Two-transitive pairs in $\mathrm{PSL}(2, q)$

Francis Buekenhout Julie De Saedeleer Dimitri Leemans

Abstract

For every group $\mathrm{PSL}(2, q)$, q a prime power, we classify all two-transitive pairs (U, U_0) consisting of a subgroup U of $\mathrm{PSL}(2, q)$ and a subgroup U_0 of U such that the action of U on the cosets of U_0 is two-transitive. We obtain twenty-one classes up to conjugacy in $\mathrm{PSL}(2, q)$ or fusion in $P\Gamma L(2, q)$ except for two cases in which we don't have that control.

1 Introduction

This paper is devoted to the classification of all 2-transitive pairs of a group $G = \mathrm{PSL}(2, q)$, q a prime power, namely all pairs of subgroups $U > U_0$ such that the action of U on the set of left cosets of U_0 is 2-transitive. Instead of "2-transitive" we also write "two-transitive". The need for this concept arose in the thesis of the second author [9] under the additional requirement that U be maximal in G. The unexpected power of the concept in some huge subgroup lattices was displayed for all sporadic groups in [5]. We quote about the relationship with those earlier papers, from [5]:

"*In the geometric study of the groups $G = \mathrm{PSL}(2, q)$ found within [9],* 2*-transitive pairs of subgroups of G are determined, namely, pairs of subgroups $(H; H_0)$ of G such that the action of H on the left cosets of H_0 is* 2*-transitive. .... The present authors observed further that this can be simplified to some extent by purely arithmetic means, and that this approach can be extended to other groups G with surprising efficiency.*"

Here, we are dealing with the general case for $G = \mathrm{PSL}(2, q)$. Our techniques are elementary and a little acrobatic in several difficult situations illustrated by Lemmas 10, 12 and 13. Our techniques are by no means standard. We reveal a

Received by the editors in January 2014 - In revised form in October 2015.
Communicated by H. Van Maldeghem.
2010 *Mathematics Subject Classification* : 20B20, 20G40.
Key words and phrases : projective special linear groups, two-transitive action.

surprising new class of groups U that we call *transfield groups* (see 5.5.1). The classification holds in Theorem 1 with twenty-one classes. Most of these are under control as to conjugation in G or fusion in $Aut(G) = P\Gamma L(2, q)$. Exceptions are classes (1) and (20) in Theorem 1. It turns out all fusions under control happen in $PGL(2, q)$. In view of applications to incidence geometry and locally s-arc transitive graphs, it is worth also to determine the 2-transitive pairs (U, U_0) with U maximal in G. This is done in our Theorem 2. Our Theorem 1 opens a door to the classification of the rank 3 coset geometries on which G acts flag-transitively. This subject has been preceded by a classification of rank 2 geometries for G in [9], [4] and [10] using a preliminary version of Theorem 2, whose proof refers to the present paper. Theorem 1 also opens a door for a similar treatment in other families of almost simple groups G. There is no need for G to be 2-transitive.

Our main preliminary tool in this paper is Dickson's classification of subgroups of $\mathrm{PSL}(2, q)$. Dickson [11] and Lemma 1 provide 14 families of subgroups each of which is a union of conjugacy classes. He deals with conjugacy, in particular the size of every conjugacy class. His statements in families 7 and 8 of our Lemma 1 include an error. The correction is not easy. This difficulty can be avoided in our Theorem 1. Our result is not an immediate consequence of Dickson's list. We take care of delicate arithmetic conditions and we look for classes of configurations that are disjoint. Also, we prepare more complex navigations in the subgroup lattice of $\mathrm{PSL}(2, q)$ such as in [4, 10].

2 Main results

In a group G, we define a *two-transitive pair* as an ordered pair (U, U_0) of subgroups of G with $U_0 < U$ and such that the action of U on the left cosets of U_0 is two-transitive. As a matter of fact, U_0 is a maximal subgroup of U. In a search for two-transitive pairs, we find it useful to first consider the condition "U_0 maximal in U" before proceeding to the full condition "2-transitive".

For every family of 2-transitive pairs provided in Theorems 1 and 2 we care for conjugacy in $\mathrm{PSL}(2, q)$ or fusion in $\mathrm{PGL}(2, q)$.

We make use of the following notations: G denotes a group $\mathrm{PSL}(2, q)$ for some prime power $q = p^n$. Every elementary abelian subgroup of some order p^m is denoted by E_{p^m}. Here, U denotes a group acting 2-transitively on a set Ω, *Ker U* is the kernel of this action, namely the set of all $u \in U$ such that $u(x) = x$ for every $x \in \Omega$. Moreover, U_0 is the stabilizer in U of some element 0 in Ω. Finally, a cyclic group of order d is often denoted by Z_d. We prove the following result.

Theorem 1. *Let $G \cong \mathrm{PSL}(2, q)$ for some prime power $q = p^n$. Let (U, U_0) be a 2-transitive pair of subgroups of G with U proper in G. Then one of the following holds:*

(1) $U \cong E_{p^m} : D$, for some $1 \leq m \leq n$ and some cyclic group D of even order (as in Lemma 1, family 8), Ker U is the unique subgroup of index 2 of U, $|\Omega| = 2$, $U_0 =$ Ker U (control of conjugation is unavailable);

(2) $U \cong E_{p^m} : (p^m - 1)$, for some m dividing n, $|\Omega| = p^m$, Ker $U = 1$, U_0 is a cyclic subgroup of order $(p^m - 1)$ (unique up to conjugacy);

(3) $U \cong \mathrm{PSL}(2,2) \cong S_3$, $|\Omega| = 2$, *Ker* $U = Z_3 = U_0$ *(unique up to conjugacy);*

(4) $U \cong \mathrm{PSL}(2,2) \cong S_3$, $|\Omega| = 3$, *Ker* $U = 1$, $U_0 \cong Z_2$ *(unique up to conjugacy);*

(5) $U \cong \mathrm{PSL}(2,3) \cong A_4$, $|\Omega| = 4$, *Ker* $U = 1$, $U_0 \cong Z_3$ *(unique up to fusion in* $\mathrm{PGL}(2,q)$*);*

(6) $U \cong A_5 \cong \mathrm{PSL}(2,5) \cong \mathrm{PSL}(2,4)$, $q = \pm 1(10)$ *and one of the following holds:*

  (a) $|\Omega| = 5$, *Ker* $U = 1$, $U_0 \cong A_4$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

  (b) $|\Omega| = 6$, *Ker* $U = 1$, $U_0 \cong D_{10}$, *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*).*

(7) $U \cong \mathrm{PSL}(2,11)$, $|\Omega| = 11$, *Ker* $U = 1$, $U_0 \cong A_5$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,11) = Aut(U)$*);*

(8) $U \cong \mathrm{PSL}(2,9) \cong A_6$, $|\Omega| = 6$, *Ker* $U = 1$, $U_0 \cong A_5$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,9)$*);*

(9) $U \cong \mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$,$|\Omega| = 7$, *Ker* $U = 1$, $U_0 \cong S_4$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,7)$*);*

(10) $U \cong \mathrm{PSL}(2,r)$ *for every* $r = p^s$, $s \geq 1$, $r > 3$ *with* $q = r^m$ *and* m *prime. Moreover, for* $p > 2$ *we also require* $m > 2$*. Here* $|\Omega| = r+1$, *Ker* $U = 1$, $U_0 \cong E_r : \frac{r-1}{(2,r-1)}$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

(11) $U \cong \mathrm{PGL}(2,r)$, r *odd*, $r = p^s$, $q = r^2$, $|\Omega| = 2$, *Ker* $U = U_0 \cong \mathrm{PSL}(2,r)$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

(12) $U \cong \mathrm{PGL}(2,r)$, r *odd*, $r = p^s$, $s \geq 1$ *with* $q = r^2$*. Here* $|\Omega| = r+1$, *Ker* $U = 1$, $U_0 \cong E_r : (r-1)$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

(13) $U \cong \mathrm{PGL}(2,3) \cong S_4$, $q = \pm 1(8)$; $|\Omega| = 3$, *Ker* $U = E_4$, $U/$*Ker* $U \cong S_3$, $U_0 \cong D_8$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

(14) *U is dihedral of order* $2d$*, for every* $d > 2$ *dividing* $\frac{q\pm1}{(2,q-1)}$; $|\Omega| = 2$, *Ker* $U = U^+ = U_0$ *where* U^+ *is the cyclic subgroup of index* 2 *of* U*, (unique up to conjugacy);*

(15) *U is dihedral of order* $2d$*, for every* d *dividing* $\frac{q\pm1}{(2,q-1)}$ *and* $3 \mid d$*. Here* $|\Omega| = 3$, *Ker* U *is the unique cyclic subgroup of index 6 in* U*. Then* U_0 *is one of the three dihedral subgroups of index 3 in* U, $U/$*Ker* $U \cong S_3$ *(unique up to conjugacy);*

(16) *U is dihedral of order* $2d$*, for every* d *even dividing* $\frac{q\pm1}{2}$*. Here* $|\Omega| = 2$, *Ker* $U = U_0$ *is one of the two dihedral subgroups of index* 2 *in* U *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

(17) *U is dihedral of order* 4; $|\Omega| = 2$, *Ker* $U = U_0$ *is one of the three dihedral subgroups of index* 2 *in* U *(unique up to conjugacy);*

(18) $U \cong \mathrm{PGL}(2,5) \cong S_5$, $|\Omega| = 5$, *Ker* $U = 1$, $U_0 \cong S_4$ *(unique up to conjugacy).*

(19) *For every* q *odd and* d *even divisor of* $q-1$ *or* $q+1$, U *is cyclic of order* d. *Here* $|\Omega| = 2$, *Ker* $U = U_0$ *is the unique subgroup of index* 2 *in* U *(unique up to conjugacy).*

(20) $U \cong U(K,k,W,H)$ *a transfield group (see 5.5.1)* , $U = W : k^* = E_{p^{sl}} : (p^s - 1)$, $s \mid n$, $|\Omega| = p^s$, $|KerU| = p^{sl}/p^s = p^{s(l-1)}$, $U/$*Ker* $U = E_{p^s} : (p^s - 1)$ *(control of conjugation is unavailable).*

(21) $U \cong C_2$, $U_0 = 1$.

These classes are pairwise disjoint. Except (1), (2), (20) and (21); (3) and (4); (6) and (10); (7) and (10); (8) and (10); (9) and (10) ; (11), (12), (13) and (18) ; (14), (15), (16) and (17).

These pairs are of key importance, for instance in the classification of locally 2-arc-transitive graphs arising from a given group G (see [12]), and also in the classification of coset geometries satisfying the property $(2T)_1$ (see [3] for a definition and motivation in this direction).

The need for the present paper became clear in the study of [4, 10] in which the present paper (Theorem 2) was indeed used.

We now turn to the situation in which U is maximal in G. Let us observe that 2-transitive actions of maximal subgroups in $\mathrm{PSL}(2,q)$ were listed in [10] Table 4, without proof. That table is slightly improved here. It is right in view of the present Theorem 1.

Theorem 2. *Let* $G \cong \mathrm{PSL}(2,q)$ *for some power* q *of a prime* p. *Let* (U,U_0) *be a 2-transitive pair of subgroups of* G *with* U *maximal in* G. *Then one of the following holds:*

(1) $U \cong E_q : \frac{q-1}{2}$, $q = 1(4)$, *Ker* U *is the unique subgroup of index* 2 *of* U, $|\Omega| = 2$, $U_0 =$ *Ker* U *(unique up to conjugacy);*

(2) $U \cong E_q : (q-1)$, q *even*, $|\Omega| = q$, *Ker* $U = 1$, U_0 *is a cyclic subgroup of order* $(q-1)$ *(unique up to conjugacy);*

(3) $U \cong \mathrm{PSL}(2,2) \cong S_3$, $|\Omega| = 2$, *Ker* $U = Z_3 = U_0$ *(unique up to conjugacy);*

(4) $U \cong \mathrm{PSL}(2,2) \cong S_3$, $|\Omega| = 3$, *Ker* $U = 1$, $U_0 \cong Z_2$ *(unique up to conjugacy);*

(5) $U \cong \mathrm{PSL}(2,3) \cong A_4$, $|\Omega| = 4$, *Ker* $U = 1$, $U_0 \cong Z_3$ *(unique up to fusion in* $\mathrm{PGL}(2,q)$*);*

(6) $U \cong A_5 \cong \mathrm{PSL}(2,5) \cong \mathrm{PSL}(2,4)$, $p \neq 2$, $p \neq 5$, *either* $q = p = \pm 1(5)$ *or* $q = p^2 = -1(5)$ *and one of the following holds.*

  (a) $|\Omega| = 5$, *Ker* $U = 1$, $U_0 \cong A_4$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*);*

  (b) $|\Omega| = 6$, *Ker* $U = 1$, $U_0 \cong D_{10}$, *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2,q)$*).*

(7) $U \cong \mathrm{PSL}(2, 11)$, $|\Omega| = 11$, *Ker* $U = 1$, $U_0 \cong A_5$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, 11) = Aut(U)$*);*

(8) $U \cong \mathrm{PSL}(2, 9) \cong A_6$, $|\Omega| = 6$, *Ker* $U = 1$, $U_0 \cong A_5$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, 9)$*);*

(9) $U \cong \mathrm{PSL}(2, 7) \cong \mathrm{PSL}(3, 2)$, $|\Omega| = 7$, *Ker* $U = 1$, $U_0 \cong S_4$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, 7)$*);*

(10) $U \cong \mathrm{PSL}(2, r)$ *for every* $r = p^s$, $s \geq 1$, $r > 3$ *with* $q = r^m$ *and* m *prime. Moreover, for* $p > 2$ *we also require* $m > 2$. *Here* $|\Omega| = r + 1$, *Ker* $U = 1$, $U_0 \cong E_r : \frac{r-1}{(2,r-1)}$, *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, q)$*);*

(11) $U \cong \mathrm{PGL}(2, r)$, r *odd*, $r = p^s$, $q = r^2$, $|\Omega| = 2$, *Ker* $U = U_0 \cong \mathrm{PSL}(2, r)$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, q)$*);*

(12) $U \cong \mathrm{PGL}(2, r)$, r *odd*, $r = p^s$, $s \geq 1$ *with* $q = r^2$. *Here* $|\Omega| = r + 1$, *Ker* $U = 1$, $U_0 \cong E_r : (r - 1)$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, q)$*);*

(13) $U \cong \mathrm{PGL}(2, 3) \cong S_4$, $q = p > 2$, $q = \pm 1(8)$, $|\Omega| = 3$, *Ker* $U = E_4$, $U/$*Ker* $U \cong S_3$, $U_0 \cong D_8$ *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, q)$*);*

(14) U *is dihedral of order* $2(q - 1)$ *or* $2(q + 1)$, q *even*, $|\Omega| = 2$, *Ker* $U = U^+ = U_0$ *where* U^+ *is the cyclic subgroup of index* 2 *of* U, *(unique up to conjugacy for each of the two possible values of* $|U|$*);*

(15) U *is dihedral of order* $(q - 1)$ *or* $(q + 1)$, q *odd*, $|\Omega| = 2$, *Ker* $U = U^+ = U_0$ *where* U^+ *is the cyclic subgroup of index* 2 *of* U, *(unique up to conjugacy for each of the two possible values of* $|U|$*).*

In the particular case where $q = 3$, *the case of* $(q + 1)$ *provides* $U = E_4$, $|\Omega| = 2$. *Then* U_0 *is one of the three subgroups of order 2 in U (unique up to conjugacy). This case is also part of case (19);*

(16) U *is dihedral of order either* $2(q - 1)$ *or* $2(q + 1)$, q *even, and* $3 \mid |U|$; $|\Omega| = 3$, *Ker* U *is the unique cyclic subgroup of index 6 in* U. *Then* U_0 *is one of the three dihedral subgroups of index 3 in* U, $U/$*Ker* $U \cong S_3$ *(unique up to conjugacy);*

(17) U *is dihedral of order either* $(q - 1)$ *or* $(q + 1)$, q *odd, and* $3 \mid |U|$; $|\Omega| = 3$, *Ker* U *is the unique cyclic subgroup of index 6 in* U. *Then* U_0 *is one of the three dihedral subgroups of index 3 in* U, $U/$*Ker* $U \cong S_3$ *(unique up to conjugacy);*

(18) U *is dihedral of order either* $(q - 1)$ *or* $(q + 1)$, q *odd*, $q > 5$, *and* $4 \mid |U|$; $|\Omega| = 2$, *Ker* $U = U_0$ *is one of the two dihedral subgroups of index 2 in* U *(two such representations up to conjugacy; they are fused in* $\mathrm{PGL}(2, q)$*); Ker* U *is dihedral,* U_0 *is dihedral of index* 2*;*

(19) U *is dihedral of order* 4, q *is one of 3,5;* $|\Omega| = 2$, *Ker* $U = U_0$ *is one of the three dihedral subgroups of index* 2 *in* U *(unique up to conjugacy).*

(20) $U \cong \mathrm{PGL}(2,5) \cong S_5$, $|\Omega| = 5$, *Ker* $U = 1$, $U_0 \cong S_4$ *(unique up to conjugacy).*

Beware of the fact that these classes are not necessarily disjoint.

3 The subgroups of $\mathrm{PSL}(2,q)$

We recall the complete subgroup structure of $\mathrm{PSL}(2,q)$ due to Dickson [11].

Dickson refers to independent work by E.H. Moore (Dickson's supervisor) and A. Wiman in 1893 and 1899 respectively. According to Dickson in his preface, Wiman got the full classification (see [21]). We were able to study the work by E.H. Moore [16] whose version of the Hauptsatz is strictly the same as Dickson's. Moreover the author states that his paper was read at the meeting of the American Mathematical Society in 1898. He published his paper in 1904 and holds that he made no use of the treatments by Burnside [6], for q even and those by Wiman and Dickson.

We follow broadly the phrasing and organisation of O. H. King [14]. King lists 22 families from (a) to (v). We observe that two families consisting of the two trivial subgroups of $\mathrm{PSL}(2,q)$ need to be added and so we provide actually 14 families of subgroups in Lemma 1 some of which include subfamilies.

For the families (m) and (n), King mentions ”a number of classes of conjugate groups” whose size is not given. These are dealt with in our families 7 and 8 of Lemma 1. That ”number of classes” is given by Dickson, but it is erroneous. This can easily be seen from an example analyzed with MAGMA [2] for $q = 64$. Magma helps us to see that for $q = 64$ there are 10 conjugacy classes of 4095 elementary abelian subgroups of order 16 and one class of 1365 such subgroups. It may further help to indicate that every subgroup in one of the 10 classes of 4095 subgroups of order 16 has a $\mathrm{PSL}(2,64)$-normalizer of order 64 and that every other has a normalizer of order 192. The lengths of classes are equal to the lengths given by Dickson. However, the number of classes of each of these two types is not as in Dickson's list. As we don't need to know how many classes there are and what are their lengths for families 7 and 8, we prefer to omit this information in the statement of Lemma 1. We come back to a general value of q as earlier. Concerning the elementary abelian subgroups of order p^m with m any natural number such that $1 \leq m \leq n-1$, we know their total number which is $\frac{(q+1)(q-1)(q-p)...(q-p^{m-1})}{(q-1)(q-p)...(q-p^{m-1})}$. We also know that conjugacy classes of them depend on one further parameter k where k is any common divisor of n and m. This number allows for control on the size of conjugacy classes. This size is $\frac{q^2-1}{(2,1,1)(p^k-1)}$ for given k (as shown by Dickson). However the question remains open as to control over the number of conjugacy classes for a fixed value of k.

The error was already detected by Patricia Vanden Cruyce in [19]. However, the correction she provided is wrong also, again as we see from a MAGMA study on the values $q \leq 97$. We cannot settle the question but our analysis for Theorem 1 allows to get around it.

A neat classification of the subgroups of $\mathrm{PSL}(2,q)$ is given with proof in Huppert [13]. In his ”Hauptsatz” (Dickson) he distributes the subgroups in 8 families with no mention of conjugacy. However, conjugacy is used in his proof.

Notice that Dickson does not give the number of conjugacy classes of the subgroups $E_{p^m} : d$, except in the particular case where $m = n$ and $d = \frac{p^n-1}{(2,q-1)}$. There are $q+1$ subgroups $E_q : \frac{q-1}{(2,q-1)}$, all conjugate.

An original and powerful approach to the classification is developed by Suzuki [17]. He classifies the finite subgroups of PSL$(2, k)$ where k is an algebraically closed field. From this he gets the distribution of all subgroups of a PSL$(2, q)$ in 4 families. He does not deal with the question of conjugacy. He provides a list of maximal subgroups of which we make use after two little corrections (see Section 4).

Let us mention also that the groups PSL$(2, q)$ are a class of finite classical groups. The subgroup structure of the classical finite simple groups was classified by Aschbacher [1] (see also Kleidman-Liebeck [15]).

Lemma 1. *[L.E. Dickson-E.H. Moore] The group* PSL$(2, q)$ *of order* $\frac{q(q^2-1)}{(2,q-1)}$*, where* $q = p^n$ *(p prime), contains exactly the following subgroups:*

1. *The identity subgroup.*
2. *A single class of* $q+1$ *conjugate elementary abelian subgroups of order* q*, denoted by* E_q*.*
3. *A single class of* $\frac{q(q+1)}{2}$ *conjugate cyclic subgroups of order* d*, denoted by either* Z_d *or* d*; for every divisor* d *of* $q-1$ *for* q *even and* $\frac{q-1}{2}$ *for* q *odd, with* $d > 1$.
4. *A single class of* $\frac{q(q-1)}{2}$ *conjugate cyclic subgroups of order* d*,denoted by either* Z_d *or* d*; for every divisor* d *of* $q+1$ *for* q *even and* $\frac{q+1}{2}$ *for* q *odd, with* $d > 1$.
5.
   - *For* q *odd, a single class of* $\frac{q(q^2-1)}{4d}$ *dihedral groups of order* $2d$*, denoted by* D_{2d}*, for every divisor* d *of* $\frac{q-1}{2}$ *with* $\frac{q-1}{2d}$ *odd, with* $d > 1$;
   - *For* q *odd, two classes each of* $\frac{q(q^2-1)}{8d}$ *dihedral groups of order* $2d$*, denoted by* D_{2d}*, for every divisor* $d > 2$ *of* $\frac{q-1}{2}$ *with* $\frac{q-1}{2d}$ *even;*
   - *For* q *even, a single class of* $\frac{q(q^2-1)}{2d}$ *dihedral groups of order* $2d$*, denoted by* D_{2d}*, for every divisor* d *of* $q-1$*, with* $d > 1$;
   - *For* q *odd, a single class of* $\frac{q(q^2-1)}{4d}$ *dihedral groups of order* $2d$*, denoted by* D_{2d}*, for every divisor* d *of* $\frac{q+1}{2}$ *with* $\frac{q+1}{2d}$ *odd, with* $d > 1$;
   - *For* q *odd, two classes each of* $\frac{q(q^2-1)}{8d}$ *dihedral groups of order* $2d$*, denoted by* D_{2d}*, for every divisor* $d > 2$ *of* $\frac{q+1}{2}$ *with* $\frac{q+1}{2d}$ *even;*
   - *For* q *even, a single class of* $\frac{q(q^2-1)}{2d}$ *dihedral groups of order* $2d$*, denoted by* D_{2d}*, for every divisor* d *of* $q+1$*, with* $d > 1$.
6.
   - *A single class of* $\frac{q(q^2-1)}{24}$ *conjugate dihedral groups of order* 4 *denoted by* 2^2 *when* $q = \pm 3(8)$;

- *Two classes each of* $\frac{q(q^2-1)}{48}$ *conjugate dihedral groups of order* 4 *denoted by* 2^2 *when* $q = \pm 1(8)$*;*
- *When q is even, the groups* 2^2 *are in the family 7.*

7. *Elementary abelian subgroups of order* p^m*, denoted by* E_{p^m} *for every natural number m, such that* $1 \leq m \leq n-1$*.*

8. *Subgroups* $E_{p^m} : D$ *which are semidirect products of an elementary abelian group* E_{p^m} *and a cyclic group D of order d,* $d > 1$*, for every natural number m such that* $1 \leq m \leq n$ *and every natural number d dividing* $\frac{p^k-1}{(1,2,1)}$*, where* $k = (n, m)$ *and* $(1, 2, 1)$ *is one of*

   - *1 for* $p > 2$ *and* $\frac{n}{k}$ *is even*
   - *2 for* $p > 2$ *and* $\frac{n}{k}$ *is odd*
   - *1 for* $p = 2$

   These subgroups are Frobenius groups.

9. - *Two classes each of* $\frac{q(q^2-1)}{48}$ *conjugates of* A_4 *when* $q = \pm 1(8)$*;*
   - *A single class of* $\frac{q(q^2-1)}{24}$ *conjugates of* A_4 *when* $q = \pm 3(8)$*;*
   - *A single class of* $\frac{q(q^2-1)}{12}$ *conjugates of* A_4 *when q is an even power of* 2*.*

10. *Two classes each of* $\frac{q(q^2-1)}{48}$ *conjugates of* S_4 *when* $q = \pm 1(8)$*.*

11. *Two classes each of* $\frac{q(q^2-1)}{120}$ *conjugate alternating groups* A_5 *when* $q = \pm 1(10)$*.*

12. - *Two classes each of* $\frac{q(q^2-1)}{2r(r^2-1)}$ *groups* $\mathrm{PSL}(2, r)$*, where q is an even power of r, for q odd;*
    - *A single class of* $\frac{q(q^2-1)}{r(r^2-1)}$ *groups* $\mathrm{PSL}(2, r)$*, where q is an odd power of r, for q odd;*
    - *A single class of* $\frac{q(q^2-1)}{r(r^2-1)}$ *groups* $\mathrm{PSL}(2, r)$*, where q is a power of r, for q even.*

13. *Two classes each of* $\frac{q(q^2-1)}{2r(r^2-1)}$ *groups* $\mathrm{PGL}(2, r)$*, where q is an even power of r, for q odd;*

14. $\mathrm{PSL}(2, q)$ *itself.*

Remark 1. *Subgroups* A_5 *are given either by case 11 (when* $q = \pm 1(10)$*) or by case 12 (when* $q = 0(5)$ *and when* $q = 4^m$*) of Lemma 1. Also, if q is even, the* $\mathrm{PGL}(2, q')$ *are given by case 12, since* $\mathrm{PGL}(2, q') \cong \mathrm{PSL}(2, q')$ *provided q is even.*

Let us briefly say that a family from Lemma 1 is isolated if it has an empty intersection with every other family. Remark 1 tells us that 11, 12 and 13 are not isolated. Recall that in even characteristic, $PSL(2, q) = PGL(2, q)$. Examples of isolated families are 1 and 14.

4 Maximal subgroups of PSL$(2, q)$

In this section, we list the maximal subgroups of PSL$(2, q)$, according to Suzuki [17], page 417. We distribute them in Table 1 and Table 2 .

Eventually in his deep and long study of subgroups of the PSL$(2, k)$, k a field, Suzuki lists the maximal subgroups of PSL$(2, q)$ in seven families and he provides hints for the proof. This requires two small corrections. The first is due to Patricia Vanden Cruyce [19] in her thesis. In family (v) of Suzuki it is required to add the condition that for $q = 5^m$ and A_5, m must be an odd prime rather than a prime. *Indeed, if* $m = 2$ *we have that* $A_5 <$ PGL$(2, 5) <$ PSL$(2, 25)$. The second correction deals with a case missing in Suzuki's list namely that A_4 is maximal in PSL$(2, 5)$. We include it in Table 2.

5 Two-transitive representations of the subgroups of PSL$(2, q)$

5.1 Preliminaries

The proof of Theorem 1 proceeds by a series of lemmas distributed in cases from section 5.2 to section 5.8 as to the structure of U from Lemma 1. It ends with section 5.9.

The following Lemma gives a necessary condition for a group to have a two-transitive action. It is a direct consequence of Lagrange's Theorem.

Lemma 2. *Let G be a group and let H be a subgroup of G. If G acts two-transitively on the cosets of H in G, then $|G|$ must be divisible by $[G\!:\!H]([G\!:\!H] - 1)$.*

A group G is said to act *regularly* on a set Ω if G is transitive on Ω and the stabilizer in G of a point $p \in \Omega$ is the identity.

Lemma 3. *[Wielandt[20], proposition 4.4 in Chapter 1] . Let (G, Ω) be a permutation group which is transitive on Ω and let G be abelian. Then G is regular.*

Corollary 1. *Let (G, Ω) be a permutation group which is transitive on Ω and let G be abelian. If G is two-transitive then $|\Omega| = 2$ and $G = S_2$.*

Proof. Following Lemma 3 the group G is regular and if G is 2-transitive then there exist at most two points. ∎

Lemma 4. *(Maschke's Theorem) [8] Let G be a finite group and let F be a field whose characteristic does not divide $|G|$. Then every finite dimensional linear representation of G on F is completely reducible.*

Proof. See [8]. ∎

From here on, G is a group PSL$(2, q)$. For H a permutation group acting 2-transitively on a set Ω, we denote by $Ker H$ the kernel of the action of H on Ω. We denote by H_0 the stabilizer in H of some element $0 \in \Omega$. Moreover we say that a subgroup U of G is *of type H* if $U \cong H$. The pair (U, U_0) is a *2-transitive pair* if $U \cong H$ for some H that is 2-transitive on a set Ω and $U_0 \cong H_0$.

	Structure	Order	Index
I	$E_q : (q-1)$	$q(q-1)$	$q+1$
II	$D_{2(q+1)}$ $q \neq 2$	$2(q+1)$	$\frac{q(q-1)}{2}$
III	$D_{2(q-1)}$	$2(q-1)$	$\frac{q(q+1)}{2}$
IV	A_5 $q = 4^r$ *r is prime*	60	$\frac{q(q^2-1)}{60}$
V	$\mathrm{PSL}(2,q') \cong \mathrm{PGL}(2,q')$ $q' > 4, q = q'^m$, m is *prime* or $q' = 2, q = q'^2$	$q'(q'^2-1)$	$\frac{q(q^2-1)}{q'(q'^2-1)}$

Table 1: The maximal subgroups of $\mathrm{PSL}(2,q)$, for q even

	Structure	Order	Index
VI	$E_q : \frac{q-1}{2}$	$\frac{q(q-1)}{2}$	$q+1$
VII	$D_{(q+1)}$ $q \neq 7,9$	$q+1$	$\frac{q(q-1)}{2}$
VIII	$D_{(q-1)}$ $q \neq 3,5,7,9,11$	$q-1$	$\frac{q(q+1)}{2}$
IX	A_4 *if* $q = p > 3$ *and* $q = 3,13,27,37(40)$ or $q = 5$	12	$\frac{q(q^2-1)}{12\times 2}$
X	S_4 *if* $q = p > 2$ *and* $q = \pm 1(8)$	24	$\frac{q(q^2-1)}{24\times 2}$
XI	A_5 if $\begin{cases} q = 5^r & r \textit{ odd prime} & \textit{or} \\ p = q = \pm 1(5) & p \textit{ prime} & \textit{or} \\ q = p^2 = -1(5) & p \textit{ prime} & \textit{or} \end{cases}$	60	$\frac{q(q^2-1)}{60\times 2}$
XII	$\mathrm{PSL}(2,q')$ $q' \neq 5, q = q'^m$ *m odd prime*	$\frac{q'(q'^2-1)}{2}$	$\frac{q(q^2-1)}{q'(q'^2-1)}$
XIII	$\mathrm{PGL}(2,q')$ $q = q'^2$	$q'(q'^2-1)$	$\frac{q(q^2-1)}{q'(q'^2-1)}$

Table 2: The maximal subgroups of $\mathrm{PSL}(2,q)$, for q odd

5.2 Case U cyclic

Let us first observe that if $U \cong C_2$ then $U_0 = 1$ gives a two-transitive pair. As the group $PSL(2, q)$ is known to have a unique conjugacy class of involutions, this pair is unique up to conjugacy. This gives class (21) of Theorem 1.

Lemma 5. *For any cyclic group H, acting two-transitively on a set Ω the following holds: $|H|$ is even, H has a unique subgroup H^+ of index 2, $|\Omega| = 2$, $Ker\ H = H^+$ and $H/H^+ \cong S_2$.*

Proof. If α is the 2-transitive action, $\alpha(H)$ is cyclic, hence regular (Lemma 3) on Ω and $|\Omega| = 2$ by Corollary 1. Hence $Ker\ H$ is the unique subgroup of index 2 in H. ∎

Lemma 6. *Let U be a cyclic subgroup of G, namely a member of one of the families 1., 3., 4. or 7. in Lemma 1. Then q is odd and U is a cyclic group of even order d dividing $q-1$ or $q+1$. Moreover, $|\Omega| = 2$ and $Ker\ U = U_0$ is the unique subgroup of index 2 in U (unique up to conjugacy in U and in G).*

Proof. Family 1. is ruled out by Lemma 2. Family 7. with $p = 2$ and $m = 1$ gives $U \cong C_2$ and $U_0 \cong 1$. Consider families 3. and 4. We apply Lemma 5. This requires that d is even, hence q is odd. Then U has indeed a unique subgroup U^+ of index 2. ∎

5.3 Case U dihedral

Lemma 7. *Let H be any dihedral group with $|H| \geq 6$, acting two-transitively on a set Ω. Let H^+ be its unique cyclic subgroup of index 2. Then one of the following holds.*

(1) $Ker\ H = H^+$ and $|\Omega| = 2$, $H_0 = H^+$ which exists and is unique in H;

(2) $Ker\ H \neq H^+$ with $Ker\ H$ cyclic, $|\Omega| = 3$ and $H/Ker\ H \cong S_3$, H_0 is dihedral of index 3. This occurs and is unique up to conjugacy in H, provided that $3 \mid |H|$;

(3) $Ker\ H \neq H^+$ with $Ker\ H$ dihedral and $|\Omega| = 2$ which exists in two versions provided that $|H^+|$ is even. Here H_0 is one of the two dihedral subgroups of index 2 in H. They are not conjugate in H but fused by $Aut\ H$.

Proof. Assume first that $Ker\ H = H^+$. Then $|\Omega| = 2$, $H_0 = H^+$ and we get (1) .

Assume next that $Ker\ H \neq H^+$. From the subgroup structure of H, $Ker\ H$ is either cyclic or dihedral.

Suppose that $Ker\ H$ is cyclic, hence $Ker\ H < H^+$. The group $H^+/Ker\ H$ is transitive on Ω. It is abelian, hence regular (Lemma 3). Then $H/Ker\ H$ is dihedral and is a 2-transitive permutation group on Ω. Thus $(H/Ker\ H)_0$ is of order 2 and transitive on $\Omega - \{0\}$. This implies that $|\Omega| = 3$. Thus H_0 is a dihedral subgroup of index 3 in H. There are three such subgroups, they are conjugate and offer a unique representation of H. It exists provided that $3 \mid |H|$. This is (2).

Suppose that $Ker\ H \neq H^+$ is dihedral. Then $H/Ker\ H$ is cyclic and acts as a 2-transitive permutation group on Ω. By Lemma 6, $|\Omega| = 2$. We see that H_0 is of index 2 in H. As $H_0 = KerH$, H_0 is dihedral. There are two such subgroups in H provided that $|H^+|$ is even. This is (3). ∎

Remark 2. *If H is the dihedral group D_4, its two-transitive representations require $|\Omega| = 2$ and $|H_0| = 2$.*

Lemma 8. *Let U be a dihedral subgroup of G, namely a member of families 5. and 6. in Lemma 1. Then one of (a) and (b) holds.*

(a) For some q, for some $d > 2$ dividing $\frac{q\pm 1}{(2,q-1)}$, U is dihedral of order $2d$. Then one of the following holds.

(1) Ker $U = U^+ = U_0$, $|\Omega| = 2$, this is unique in U.

(2) Ker $U \neq U^+$ with Ker U cyclic, $|\Omega| = 3$ and $U/\mathit{Ker}\ U \cong S_3$, U_0 is dihedral of index 3. This occurs and is unique up to conjugacy in U, provided that $3 \mid |U|$.

(3) Ker $U \neq U^+$ with Ker U dihedral and $|\Omega| = 2$ which exists in two versions provided that $|U^+|$ is even. Here U_0 is one of the two dihedral subgroups of index 2 in U. They are not conjugate in U but fused by Aut U.

(b) If U is dihedral of order 4, $|\Omega| = 2$, Ker $U = U_0$ is one of the three dihedral subgroups of index 2 in U. They are not conjugate in U but fused by Aut U. These subgroups come from class (7) of Lemma 1 with $p = 2$.

Proof. If U has order 4, remark 2 applies and we get (b). If the order of U is at least 6, then Lemma 7 applies. Let U^+ be the unique cyclic subgroup of index 2 of U. Let us consider cases (1), (2) and (3) of Lemma 7.
In case (1), *Ker* $U = U^+ = U_0$, $|\Omega| = 2$ and we get (a1).
In case (2), *Ker* $U \neq U^+$ with *Ker* U cyclic, $|\Omega| = 3$ and $U/\mathit{Ker}\ U \cong S_3$, U_0 is dihedral of index 3. This occurs and is unique provided that $3 \mid |U|$ and we get (a2).
In case (3), *Ker* $U \neq U^+$ with *Ker* U dihedral and $|\Omega| = 2$ which exists in two versions provided that $|U^+|$ is even. Here U_0 is one of the two dihedral subgroups of index 2 in U. They are not conjugate but fused by Aut U. This is (a3). ∎

5.4 Case U elementary abelian

Lemma 9. *If U is a subgroup E_{p^m} for any natural number m, such that $1 \leq m \leq n-1$, then $p^m = 2$, $\mid \Omega \mid = 2$ and Ker $U = 1$.*

Proof. Immediate by Lemma 2. ∎

Observe that in the case where $p = 2$ and $m = 1$, we get case (21) of Theorem 1 in even characteristic.

5.5 Case U elementary abelian extended by a non trivial cyclic subgroup

Here, we proceed to our analysis for U in family 8. of Lemma 1.

5.5.1 A construction of examples: The transfield groups

Let us consider the affine line $AG(1, q)$ with $q = p^n$ and the field $K := F_q$ which can be identified with $AG(1, q)$ after a choice of points 0 as origin and 1 as unity in $AG(1, q)$. Consider a subfield $k = F_{p^i}$ where i divides n. The group of translations E_q of $AG(1, q)$ is a vector space V over F_{p^i}. Every k-subspace W of V is invariant under the multiplicative group k^* of F_{p^i}. Henceforth, $W : k^*$ is a group in family 8 of Lemma 1. For every line A of W on 0, the stabilizer of A in $W : k^*$ is the group $AGL(1, F_{p^i})$ which is 2-transitive on A. For every hyperplane H of W such that $H \cap A = \{0\}$, we have $W = A \oplus H$. We define $U := W : k^*$ and we get that H is normal in U.

Let Ω be the set of affine hyperplanes of $A(W)$ parallel to H. Then U acts on Ω, $Ker\ U = H$, $U_0 \equiv H : k^*$ and U/H acts on Ω as the 2-transitive group $AGL(1, F_{p^i})$.

In summary, for any subfield k of F_q, for any k-subspace W of E_{p^n}, for any k-hyperplane H of W, the groups $U := W : k^*$, where k^* represents the multiplicative group and $U_0 = H : k^*$, constitute a 2-transitive pair with $Ker\ U = H$ and $U/H \equiv AGL(1, k)$ in its standard representation. We call the object U depending on k, W and H a *transfield group* and we denote it by $U(K, k, W, H)$.

Remark 3. *The conjugacy of two transfield groups $U(K, k, W_1, H_1)$ and $U(K, k, W_2, H_2)$ requires that $dimW_1 = dimW_2$ but this is by no means sufficient. It is a matter escaping to control thus far as explained in remark 4, section 4 of [4] that we repeated in section 3.*

5.5.2 The reduction pursued

We pursue the reduction of cases in view of the proof of Theorem 1. Assume that U is as in family 8 of Lemma 1. Namely $U = E_{p^m} : D$ which is a semidirect product of an elementary abelian E_{p^m} with $1 \leq m \leq n$ and a group D where D is cyclic of some order d, $d > 1$ and dividing $\frac{q-1}{(2,q-1)}$. Let us recall that U is not necessarily maximal in $G = \mathrm{PSL}(2, q)$.

We recall that G acts two-transitively on the projective line $P_1(q)$, $q = p^n$, p prime, $n \geq 1$. For any point ∞ of $P_1(q)$, we have that $P_1(q) - \{\infty\}$ is the affine line $AG(1, q)$ on which G_∞ acts as $E_q : \frac{q-1}{(2,q-1)} \leq AGL(1, q)$. Also for $0 \in AG(1, q)$ we get $G_{\infty 0}$ which is the cyclic group $\frac{q-1}{(2,q-1)}$.

We assume that U is a subgroup of G_∞. We look for all 2-transitive actions of U. Let α be such an action on a set Ω in which the stabilizer of some point O belonging to Ω is $U_{\mathrm{O}} = E_{p^i} : D'$ with $E_{p^i} \leq E_{p^m}$, $i \geq 1$ and $D' \leq D$. We use the notation $Ker\ U$ instead of $Ker\ \alpha$ for the kernel of the action.

In order to pursue we need the possible candidates for *Ker* $U \trianglelefteq U$ and so we need the normal subgroups of U.

Lemma 10. *Let U be a group $E_{p^m} : D$ as in family 8 of Lemma 1 together with a 2-transitive action of U on a set Ω. This action is determined by a subgroup U_0 of U and a kernel Ker U. Then one of the following holds:*

(1) Ker U contains E_{p^m} and we get a two-transitive action of the cyclic group D provided D has even order; here $|\Omega| = 2$, $U_0 = Ker\ U = E_{p^m} : D^+$, where D^+ is the subgroup of index 2 of D;

(2) Ker $U = 1$ and U is an affine group $AG(1, p^m)$, over a subfield of order p^m in F_q; here Ω is the affine line, $|D| = p^m - 1$ and $|\Omega| = p^m$;

(3) Ker U is a proper subgroup of E_{p^m} where m divides n, and U is a transfield group as in 5.5.1.

Proof. First we may assume that U is a subgroup of $\mathrm{PSL}(2, q)$, but also that it is a subgroup of $\mathrm{PGL}(2, q)$ and actually that it also is a subgroup of $AGL(1, q)$. The latter is the choice we make. Without loss of generality, we can choose $H = AGL(1, q) = E_{p^n} : (p^n - 1)$ where $(p^n - 1)$ is a cyclic group C containing D. This group has a standard two-transitive representation on the set $\tilde{\Omega}$ of points of the affine line $AG(1, q)$.

We start by looking for the normal subgroups of U in view of candidates for *Ker* U. Since $D \le C$, D fixes a unique point $\overline{0} \in AG(1, q)$. We consider the orbit $\overline{\Omega}$ of $\overline{0}$ under U and under E_{p^m}.

We follow with an observation concerning C. Without loss of generality, we may assume that every element of C is a mapping $x \to ax$ with $a \in F_q - \{0\}$.

The conjugates of these latter elements in H are the mappings $x \to ax + b$ with $b \in F_q$ and the $x \to x + b$ are the elements of a E_{p^n}. Any quotient of two such conjugates is an element of E_{p^n}.

Therefore, any normal subgroup of U containing some mapping $x \to ax + b$ with $a \ne 1$ contains E_{p^m}. If *Ker* U contains E_{p^m}, Lemma 5 applies and we get case (1).

We now assume that *Ker* U is contained in E_{p^m}. Then *Ker* U is an E_{p^s} for some s such that $0 \le s < m$. For $s = 0$, *Ker* $U = 1$. Then U is a sharply 2-transitive group by Lemma 3 applied to the action of D on $\Omega - \{O\}$. Then results due independently to Zassenhaus [22] and Tits [18], also Carmichael [7], give us case (2). This amounts to the construction of a field from U whose multiplicative group is D and whose additive group is E_{p^m}.

We are left with the case where $s \ge 1$. Now E_{p^m} is a vector space V of dimension m over F_p. The group D acts as a linear group on V. It admits an invariant subspace E_{p^s}. Since p does not divide d, the linear representation of D on V is totally reducible by Maschke's Theorem (see Lemma 4). Therefore there is a subspace $E_{p^{m-s}}$ disjoint from E_{p^s} which is invariant by D. The group $E_{p^{m-s}} : D$ is the abstract group $U/Ker\ U$ and it is 2-transitive on some set Ω. In this action $E_{p^{m-s}}$ is regular on Ω, hence $|\Omega| = p^{m-s}$. Then D fixes a point y in Ω, D is regular on $\Omega - \{y\}$ and so $|D| = p^{m-s} - 1$. Therefore, U is the affine group $AGL(1, k)$ over a subfield k of $GF(q)$. Now E_{p^m} is a k-vector space in which $E_{p^{m-s}}$ is a k-subspace of dimension 1 and E_{p^s} is a complementary k-subspace hence a hyperplane. Hence, $U, k, W := E_{p^m}, H := E_{p^s}$ constitute a transfield group. This gives case (3) of the Lemma. ∎

5.6 Case U is PSL$(2,r)$

For all of the following Lemmas, let us put $|\Omega| - 1 =: a$.

Lemma 11. *Let U be* PSL$(2,r)$. *Then one of the following holds:*

(1) $r = 2$, $U \cong S_3$, *Ker* $U \cong U_0 \cong Z_3$, $|\Omega| = 2$ *(unique in U);*

(2) $r = 2$, $U \cong S_3$, *Ker* $U = 1$, $|\Omega| = 3$, $U_0 \cong Z_2$ *(unique up to conjugacy in U and in* PSL$(2,q)$*);*

(3) $r = 3$, $U \cong A_4$, *Ker* $U = 1$, $|\Omega| = 4$, $U_0 \cong Z_3$ *(unique in U and unique up to fusion in* PGL$(2,q)$*);*

(4) $r > 3$, *Ker* $U = 1$, $|U_0| > \frac{r^3-r}{2\left(\frac{1}{\sqrt{2}}r^{3/2}+1\right)}$.

Proof. Either U is simple or $r \leq 3$.

For $r = 3$, U is A_4. Then either *Ker* $U \cong E_4$ or *Ker* $U = 1$. In the first case, $U/$*Ker* $U \cong Z_3$ and this group has no 2-transitive action. In the second case, E_4 acts as a regular group, $|\Omega| = 4$, $|U_0| = 3$ and we get (3).

For $r = 2$, $U \cong S_3$ and either *Ker* $U \cong Z_3$ or *Ker* $U = 1$. This gives immediately either (1) or (2). Observe that (1) and (2) fit with (a1) and (a2) in Lemma 8.

If U is simple, we get $r > 3$ and *Ker* $U = 1$. We observe that $(a+1)a$ cannot be equal to $r(r^2-1) = r^3 - r$ for otherwise U is sharply 2-transitive. Then U has a regular normal subgroup by [22, 18, 7] contradicting the simplicity of U.

Therefore we have $a^2 < (a+1)a \leq \frac{r(r^2-1)}{2} < \frac{1}{2}r^3$. Hence $a < \frac{1}{\sqrt{2}}r^{3/2}$ and $a + 1 < \frac{1}{\sqrt{2}}r^{3/2} + 1$.

Also,

$$|U_0|.|\Omega| = |U_0|.(a+1) \geq \frac{1}{2}r(r^2-1).$$

Hence, we get (4). ∎

We now deal with case (4) of Lemma 11.

Observe that

$$|U_0| > \frac{r^3 - r}{2\left(\frac{1}{\sqrt{2}}r^{3/2}+1\right)} > \frac{1}{2}\left(\frac{r^3-r}{r^{3/2}+1}\right).$$

We make use of the latter bound to give an elementary proof of the following Lemma.

Lemma 12. *Let U be* $\mathrm{PSL}(2,r)$, $r > 3$, *Ker* $U = 1$, $|U_0| > \frac{1}{2}\frac{r^3-r}{r^{3/2}+1}$. *Then one of the following occurs:*

(1) *For every r, $U_0 \cong E_r : \frac{r-1}{(2,r-1)}$, $|\Omega| = r+1$. This exists and is a unique permutation group for U, (this is unique up to conjugacy in U; observe that there are two classes as U in G and these are fused in* $\mathrm{PGL}(2,q)$*);*

(2) *for $r = 11$, $U_0 \cong A_5$, $|\Omega| = 11$. There are two such representations in U. In G, there are four such representations, involving 2 classes of A_5 and 2 classes of* $\mathrm{PSL}(2,11)$*; they fuse in* $\mathrm{PGL}(2,q)$*;*

(3) *for $r = 9$, $U \cong A_6$, $U_0 \cong A_5$, $|\Omega| = 6$. There are two such representations in U. In G, there are four such representations, involving 2 classes of A_5 and 2 classes of A_6; they fuse in* $\mathrm{PGL}(2,q)$*;*

(4) *for $r = 7$, $U \cong$* $\mathrm{PSL}(3,2)$, *$U_0 \cong S_4$, $|\Omega| = 7$. There are two such representations in U. In G, there are four such representations, involving 2 classes of S_4 and 2 classes of* $\mathrm{PSL}(3,2)$*; they fuse in* $\mathrm{PGL}(2,q)$.

Proof. We consider subcases in which every entry represents a type of maximal subgroup U_0 of $\mathrm{PSL}(2,r)$ according to Tables 1 and 2.

Subcase 1. $U_0 \cong E_r : \frac{r-1}{(2,r-1)}$

Here, $\frac{|U|}{|U_0|} = r+1 = |\Omega|$. This is the standard representation of U, which is unique. Hence we get (1) in view of the fact that G contains two conjugacy classes of $\mathrm{PSL}(2,r)$.

Subcase 2. U_0 is $\mathrm{PSL}(2,r')$ or $\mathrm{PGL}(2,r')$

Here $r = p^n$, $r' = p^m$ with $m \mid n$, $m \neq n$ and $n = mv$ where v is prime, $v \geq 2$.

If U acts 2-transitively on the cosets of U_0, then necessarily, $|U_0| \geq |U|/|U_0| - 1$ or in other words,

$$|U_0|^2 + |U_0| \geq |U|$$

Let us first assume that r is odd and $U_0 = PSL(2,r')$. Then

$$|U_0|^2 + |U_0| \geq |U| \geq \frac{r'^2(r'^4-1)}{2} = 2(\frac{r'(r'^2-1)}{2})^2 + r'(r'^2-1) = 2|U_0|^2 + |U_0|$$

a contradiction. Similar computations permit to exclude the case where r is even. Therefore $v = 2$, $r = r'^2$. Since U_0 is maximal in U, we need only consider the case $U_0 = \mathrm{PGL}(2,r')$.

We replace r' by $r^{1/2}$.

Now $|U_0| = r^{1/2}(r-1)$ because $U_0 \cong \mathrm{PGL}(2,r^{1/2})$ and

$$a+1 = |\Omega| = \frac{\frac{r(r^2-1)}{(2,r-1)}}{r^{1/2}(r-1)} = \frac{r^{1/2}(r+1)}{(2,r-1)}.$$

Thus
$$a = \frac{r^{3/2} + r^{1/2}}{(2, r-1)} - 1 \quad (a)$$
and we recall that a divides $|U_0|$.

We deal first of all with the case $r-1$ even. Then $(2, r-1) = 2$. Hence, by (a)

$r^{3/2} + r^{1/2} - 2$ divides $2(r^{3/2} - r^{1/2})$ so that it divides
$$(2r^{3/2} - 2r^{1/2}) - 2(r^{3/2} + r^{1/2} - 2) = 4 - 4r^{1/2} \text{ and also } 4r^{1/2} - 4.$$
Thus $r^{3/2} \leq (4r^{1/2} - 4) - r^{1/2} + 2 = 3r^{1/2} - 2$. This is a contradiction for all $r > 3$, as required in the present lemma.
Therefore $r - 1$ is odd and $(2, r-1) = 1$.

By (e) $r^{3/2} + r^{1/2} - 1$ divides $r^{3/2} - r^{1/2}$, so that it divides
$$(r^{3/2} - r^{1/2}) - (r^{3/2} + r^{1/2} - 1) = 1 - 2r^{1/2} \text{ and also } 2r^{1/2} - 1.$$
Therefore $r^{3/2} \leq r^{1/2}$, a contradiction.
Thus the assumption of Subcase 2 cannot hold.

Subcase 3. U_0 is one of $D_{r\pm 1}$ for q odd and $D_{2(r\pm 1)}$ for q even.

In each case $a+1$ is the index of U_0 in U. Therefore $a = \frac{r(r\mp 1)}{2} - 1$. Recalling that a divides $|U_0|$ we get $\frac{r(r\mp 1)}{2} - 1 \mid \frac{2(r\pm 1)}{(2,r-1)}$. Therefore,
$$r^2 - r - 2 \leq r(r \mp 1) - 2 \leq 4(r \pm 1) \leq 4r + 4.$$
This yields $r^2 \leq 5r + 6$ and therefore, $r \leq 5$. And $r > 3$ by our hypothesis, hence $r = 4$ or 5.

For $r = 5$, $U \cong \mathrm{PSL}(2,5) \cong A_5$ with $|\Omega| = 6$, $U_0 \cong D_{10}$ which is not in the hypothesis of the present subcase.

For $r = 4$, $U \cong \mathrm{PSL}(2,4) \cong A_5$ with $|\Omega| = 5$, $U_0 \cong A_4$ which is not in the hypothesis of the present subcase.

Subcase 4. U_0 is one of A_4, S_4, A_5.

4.1. Assume U_0 is A_5 Then $60 = |U_0| \geq \frac{1}{2}\frac{r^3 - r}{r^{3/2}+1}$ and we get $24 > r$. Hence r is one of $19, 16, 11, 9, 5$ or 4 (we left aside the values of r for which $\mathrm{PSL}(2, r)$ does not contain any A_5). For $r = 19$, $a + 1 = 57$, $a = 56$ and this does not divide $|U|$. For $r = 16$, $a + 1 = 68$, $a = 67$ and this does not divide $|U|$.

For $r = 11$, $a + 1 = 11$, $a = 10$ and we get (2) provided we apply obvious conjugation and fusion criteria.

For $r = 9$, $U \cong \mathrm{PSL}(2, 9) \cong A_6$, $a + 1 = 6$, $a = 5$ and we get (3) provided we apply obvious conjugation and fusion criteria.

For $r = 5$ and $r = 4$ we have $\mathrm{PSL}(2,5) \cong \mathrm{PSL}(2,4) \cong A_5$. This case is impossible: indeed it gives us $U = U_0$.

4.2. Assume U_0 is S_4. Then $24 = |U_0| \geq \frac{1}{2}\frac{r^3-r}{r^{3/2}+1}$ and we get $16 > r$. Hence r is one of 9 or 7 (we left aside the values of r for which $\mathrm{PSL}(2,r)$ does not contain any S_4).

For $r = 9$, $\mathrm{PSL}(2,9) \cong A_6$. Then $a+1 = 15$, $a = 14$ and so 7 divides $|A_6|$, a contradiction.

For $r = 7$, there are two conjugacy classes of S_4 in $\mathrm{PSL}(2,7)$ and we get (4) provided we apply obvious conjugation and fusion criteria.

4.3. Assume U_0 is A_4. Then $12 = |U_0| \geq \frac{1}{2}\frac{r^3-r}{r^{3/2}+1}$ and we get $9 > r$. Hence r is one of 5 or 4 (we left aside the values of r for which A_4 is not maximal in $\mathrm{PSL}(2,r)$).

Observe that for $r = 4$, $A_4 \cong E_{2^2} : (4-1)$ is maximal in $\mathrm{PSL}(2,4)$.

For $r = 5$ or 4, $\mathrm{PSL}(2,5) \cong \mathrm{PSL}(2,4) \cong A_5$ and we get the standard representation corresponding to $r = 4$ hence (1). ■

5.7 Case U is $PGL(2,r)$

We now deal with the case where $U = \mathrm{PGL}(2,r)$ with r odd.

Lemma 13. *Let U be $\mathrm{PGL}(2,r)$ with r odd. Then one of the following occurs:*

(1) $U_0 = Ker\ U \cong \mathrm{PSL}(2,r)$, $|\Omega| = 2$;

(2) $Ker\ U = 1$, $U_0 \cong E_r : (r-1)$, $|\Omega| = r+1$;

(3) $r = 3$, $U \cong S_4$, $q = \pm 1(8)$, $Ker\ U \cong E_4$, $U/Ker\ U \cong S_3$, $U_0 \cong D_8$, $|\Omega| = 3$;

(4) $r = 5$, $U \cong S_5$, $U_0 \cong S_4$, $Ker\ U \cong 1$, $|\Omega| = 5$.

Proof. For $r = 3$, U is indeed S_4 which exists if and only if $q = \pm 1(8)$. There are three representations as we want. The first is of degree 2 with A_4 as point stabilizer. This is a particular case of (1). The second is the standard representation on 4 letters, which is a special case of (2). The third is on the three cosets of D_8, hence it gives (3).

Let $r > 3$. Then $\mathrm{PSL}(2,r)$ is simple. Thus, either $Ker\ U \cong \mathrm{PSL}(2,r)$ or $Ker\ U = 1$. In the first case, we get (1). In the second case, we shall show that (2) or (4) hold. As the action is faithful on Ω, and as $\mathrm{PSL}(2,r)$ is a proper normal subgroup of $\mathrm{PGL}(2,r)$, the group $\mathrm{PSL}(2,r)$ is transitive on Ω.

Next we show that $\mathrm{PSL}(2,r)$ is primitive. Assume by way of contradiction that it is not. Then the stabilizer of a point is a subgroup H that is not maximal in $\mathrm{PSL}(2,r)$. Hence there exists a subgroup K with $H < K < \mathrm{PSL}(2,r)$. Now, the group U necessarily is also imprimitive for it preserves the blocks given by K and its cosets. Hence U is not 2-transitive, a contradiction. As a next step to get $\mathrm{PSL}(2,r)$ in its standard representation we consider each of its primitive representations under the restriction that r is odd. We consider every maximal subgroup U_0^+ of $\mathrm{PSL}(2,r) = \mathrm{PGL}(2,r)^+$, as in Table 2.

Case 1. $U_0^+ = E_r : \frac{(r-1)}{2}$. This provides indeed the standard two-transitive representation of $\mathrm{PSL}(2,r)$ and of $\mathrm{PGL}(2,r)$ as well. Hence case (2) of our lemma.

Case 2. $U_0^+ = D_{r+1}$ with $r \neq 7,9$, $|\Omega| = \frac{r(r-1)}{2}$ therefore $\frac{r^2-r}{2}.\left(\frac{r^2-r}{2}-1\right) \mid r(r^2-1) = |\mathrm{PGL}(2,r)|$. Thus $r^2-r-2 \mid 4(r+1)$. Hence $(r-2)(r+1) \mid 4(r+1)$. Thus $(r-2) \mid 4$ hence $r=3$, a contradiction with our hypothesis.

Case 3. $U_0^+ = D_{r-1}$ with $r \neq 3,5,7,9,11$, $|\Omega| = \frac{r(r+1)}{2}$ therefore $\frac{r^2+r}{2}.\left(\frac{r^2+r}{2}-1\right) \mid r(r^2-1) = |\mathrm{PGL}(2,r)|$. Hence $r^2+r-2 \mid 4(r-1)$. Thus $(r+2) \mid 4$ hence $r=2$, a contradiction with the hypothesis of the present lemma.

Case 4. $U_0^+ = A_4$, with r prime and $r = 3,13,27,37(40)$ or $r=5$, $|\Omega| = \frac{r(r^2-1)}{24}$. Here, $|U_0| = 24$, hence $|\Omega|-1 = \frac{r(r^2-1)}{24} - 1 \mid 24$ and so $r < 9$, r is one of 3 or 5. Case $r=3$ was ruled out at the beginning of the proof. Hence $r=5$. Then $U = \mathrm{PGL}(2,5) \cong S_5$, $|\Omega| = 5$, hence $U_0 = S_4$. Which is case (4) of our lemma.

Case 5. $U_0^+ = S_4$, with r prime and $r = \pm 1(8)$, $|\Omega| = \frac{r(r^2-1)}{48}$. Here, $\mid U_0 \mid = 48$, hence $|\Omega| - 1 = \frac{r(r^2-1)}{48} - 1 \mid 48$ and so $r < 14$. Then $r=7$. Therefore $U = \mathrm{PGL}(2,7)$, $|\Omega| = 7$, $\mid U_0 \mid = 48$, but there is no such subgroup in $\mathrm{PGL}(2,7)$.

Case 6. $U_0^+ = A_5$, with
$$\begin{cases} r = 5^m & m \textit{ odd prime} \quad \textit{or} \\ r = p = \pm 1(5) & p \textit{ prime} \quad \textit{or} \\ r = p^2 = -1(5) & p \textit{ prime} \end{cases}$$
and $|\Omega| = \frac{r(r^2-1)}{120}$. Here, $\mid U_0 \mid = 120$, hence $|\Omega| - 1 = \frac{r(r^2-1)}{120} - 1 \mid 120$ and so $r < 26$. In view of the conditions for A_5 to be maximal the first condition $r = 5^m$ with m odd prime is in contradiction with $r < 26$. If $r = \pm 1(5)$ and r is prime, then r is one of 11 or 19. If $r = -1(5)$ and r is the square of a prime, then r is one of 4 or 9. We are left with the values $4,9,11,19$ for r.

The values $r = 4,19$ may be ruled out by $|\Omega| - 1 = \frac{r(r^2-1)}{120} - 1 \mid 120$, indeed they lead to a contradiction.

If $r = 11$, $U = \mathrm{PGL}(2,11)$, $|\Omega| = 11$, $\mid U_0 \mid = 120$ but there is no such subgroup in $\mathrm{PGL}(2,11)$.

If $r = 9$, $U = \mathrm{PGL}(2,9)$, $|\Omega| = 6$, $\mid U_0 \mid = 120$ but there is no such subgroup in $\mathrm{PGL}(2,9)$.

Case 7. This case is ruled out using the same argument as in the beginning of Subcase 2 of the proof of Lemma 12.

Case 8. $U_0^+ = \mathrm{PGL}(2,r')$ with $r = r'^2$, $|\Omega| = \frac{r(r^2-1)}{2r'(r'^2-1)}$. Here, $\mid U_0 \mid = 2r'(r'^2 - 1)$, hence
$$|\Omega| - 1 = \frac{r'(r+1)}{2} - 1 \mid 2r'(r'^2-1) \qquad (d)$$
This is equivalent to $r'^3 + r' - 2 \mid 4r'^3 - 4r'$. A factor common to the divisor and r' is at most 2, hence it is 1. Then $r'^3 + r' - 2 \mid 4r'^2 - 4$ which implies $r'^2 + r' + 2 \mid$

$4r' + 4$. We obtain $r'^2 + r' + 2 \leq 4r' + 4$, hence $r' < 4$ and so $r' = 3, r = 9$. But this is in contradiction with (d). ∎

5.8 Case U is A_4, S_4, A_5

Lemma 14. *Let U be one of A_4, S_4 and A_5. Then one of the following holds:*

(1) $U = A_4$, Ker $U = 1$, $|\Omega| = 4$, $U_0 = Z_3$ (unique in U and unique up to fusion in $\mathrm{PGL}(2,q)$);

(2) $U = S_4$, $U_0 =$ Ker $U \cong A_4$, $|\Omega| = 2$ (two such representations up to conjugacy in U; they are fused in $\mathrm{PGL}(2,q)$);

(3) $U = S_4$, Ker $U = 1$, $U_0 \cong D_6$, $|\Omega| = 4$, (two such representations up to conjugacy in U; they are fused in $\mathrm{PGL}(2,q)$);

(4) $U = S_4$, Ker $U \cong E_4$, $U/$Ker $U \cong S_3$, $U_0 \cong D_8$, $|\Omega| = 3$ (unique in U and unique up to fusion in $\mathrm{PGL}(2,q)$);

(5) $U = A_5$, Ker $U = 1$, $U_0 \cong A_4$,$|\Omega| = 5$. This exists and is a unique permutation group for U, (two such representations up to conjugacy in G; they are fused in $\mathrm{PGL}(2,q)$);

(6) $U = A_5$, Ker $U = 1$, $U_0 \cong D_{10}$, $|\Omega| = 6$. This exists and is a unique permutation group for U, (two such representations up to conjugacy in G; they are fused in $\mathrm{PGL}(2,q)$);

Proof. Every matter of conjugacy or fusion is straightforward. For $U = A_4$, case (3) of Lemma 11 applies. For $U = S_4$, cases (1), (2), and (3) of Lemma 13 apply, since $S_4 \cong \mathrm{PGL}(2,3)$. For $U = A_5$, case (1) of Lemma 12 applies twice, since $A_5 \cong \mathrm{PSL}(2,4)$ and also $A_5 \cong \mathrm{PSL}(2,5)$. ∎

5.9 Proof of Theorem 1

The proof requires an analysis of each of the 14 families in Lemma 1. These families have been distributed as follows. Family 1 is part of section 5.2 and does not contribute to Theorem 1. Family 2 is part of section 5.4 (and 5.5). It does not contribute to Theorem 1. Families 3 and 4 are part of section 5.2 and they contribute to cases (19) and (21) of Theorem 1. Family 5 is part of section 5.3 and it contributes to cases (14), (15) and (16) of Theorem 1. Family 6 is part of section 5.3 and it contributes to case (17) of Theorem 1. Family 7 is part of section 5.4 (and 5.5) and it contributes to case (21) of Theorem 1. Family 8 is part of section 5.5 and it contributes to cases (1), (2) and (20) of Theorem 1. Families 9, 10 and 11 are part of section 5.8 and they contribute to cases (5), (6), (11), (12) and (13) of Theorem 1. Family 12 is part of section 5.6 and it contributes to cases (3), (4), (5), (7), (8), (9) and (10) of Theorem 1. Family 13 is part of section 5.7 and it contributes to cases (11), (12), (13) and (18) of Theorem 1. Family 14 is part of section 5.6. However, it is excluded by the fact that U is assumed to be a proper subgroup of G.

Hence, Theorem 1 readily follows from Lemmas 5, 6, 7, 8, 9, 10, 11, 12 and 13 and 14. We recall that A_5 is covered in the role of U as PSL$(2,5)$ and PSL$(2,4)$, that S_4 is covered as PGL$(2,3)$ and that A_4 is covered as PSL$(2,3)$.

If PSL$(2,r)$ = PGL$(2,r)$, namely r even, we apply Lemma 11 and 12 . Finally, when r is odd we apply Lemma 13.

We check that each case stated in Theorem 1 has been covered in one at least of the Lemmas.

5.10 Proof of Theorem 2

The proof requires an analysis of each of the 13 families I, II, ..., XIII in Tables 1 and 2. In this section we deal with cases in Theorem 1 and in Theorem 2 bearing the same name (like (6) for instance). In order to distinguish these the first is now called 1.6 and the second is called 2.6.

Family I is part of cases 1.1, 1.2 and 1.20 and so 2.2. Families II and III are part of cases 1.14, 1.15 and 1.17 and so 2.14 and 2.16. Family IV is part of case 1.6 and so 2.6. Family V is part of cases 1.3, 1.4, 1.10 and so 2.3, 2.4, 2.10. Family VI is part of cases 1.1, 1.2, 1.20 and so 2.1. Families VII and VIII are part of cases 1.14, 1.15, 1.16, 1.17 and so 2.15, 2.17, 2.18, 2.19. Family IX is part of cases 1.2, 1.5 and so 2.2, 2.5. Family X is part of cases 1.11, 1.13 and so 2.11, 2.13. Family XI is part of cases 1.6, 1.10 and so 2.6, 2.10. Family XII is part of cases 1.5, 1.7, 1.8, 1.9, 1.10 and so 2.5, 2.7, 2.8, 2.9, 2.10. Family XIII is part of cases 1.11, 1.12, 1.13, 1.18 and so 2.11, 2.12, 2.13, 2.20.

References

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math* , 76:469–514, 1984.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: the user language. *J. Symbolic Comput.*, (3/4):235–265, 1997.

[3] F. Buekenhout, P. Cara, M. Dehon, and D. Leemans. Residually weakly primitive geometries of small almost simple groups : a synthesis. In A. Pasini, editor, *Topics in Diagram Geometry*, *Quaderni Mat.*, 12:1–27. 2003.

[4] F. Buekenhout, J. De Saedeleer and D. Leemans. On the rank two geometries of the groups PSL$(2,q)$: part II. *Ars Mathematica Contemporanea*, 6(2):365–388, 2013.

[5] F. Buekenhout and M. Mixer. 2-Transitive Group Arithmetic. *Atti del Seminario Matematico e Fisico dell' Università di Modena e Reggio Emilia*, LVIII: 129–142, 2011.

[6] W. Burnside. *Theory of Groups of Finite Order. 2nd ed.* Dover Publications, Inc, New York, 1955.

[7] R. D. Carmichael. Algebras of certain doubly transitive groups. *Amer J. Math.* 53: 631–644, 1931.

[8] M. J. Collins. Representations and characters of finite groups. *Cambridge Studies in Advanced Mathematics*, 22. Cambridge University Press, Cambridge, 1990. xii+242 pp.

[9] J. De Saedeleer. *The residually weakly primitive and locally two-transitive rank two geometries for the groups* $\mathrm{PSL}(2,q)$. PhD thesis, Université Libre de Bruxelles, 2010.

[10] J. De Saedeleer and D. Leemans. On the rank two geometries of the groups $\mathrm{PSL}(2,q)$: part I. *Ars Mathematica Contemporanea*, 3(2):177–192, 2010.

[11] L. E. Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[12] M. Giudici, C. H. Li, and C. E. Praeger. Analyzing finite locally s-arc transitive graphs. *Trans. Amer. Math. Soc.* (electronic), 356(1):291–317, 2004.

[13] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[14] O.H. King. The subgroup structure of finite classical groups in terms of geometric configurations. *Survey in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, 29–56. Cambridge Univ. Press, Cambridge, 2005.

[15] P. B. Kleidman, M. W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Math. Soc. Lecture Note Series, 129, Cambridge Univ. Press, Cambridge, 1990.

[16] E. H. Moore. The subgroups of the generalized finite modular group. *Decennial Publications of the University of Chicago*, 9:141–190, 1904.

[17] M. Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

[18] J. Tits. Généralisation des groupes projectifs I, II, III, IV. *Académie Royale de Belgique, Bulletin de la classe des Sciences*, 35: 197–208, 224–233, 568–589, 756–773, 1949.

[19] P. Vanden Cruyce. *Géométries des groupes* $PSL(2,q)$. PhD thesis, Université Libre de Bruxelles, 1985.

[20] H. Wielandt. *Finite permutation groups*. Translated from the German by R. Bercov. Academic Press, New York, 1964.

[21] A. Wiman. Bestimmung aller untergruppen einer doppelt unendlichen reihe von einfachen gruppen. *Bihan till K. Svenska Vet.-Akad.Handl.*, 25:1–147, 1899.

[22] H. Zassenhaus. Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. *Hamburg Abh.*, 11:17–40, 1936.

Université Libre de Bruxelles
C.P.216 - Géométrie
Boulevard du Triomphe
B-1050 Bruxelles

University of Auckland,
Department of Mathematics,
Private Bag 92019,
Auckland, New Zealand
email : j.desaedeleer@auckland.ac.nz