Journal of Geometry
Vol.27 (1986)

0047-2468/86/020188-07$1.50+0.20/0

REGULAR SETS ON THE PROJECTIVE LINE

Jennifer D. Key, Johannes Siemons and Ascher Wagner

We show that if G is the group $P\Gamma L(2,q)$(for q a prime-power) acting on the points of the projective line in the usual way, then for $q>27$ there is a set Λ of 5 points such that no non-trivial element of G fixes Λ .

1. INTRODUCTION

A set of elements in a geometry with an automorphism group G is said to be G-regular if the identity automorphism is the only automorphism in G that leaves these elements invariant as a set. In [5] it was shown that G-regular sets of points exist in general when G is the automorphism group of a finite projective or affine space of geometric dimension at least two over a field of at least three elements. Here we obtain a similar result for the line : see Theorem, Section 3.

For groups acting on sets, using the classification theorem for finite simple groups, it was shown by Cameron, Neumann and Saxl [1] that all finite primitive groups of sufficiently large degree, not containing the alternating group of the same degree, have regular sets.

2. NOTATION

For permutation groups we use in general the standard notation of Wielandt [6], and for finite geometries that of Dembowski [3]. Variations from these are stated below.

The symmetric and alternating groups acting on a set Ω of finite size n are denoted by $\mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega)$ respectively, or by S_n and A_n . If $G \leq \mathrm{Sym}(\Omega)$ and $\Delta \subseteq \Omega$, then $G_{\{\Delta\}}$ denotes the global stabilizer of Δ in

G, and $G_{(\Delta)}$ denotes the pointwise stabilizer of Δ in G. We will refer to $G_{\{\Delta\}}/G_{(\Delta)}$ as the restriction of G to Δ, denoted G^{Δ}. The set Δ is a *G-regular set* if $G_{\{\Delta\}} = 1$; if $|\Delta| = k$ then it will be referred to as a *regular k-set* for G. When there is no ambiguity concerning the group G, we will speak merely of *regular sets* or *regular k-sets*.

The projective semi-linear group $P\Gamma L(2,q)$ where $q = p^n$, p a prime, will act in the natural way on the projective line $PG(1,q)$ of point set $\Omega = \{\infty\} \cup GF(q)$. If t_1, t_2, t_3, t_4 denote the co-ordinates of four distinct points on the projective line then their *cross-ratio* r is defined by

$$r = (t_1,t_2;\ t_3,t_4) = \frac{(t_3-t_1)(t_4-t_2)}{(t_4-t_1)(t_3-t_2)} \ .$$

If the points are taken in all possible different orders, then the set of cross-ratios obtained is $\{r,r^{-1},1-r,(1-r)^{-1},\ 1-r^{-1},(1-r^{-1})^{-1}\}$ (see, for example [4] p.41). The projective general linear group $PGL(2,q)$ is the subgroup preserving the cross-ratio.

3. REGULAR SETS

We note here that in all cases where non-trivial computations are required, we have used the Cayley language of J. Cannon [2], on the Birmingham University Computer.

Before giving the theorem, we need a lemma.

LEMMA : Let G be $P\Gamma L(2,q)$ in its natural action on the points Ω of the projective line, where $\Omega = K \cup \{\infty\}$, for $K = GF(q)$, $q = p^n$ and p a prime. Let $A = Aut(K) = \langle\tau\rangle$. For each a in $K\setminus\{0,1\}$, let $\mathcal{C}(a) = \{a,a^{-1},1-a,(1-a)^{-1},\ 1-a^{-1},\ (1-a^{-1})^{-1}\}$, and let $\mathcal{S}(a) = \bigcup_{\sigma\in A} \mathcal{C}(a)^{\sigma}$. Then if $q>11$, $q\neq 16$, there exists a in K such that $|\mathcal{S}(a)| = 6n$.

PROOF : Let $\Delta = \{\infty,0,1\}$ and let $H = G_{\{\Delta\}}$. If g_1 and g_2 are the elements of H defined by $g_1 : x \to \frac{1}{x}$, $g_2 : x \to 1-x$ for each $x\in\Omega$, then $H = LA$ where $L = \langle g_1,g_2\rangle \simeq S_3$. Further, $A = Z(H)$, the centre of H. Then if a is any element of $K\setminus\{0,1\}$, $\mathcal{S}(a)$ is clearly the orbit of a under H, and $\mathcal{C}(a)$ is the orbit of a under L. Thus $|\mathcal{S}(a)| = 6n$ if and only if H acts regularly on $\mathcal{S}(a)$, i.e. if and only if $H_a = 1$. Any g in H_a can be written $g = h\sigma^{-1}$ where $h\varepsilon L$, $\sigma^{-1}\varepsilon A$, and $a^h = a^\sigma$. Since $\sigma\varepsilon Z(H)$, this implies that for any integer s, $a^{h^s} = a^{\sigma^s}$. If $h^s = 1$ then $a^{\sigma^s} = a$. If we choose a to be outside all proper subfields of K then this implies that $\sigma^s = 1$. Since all elements h of L have order 1, 2 or 3, the same must be true for the corresponding σ.

Suppose firstly that $2\nmid n$ and $3\nmid n$. Then $\sigma = 1$ and $a^h = a^\sigma = a$. Thus a satisfies one of the equations:

$$a=a^{-1},\ a=1-a,\ a=(1-a)^{-1},\ a=1-a^{-1},\quad \text{or}\quad a=(1-a^{-1})^{-1},$$

$$\text{i.e.}\qquad a^2=1,\ 2a=1,\ a=0 \text{ or } 2,\ \text{ or }\ a^2-a+1=0\ .$$

If we choose a not to satisfy any of these equations, and also to be outside any subfield of K, then $H_a = 1$ as required. If $n=1$ then we need $7<q=p$ in order to make such a choice, i.e. $q\geqslant 11$ and q prime. If $n>1$, the solutions of the first three equations above are in any subfield, so we need $2<q-p^{n/2}$, which is clearly satisfied for $q = p^n>11$.

Now suppose that $2|n$ and $3\nmid n$, i.e. $n=2m$ where $3\nmid m$. Then the three involutions in L allow also the possibility $\sigma=\tau^m$,

$$\text{i.e.}\qquad a^{p^m}=a^{-1},\ a^{p^m}=1-a\ \text{ or }\ a^{p^m}=(1-a^{-1})^{-1},\ \text{ i.e.}$$

$$a^{p^{m+1}}-1=0,\ a^{p^m}+a-1=0\ \text{ or }\ a^{p^{m+1}}-a^{p^m}-a=0\ .$$

Counting these possibilities for a together with those for $a^h=a$, we need $2+3p^m < p^{2m} - p^m$, i.e. $2 < p^m(p^m-4)$. For $p^m\geqslant 5$ this will hold, giving the result for $q=p^{2m}\geqslant 25$ when $3\nmid m$.

If $n=3m$ where $2\nmid m$ then for h in L of order 3 we have $a^h=a^{\tau^m}$ or $a^{\tau^{2m}}$, i.e. $a^{p^m}=1-a^{-1}$ or $a^{p^{2m}}=1-a^{-1}$. Since h and h^{-1} give the same set of solutions, we require, as above,

$$2+ (p^m+1) + (p^{2m}+1) < p^{3m} - p^m\ ,\ \text{i.e.}$$

$$(3+p^m)(p^m-1) < q(p^m-2) + 1 \ .$$

This is satisfied for $p^m \geq 3$, i.e. for $q=p^{3m} \geq 27$ when $2 \nmid m$.

Finally take $n=6m$, so that all possibilities can occur. As before we obtain

$$2 + (1+(q-1)/(p^{2m}-1)) + 3p^{3m} < q-p^{3m} \ , \text{ i.e.}$$
$$(4p^{3m}+3)(p^{2m}-1)+1 < q(p^{2m}-2) \ .$$

This is satisfied for $p^m \geq 2$, i.e. for $q=p^{6m} \geq 64$.

This completes the proof of the lemma.

THEOREM : Let G be $P\Gamma L(2,q)$ in its natural action on the points Ω of the projective line, where $q = p^n$ and p is a prime. Then G has a regular 5-set if and only if $q \geq 19$, $q \notin \{25,27\}$. G has a regular 6-set if $q \in \{13,17,25,27\}$ and G has no regular k-set for any k if $q \leq 11$ or $q=16$.

PROOF : We first take $q=p$, prime. If $q \geq 11$ then we can choose $a \in K=GF(p)$ such that $|\mathcal{C}(a)|=|\mathcal{S}(a)|=6$, by the lemma. Let $\Delta=\{\infty,0,1,a\}$ where a is chosen in this way. Then $G_{\{\Delta\}}$ is the Klein 4-group. Let $\Lambda=\{\infty, 0,1,a,b,\}$ where $b \in \Omega \setminus \Delta$. Then the five possible cross-ratio sets formed by each choice of a 4-subset of Λ are

$$\mathcal{C}(a),\ \mathcal{C}(b),\ \mathcal{C}(b/a),\ \mathcal{C}((b-1)/(a-1)),\ \mathcal{C}(a(b-1)/b(a-1)) \ .$$

If we choose b such that $a \notin \mathcal{C}(b) \cup \mathcal{C}(b/a) \cup \mathcal{C}((b-1)/(a-1)) \cup \mathcal{C}(a(b-1)/b(a-1))$ then if $g \in G_{\{\Lambda\}}$ we must have $g \in G_{\{\Delta\}} \cap G_b$. Each cross-ratio set gives 6 possibilities, so we exclude at most 24 values of b . If we also require $G_{\{\Delta\}} \cap G_b=1$, then a further 6 possible values are to be excluded. Thus if $24 + 6 < q-1$ i.e. $q > 31$ we can choose b outside of these values, and thus such that $G_{\{\Lambda\}}=1$. This gives the result for $q \geq 37$. For $p=q \leq 31$ we obtain the stated results by direction computation.

Now let $q=p^n$ where we suppose that $K=GF(q)$ has a subfield $F=GF(p^m)$ where $p^m \geq 11$, $p^m \neq 16$. By the lemma, we can choose a in F such that $|\mathcal{S}(a)|=6m$. Let $\Delta=\{\infty,0,1,a\}$, $\Lambda=\Delta \cup \{b\}$ where $b \in \Omega \setminus \Delta$. Then $h \in G_{\{\Lambda\}}$ can be written in the form $g\sigma^{-1}$ where $g \in PGL(2,q)$, $\sigma \in A$. Since g preserves cross ratios and $\Lambda^g=\Lambda^\sigma$, if we choose b to be outside of any subfield of K , we must have $\Delta^{g\sigma^{-1}}=\Delta$ i.e. $\Delta^{g}=\Delta^{\sigma}$. Since, further, a is chosen to satisfy $|\mathcal{S}(a)| = 6m$, this can only happen if σ induces the identity automorphism on F , i.e. $\sigma\varepsilon<\tau^{m}>$, where $A=<\tau|\tau^{n}=1>$ and $m|n$. Let $H=PGL(2,F)$. Then $g\varepsilon H_{\{\Delta\}}$, and $H_{\{\Delta\}}$ is the Klein 4-group because of our choice of a . Now we count the maximum possible number of $b\varepsilon K$ such that b is not in any proper subfield of K and such that b could be fixed by a non-identity element $g\sigma^{-1}$ of $G_{\{\Delta\}}$. If $g=1$ then $b^{\sigma}=b$ has no solutions for $\sigma\neq1$ as b is not in any subfield. If g is one of the involutions in $H_{\{\Delta\}}$, i.e. one of the linear maps $x\to a/x$, $x\to(x-a)/(x-1)$ or $x\to a(x-1)/(x-a)$, then $b^{g}=b^{\sigma}$, for $\sigma\varepsilon<\tau^{m}>$, has at most $p^{rm}+1$ solutions b where $\sigma=\tau^{rm}$, and $0\leqslant r\leqslant\frac{n}{m}-1$. Thus to choose b outside of these possible values we need

$$3\sum_{r=0}^{\frac{n}{m}-1}(p^{rm}+1) < p^{n}-p^{n/2} \text{ , i.e. } \frac{3(p^{n}-1)}{(p^{m}-1)}+3\frac{n}{m} < p^{n}-p^{n/2}$$

whence $(3\frac{n}{m}+p^{n/2})(p^{m}-1) < p^{n}(p^{m}-4)+3$.
Now $m|n$, so $m\leqslant\frac{n}{2}$, and $p^{m}\geqslant11$, so that $(3\frac{n}{m}+p^{n/2})(p^{m}-1) <$ $(3n+p^{n/2})p^{n/2} = p^{n}+3np^{n/2}$, and $p^{n}(p^{m}-4)+3>7p^{n}$.

Clearly $7p^{n}>p^{n}+3np^{n/2}$ is equivalent to $p^{n/2}>\frac{n}{2}$ which is true. This gives the result required for K containing a proper subfield of size $p^{m}\geqslant11$, $p^{m}\neq16$. If $p\geqslant11$, $q=p^{n}$ where $n\geqslant2$, then the result follows.

Now let $p\varepsilon\{2,3,5,7\}$. Deal first with $p=5$ or 7 . If $q=p^{n_1n_2}$ where $n_1\geqslant2$, $n_2\geqslant2$ then we have the result by the above. Thus if $n\geqslant4$ and n is composite we have the result. Let $q=p^{n}$ where $p\varepsilon\{5,7\}$ and n is a prime $\geqslant3$. Then if $F=GF(p)$ and $a=-1$, $|\mathcal{C}(a)| = 3$ and if $H=PGL(2,F)$ then $H_{\{\Delta\}}$ is dihedral of order 8 (where $\Delta = \{\infty,0,1,a\}$). Every $\sigma\varepsilon Aut(K)$ induces the identity automorphism on F . Now if $b^{g}=b^{\sigma}$ then as $g\varepsilon H_{\{\Delta\}}$ must satisfy $g^{4}=1$, and since g and σ commute, we have also $b^{\sigma^{4}}=b$. As b is to be chosen to the outside of all subfields of K , this implies that $\sigma^{4}=1$. But $\sigma=\tau^{r}$ where $|\tau|=n$ is an odd prime. Thus $\sigma=1$. For each $g\varepsilon H_{\{\Delta\}}$, $g\neq1$, $b^{g}=b$ has at most two possible solutions, giving at most 14 elements b fixed by some g . Clearly $p^{n}-p>14$ for $p\varepsilon\{5,7\}$, $n\geqslant3$ (n prime). This leaves only the case $q=5^{2}$ and $q=7^{2}$. Both these were done by direct computation : for $q=5^2$ there are no regular 5-sets (although there are regular 6-sets), and for $q=7^2$ there are regular 5-sets.

For $q=3^n$ where $n_1\geq 3$, $n_2\geq 2$ then we have the result by the above argument. Thus, if n is composite, $n\geq 6$, we have the result. If n is a prime ≥ 5 , $q=3^n$, let $F=GF(3)$, and take $a=-1$. Then $H_{\{\Delta\}}=S_4$, where $H=PGL(2,F)$. If $b^{g\sigma^{-1}}=b$ for $g\in H_{\{\Delta\}}$, $\sigma\in Aut(K)$ then g has order 1,2,3 or 4 , and we must have the same for σ . But $|Aut(K)|=n$ is a prime, ≥ 5 . Thus $\sigma=1$,, and $b^g=b$. The 23 non-identity elements of $H_{\{\Delta\}}$ consists of 4 pairs of elements $\{g,g^{-1}\}$ of order 3, 3 pairs of elements $\{g,g^{-1}\}$ of order 4 and 9 involutions. Since $b^g=b$ is equivalent to $b^{g^{-1}}=b$, the maximum possible number of $b\in K\setminus F$ that may satisfy $b^g=b$ is $32<p^n-p$ for $n\geq 5$ (n prime, p=3) . For $q=3^2$, 3^3, 3^4 we obtain, by direct computation, the following: there is no regular set at all for $q=3^2$; there are no regular 5-sets, but there are regular 6-sets for $q=3^3$; there are regular 5-sets for $q=3^4$.

For $q=2^n$ where $n=n_1n_2$ and $n_2\geq 5$, $n_2\geq 2$ we have the result by the earlier argument, i.e. for $n\geq 10$, n composite we can find regular 5-sets. Now let $q=2^n$ where n is a prime, $n\geq 7$. Let $\Lambda=\{\infty,0,1,a,b\}$ be a 5-set and let $g\in G_{\{\Delta\}}$. Then on Λ , g can have the following cyclic structure: $5^1,4^1 1^1,3^1 2^1,3^1 1^2,2^2 1^1,2^1 1^3, 1^5$. Now $|G|=(2^n+1)2^n(2^n-1)n=(4^n-1)2^n n$. Since n is odd and $4=-1(\mathrm{mod}5)$, $4^n=-1(\mathrm{mod}5)$, i.e. 5 does not divide $|G|$. Also, $2=-1(\mathrm{mod}3)$ implies that $2^n=-1(\mathrm{mod}3)$ (since n is odd) and so 3 does not divide the stabilizer of a point in G . Also, 2 does not divide the stabilizer of 2 points, so that we have only the cyclic structures $4^1 1^1,2^2 1^1,1^5$ to consider. For the case 1^5, if $h=g\sigma^{-1}\in G_{\{\Lambda\}}$ then since h fixes ∞,0 and 1, $g=1$ and $h=\sigma^{-1}$. But if $\sigma\neq 1$ then σ has prime order n and fixes no field element. Suppose $g\sigma^{-1}$ has the form $2^2 1^1$ on Λ . Then $g\sigma^{-1}$ is an involution and must be linear. Now if we choose b such that $b\notin\mathcal{C}(a)$ and $b\neq a^2$, $a\neq b^2$, such elements cannot occur. Elements of the form $4^1 1^1$ do not occur since the Sylow 2-subgroup is elementary abelian. Thus for $n\geq 7$, $q=2^n$ where n is prime, we can find regular 5-sets.

It remains to consider 2^n where $n\leq 9$. For $n=2,3,4$ there are no regular sets. For $n=5$ and $n=6$ we have the result by direct construction of the groups. For n=8 and 9 the groups were too large to construct easily, but here an analysis of the equations satisfied by b in the relation $b^g=b^\sigma$ led to the solution that the regular 5-sets could be found.

The other small values of q were covered by direct computation of the groups.

BIBLIOGRAPHY

[1] P.J. Cameron, P.M. Neumann and J. Saxl, On groups with no regular orbit on the set of subsets, Arch.Math. 43 (1984), 295-296.

[2] J. Cannon, "An Language for Group Theory", Cayley Manual, Sidney University, July 1982.

[3] P. Dembowski, "Finite Geometries", Springer, Berlin, 1968.

[4] D.R. Hughes and F.C. Piper, "Projective Planes", Springer 1973.

[5] J.D. Key and J. Siemons, Regular sets and geometric groups, (submitted).

[6] H. Wielandt, "Finite Permutation Groups", Academic Press, New York, 1964.

J.D. Key & A. Wagner
Department of Mathematics
University of Birmingham
P.O. Box 363
Birmingham B15 2TT
UK

J. Siemons
School of Mathematics and Physics
University of East Anglia
University Plain
Norwich NR4 7TJ
UK

(Eingegangen am 21. Juni 1985)