▮

THEOREM 2.3. *Let G be a finite simple group with $\omega\,(G) \leq 5$. If every element in $G\backslash\{1\}$ has prime power order and the Sylow 2-subgroups are abelian then either $G \cong \mathrm{PSL}\,(2,4)$ (and $\omega\,(G) = 4$), or $G \cong \mathrm{PSL}\,(2,8)$ (and $\omega\,(G) = 5$).*

Proof. According to Lemma 2.1 and Suzuki's result about *CN*-groups with abelian Sylow 2-subgroups, we have to consider the group $\mathrm{PSL}\,(2,2^n)$ for $n \geq 2$. This group contains cyclic subgroups of order $2^n - 1$ and $2^n + 1$, respectively; see [6] 2.8.3. One of these numbers is divisible by 3. As there are no elements of mixed order in G, that number is in fact equal to 3 or to 3^2. From $3 \in \{2^n - 1, 2^n + 1\}$ we conclude $3 = 2^n - 1$ and $G \cong \mathrm{PSL}\,(2,4)$. As $3^2 + 1$ is not a power of 2, there remains the case $3^2 = 2^n + 1$ and $G \cong \mathrm{PSL}\,(2,8)$. ▮

Thus we know the simple groups G with $\omega\,(G) \leq 5$ and $r \in \{t, p, q, p^2, q^2\}$. We turn to the case $r = t^2$; then we still know that G is a *CN*-group, and $t = 2$. However, the Sylow 2-subgroups need no longer be abelian. We need M. Suzuki's results from [18] and [19]:

THEOREM 2.4. *Let G be a nonsolvable CN-group. Then G is isomorphic to one of the groups $\mathrm{Sz}(2^{2m+1})$, $\mathrm{PSL}\,(2,2^n)$, $\mathrm{PSL}\,(2,p)$, $\mathrm{PSL}\,(2,9)$, or $\mathrm{PSL}\,(3,4)$, where $m \geq 1$, $n \geq 2$, and p is a Fermat or a Mersenne prime.* ▮

Recall that Fermat primes are primes of the form $2^{(2^n)} + 1$; and Mersenne primes are primes of the form $2^n - 1$. For $s = 2^{2m+1}$, the group $\mathrm{Sz}(s)$ is the so-called *Suzuki group* of order $(s^2+1)s^2(s-1)$ which should not be confused with the sporadic simple group found by M. Suzuki. See [10] XI §3 or Sections 21, 22, and 24 in [12] for a discussion of these groups and their subgroups.

EXAMPLE 2.5. *The group* $\mathrm{PSL}\,(2,9)$ *satisfies* $\omega\,(\mathrm{PSL}\,(2,9)) = 5$.

Proof. The order of $\mathrm{PSL}\,(2,9)$ is $\frac{(9^2-1)(9^2-9)}{(9-1)2} = 2^3\cdot 3^2\cdot 5$. A Sylow 3-subgroup is represented by the elementary abelian group of transvections

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \,\middle|\, x \in \mathrm{GF}(9) \right\}.$$

Sylow 2-subgroups are dihedral: in fact, taking a generator a of the multiplicative group of the Galois field $\mathrm{GF}(9)$ we obtain the element

$$Q := \pm \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{PSL}\,(2,9)$$

of order 4, and notice that the involution

$$J := \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{PSL}\,(2,9)$$

satisfies $J^{-1}QJ = Q^{-1}$. Thus $\mathrm{PSL}\,(2,9)$ contains elements of order $1, 2, 4, 3$, and 5, respectively. I claim that elements of the same order in $\mathrm{PSL}\,(2,9)$ are conjugates in the group $\Gamma\mathrm{L}(2,9) = \mathrm{Aut}\,(\mathrm{GF}(9)) \ltimes \mathrm{GL}_2 9$ of all semilinear bijections of $\mathrm{GF}(9)^2$.

The field $\mathrm{GF}(9)$ is obtained by adjoining an element i with $i^2 = -1$ to $\mathrm{GF}(3)$. The Galois group $\mathrm{Aut}\,(\mathrm{GF}(9))$ is generated by the involution $x+iy \mapsto (x+iy)^3 = \overline{x+iy} := x - iy$. The relevant cyclotomic polynomials split over $\mathrm{GF}(9)$ as

$$\begin{aligned} X^5 - 1 &= (X-1)(X^2+bX+1)(X^2+\bar{b}X+1) \quad \text{and} \\ X^8 - 1 &= (X-1)(X+1)(X-i)(X+i)(X-a)(X+a)(X-\bar{a})(X+\bar{a}) \end{aligned}$$

where $b = -1-i$ and $\bar{b} = -1+i$; the element a is still a generator of the multiplicative group of $\mathrm{GF}(9)$ (and satisfies $a^2 \in \{i, -i\}$). Every element of order 5 in $\mathrm{PSL}\,(2,9)$ is of the form $\pm M$ for some matrix $M \in \mathrm{SL}\,(2,9)$ of order 5. The characteristic polynomial χ_M of M divides X^5-1. Therefore, we have $\chi_M(X) = X^2 + cX + 1$ with $c \in \{b, \bar{b}\}$, and a change of basis (that is, conjugation in $\mathrm{GL}_2 9$) yields

$$M = \begin{pmatrix} 0 & 1 \\ -1 & -c \end{pmatrix}.$$

The two conjugacy classes in $\mathrm{GL}_2 9$ are fused under $\mathrm{Aut}\,(\mathrm{GF}(9))$.

Any element of order 2 in $\mathrm{PSL}\,(2,9)$ is represented by a matrix of order 2 or 4 in $\mathrm{SL}\,(2,9)$. As the only involution in $\mathrm{SL}\,(2,9)$ is the central one, we infer that involutions in $\mathrm{PSL}\,(2,9)$ are induced by matrices with eigenvalues that are roots of $X^2+1=(X-i)(X+i)$. We obtain that this matrix is a conjugate of J. Elements of order 4 are represented by matrices with eigenvalues that are primitive roots of X^8-1. This leads to conjugates of $\pm Q$ and $\pm Q^{-1}$. Again, the two conjugacy classes under $\mathrm{GL}_2 9$ are fused under $\mathrm{Aut}\,(\mathrm{GF}(9))$.

The elements of order 3 are the (nontrivial) transvections, which form a single conjugacy class in $\mathrm{GL}_2 9$.

Finally, we have to show that there are no elements of mixed order in $\mathrm{PSL}\,(2,9)$. An easy way to do this is to consider the group Alt_6 which is isomorphic to $\mathrm{PSL}\,(2,9)$; compare [9] II 6.14. One could also proceed as in the proof of 2.2. ∎

REMARK 2.6. The fact that all elements of order 3 (those with and those without fixed points) belong to a single orbit under $\mathrm{Aut}\,(\mathrm{Alt}_6)$ reflects the fact that Alt_6 admits an automorphism that is *not* induced by an inner automorphism of Sym_6. The group Alt_6 is characterized among all alternating groups by the existence of such an unexpected automorphism, compare [13].

LEMMA 2.7. *No simple Suzuki group* $\mathrm{Sz}(2^{2m+1})$ *satisfies* $\omega\left(\mathrm{Sz}(2^{2m+1})\right)\le 5$.

Proof. The assertion follows easily using the facts that $\mathrm{Sz}(2^{2m+1})$ contains cyclic groups of orders 4, $2^{2m+1}-1$, $2^{2m+1}+2^{m+1}+1$, and $2^{2m+1}-2^{m+1}+1$, respectively; compare [10] XI 3.10 or [12] 24.7. Thus $\omega\left(\mathrm{Sz}(2^{2m+1})\right)\le 5$ implies that two of these numbers coincide. One easily sees that this implies $m=0$. But $\mathrm{Sz}(2)$ has order 20 and is not simple. ∎

LEMMA 2.8. *For each natural number* $n\ge 2$ *we have* $\omega\,(\mathrm{PSL}\,(3,2^n))>5$.

Proof. This group contains a subgroup isomorphic to $\mathrm{SL}\,(2,2^n)$, and thus elements of order $1,2,2^n-1$, and 2^n+1, respectively; see [6] 2.8.3. Moreover, the group $\mathrm{PSL}\,(3,2^n)$ contains elements of order 4, represented, for instance, by

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus $\omega\,(\mathrm{PSL}\,(3,2^n))\le 5$ implies that the numbers 2^n-1 and 2^n+1 are primes. One of these is divisible by 3, and we infer $2^n=4$. Now $\mathrm{PSL}\,(3,4)$ has order $2^6\cdot 3^2\cdot 5\cdot 7$. Therefore, there are at least 6 orbits, containing elements of order $1,2,4,3,5$, and 7, respectively. ∎

The case $n=1$ that was left in 2.8 indeed leads to another example of a simple group G with $\omega\,(G)=5$:

EXAMPLE 2.9. *For* $\mathrm{PSL}\,(3,2)\cong\mathrm{PSL}\,(2,7)$ *we have* $\omega\,(\mathrm{PSL}\,(3,2))=5$.

Proof. See [9] II 6.14 for a proof that the groups $\mathrm{PSL}\,(3,2)$ and $\mathrm{PSL}\,(2,7)$ are isomorphic. They have order $2^3 \cdot 3 \cdot 7$. Consider an element $x \in \mathrm{PSL}\,(2,7)$ whose order is divisible by 7. Then x centralizes an element y of order 7. Now y is a transvection, whose centralizer in $\mathrm{PSL}\,(2,7)$ coincides with the subgroup generated by y. This shows that the order of any element of $\mathrm{PSL}\,(2,7)$ either equals 7 or divides $2^3 \cdot 3$.

We consider the action on the projective plane with 7 points and 7 lines; that is, we interpret the group as $\mathrm{PSL}\,(3,2)$. Every element whose order is different from 7 fixes at least one line, and is thus contained in a conjugate of the affine group, which is isomorphic to Sym_4. Therefore, these elements have order $1, 2, 3$, or 4, and we see that all elements of order 3 and 4, respectively, belong to the same orbit. The involutions are transvections, and thus conjugates in $\mathrm{PSL}\,(3,2)$. It remains to study elements of order 7, we do this in the isomorphic group $\mathrm{PSL}\,(2,7)$: there the elements of order 7 are transvections, and conjugates under $\mathrm{GL}_2 7$. ∎

LEMMA 2.10. *Let p be a Fermat or a Mersenne prime. Then the group $\mathrm{PSL}\,(2,p)$ satisfies $\omega\,(\mathrm{PSL}\,(2,p)) \le 5$ exactly if $p \in \{3,5,7\}$. The group $\mathrm{PSL}\,(2,3) \cong \mathrm{Alt}_4$ is not simple (and satisfies $\omega\,(\mathrm{PSL}\,(2,3)) = 3$), the group $\mathrm{PSL}\,(2,5) \cong \mathrm{Alt}_5$ satisfies $\omega\,(\mathrm{PSL}\,(2,5)) = 4$, and $\mathrm{PSL}\,(2,7) \cong \mathrm{PSL}\,(3,2)$ is a group with $\omega\,(\mathrm{PSL}\,(2,7)) = 5$.*

Proof. It suffices to consider the case $p > 7$. As p is a Fermat or a Mersenne number, we have $p = 2^n + \varepsilon$, where $\varepsilon \in \{1,-1\}$. We have $n > 3$, and the order of $\mathrm{PSL}\,(2,p)$ is $\left((2^n+\varepsilon)^2 - 1\right)(2^n+\varepsilon)/2 = 2^n(2^{n-1}+\varepsilon)p$. Thus the Sylow 2-subgroups of $\mathrm{PSL}\,(2,p)$ have order $2^n \ge 16$. The Sylow subgroups are dihedral groups (see [9] II 8.10), and contain an element of order $2^{n-1} \ge 8$, which means $\omega\,(\mathrm{PSL}\,(2,p)) \ge 6$. ∎

REMARK 2.11. It remains (under our present hypothesis that r is a prime power) to consider the groups $\mathrm{PSL}\,(2,2^n)$, where $n \ge 2$. These groups have elementary abelian Sylow 2-subgroups, and they contain elements of order 2^n+1 as well as elements of order $2^n - 1$. Therefore, $\omega\,(\mathrm{PSL}\,(2,2^n)) \le 5$ implies $n \in \{2,3\}$; see 2.2, and we have the following result:

THEOREM 2.12. *Let G be a simple group with $\omega\,(G) \le 5$, and assume that every element of G has prime power order. Then G is isomorphic to one of the groups $\mathrm{PSL}\,(2,4)$, $\mathrm{PSL}\,(2,7) \cong \mathrm{PSL}\,(3,2)$, $\mathrm{PSL}\,(2,8)$, or $\mathrm{PSL}\,(2,9)$.* ∎

3. GROUPS WITH ELEMENTS OF MIXED ODD ORDER.

We recall an old result due to Burnside [1]: If G is a finite simple group of even order all of whose elements either have odd order or have order 2, then G is isomorphic to $\mathrm{SL}\,(2,2^n)$ for some natural number $n > 1$. See [2] Th. 56, p.99 for a more recent proof of that result.

In the case where $r = pq$ is odd, this allows to conclude that our group G is covered by the reasoning in the previous section. However, we need to know $t = 2$; that is, we have to refer to the Odd Order Theorem [4].

A different approach (also using the Odd Order Theorem) to the case $r = pq$ is the following. M. Suzuki [20] has also classified simple *C*-groups (where the centralizer of any involution is 2-closed; that is, has a normal Sylow 2-subgroup, see [6] p. 444). The result is: every simple *C*-group is isomorphic to one of the groups $\mathrm{PSL}(2,p)$, $\mathrm{PSL}(2,9)$, $\mathrm{PSL}(2,2^n)$, $\mathrm{Sz}(2^n)$, $\mathrm{PSU}\left(3,2^{2n}\right)$, or $\mathrm{PSL}(3,2^n)$; where p is a Fermat or Mersenne prime, and $n \geq 2$. Compare [6] p. 466.

From $r = pq$ we infer that centralizers of involutions are contained in Sylow 2-subgroups; thus it is trivial that these groups are 2-closed. According to Suzuki's result and our observations in 2.10, 2.5, 2.11, 2.7, and 2.8, it only remains to study the groups $\mathrm{PSU}\left(3,2^{2n}\right)$. We will show that these groups contain elements of order 4. This means that no new examples occur for $r = pq$.

The group $\mathrm{PSU}\left(3,2^{2n}\right)$ is obtained as a quotient of the special unitary group $\mathrm{SU}\left(3,2^{2n}\right)$ of 3×3 matrices A with determinant 1 over the field $\mathrm{GF}(2^{2n})$, subject to the additional requirement that A^{-1} is obtained by transposing A and applying the (unique) involution $\sigma \in \mathrm{Aut}\left(\mathrm{GF}(2^{2n})\right)$ to each entry. (Note that $x^\sigma = x^{(2^n)}$.) The kernel of this quotient is the center $\left\{c\cdot \mathrm{id} \,\middle|\, c \in \mathrm{GF}(2^{2n}), c^3 = 1 = c^\sigma c\right\}$ of $\mathrm{SU}\left(3,2^{2n}\right)$.

For every pair $(a,b) \in \mathrm{GF}(2^{2n})$ with $aa^\sigma = b + b^\sigma$, the matrix

$$M(a,b) := \begin{pmatrix} b & 1+b & a \\ 1+b & b & a \\ a^\sigma & a^\sigma & 1 \end{pmatrix}$$

belongs to $\mathrm{SU}\left(3,2^{2n}\right)$. It is easy to see that it satisfies

$$M(a,b)^2 = \begin{pmatrix} 1+aa^\sigma & aa^\sigma & 0 \\ aa^\sigma & 1+aa^\sigma & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Thus $M(a,b)^4$ is trivial, and every pair (a,b) with $aa^\sigma = b + b^\sigma$ and $b \neq b^\sigma$ induces an element of order 4 in $\mathrm{PSU}\left(3,2^{2n}\right)$. Such pairs exist since the norm map $N(a) := aa^\sigma$ corresponding to the quadratic extension of $\mathrm{GF}(2^{2n})$ over the fixed field of σ is a surjective map.

4. GROUPS WITH ELEMENTS OF MIXED EVEN ORDER.

There remains the case where $r \in \{2p, 2q\}$. Here we need the following deep result by D. Gorenstein [5]:

THEOREM 4.1. *Let G be a finite simple group whose Sylow 2-subgroups are abelian, and assume that every involution in G has solvable centralizer. Then G is isomorphic to* $\mathrm{PSL}(2,f)$*, where $f \geq 5$ is even or congruent to 3 or to 5 modulo 8.* ∎

This result applies in the case $r \in \{2p, 2q\}$: the centralizer of an involution contains only elements of orders dividing r, and is solvable by Burnside's $p^\alpha q^\beta$-Theorem. The Sylow 2-subgroups are (elementary) abelian since there are no elements of order 4. The groups $\mathrm{PSL}(2,2^n)$ have been treated in 2.11. Thus we may assume that the prime power f is odd. In this case, the additional restriction on f in 4.1 is just the requirement that the order $\frac{f^2-1}{2}f$ of $\mathrm{PSL}(2,f)$ is not divisible by 8: this is equivalent to requiring that f^2 is not congruent to 1 modulo 16.

In the case that we are interested in, we have $\frac{f^2-1}{2}f = 4p^\alpha q^\beta$, and may assume $f = p^\alpha$. Then $(f+1)(f-1) = f^2 - 1 = 8q^\beta$ implies $2^\gamma q^\delta = f+1 = f-1+2 = 2^{3-\gamma}q^{\beta-\delta}+2$ with $\gamma \in \{1,2\}$ and $0 \leq \delta \leq \beta$. Thus $\delta > 0$ implies the contradiction $0 \equiv 2 \pmod q$, and we end up with $f \in \{1,3\}$. But then $\mathrm{PSL}(2,f)$ is not simple.

We can thus formulate our conclusive result.

THEOREM 4.2. *Each finite simple group G with $\omega(G) \leq 5$ is isomorphic to one of the following:*

$$\begin{array}{rcl} \mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) & \cong & \mathrm{Alt}_5\,, \\ \mathrm{PSL}(2,7) & \cong & \mathrm{PSL}(3,2)\,, \\ \mathrm{PSL}(2,8)\,, & & \\ \textit{or} \quad \mathrm{PSL}(2,9) & \cong & \mathrm{Alt}_6\,. \end{array}$$ ∎

REMARK 4.3. Using (implicitly) the classification of finite simple groups, we could replace the discussion of groups with elements of mixed order by a reference to the following result, proved by J. Zhang [23] 3.1:

Let G be a finite simple group. Assume that elements of G belong to the same orbit under $\mathrm{Aut}(G)$ *if they have the same order. Then G is isomorphic to one of the groups* $\mathrm{PSL}(2,5)$, $\mathrm{PSL}(2,7)$, $\mathrm{PSL}(2,8)$, $\mathrm{PSL}(2,9)$, $\mathrm{PSL}(3,4)$.

In fact, J. Zhang has classified all finite groups with the property that elements of the same order are in the same orbit under automorphisms.

REFERENCES

1. Burnside, W.: *On a class of groups of finite order*, Transactions of the Cambridge Philos. Soc. **18** (1900), 269–276.
2. Collins, M.J.: *Representations and characters of finite groups*, Cambridge studies in advanced mathematics, vol. 22, Cambridge University Press, Cambridge, 1990.
3. Feit, W., M. Hall, and J.G. Thompson: *Finite groups in which the centralizer of every non-identity element is nilpotent*, Math. Z. **74** (1960), 1–17.

4. Feit, W., and J.G. Thompson: *Solvability of groups of odd order*, Pac. Jour Math. **13** (1963), 775–1029.
5. Gorenstein, D.: *Finite groups in which Sylow* 2*-subgroups are abelian and centralizers of involutions are solvable*, Canad. J. Math. **17** (1965), 860–896.
6. Gorenstein, D.: *Finite groups*, Harper & Row, New York etc., 1968.
7. Hayashi, M., and Y. Tanaka: *On the finite simple groups all of whose 2-local subgroups are solvable*, J. Algebra **210** (1998), p365-384.
8. Herzog, M.: *On finite simple groups of order divisible by three primes only*, J. Algebra **10** (1968), 383–388.
9. Huppert, B.: *Endliche Gruppen I*, Springer, Berlin etc., 1967.
10. Huppert, B., and N. Blackburn: *Finite groups III*, Springer, Berlin etc., 1982.
11. Jacobson, N.: *Basic algebra I*, 2nd ed., Freeman, New York, 1985.
12. Lüneburg, H.: *Translation planes*, Springer, Berlin etc., 1980.
13. Mäurer, H.: *Zur Automorphismengruppe der symmetrischen Gruppen*, Mitt. Math. Ges. Hamb. **11** (1983), 265–266.
14. Mäurer, H., and M. Stroppel: *Groups that are almost homogeneous*, Geometriae Dedicata **68** (1997), 229–243.
15. Schwachhöfer, M., and M. Stroppel: *Finding representatives for the orbits under the automorphism group of a bounded abelian group*, J. Algebra **211** (1999), 225–239.
16. Stroppel, M.: *Locally compact groups with many automorphisms*, J. Group Theory **4** (2001), 427–455.
17. Stroppel, M.: *Locally compact groups with few orbits under automorphisms*, Manuscript, Stuttgart, 2001.
18. Suzuki, M.: *Finite groups with nilpotent centralizers*, Trans. Amer. Math. Soc. **99** (1961), 425–470.
19. Suzuki, M.: *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 105–145.
20. Suzuki, M.: *Finite groups in which the centralizer of any element of order* 2 *is* 2*-closed*, Ann. Math. **82** (1965), 191–212.
21. Suzuki, M.: *Group theory II*, Springer, New York etc., 1986.
22. Walter, J.H. *The characterization of finite groups with abelian Sylow 2-subgroups*, Ann. Math. **89** (1969), 405–514.
23. Zhang, J. *On finite groups all of whose elements of the same order are conjugate in their automorphism groups*, J. Algebra **153** (1992), 22-36.