

**Abhandlungen  
aus dem  
Mathematischen  
Seminar der  
Universität Hamburg**

**BAND 58/1988**

**Vandenhoeck & Ruprecht  
in Göttingen**

# On the relationship between the lengths of orbits on $k$ -sets and $(k + 1)$ -sets

by J. SIEMONS and A. WAGNER

## 1. Introduction

Let  $G$  be a permutation group on a set  $\Omega$ . A sizable literature has grown up which considers the action of  $G$  on the unordered subsets of  $\Omega$ ; see for example [7] for a short survey. In this field one of the basic results is that the number of orbits on  $(k + 1)$ -sets is not less than the number of orbits on  $k$ -sets (in the finite case one must, of course, take  $k \leq \frac{1}{2}|\Omega|$ ). It would be nice to have a theorem, in some sense analogous to the above, concerning the *lengths* of the orbits.

There are many examples where an orbit on  $k$ -sets is longer than any orbit on  $(k + 1)$ -sets, see the end of § 2. None-the-less intuition suggests that such a situation is somewhat exceptional. In this paper we attempt to give more plausibility to this assertion. In fact we shall consider a rather more general situation and then classify all exceptions when  $k = 2$ .

### Theorem.

*Let  $G$  be a transitive permutation group of degree  $n > 4$ . Suppose there is some 2-element subset  $\Delta$  such that  $|\Delta^G| > |\Sigma^G|$  for every 3-element subset  $\Sigma$  containing  $\Delta$ . If  $G$  is primitive then  $G = PSL(2,5)$  in its natural action on six points. Otherwise  $G$  has three blocks of imprimitivity  $\Omega_1, \Omega_2$  and  $\Omega_3$  with  $|\Omega_i|$  a power of 2. Furthermore  $\Delta^G = \{\{\alpha, \beta\} \mid \alpha \in \Omega_i \neq \Omega_j \ni \beta\}$  and  $G$  has order  $3 \cdot |\Omega_i|^2 \cdot |G_{\{\Delta\}}|$  with  $|G_{\{\Delta\}}| \leq 2$ .*

In § 2 we obtain a preliminary result – theorem 2.1 – which in § 3 is used to prove the main theorem. There we also give an explicit construction of imprimitive groups satisfying the assumptions of the theorem. We furthermore show that the incidence relation between  $\Delta^G$  and  $\Sigma^G$  gives rise to cubic graphs with  $G$  as automorphism group, including the Petersen graph for  $PSL(2,5)$ .

We wish to thank Alan Camina for helpful discussions.

## 2. A preliminary theorem

Our notation is standard. When  $G$  is a permutation group on the set  $\Omega$  and  $\Gamma \subset \Omega$  then  $G_{(\Gamma)}$  denotes the set-wise stabilizer and  $G_\Gamma$  the point-wise stabilizer of  $\Gamma$ . The group  $G^\Gamma = G_{(\Gamma)}/G_\Gamma$  is considered as a permutation group on  $\Gamma$ . The set of all  $G$ -images of  $\Gamma$  is denoted by  $\Gamma^G$ . Our first theorem is a general and elementary result.

**Theorem 2.1.**

Let  $G$  be a transitive permutation group on a finite set  $\Omega$  and let  $\Delta$  be a given subset of  $\Omega$  of cardinality  $k < |\Omega|$ . Suppose that  $|\Sigma^G| < |\Delta^G|$  for every set  $\Sigma \supset \Delta$  of cardinality  $k + 1$ . Then

$$k + 1 \geq |\Delta^{G(\Sigma)}| > |\Sigma^{G(\Delta)}| \geq 1. \quad (1)$$

If furthermore  $k \geq 2$  then either (i): every 2-element subset of  $\Omega$  is contained in some  $G$ -image of  $\Delta$  or (ii):  $G$  is imprimitive with blocks of imprimitivity  $\Omega_1, \dots, \Omega_r$  ( $1 < |\Omega_i| < |\Omega|$ ) each intersecting  $\Delta$  in at most 1 point such that every 2-element subset of the form  $\{\alpha_i, \alpha_j\}$  with  $\alpha_i \in \Omega_i \neq \Omega_j \ni \alpha_j$  is contained in some  $G$ -image of  $\Delta$ .

In the context of conclusion (i) of the theorem it is worthwhile to mention Rudio's criterion for primitivity, see for instance theorem 8.1 in [8]. If  $G$  is primitive then the  $G$ -images of  $\Delta$  also separate points, that is, for a given 2-element set some  $G$ -image of  $\Delta$  contains one of the points but not both.

*Proof.* The order of  $G$  may be expressed in two ways:  $|G| = |\Delta^G| \cdot |G_{(\Delta)}| = |\Delta^G| \cdot |\Sigma^{G(\Sigma)}| \cdot |G_{(\Delta)}(\Sigma)|$  and  $|G| = |\Sigma^G| \cdot |G_{(\Sigma)}| = |\Sigma^G| \cdot |\Delta^{G(\Sigma)}| \cdot |G_{(\Sigma)}(\Delta)|$ . From the assumption  $|\Sigma^G| < |\Delta^G|$  it follows that

$$|\Delta^{G(\Sigma)}| > |\Sigma^{G(\Delta)}| \geq 1 \text{ and clearly } k + 1 \geq |\Delta^{G(\Sigma)}|.$$

If  $|\Delta| \geq 2$  we shall say that two distinct points  $\alpha, \beta$  in  $\Omega$  are *joined* if  $\{\alpha, \beta\}$  is contained in some  $G$ -image of  $\Delta$ . It is obvious that the relation "not joined" is  $G$ -invariant, reflexive and symmetric. Furthermore we assert that it is transitive. For, if  $\alpha, \beta, \gamma$  were three points with  $(\alpha, \beta)$  and  $(\beta, \gamma)$  not joined but with  $(\alpha, \gamma)$  joined, we may assume without loss of generality that  $\{\alpha, \gamma\} \subseteq \Delta \subset \Sigma = \Delta \cup \{\beta\}$ . As  $|\Delta^{G(\Sigma)}| \geq 2$  by (1) either  $\{\alpha, \beta\}$  or  $\{\beta, \gamma\}$  is contained in a  $G_{(\Sigma)}$ -image of  $\Delta$ , a contradiction. Therefore to be not joined is a  $G$ -invariant equivalence relation that clearly is not the identity relation. If not to be joined is the all-relation then every pair of distinct points is joined so that we are in the case (i) of the theorem. In all other cases the equivalence classes  $\Omega_1, \dots, \Omega_r$  of the relation form a system of imprimitivity so that by definition any pair of points from distinct classes is joined. It is now also clear that  $\Delta$  can not have two or more points in common with any of the  $\Omega_i$ 's.  $\square$

For the case when the set  $\Delta$  in theorem 2.1 consists of a single point we obtain

**Corollary 2.2.**

If  $G$  is a permutation group acting transitively on the finite set  $\Omega$  such that  $|\Omega| > |\Sigma^G|$  for every 2-set  $\Sigma \subset \Omega$ , then  $G$  is an elementary abelian 2-group acting regularly on  $\Omega$ .

*Proof.* Let  $\beta \neq \alpha$  be a point in some  $G_\alpha$ -orbit and put  $\Sigma = \{\alpha, \beta\}$ . Then inequality (1) shows that  $|\beta^{G_\alpha}| = 1$  so that  $G$  is regular. At the same time  $|\alpha^{G(\Sigma)}| = 2$  shows that every pair of points can be interchanged by a (unique) element. This implies that  $G$  is an elementary abelian 2-group.  $\square$

In [4], lemma 2.1, it has been noted that for a regular group  $G$  of degree  $n$  and a given  $k < n - 1$ , there always exists a set  $\Sigma$  with  $|\Sigma| = k + 1$  and  $|\Sigma^G| = |G|$  except when  $k = 1$  and  $G$  is an elementary abelian 2-group.

The lengths of orbits on subsets for groups of degree  $n \leq 8$  is given in [6]; in [2] M. Strati has examined the orbit lengths for primitive groups of degree up to 20. There in particular the following situation was considered: some subset  $\Delta$  of size  $k$  has  $|\Delta^G| = |G|$  and  $|\Sigma^G| < |G|$  for every  $(k+1)$ -element subset  $\Sigma$  containing  $\Delta$ . The list of groups with this property includes  $PSL(2,11)$  with  $n = 12$  and  $k = 5$ ,  $PSL(2,13)$  with  $n = 14$  and  $k = 6$ ,  $PSL(2,16)$  with  $n = 17$  and  $k = 5$ , in their natural representations. A further example is  $Alt(7)$  in its representation of degree 15 with  $k = 6$ .

### 3. Proof of the main theorem

For the remainder let  $G$  be a group as in the theorem of section 1. Thus  $G$  satisfies the following hypothesis

(\*):  $G$  acts transitively on a finite set  $\Omega$  of  $n > 4$  points. There is some set  $\Delta$  of cardinality 2 such that  $|\Sigma^G| < |\Delta^G|$  for every set  $\Sigma$  of cardinality 3 containing  $\Delta$ .

The proof is organized according to the two cases in theorem 2.1. In the first case  $G$  is doubly homogeneous and so in particular primitive on  $\Omega$ . This situation is dealt with first.

#### 3.1 The primitive case

##### Lemma 3.1.

If  $G$  satisfies (\*) and acts primitively on  $\Omega$ , then

- (i)  $G$  is doubly transitive on  $\Omega$ ,
- (ii) for any 3-set  $\Sigma$  the group  $G^\Sigma$  is transitive on  $\Sigma$ , and
- (iii)  $G_{(\Delta)}$  is an elementary abelian 2-group having orbits of length  $\leq 2$  on  $\Omega$ .

*Proof.* As  $|\Delta| = 2$  theorem 2.1(i) implies that  $G$  is doubly homogeneous on  $\Omega$ . Let  $\Sigma$  be an arbitrary 3-set. As its 2-element subsets are images of  $\Delta$ , the inequality (1) of theorem 2.1 shows that  $G_{(\Sigma)}$  must move each of these 2-sets. This implies that  $G_{(\Sigma)}$  is transitive on the points of  $\Sigma$ . As this holds for any 3-set and as  $|\Omega| \geq 4$  simple arguments show that  $G$  is doubly transitive, compare also to lemma 2.2 in [5]. This proves (i) and (ii) above.

Let  $\sigma$  be in  $\Omega \setminus \Delta$  and  $\Sigma = \Delta \cup \{\sigma\}$ . As  $3 > |\Sigma^{G_{(\Delta)}}|$  by inequality (1) of theorem 2.1 the  $G_{(\Delta)}$ -orbit of  $\sigma$  has length at most 2. This implies that the square of every element in  $G_{(\Delta)}$  is the identity so that  $G_{(\Delta)}$  is an elementary abelian 2-group.  $\square$

##### Lemma 3.2.

If  $G$  satisfies (\*) and acts primitively on  $\Omega$  then  $G$  has no regular normal subgroup.

*Proof.* Suppose  $1 < N \triangleleft G$  is a regular normal subgroup. Then  $N$  is an elementary abelian  $p$ -group (theorem 11.1 in [8]), say  $|\Omega| = |N| = p^d$ , and  $G$  is a subgroup of the affine linear group  $AGL(d,p)$ . We show that this leads to a contradiction.

*Case 1:*  $p > 3$ . Let  $A (\subseteq \Omega)$  be a line of the affine  $d$ -dimensional space  $AG(d,p)$  and  $\Sigma \subset A$  any set of three points on  $A$ . Since  $G_{(\Sigma)} \subseteq (AGL(d,p))_{(A)}$  we have that  $(G_{(A)})^A \subseteq (AGL(A))_{(\Sigma)}$  acts transitively on the points of  $\Sigma$ , by lemma 3.1. (ii). Simple counting arguments now show that none of the groups  $AGL(1,p)$  have this property for  $p > 3$ .

*Case 2:*  $p = 3$ . This can be ruled out as follows. Since the order of  $G_\alpha$  is not divisible by 3 the normal subgroup  $N$  is the Sylow 3-subgroup of  $G$ . Thus  $G$  contains precisely  $n - 1$  elements of order 3 each leaving  $n/3$  sets of size 3 invariant. Therefore  $a := |\{(\Sigma, g) | g \in G_{(\Sigma)}, |g| = 3\}| = (n - 1)n/3$ . On the other hand an element in  $G_{(\Sigma)}$  cyclically permuting the points of  $\Sigma$  is, without loss of generality, an element of order 3. Lemma 3.1. (ii) now implies that  $a \geq \binom{n}{3} \cdot 2$  so that we have the contradiction  $n \leq 3$ .

*Case 3:*  $p = 2$ . Here any 3-set  $\Sigma$  is contained in a unique affine subplane  $\Pi$  of 4 points, say  $\Pi = \Sigma \cup \{\sigma\}$ . It follows that  $G_{(\Sigma)} \subseteq G_\sigma$  and  $G_{(\Sigma), \sigma'} \subseteq G_{\sigma, \sigma'}$  for a point  $\sigma' \in \Sigma$ . Since  $|G_{(\Sigma)} : G_{(\Sigma), \sigma'}| = 3$  we have  $|G_{(\Sigma)}| \leq 3|G_{\sigma, \sigma'}|$ . On the other hand  $|\Sigma^\sigma| < |\Delta^\sigma|$  implies that  $|G_{(\Sigma)}| > |G_{(A)}| = 2|G_{\sigma, \sigma'}|$ , as  $G$  is doubly transitive. From this it can be seen that  $G_{(\Sigma)}$  has order  $3|G_{\sigma, \sigma'}|$  independently of  $\Sigma$  so that every orbit on 3-sets has length  $n(n - 1)/3$ . It follows that  $G$  has  $(n - 2)/2$  orbits on 3-sets.

We now determine the number of orbits on 3-sets in a different way. Let  $S$  be a Sylow 3-subgroup of  $G$  and consider  $NS$ . By lemma 3.1. (iii) this is a Frobenius group with kernel  $N$  and complement  $S$ . By a well-known result (see for instance theorem 10.3.1. in [3])  $S$  is cyclic. This implies in particular that all subgroups in  $G$  of order 3 are conjugate. Let  $\Sigma$  and  $\Sigma'$  be any two 3-sets in  $\Omega$ , let  $A$  be a Sylow 3-subgroup of  $G_{(\Sigma)}$  and let  $B$  be a Sylow 3-subgroup of  $G_{(\Sigma')}$ . When  $B$  is conjugated onto  $A$  by an element  $g$  in  $G$  then  $g$  maps  $\Sigma'$  onto one of the 3-cycles of  $A$ . This shows that there are at most  $(n - 1)/3$  orbits on 3-sets. The inequality  $(n - 2)/2 \leq (n - 1)/3$  implies  $n = 4$  and  $G = Alt(4)$  which violates our assumption (\*).  $\square$

The following lemma is a general result based upon Aschbacher's classification [1] of doubly transitive groups with abelian two-point stabilizer.

### Lemma 3.3.

*Let  $H$  be a doubly transitive permutation group of degree  $n$  without regular normal subgroup such that the stabilizer of two distinct points is an elementary abelian 2-group. Then  $H = PSL(2,5)$  with  $n = 6$ ,  $H = PSL(3,2)$  with  $n = 7$  or  $H$  is the smallest Ree group,  $H \cong P\Gamma L(2,8)$ , and  $n = 28$ .*

*Proof.* It is easy to verify that  $H_{\alpha, \beta}$  is an elementary abelian 2-group when  $H$  is one of the three groups in the lemma.

Let conversely  $1 \neq M$  be the minimal normal subgroup of  $H$ . According to the theorem in [1] we have  $H = PSL(3,2)$ ,  $H$  is the smallest Ree group with  $n = 28$  or  $M = PSL(2,q)$ ,  $PSU(3,q)$ ,  $Sz(q)$ , or  $R(q)$ . By considering the order and structure of  $M_{\alpha, \beta}$  (i.e.  $q^2 - 1/d$  with  $d = (3,q - 1)$ ,  $(q - 1)$  and  $(q - 1)$  respectively) the last 3 cases

can be ruled out immediately. When  $M = PSL(2, q)$  then  $M_{\alpha, \beta}$  is a cyclic group of order  $q - 1$  ( $q$  even) or  $(q - 1)/2$  ( $q$  odd). This implies  $(q - 1)/2 = 2$  and so  $q = 5$ .  $\square$

We now complete the proof of the main theorem in the primitive case.

**Lemma 3.4.**

*Let  $G$  be a primitive permutation group satisfying (\*). Then  $G$  is  $PSL(2, 5)$  in its natural action of degree 6.*

*Proof.* By lemmas 3.1 and 3.3 only the groups  $G = PSL(2, 5)$  with  $n = 6$ ,  $G = PSL(3, 2)$  with  $n = 7$  and  $G \cong P\Gamma L(2, 8)$  with  $n = 28$  can occur.

$G = P\Gamma L(2, 8)$ . This is the action on the 28 cosets of the normalizer of a Sylow 3-subgroup  $S$  where  $S$  is a cyclic group of order 9 extended by the field automorphism of order 3. This group contains just 8 elements of order 3 and as the stabilizer of 2 points has order co-prime to 3 we have precisely 28.8 elements of order 3. These 3-elements leave  $28.8.9 < \binom{28}{3}$  sets of size 3 invariant, in contradiction to lemma 3.1.(ii).

$G = PSL(3, 2)$ . Here  $G$  is transitive on the 7 lines of the 7-point plane and is also transitive on the set of 28 triangles. However, the orbit on 2-sets has size  $21 < 28$ .

$G = PSL(2, 5)$ . This group is transitive on the 15 sets of size two. On 3-sets it has 2 orbits of size 10 each and so satisfies (\*).  $\square$

We note that the action of  $G = PSL(2, 5)$  on the subsets of  $\Omega = GF(5) \cup \{\infty\}$  yields a construction of the Petersen graph. Let  $\Delta \subset \Omega$  be of size 2,  $\Sigma \subset \Omega$  of size 3 and put  $E = \Delta^G$ ,  $P = \Sigma^G$ . Then the incidence relation (i.e. containment) between  $P$  and  $E$  can be shown to be that of the Petersen graph with  $P$  as point set and  $E$  as edge set.

### 3.2 The imprimitive case

We now suppose that  $G$  is an imprimitive group satisfying the hypothesis (\*). According to theorem 2.1(ii) there is a system  $\bar{\Omega} = \{\Omega_1, \Omega_2, \dots, \Omega_r\}$  of imprimitivity such that a pair of points is contained in a  $G$ -image of  $\Delta$  if and only if they are not in the same  $\Omega_i$ . This implies in particular that the permutation group  $\bar{G} = G/G_{(\Omega_1), (\Omega_2), \dots, (\Omega_r)}$  is doubly homogeneous on the  $r$  elements of  $\bar{\Omega}$  and hence primitive.

**Lemma 3.5.**

*Let  $G$  be an imprimitive group satisfying (\*).*

- (i) *If  $\alpha, \alpha' \in \Omega_i$  and  $\beta \notin \Omega_i$  for some  $i = 1, \dots, r$  then some element in  $G$  interchanges  $\alpha, \alpha'$  and fixes  $\beta$ .*
- (ii) *If  $r \geq 3$  and if  $\bar{\Sigma}$  are any 3 blocks in  $\bar{\Omega}$  then some element in  $\bar{G}_{(\bar{\Sigma})}$  permutes  $\bar{\Sigma}$  cyclically.*
- (iii) *For 3 distinct indices  $i, j, k$  let  $H = G_{(\Omega_i \cup \Omega_j \cup \Omega_k)}$  and  $\alpha \in \Omega_i$ . Then  $\Omega_j$  is contained in or is an orbit of  $H_\alpha$ .*

Proof. (i) Put  $\Sigma = \{\alpha, \alpha', \beta\}$ . As  $\{\alpha, \beta\}$  and  $\{\alpha', \beta\}$  are  $G$ -images of  $\Delta$  but not  $\{\alpha, \alpha'\}$ , some element in  $G_{(\Sigma)}$  interchanges  $\alpha, \alpha'$  fixing  $\beta$ , this follows from inequality (1) in theorem 2.1.

(ii) Let  $\bar{\Sigma} = \{\Omega_1, \Omega_2, \Omega_3\}$  and choose points  $\alpha_i$  in  $\Omega_i$ ,  $1 \leq i \leq 3$ . Put  $\Sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ . Then, again by inequality (1), some  $g$  in  $G_{(\Sigma)}$  acts as a 3-cycle on  $\Sigma$ . As the  $\Omega_i$ 's are blocks of imprimitivity the corresponding element  $\bar{g}$  in  $\bar{G}_{(\bar{\Sigma})}$  is a 3-cycle on  $\bar{\Sigma}$ .

(iii) Let  $\alpha \in \Omega_i, \beta \in \Omega_k$  and let  $\alpha_1, \alpha_2$  be any two points in  $\Omega_j$ . Put  $\Sigma_i = \{\alpha, \beta, \alpha_i\}$  for  $i = 1, 2$ . As we have seen above there are  $g_i \in G_{(\Sigma_i)} \subseteq H$  with  $g_1 = (\alpha_1, \alpha, \beta) \dots$  and  $g_2 = (\alpha_2, \beta, \alpha) \dots$  so that  $g_2 g_1(\alpha) = \alpha$  and  $g_2 g_1(\alpha_1) = \alpha_2$ .  $\square$

**Lemma 3.6.**

*If  $G$  satisfies (\*) and is imprimitive with  $r > 4$  blocks of imprimitivity then  $r = 6$  and  $\bar{G}$  is  $PSL(2,5)$  in its natural action.*

*Proof:* We shall prove that  $\bar{G}$  in its action on  $\bar{\Omega}$  satisfies the assumptions of theorem 2.1. As we clearly are in the primitive case for this action the lemma then follows from the previous section and in particular from lemma 3.4.

Let  $\bar{\Delta} = \{\Omega_1, \Omega_2\}$  and  $\Omega_3$  some further block of imprimitivity. Put  $\bar{\Sigma} = \{\Omega_1, \Omega_2, \Omega_3\}$ . We have to show that  $|\bar{\Delta}^{\bar{G}}| > |\bar{\Sigma}^{\bar{G}}|$  or, equivalently  $|G_{(\Omega_1, \Omega_2, \Omega_3)}| > |G_{(\Omega_1, \Omega_2)}|$ . Let  $H$  denote the group  $G_{(\Omega_1, \Omega_2, \Omega_3)}$  and  $a$  the order of  $G_{(\Omega_1, \Omega_2)}$ . As the points of  $\Omega_1 \cup \Omega_2$  are joined by  $m^2$   $G$ -images of  $\Delta$  where  $m = |\Omega_i|$  and  $\Delta = \{\alpha_1, \alpha_2\}$  with  $\alpha_1 \in \Omega_1, \alpha_2 \in \Omega_2$ , and as these  $G$ -images clearly are  $G_{(\Omega_1, \Omega_2)}$ -images, we have  $a = m^2 |G_{(\Delta)}|$ . We now determine the order of  $H$ . Let  $\Sigma = \{\alpha_1, \alpha_2, \alpha_3\}$  with  $\alpha_3 \in \Omega_3$ . Then  $G_{(\Sigma)} \subseteq H$  as  $\Omega_1, \Omega_2, \Omega_3$  are blocks of imprimitivity so that  $H_{(\Sigma)} = G_{(\Sigma)}$ . Applying lemma 3.5 (iii) twice shows that any pair  $\bar{\alpha}_1, \bar{\alpha}_2$  with  $\bar{\alpha}_1 \in \Omega_1$  and  $\bar{\alpha}_2 \in \Omega_2$  is contained in at least one  $H$ -image of  $\Sigma$ . Thus  $|\Sigma^H| \geq m^2$ , ( $m = |\Omega_i|$ ), so that  $|H| \geq |H_{(\Sigma)}| m^2 = |G_{(\Sigma)}| m^2$ . As  $|G_{(\Sigma)}| > |G_{(\Delta)}|$  by assumption, we have  $|G_{(\Omega_1, \Omega_2, \Omega_3)}| > |G_{(\Omega_1, \Omega_2)}|$  and the proof of the lemma is complete.  $\square$

**Lemma 3.7.**

*If  $G$  satisfies (\*) and is imprimitive let  $\Delta = \{\alpha_1, \alpha_2\}$  with  $\alpha_1 \in \Omega_1$  and  $\alpha_2 \in \Omega_2$ . Then*

- (i)  $G_{(\Delta)}$  is the identity on  $\Omega_1 \cup \Omega_2$ ,
- (ii) in  $\bar{G}$  no two blocks can be interchanged,
- (iii)  $r = 3$  with  $\bar{G} = Alt(3)$ .

*Proof.* (i) Let  $\beta \in \Omega_1 \cup \Omega_2 \setminus \Delta$  and  $\Sigma = \{\alpha_1, \alpha_2, \beta\}$ . Then inequality (1) gives  $1 = |\Sigma^{G_{(\Delta)}}| = |\Sigma^{G_{(\Delta)}}|$  so that  $G_{(\Delta)}$  fixes every point in  $\Omega_1 \cup \Omega_2 \setminus \Delta$ . As the  $\Omega_i$ 's are blocks of imprimitivity also  $\alpha_1$  and  $\alpha_2$  are fixed by  $G_{(\Delta)}$ .

(ii) Suppose that in  $G$  two blocks  $\Omega_1$  and  $\Omega_2$  can be interchanged so that there is some  $g$  in  $G$  with  $\Omega_1^g = \Omega_2$  and  $\Omega_2^g = \Omega_1$ . Let  $\Delta$  be as above. Then by lemma 3.5.(i) we may assume that  $g$  fixes  $\Delta$  as a set so that by part (i) above  $g$  would have to be the identity on  $\Omega_1 \cup \Omega_2$ , a contradiction.

(iii) As  $\bar{G}$  is doubly homogeneous but not doubly transitive (by (ii)) lemma 3.6 implies that  $r \leq 4$  and hence  $r = 3$  with  $\bar{G} = Alt(3)$ .  $\square$

**Lemma 3.8.**

If  $G$  satisfies (\*) and is imprimitive with blocks  $\Omega_1, \Omega_2, \Omega_3$  then

- (i) If  $\alpha_1 \in \Omega_1$  then  $G_{\alpha_1}$  acts transitively as an elementary abelian 2-group on  $\Omega_2$  and on  $\Omega_3$ . In particular  $|\Omega_i| = 2^x$  for some integer  $x$ .
- (ii) Let  $M = G_{(\Omega_1)}$ . Then  $M = G_{(\Omega_i)}$ ,  $i = 2$  and  $3$ , and  $M$  is normal in  $G$  with  $|G : M| = 3$ .
- (iii) The group  $G_{(\Delta)}$  is normal in  $M$  with  $|M : G_{(\Delta)}| = 2^{2x}$  and has order  $\leq 2$ .

*Proof.* (i) Let  $H = G_{\alpha_1}$ . By lemma 3.7. (ii)  $H$  fixes both  $\Omega_2$  and  $\Omega_3$  as sets and is transitive on  $\Omega_i$  ( $i = 2$  or  $3$ ) by lemma 3.5.(i). When  $\alpha_2 \in \Omega_2$  then  $H_{\alpha_2}$  is the identity on  $\Omega_1 \cup \Omega_2$  (put  $\Delta = \{\alpha_1, \alpha_2\}$  in lemma 3.7.(i)). This together with lemma 3.5.(i) implies that  $H$  acts transitively as an elementary abelian 2-group on  $\Omega_i$  for  $i = 2$  or  $3$ . Thus  $|\Omega_i| = 2^x$ .

(ii) this follows immediately from lemma 3.7.(ii).

(iii) Let  $\Delta = \{\alpha_1, \alpha_2\}$  with  $\alpha_i \in \Omega_i$ . Thus  $G_{(\Delta)} (\subset M)$  fixes every point of  $\Omega_1 \cup \Omega_2$ . By the argument in (i) above  $|M : G_{(\Delta)}| = 2^{2x}$ . If  $m \in M$  then also  $(G_{(\Delta)})^m$  fixes  $\Delta$  so that  $G_{(\Delta)}$  is normal in  $M$ .

Let  $K = G_{(\Sigma)}$  with  $\Sigma = \{\alpha_1, \alpha_2, \alpha_3\}$ ,  $\alpha_i \in \Omega_i$ . Then  $K_{\alpha_1}$ , by lemma 3.7. (ii), is the identity on  $\Sigma$ . Taking  $\Delta_i = \Sigma \setminus \{\alpha_i\}$  we have  $K_{\alpha_1} \subseteq G_{(\Delta_i)}$  for  $i = 1, 2, 3$  so that  $K_{\alpha_1} = 1$  by lemma 3.7.(i). This shows that  $K$  has order 3. The hypothesis (\*) now implies that  $|G_{(\Delta)}| \leq 2$ .  $\square$

With the above lemma the proof of the main theorem is complete. We conclude with a construction of an infinite family of imprimitive groups that satisfy the hypothesis (\*).

**3.3 A construction of imprimitive groups with short orbits on 3-sets**

Let  $V$  be the vector space over  $GF(2)$  of dimension  $x$  with a fixed subspace  $F$  of dimension at most 1. Let  $\Omega = \{(i, v) | i \in \mathbb{Z}/3, v \in V\}$  and  $G$  the set  $\{(j; t_0, t_1, t_2) | j \in \mathbb{Z}/3, t_i \in V \text{ and } t_0 + t_1 + t_2 \in F\}$  acting on  $\Omega$  by the rule  $(j; t_0, t_1, t_2) : (i, v) \mapsto (i + j, v + t_i)$ . Thus  $G$  is a permutation group on  $\Omega$  of order  $|G| = 3 \cdot |V|^2 \cdot |F|$  acting transitively with blocks of imprimitivity  $\Omega_i = \{(i, v) | v \in V\}$ ,  $i = 0, 1$  or  $2$ .

Let  $\Delta = \{(0, v), (1, v)\}$  for some  $v \in V$ . It is easy to see that

- (i):  $G_{(\Delta)} = G_{\Delta}$  has order  $|F| \leq 2$ .
- If  $\Sigma = \{(0, v), (1, v), (2, \bar{v})\} \supset \Delta$  for some  $\bar{v} \in V$  then
- (ii):  $G_{(\Sigma)}$  induces a cycle on  $\Sigma$  and has order 3.
- If  $\Sigma' = \{(0, v), (1, v), (0, \bar{v})\} \supset \Delta$  for some  $v \neq \bar{v} \in V$  then
- (iii):  $G_{(\Sigma')}$  has order  $2|F|$ .

This shows that  $|\Sigma^G| < |\Delta^G|$  for any 3-set containing  $\Delta$  so that  $G$  is a genuine exception to the main theorem.

Let  $\Sigma$  be a 3-set as in (ii) above. Counting the number of pairs  $(\Delta^*, \Sigma^*)$  with  $\Delta^* \in \Delta^G$ ,  $\Sigma^* \in \Sigma^G$  and  $\Delta^* \subset \Sigma^*$  we observe that

- (iv) every  $\Delta^*$  is contained in  $|F|$  3-sets from  $\Sigma^G$ , and clearly
- (v) every  $\Sigma^*$  contains 3 sets from  $\Delta^G$ .



Thus, if  $|F| = 2$ , then the containment relation between  $\Sigma^G$  and  $\Delta^G$  yields a graph with  $\Sigma^G$  as set of vertices and  $\Delta^G$  as set of edges. This graph has valency 3 with  $G$  acting both vertex and edge transitively.

### References

- [1] M. ASCHBACHER, Doubly transitive groups in which the stabilizer of two points is abelian, *Journal of Algebra* **18**, 114–136, 1971.
- [2] L. DI MARTINO, private communication, September 1986.
- [3] D. GORENSTEIN, *Finite Groups*, Harper and Row, New York and London, 1968.
- [4] J. KEY and J. SIEMONS, Regular sets and geometric groups, *Resultate der Mathematik*, **11** 97–116, 1987.
- [5] P. NEUMANN, Generosity and characters of multiply transitive permutation groups, *Proceedings L.M.S. (3)*, **31**, 457–481, 1975.
- [6] I. SOICHER, “The computation of Galois groups“, MSc. Thesis, Université Concordia, Montreal, 1981.
- [7] A. WAGNER, “Orbits on finite incidence structures“, *Symposia Mathematica, Istituto Nazionale di Alta Matematica Francesco Severi*, **28**, 219–229, 1986.
- [8] H. WIELANDT, *Permutation Groups*, Academic Press, New York and London 1964.

*Eingegangen am 6.07.1987*

Anschrift der Autoren: J. Siemons, School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom. A. Wagner, Department of Mathematics, University of Birmingham, Birmingham B15 2TT, United Kingdom.