

RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

ANDREA LUCCHINI

On imprimitive groups with small degree

Rendiconti del Seminario Matematico della Università di Padova,
tome 86 (1991), p. 131-142

http://www.numdam.org/item?id=RSMUP_1991__86__131_0

© Rendiconti del Seminario Matematico della Università di Padova, 1991, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques*
<http://www.numdam.org/>

On Imprimitve Groups with Small Degree.

ANDREA LUCCHINI(*)

1. Introduction.

Given a group G and a subgroup H , with $[H; G]$ we indicate the lattice of all subgroups K such that $H \leq K \leq G$; $[H; G]$ is called an interval in the subgroup lattice of G .

The following question is open: is every finite lattice L isomorphic to an interval in the subgroup lattice of a finite group?

As a particular case, one can consider a lattice L of length 2, consisting of a least, a largest and n pairwise incomparable elements: a lattice with these properties is indicated by the symbol \mathfrak{N}_n (for some history of the question, which comes from universal algebra, see [1]). In this case the problem can be formulated in the following equivalent way: for which n is it possible to find a group G with a subgroup H such that any proper subgroup of G containing H is maximal and H is contained in exactly n maximal subgroups M_1, \dots, M_n of G ?

If $n - 1$ is a prime power the question has an affirmative answer: indeed if F is a field of $n - 1$ elements, V is a 2-dimensional vector space over F and G is the group of permutations $x \rightarrow ax + v$ over V , where $a \in F$, $a \neq 0$, $v \in V$, then the subgroups of G containing $H = \{ax \mid a \in F, a \neq 0\}$ form an interval \mathfrak{N}_n . But if $n - 1$ is not a prime power it remains an open question whether there exist or not G and H with $[H; G] \cong \mathfrak{N}_n$. It is only known that in this case G cannot be solvable. \mathfrak{N}_7 and \mathfrak{N}_{11} have been exhibited as intervals in the subgroup lattice of the alternating group of degree 31 (see [5]).

There is a natural translation of this problem in terms of permutation groups: in fact G acts as a transitive permutation group on the cosets of H in G , the kernel of this action is H_G , the core

(*) Indirizzo dell'A.: Dipartimento di Matematica Pura e Applicata, Via Belzoni 7, 35131 Padova, Italy.

of H in G , and there is a bijection between the systems of imprimitivity of G/H_G for this action and the subgroups M_i of G containing H .

So the problem that we are going to study is the following: let G be a transitive, imprimitive subgroup of $\text{Sym}(n)$, the symmetric group of degree n , with the property that all the systems of imprimitivity are maximal: how many systems of imprimitivity does G admit?

In this paper we study this last problem in a very particular case: when G is an imprimitive subgroup of $\text{Sym}(p^2)$ or of $\text{Sym}(pq)$ where p and q are distinct primes: in this situation all the systems of imprimitivity are automatically maximal.

The main results that we prove are the following:

THEOREM 1. *Let G be a transitive, imprimitive permutation group of degree p^2 and let n be the number of systems of imprimitivity for G . If $n \geq 2$ then $G \leq \text{Sym}(p) \times \text{Sym}(p)$ and either $n = 2$ or G is a subgroup of the group of permutations over a 2-dimensional vector space V over $GF(p)$ of the form $x \mapsto ax + v$, where $a \in (GF(p))^*$, $v \in V$, and $n = p + 1$.*

THEOREM 2. *Let G be a transitive, imprimitive permutation group of degree pq , p and q primes, $p > q$, and let n be the number of systems of imprimitivity for G . Suppose $n \geq 2$: then either $n = 2$ or $n = p + 1$. Precisely:*

- i) *There is at most one system with blocks of cardinality p .*
- ii) *If G has a block of imprimitivity with p elements and one with q elements, then $G \leq \text{Sym}(p) \times \text{Sym}(q)$.*
- iii) *If G has at least two different systems of imprimitivity, both with blocks of cardinality q (in particular if $n \geq 3$) then q divides $p - 1$ and one of the following holds:*
 - a) *G is a non abelian group of order pq ; G has exactly $p + 1$ systems of imprimitivity, one of them has blocks of cardinality p while all the other ones have blocks of cardinality q ;*
 - b) *$G = \text{PSL}(2, 7)$, $p = 7$, $q = 3$ and G has exactly two systems of imprimitivity, both with blocks of cardinality 3;*
 - c) *$G = \text{PSL}(2, 11)$, $p = 11$, $q = 5$ and G has exactly two systems of imprimitivity, both with blocks of cardinality 5.*

These results can be equivalently stated in terms of the subgroup lattice in the following way:

COROLLARY 1. *Suppose $|G:H| = p^2$ and that M_1, \dots, M_n are the maximal subgroups of G properly containing H .*

i) If $n \geq 2$, then $G/H_G \leq \text{Sym}(p) \times \text{Sym}(p)$;

ii) If $n \geq 3$, then G/H_G is a subgroup of the group of permutations over a 2-dimensional vector space V over $GF(p)$ of the form $x \mapsto ax + v$, where $a \in (GF(p))^*$, $v \in V$, and $n = p + 1$.

COROLLARY 2. Suppose $|G:H| = pq$ and that M_1, \dots, M_n are the maximal subgroups of G properly containing H .

i) If $n \geq 2$ and there exist i and j with $|M_i:H| = p$, $|M_j:H| = q$, then $G/H_G \leq \text{Sym}(p) \times \text{Sym}(q)$;

ii) If $n \geq 2$ and there exist i and j with $|M_i:H| = |M_j:H| = q$, then one of the following holds:

a) H is normal in G , G/H is a non abelian group of order pq and $n = p + 1$;

b) $G/H_G \cong \text{PSL}(2, 7)$, $q = 3$, $p = 7$ and $n = 2$;

c) $G/H_G \cong \text{PSL}(2, 11)$, $q = 5$, $p = 11$ and $n = 2$.

In particular we get a curious and unexpected consequence:

COROLLARY 3. Suppose $H \leq G$ with $|G:H| = pq$; if H is properly contained in at least three different proper subgroups of G , then H is normal in G .

Theorem 1 can be compared with a similar result proved by Wielandt in the contest of S -rings: see in particular [6], Lemma 26.3.

1. Some preliminary remarks.

Proofs of Theorem 1 and 2 will be given, respectively, in Section 2 and 3, while this section contains some general remarks on imprimitive groups, that will be useful in both proofs.

1.1 LEMMA. Suppose that a transitive, imprimitive group G contains two different systems of imprimitivity $\mathcal{B} = \{B_1, \dots, B_r\}$, $\mathcal{I} = \{C_1, \dots, C_s\}$ and that \mathcal{B} is a minimal system of imprimitivity for G : then either $|B_i \cap C_j| \leq 1$ for all $1 \leq i \leq r$, $1 \leq j \leq s$ or \mathcal{B} is a refinement of \mathcal{I} .

PROOF. Suppose that $B_i \cap C_j$ and $B_{i^*} \cap C_{j^*}$ are both non empty: chosen $x \in B_i \cap C_j$ and $y \in B_{i^*} \cap C_{j^*}$, since G is transitive, there exists $g \in G$ such that $x^g = y$: it is also $(B_i \cap C_j)^g = B_{i^*} \cap C_{j^*}$ so the non empty intersections of blocks of the first partition with those of the second have all

the same cardinality. If this cardinality is different from 1, then these intersections are a system of imprimitivity for G : being \mathcal{B} minimal, this system of imprimitivity is equal to \mathcal{B} : therefore \mathcal{B} is a refinement of \mathcal{T} . ■

1.2 LEMMA. *Let G be a transitive, imprimitive group of degree $n = rs$ and let $\mathcal{B} = \{B_1, \dots, B_r\}$, $\mathcal{T} = \{C_1, \dots, C_s\}$ be two minimal systems of imprimitivity for G , with $|B_i| = s$ and $|C_j| = r$: then $G \leq \text{Sym}(r) \times \text{Sym}(s)$.*

PROOF. By (1.1) $|B_i \cap C_j| \leq 1$: since $|B_i| = s = |\mathcal{T}|$ it must be $|B_i \cap C_j| = 1$ for all $1 \leq i \leq r$, $1 \leq j \leq s$. It will be convenient to label (i, j) the unique element in $B_i \cap C_j$; in this way $\Omega = \{(i, j) \mid 1 \leq i \leq r, 1 \leq j \leq s\}$ and the blocks are respectively the «rows» $B_i = \{(i, k) \mid 1 \leq k \leq s\}$ and the «columns» $C_j = \{(k, j) \mid 1 \leq k \leq r\}$. Let $\pi_{\mathcal{B}}: G \rightarrow \text{Sym}(\mathcal{B})$, $\pi_{\mathcal{T}}: G \rightarrow \text{Sym}(\mathcal{T})$ be the mappings that send an element g of G into the permutation induced by g on the set of the «rows» or respectively of the «columns». Let $g \in \ker(\pi_{\mathcal{B}}) \cap \ker(\pi_{\mathcal{T}})$: for each $(i, j) \in \Omega$, $\{(i, j)g\} = B_i g \cap C_j g = B_i \cap C_j = \{(i, j)\}$; so g fixes all the elements of Ω . Therefore $\ker(\pi_{\mathcal{B}}) \cap \ker(\pi_{\mathcal{T}}) = 1$ and $(\pi_{\mathcal{B}}, \pi_{\mathcal{T}}): G \rightarrow \text{Sym}(\mathcal{B}) \times \text{Sym}(\mathcal{T})$ is an injective homomorphism. ■

2. Proof of Theorem 1.

Throughout this section we assume that G is a transitive, imprimitive permutation group on a set Ω , with $|\Omega| = p^2$, and that there exist at least two distinct systems of imprimitivity, $\mathcal{B} = \{B_1, \dots, B_p\}$, $\mathcal{T} = \{C_1, \dots, C_p\}$; obviously $|B_i| = |C_j| = p$ and both these systems of imprimitivity are minimal. The situation is the same that is described in Lemma 1.2, so we may assume $\Omega = \{(i, j) \mid 1 \leq i \leq p, 1 \leq j \leq p\}$ and $G \leq \text{Sym}(p) \times \text{Sym}(p)$, where $g = (\phi, \psi)$ acts on Ω by the position $(i, j)(\phi, \psi) = (i\phi, j\psi)$. In particular, p^2 divides $|G|$, p^3 does not divide $|G|$.

Suppose now that G has a third system of imprimitivity, $\mathcal{D} = \{D_1, \dots, D_p\}$. By (1.2) D_k meets each B_i and C_j in exactly one point; therefore, if we call H the stabilizer in G of $(1, 1)$, $M_1 = \{g \in G \mid B_1 g = B_1\}$, $M_2 = \{g \in G \mid C_1 g = C_1\}$, $M_3 = \{g \in G \mid D_1 g = D_1\}$, we get $|G: M_i| = |M_i: H| = p$, $M_i \cap M_j = H$ if $i \neq j$ (we are assuming $(1, 1) \in D_1$). Furthermore, transitivity of G implies that H contains no nontrivial normal subgroups of G .

Let S_i be a minimal normal subgroup of G contained in M_i ; $S_i \neq 1$ otherwise we would have $G \leq \text{Sym}(p)$ and p^2 would not divide $|G|$. For

$i \neq j$, we get $G = M_j S_i$; it follows that S_i acts transitively on the right cosets of M_j in G , so p divides $|S_i|$ and p^2 does not divide $|S_i|$: but then S_i is simple.

Let P_i be a subgroup of S_i with $|P_i| = p$: $P_1 \times P_2$ is a Sylow p -subgroup of G and it is contained in $S_1 \times S_2$ which is a normal subgroup of G . It follows $P_3 \leq S_1 \times S_2$ hence $1 \neq S_3 \cap (S_1 \times S_2)$. Since S_3 is a minimal normal subgroup of G we have $S_3 \leq (S_1 \times S_2)$. It is now clear that S_i is cyclic of order p , $G = H(S_1 \times S_2)$, $(S_1 \times S_2) \cap H = 1$, $C_H(S_1 \times S_2) = 1$. $S = S_1 \times S_2$ can be thought as a vector space of dimension 2 over $\mathbb{Z}/p\mathbb{Z}$; since H normalizes S_1 , S_2 and S_3 it follows that H acts on $S_1 \times S_2$ by scalar multiplications. So G is a subgroup of the group of permutations $x \mapsto ax + s$ over S , where $a \in (GF(p))^*$, $s \in S$, and the systems of imprimitivity of G are in bijective correspondence with the maximal subgroups of G containing H , i.e. with the $p + 1$ one dimensional subspaces of S . This concludes the proof of Theorem 1.

3. Proof of Theorem 2.

Throughout this section we denote with G a transitive, imprimitive permutation group on a set Ω with $|\Omega| = pq$, where p and q are distinct primes with $p > q$.

A block of imprimitivity of G has cardinality either p or q ; in particular all the systems of imprimitivity of G are minimal.

If G has two systems of imprimitivity whose blocks have cardinality respectively p and q , then we are in the situation described in Lemma 1.2 and so $G \leq \text{Sym}(p) \times \text{Sym}(q)$.

This proves (ii) of Theorem 2.

Observe that G has at most a unique system of imprimitivity whose blocks have cardinality p (if $\mathcal{B} = \{B_1, \dots, B_q\}$, $\mathcal{C} = \{C_1, \dots, C_q\}$ are two different systems of imprimitivity with $|B_i| = |C_j| = p$, then, by (1.1), B_i meets each C_j in at most one element, and so, since $|\mathcal{C}| = q$, it follows $|B_i| \leq q$, a contradiction). In particular it follows that if G has three different systems of imprimitivity (or more) then at least two of them must have blocks of cardinality q . This is statement (i) of Theorem 2.

From now on we assume that G has two systems of imprimitivity, $\mathcal{B} = \{B_1, \dots, B_p\}$, $\mathcal{C} = \{C_1, \dots, C_p\}$, both with blocks of cardinality q : our aim is to determine the structure of this group G .

Let $\pi_{\mathcal{B}}: G \rightarrow \text{Sym}(\mathcal{B})$, $\pi_{\mathcal{C}}: G \rightarrow \text{Sym}(\mathcal{C})$ be the mappings that send an element g of G into the permutation induced by g on the set $\{B_1, \dots, B_p\}$ of the blocks \mathcal{B} , or respectively on the set $\{C_1, \dots, C_p\}$ of the blocks of \mathcal{C} . $\pi_{\mathcal{B}}$ and $\pi_{\mathcal{C}}$ are homomorphisms from G into $\text{Sym}(p)$ and

both $G\pi_{\mathcal{B}}$ as $G\pi_{\mathcal{F}}$ are transitive permutation groups of degree p , and so in particular primitive permutation groups.

$$(3.1) \quad \ker(\pi_{\mathcal{B}}) \cap \ker(\pi_{\mathcal{F}}) = 1.$$

PROOF. Let $g \in \ker(\pi_{\mathcal{B}}) \cap \ker(\pi_{\mathcal{F}})$: $B_i g = B_i$ and $C_j g = C_j$ for every $1 \leq i, j \leq p$. On the other hand for any $\omega \in \Omega$ there exist suitable i and j with $\{\omega\} = B_i \cap C_j$, but then $\{\omega g\} = B_i g \cap C_j g = B_i \cap C_j = \{\omega\}$; i.e. g fixes all the elements ω in Ω and so it is the identity. ■

(3.2) *If $g \in G$ has order p then g does not fix any point of Ω .*

PROOF. Suppose, by contradiction, that $\omega g = \omega$; $\{\omega\} = B_i \cap C_j$ for suitable $1 \leq i, j \leq p$. So in particular $B_i g = B_i$ but this implies that $g\pi_{\mathcal{B}} = 1$ since $g\pi_{\mathcal{B}}$ is an element in $\text{Sym}(p)$ with a fixed point and whose order divides p . In the same way from $C_j g = C_j$ it follows $g\pi_{\mathcal{F}} = 1$; hence $g \in \ker(\pi_{\mathcal{B}}) \cap \ker(\pi_{\mathcal{F}}) = 1$ by (3.1). ■

$$(3.3) \quad \ker(\pi_{\mathcal{B}}) = \ker(\pi_{\mathcal{F}}) = 1$$

PROOF. By (3.1) it is enough to prove that $\ker(\pi_{\mathcal{B}}) = \ker(\pi_{\mathcal{F}})$. Suppose, by contradiction, that $\ker(\pi_{\mathcal{B}})$ is not contained in $\ker(\pi_{\mathcal{F}})$: then $\ker(\pi_{\mathcal{B}})\pi_{\mathcal{F}}$ is a non trivial normal subgroup of the primitive permutation group $G\pi_{\mathcal{F}}$: so it is transitive of degree p and of consequence p divides $|\ker(\pi_{\mathcal{B}})|$. So $\ker(\pi_{\mathcal{B}})$ contains an element g of order p ; g sends each block B_i of \mathcal{B} into itself without fixing any point (by (3.2)) but this is impossible since $|g| = p$ and $|B_i| = q$. The converse inclusion is proved in the same way. ■

Now let t be an assigned element of order p in G (it exists since G is transitive of degree pq). By (3.2) t is the product of q cycles of length p . Let A_1, \dots, A_q be the orbits of t on Ω . $\mathcal{A} = \{A_1, \dots, A_q\}$ is a partition of Ω in subsets of cardinality p . Furthermore:

$$(3.4) \quad |A_i \cap B_j| = |A_i \cap C_k| = 1 \quad \text{for all } 1 \leq i \leq q, 1 \leq j, k \leq p.$$

PROOF. We claim first that $|A_i \cap B_j| \leq 1$. In fact, suppose by contradiction, that ω_1 and ω_2 are two different elements in $A_i \cap B_j$: since A_i is an orbit of t , $\omega_2 = \omega_1 t^k$ for a suitable k : it follows $B_j t^k = B_j$ and of consequence $(A_i \cap B_j) t^k = A_i \cap B_j$; so $A_i \cap B_j$ is a union of orbits of t^k , but all these orbits have length p , hence p divides $|A_i \cap B_j| \leq |B_j| \leq q$, a contradiction. Finally, since $|B_j| = q = |\mathcal{A}|$, we conclude $|A_i \cap B_j| = 1$. The same argument can be repeated with C_k in place of B_j . ■

Now it will be convenient to label (i, j) the unique element in $A_i \cap B_j$: in this way $\Omega = \{(i, j) \mid 1 \leq i \leq q, 1 \leq j \leq p\}$, the orbits of t are the «rows» $A_i = \{(i, k) \mid 1 \leq k \leq p\}$ while the blocks of \mathcal{B} are the «columns» $B_j = \{(k, j) \mid 1 \leq k \leq q\}$. Furthermore with each C_i is associated an injective map σ_i from $\{1, \dots, q\}$ into $\{1, \dots, p\}$ by the position $\{(j, j\sigma_i)\} = C_i \cap A_j$: in this way it results $C_i = \{(x, x\sigma_i) \mid 1 \leq x \leq q\}$ and so the system of imprimitivity \mathcal{I} can be represented by a set of p injective maps $\{\sigma_1, \dots, \sigma_p\}$ from $\{1, \dots, q\}$ into $\{1, \dots, p\}$. Moreover we may assume $i\sigma_1 = i$ for all $1 \leq i \leq q$. In this notation we have $t = \prod_{1 \leq i \leq q} ((i, j_1), \dots, (i, j_p))$ where $\tau = (j_1, \dots, j_p) \in \text{Sym}(p)$. We have proved above that $G\pi_{\mathcal{B}} = G^*$ is isomorphic to G ; we study now the structure of G^* :

$$(3.5) \quad G^* = \langle \tau \rangle K \quad \text{if } K = \text{Stab}_{G^*}(\{1, \dots, q\}).$$

PROOF. Since $|t| = p$ and $\pi_{\mathcal{I}}$ is injective, $\langle t \rangle$ acts transitively on the set $\{C_1, \dots, C_p\}$ of the blocks of \mathcal{I} ; in particular $G = \langle t \rangle \Gamma$ where $\Gamma = \{g \in G \mid C_1 g = C_1\}$. It follows $G^* = \langle t \rangle \pi_{\mathcal{B}} \Gamma \pi_{\mathcal{B}} = \langle \tau \rangle \Gamma \pi_{\mathcal{B}}$. So to conclude we have to prove that $\Gamma \pi_{\mathcal{B}} \leq \text{Stab}_{G\pi_{\mathcal{B}}}(\{B_1, \dots, B_q\})$. But this is clear since if $g \in \Gamma$ then $C_1 g = C_1$ and so g must permute into itself the subset $\{B_1, \dots, B_q\}$ of the blocks of \mathcal{B} with non trivial intersection with C_1 . ■

(3.6) *If G is solvable, then G is a non abelian group of order pq and q divides $p - 1$.*

PROOF. Since G is transitive of degree pq , $|G| = ps$ where q divides s . On the other hand G is isomorphic with $G\pi_{\mathcal{B}}$; this latter group, being a solvable transitive permutation group of degree p is similar to a subgroup M of $\text{Aff}(1, p)$, the group of bijection $\phi_{a,b}$ from $\mathbb{Z}/p\mathbb{Z}$ into itself of the form $x\phi_{a,b} = ax + b$, with $a \in (\mathbb{Z}/p\mathbb{Z})^*$ and $b \in \mathbb{Z}/p\mathbb{Z}$; it is not restrictive to identify τ with the translation $x\tau = x + 1$. So we have $M = Mo\langle \tau \rangle$ where $Mo = \text{Stab}_M(0)$ is cyclic of order s ; let $Mo = \langle \phi \rangle$: $x\phi = ax$ where a is an element of order s in $(\mathbb{Z}/p\mathbb{Z})^*$. By (3.5) there exists k such that $\phi\tau^k$ maps into itself an assigned subset of $\mathbb{Z}/p\mathbb{Z}$, say X , of cardinality q ; on the other hand $x(\phi\tau^k)^r = a^r x + (a^r - 1/a - 1)k$ from which it follows that $\phi\tau^k$ has a unique fixed point $(x = k/1 - a)$ and acts on the remaining $p - 1$ points as the product of $p - 1/s$ cycles of length s . This is equivalent to say that the orbits of $\phi\tau^k$ have all, except from 1 of length 1, the same length s ; since X must be a union of some of these orbits and q divides s , we conclude $s = q$. ■

To conclude we have to deal with the case when G is not solvable; under this hypothesis, by a famous result of Burnside ([2], Th. 21.3),

$G^* = G\pi_{\mathfrak{g}}$ is 2-transitive; from this we can deduce:

$$(3.7) \quad p \leq q^2 - q + 1.$$

PROOF. Since G^* is 2-transitive, $\{1, 2\}G^*$ is the set of all the subsets of $\{1, \dots, p\}$ with 2 elements: hence it has cardinality $p(p-1)/2$. On the other hand $\{1, 2\}G^* = \{1, 2\}K\langle\tau\rangle$ and every element of $\{1, 2\}K$ is a subset of $\{1, \dots, q\}$. So the possibilities for $\{1, 2\}G^*$ are at most $p\binom{q}{2}$; hence it must be $pq(q-1)/2 \geq p(p-1)/2$ i.e. $q(q-1) \geq p-1$. ■

To conclude we need the classification of transitive permutation groups of degree p ([3], [4]), i.e.:

(3.8) *There exists a normal subgroup S of $G^* \leq \text{Sym}(p)$ and one of the following holds:*

- (i) $S = \text{Alt}(p) \leq G^* \leq \text{Sym}(p)$, $p \geq 5$;
- (ii) $S = \text{PSL}(d, r) \leq G^* \leq \text{P}\Gamma\text{L}(d, r)$ and $p = r^d - 1/r - 1$;
- (iii) $S = G^* = M_{11}$, $p = 11$;
- (iv) $S = G^* = M_{23}$, $p = 23$;
- (v) $S = G^* = \text{PSL}(2, 11)$, $p = 11$;

We now analyze each of these possibilities:

(3.9) $S \neq \text{Alt}(p)$, i.e. we can exclude possibility (i).

PROOF. Suppose $S = \text{Alt}(p) \triangleleft G^* \leq \text{Sym}(p)$: $\text{Alt}(p)$ is $p-2$ transitive, moreover $q \leq p-2$. Hence S , and consequently G^* also, is q -transitive in contradiction with $\{1, \dots, q\}G^* = \{1, \dots, q\}\langle\tau\rangle$. ■

(3.10) $S \neq M_{11}$ and $S \neq M_{23}$, so we can exclude also possibilities (iii) and (iv).

PROOF. In both cases $S \triangleleft G^*$ implies G^* 4-transitive and, by (3.7) $q \geq 4$: $\{1, 2, 3, 4\}G^* = \{1, 2, 3, 4\}K\langle\tau\rangle$ and every element of $\{1, 2, 3, 4\}K$ is a subset of $\{1, \dots, q\}$. So, arguing as in (3.7), we get $p\binom{q}{4} \geq \binom{p}{4}$.

Let $S = M_{11}$: since $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8$ and $11 = p \leq q^2 - q + 1$ (by

(3.7)), q must be 5: we would have

$$p \binom{q}{4} = 11 \binom{5}{4} \geq \binom{p}{4} = \binom{11}{4},$$

but this is false.

In a similar way, $S = M_{23}$ yields, since $|M_{23}| = 23 \cdot 11 \cdot 9 \cdot 7 \cdot 5 \cdot 2^7$, $q \leq 11$ and finally $23 \binom{11}{4} \geq \binom{23}{4}$, but also this is false. ■

(3.11) *If $S = PSL(d, r)$ then $G^* = PSL(3, 2)$.*

PROOF. Suppose $S = PSL(d, r) \leq G^* \leq P\Gamma L(d, r)$ where $r = \rho^h$ is a prime power. First we claim that $(h, pq) = 1$. In fact, if by contradiction, p divides h , then $h \geq p = 1 + r + \dots + r^{d-1} \geq 1 + r \geq 1 + \rho^h$, but this is false; if we suppose, again by contradiction, that q divides h , then from $p \leq q^2 - q + 1$, we deduce $1 + \rho^q \leq 1 + \rho^h \leq p \leq q^2 - q + 1$, but the relation $1 + \rho^q \leq q^2 - q + 1$ never holds.

Our assumption is that $G^* \cong G$ can be represented as a transitive permutation group of degree pq admitting a subgroup H of index pq that is the intersection of two subgroups of index p . Since $|G^*:S|$ divides $|P\Gamma L(d, r):PSL(d, r)| = h$ and $(h, pq) = 1$ we conclude $|S:S \cap H| = pq$, i.e. S also is transitive of degree pq . Moreover S must contain two subgroups M_1 and M_2 , both of index p , whose intersection $S \cap H$ has index pq . We analyze now when this is possible. Since p is a prime, $PSL(d, r) = SL(d, r)$ and the representations of $PSL(d, r)$ as a transitive permutation group of degree p are all equivalent either to the action on the points or to the action on the hyperplanes of $PG(d - 1, q)$. So a maximal subgroup of degree p in $PSL(d, r)$ coincides either with the stabilizer of a point or with the stabilizer of a hyperplane.

The cases that may occur are the following:

1) $M_1 = \text{Stab}(P_1)$ and $M_2 = \text{Stab}(P_2)$ where P_1 and P_2 are two distinct points of $PG(d - 1, r)$. With a suitable choice of coordinates we may assume $P_1 = (1, 0, \dots, 0)$ and $P_2 = (0, 1, \dots, 0)$. The matrices that fix P_1 and P_2 are of the form:

$$\begin{bmatrix} a & 0 & & \\ 0 & b & 0 & \\ x_1 & y_1 & & \\ \dots & \dots & A & \\ x_{d-2} & y_{d-2} & & \end{bmatrix}$$

with $a, b \in GF(r)^*$, $x_i, y_j \in GF(r)$ and $a \cdot b \cdot \det(A) = 1$: this implies that $|S: M_1 \cap M_2| = p \cdot r \cdot r^{d-1} - 1/r - 1$. We want $r \cdot r^{d-1} - 1/r - 1 = q$; this implies $d = 2$ and $r = q$; so $p = q + 1$ and, since p is a prime, we get $q = 2$ and $S = SL(2, 2)$; but in this case G is solvable and we have already discussed this possibility.

The same happens for the intersection of the stabilizers of two hyperplanes.

2) $M_1 = \text{Stab}(P)$ and $M_2 = \text{Stab}(\pi)$ where π is a hyperplane and P is a point with $P \notin \pi$.

We may choose the coordinates so that $P = (1, 0, \dots, 0)$ and π has equation $x_0 = 0$. Now the matrices that fix P and π have form:

$$\begin{bmatrix} a & 0 \\ 0 & A \end{bmatrix},$$

where $a \in GF(r)^*$ and $a \cdot \det(A) = 1$. We get $|S: M_1 \cap M_2| = p \cdot r^{d-1}$ and $p \cdot r^{d-1} = p \cdot q$ implies $d = 2$, $r = q$, $S = PSL(2, 2)$: we conclude as above.

3) $M_1 = \text{Stab}(P)$ and $M_2 = \text{Stab}(\pi)$ where π is a hyperplane and P is a point with $P \in \pi$. We choose the coordinates so that $P = (1, 0, \dots, 0)$ and π has equation $x_1 = 0$. The matrices that fix P and π are those of the form:

$$\begin{bmatrix} a & 0 & 0 & \dots & 0 \\ x_1 & b & y_1 & \dots & y_{d-2} \\ x_2 & 0 & & & \\ \dots & \dots & & A & \\ x_{d-1} & 0 & & & \end{bmatrix},$$

with $a, b \in GF(r)^*$, $x_i, y_j \in GF(r)$ and $a \cdot b \cdot \det(A) = 1$. Hence $|S: M_1 \cap M_2| = p \cdot r^{d-1} - 1/r - 1$ and, of consequence, it must be $q = r^{d-1} - 1/r - 1$. Since q is a prime, this implies that $d - 1$ must be a prime. On the other hand from $p = r^{d-1} - 1/r - 1$ it follows that d also is a prime, and this happens if and only if $d = 3$. Now $q = 1 + r$ implies that r is even and q is a Fermat prime, i.e. $q = 1 + 2^{2^m}$. If $m \neq 0$ $p = 1 + 2^{2^m} + 2^{2^{m+1}}$ is divisible by 3 in contradiction with p prime. So the only possibility is $m = 0$ and $S = PSL(3, 2)$.

Since $PSL(3, 2) = P\Gamma L(3, 2)$ we conclude that if G^* contains a normal subgroup S with the wanted properties, then

$$G^* = PSL(3, 2). \quad \blacksquare$$

Therefore we have proved that if G is not solvable then

$$G \cong PSL(3, 2) \text{ or } G \cong PSL(2, 11).$$

Suppose $G \cong PSL(3, 2) \cong PSL(2, 7)$: $|G| = 8 \cdot 3 \cdot 7$, in particular a Sylow 2-subgroup of G has index $7 \cdot 3 = pq$ and it is contained in exactly 2 maximal subgroups, both of index 7 in G : so G acts as a transitive group of degree 21 on the set of cosets of a Sylow 2-subgroup with exactly two systems of imprimitivity.

$G \cong PSL(2, 11)$ contains two conjugacy classes of subgroups of index $pq = 11 \cdot 5$: the subgroups belonging to the first class are maximal; on the other hand a subgroup of the second class is contained in exactly two maximal subgroups, both of index 11: therefore to each of these subgroups is associated a representation of G as a transitive permutation group of degree 55 with exactly two systems of imprimitivity.

Theorem 2 is now completely proved: in fact we have shown that a transitive, imprimitive group G of degree pq which has two systems of imprimitivity whose blocks have cardinality q is either isomorphic to $PSL(2, 11)$ or to $PSL(2, 7)$, and in both these cases the two given systems of imprimitivity are the only ones that G admits, or G is a non abelian group of order pq , which has exactly $p + 1$ systems of imprimitivity, one of them with blocks of cardinality p .

3.12 REMARK. It follows immediately from what we have proved that: if a transitive permutation group of degree pq , say G , has at least three different systems of imprimitivity $\mathcal{A} = \{A_1, \dots, A_q\}$, $\mathcal{B} = \{B_1, \dots, B_p\}$, $\mathcal{C} = \{C_1, \dots, C_p\}$, with $|A_1| = p$, $|B_1| = |C_1| = q$, then G is a non abelian group of order pq . However this result can also be proved without making use of the classification of the transitive permutation groups of degree p . We give a sketch of this alternative proof.

It can be assumed: $\Omega = \{(i, j) \mid 1 \leq i \leq q, 1 \leq j \leq p\}$, $A_i = \{(i, x) \mid 1 \leq x \leq p\}$, $B_j = \{(x, j) \mid 1 \leq x \leq q\}$, $C_k = \{(x, x\sigma_k) \mid 1 \leq x \leq q\}$, where, as before, σ_k is an injective map from $\{1, \dots, p\}$ into $\{1, \dots, q\}$. If $g \in G$, then $g = (\alpha_g, \beta_g)$ with $\alpha_g \in \text{Sym}(p)$, $\beta_g \in \text{Sym}(q)$; moreover, since it is transitive, G contains an element of order p : this element must have form $(1, \tau)$ with $\tau \in \text{Sym}(p)$ and $|\tau| = p$. Since $C_i(1, \tau) = C_{if}$ for a suitable f in $\text{Sym}(p)$, it is easy to prove that it can be assumed $\sigma_j = \sigma_1 \tau^{j-1}$ for each $1 \leq j \leq p$. Let now $(1, \rho)$ be another element of order p in G . $C_i(1, \rho) = C_{ig}$, with $g \in \text{Sym}(p)$, implies $x\sigma_1 \tau^i \rho = x\sigma_1 \tau^{i+ig}$ for each $1 \leq i \leq p$: one can prove that this happens only if $\langle \rho \rangle = \langle \tau \rangle$: but then $\langle \tau \rangle$ is normal in G , and of consequence G is solvable. ■

REFERENCES

- [1] P. P. PÁLFY, *On Feit's examples of intervals in subgroup lattices*, J. Algebra, **116** (1988), pp. 471-479.
- [2] B. HUPPERT, *Endliche Gruppen*, Springer-Verlag, Berlin (1967).
- [3] P. M. NEUMANN, *Permutationsgruppen von Primzahlgrad und verwandte Themen*, Vorlesungen Math. Inst. Giessen, **5** (1977).
- [4] P. M. NEUMANN, *Transitive permutation groups of prime degree*, Proc. Second. Int. Conf. Theory of Groups, Canberra (1973), pp. 520-535.
- [5] W. FEIT, *An interval in the subgroup lattice of a finite group which is isomorphic to M_7* , Algebra Universalis, **17** (1983), pp. 220-221.
- [6] H. WIELANDT, *Finite Permutation Groups*, Academic Press, New York and London (1964).

Manoscritto pervenuto in redazione l'8 ottobre 1990.