SHARPLY TRANSITIVE SETS IN PGL$_2$(K)

SEAN EBERHARD

Abstract. Here is a simplified proof that every sharply transitive subset of PGL$_2$(K) is a coset of a subgroup.

Let $G$ be a group acting on a set $\Omega$ on the left. A subset $S \subseteq G$ is called sharply transitive, or regular, if for every $x, y \in \Omega$ there is a unique $g \in G$ such that $gx = y$. For example, sharply transitive subsets of $S_n$ can be identified with $n \times n$ Latin squares, while sharply 2-transitive subsets, i.e., sets which are sharply transitive for the action on ordered pairs, can be identified with affine planes of order $n$.

In this note we consider $G = \text{PGL}_2(K)$ and its action on the projective line $\mathbb{P}^1(K)$, where $K$ is a finite field of order $q$. It follows from Dickson’s classification of the subgroups of $\text{PSL}_2(K)$ that the only regular subgroups of $\text{PGL}_2(K)$ are

1. cyclic groups $C_{q+1}$,
2. dihedral groups $D_{(q+1)/2}$ ($q$ odd),
3. $A_4$ ($q = 11$),
4. $S_4$ ($q = 23$),
5. $A_5$ ($q = 59$)

(see [B] or [VM]), and there is a single conjugacy class of subgroups in each case. Remarkably, other than these subgroups and their cosets, there are no further regular subsets of $G$.

Theorem 1 ([BL,T,BK]). If $S \subseteq \text{PGL}_2(K)$ is sharply transitive on $\mathbb{P}^1$ and $1 \in S$ then $S$ is a subgroup.

This result was originally conjectured by Bonisoli in [B]. The complete proof is spread across several papers: in [BL,T], Bader, Lundardon, and Thas classified flocks of the hyperbolic quadric in $\mathbb{P}^3$, and the equivalence with regular sets was noted in [BK]. The original proof is somewhat involved. See [T2] for a more recent summary. A partly simplified proof is given by Durante and Siciliano [DS], but for the main technical step the reader is referred to [T]. Here we give a short, self-contained, direct proof avoiding the detour through flocks. Still, the interested reader will find close analogies with [DS,T].

The key step is the following lemma, which can be seen as a version of Segre’s “lemma of the tangents” (see [S, (2)]).

---

SE has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement No. 803711).
Lemma 2. Suppose $S$ is a regular subset of $\text{PGL}_2(K)$ containing the elements

\[
g_1 = \begin{pmatrix} 0 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix},
\]
\[
g_3 = \begin{pmatrix} a_3 & b_3 \\ 0 & d_3 \end{pmatrix}, \quad g_4 = \begin{pmatrix} a_4 & b_4 \\ c_4 & 0 \end{pmatrix}.
\]

Then

\[b_1 d_2 a_3 c_4 = c_1 a_2 d_3 b_4.\]

Here and below elements of $\text{PGL}_2(K)$ are written as matrices, understanding that the expression is determined only up to a scalar. Elements of $\mathbb{P}^1$ will be written as $(x:y)$.

Proof. Assume first that $g_1, g_2, g_3, g_4$ are distinct. Label the elements of $S$ as $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} (i = 1, \ldots, q+1)$.

By regularity, the columns $(a_i : c_i)$ and $(b_i : d_i)$ both trace out $\mathbb{P}^1$. Since $S^{-1}$ is also regular, the same is true of the rows $(a_i : b_i)$ and $(c_i : d_i)$. By excluding 0 and $\infty$ in each case, it follows that the products

\[
\prod_{i \neq 1,2} a_i/b_i, \prod_{i \neq 2,4} b_i/d_i, \prod_{i \neq 3,4} d_i/c_i, \prod_{i \neq 1,3} c_i/a_i
\]

are each equal to the product of all the nonzero elements of $K$, which is $-1$. By multiplying these together we get

\[
\frac{b_1 d_1 a_3 b_3 c_4 a_4}{d_1 c_1 c_2 a_2 b_3 d_3 b_4} \prod_{i > 4} a_i b_i d_i c_i \frac{1}{a_i} = 1.
\]

Simplifying gives the claimed relation.

The only possible coincidences between $g_1, g_2, g_3, g_4$ are $g_1 = g_4$ and $g_2 = g_3$. In these cases the proof is similar. \qed

We can now prove Theorem 1. Let $S \subseteq \text{PGL}_2(K)$ be a regular set containing 1. Let $g, h \in S \setminus \{1\}$. It suffices to prove $gh \in S$. By regularity, for each $x \in \mathbb{P}^1$ there is a unique $k \in S$ such that

\[kh^{-1}x = gx.\]

Moreover $k \neq h$, because $g$ has no fixed points (likewise $k \neq g$). Since $\mathbb{P}^1$ has size $q + 1$ and there are at most $q$ possibilities for $k$, there is some $k \in S$ such that $g^{-1}kh^{-1}$ has at least two fixed points, say $x$ and $y$. Since $x$ and $gx$ are distinct, we may coordinatize $\mathbb{P}^1$ in such a way that

\[x = (1:0), \quad gx = (0:1).\]

Since $h$ has no fixed points, $h(1:0) \neq (1:0)$, so there is some $u \in \text{PGL}_2(K)$ of the form

\[u = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\]

such that $hu(0:1) = (1:0)$. For this $u$ we have

\[ku(0:1) = kh^{-1}(1:0) = g(1:0) = (0:1).\]
Thus $Su$ is a regular set containing the elements

$$
gu = \begin{pmatrix} 0 & b \\ 1 & * \end{pmatrix}, \quad ku = \begin{pmatrix} a & 0 \\ * & 1 \end{pmatrix},
$$

$$
u = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \quad hu = \begin{pmatrix} * & 1 \\ c & 0 \end{pmatrix},
$$

for unknown nonzero values $a, b, c$ (and further unknown values hidden by $*$). By the lemma, we must have $a = bc$. Hence

$$
hk^{-1}g = (hu)(ku)^{-1}(gu)u^{-1}
$$

$$
= \begin{pmatrix} * & 1 \\ c & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ * & a \end{pmatrix} \begin{pmatrix} 0 & b \\ 1 & * \end{pmatrix} \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}
$$

$$
= \begin{pmatrix} a & * \\ 0 & bc \end{pmatrix}
$$

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

Since $hk^{-1}g$ has at least two fixed points ($x$ and $y$), we must have $hk^{-1}g = 1$. Hence $gh = k \in S$, as required.

References

[B] A. Bonisoli, The regular subgroups of the sharply 3-transitive finite permutation groups, Combinatorics '86 (Trento, 1986), 1988, pp. 75–86. MR931307

[BK] A. Bonisoli and G. Korchmáros, Flocks of hyperbolic quadrics and linear groups containing homologies, Geom. Dedicata 42 (1992), no. 3, 295–309. MR1164537

[BL] L. Bader and G. Lunardon, On the flocks of $Q^+(3, q)$, Geom. Dedicata 29 (1989), no. 2, 177–183. MR988267

[DS] N. Durante and A. Siciliano, $(B)$-geometries and flocks of hyperbolic quadrics, J. Combin. Theory Ser. A 102 (2003), no. 2, 425–431. MR1979544

[S] B. Segre, Ovals in a finite projective plane, Canadian J. Math. 7 (1955), 414–416. MR71034

[T1] J. A. Thas, Flocks, maximal exterior sets, and inversive planes, Finite geometries and combinatorial designs (Lincoln, NE, 1987), 1990, pp. 187–218. MR1079748

[T2] , Finite fields and Galois geometries, Finite fields and applications, 2008, pp. 251–265. MR2436341

[VM] R. C. Valentini and M. L. Madan, A hauptsatz of L. E. Dickson and Artin-Schreier extensions, J. Reine Angew. Math. 318 (1980), 156–177. MR579390

Sean Eberhard, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

Email address: eberhard@maths.cam.ac.uk