Arch. Math., Vol. 38, 391–403 (1982)

0003-889X/82/3805-0013 $ 01.50 + 0.20/0

On partitions and permutation groups on unordered sets

By

JOHANNES SIEMONS

I. Introduction. From the action of a permutation group G on a finite set S one obtains a family of permutation representations (G, X_k) where G acts in the natural way on the system X_k of k-element subsets of S. These representations are highly interconnected (by generalised conjugation, see theorem 4.5) and one expects therefore general relations between the permutation invariants of (G, X_k) and (G, X_l). In this paper we establish the following theorem (4.2): The orbits of G on X_k determine, independently of the group in question, all G-orbits on X_l whenever $l \leqq k$ and $l + k \leqq n$, the number of points in S. This theorem is an important generalization of a now classical result of Livingstone and Wagner [10] which asserts that the number of orbits of (G, X_k) is at least as large as the number of orbits of (G, X_l). There are quite a number of independent proofs for this result due among others to Wielandt [18], Kantor [8] and Cameron [3]; this paper provides a new proof in this list. As a corollary (4.3) to theorem 4.2 we obtain an expression for the difference between the orbit numbers of (G, X_k) and (G, X_l).

The actual calculation of the G-orbits on X_l is based upon a process of formal differentiation in an algebra over the subset lattice of S which we discuss in chapters 2 and 3. Our main theorem 4.2 amounts to a combinatorial property of this lattice rather than to a particular property of permutation groups. For this reason we obtain a corresponding more general result (3.3) which is valid for the much wider class of C-D-partitions (see definitions in Chapter 3) of the subset lattice of S. Partitions of this type were first introduced by Dembowski [5] as generalized orbits. In an earlier paper [14] we have shown that an analogue of theorem 3.3 holds for any finite incidence structure of maximal rank. We note that theorem 4.2 remains true for permutation groups on infinite sets. This result is due to Bercov and Hobby [1] who conjectured our theorem.

In chapter 5 we consider the equivalence relations between permutation groups on S defined by $G \approx_k H$ provided G and H have the same orbits on the k-element subsets of S. The closure $G^{(k)}$ of G is defined to be the largest group on S for which $G^{(k)} \approx_k G$. This closure property occurs in a very natural way in the context of geometrical groups. In fact, any geometry whose incidence relations are expressible in terms of unordered k-relations on its underlying point set has the property that its full automorphism group is k-closed. As a corollary to theorem 4.2 every k-closed

group of degree n is $(k+1)$-closed for $k \leqq n \cdot \frac{1}{2}$ and more generally $G \approx_k H$ implies $G \approx_{k-1} H$.

We show that if $G \approx_k H$ for sufficiently many values of k, then G and H share global permutation properties like primitivity (theorem 5.2) and certain prime divisors (theorems 5.4 and 5.5). In general however $G \approx_k H$ for all k does not imply $G = H$. A yet open problem is the classification of all groups for which this implication holds. Such a result would determine all groups on S which are full automorphism groups of some geometry on S.

A related question goes into the opposite direction: What can we say about the orbits of (G, X_{k+1}) if the orbits of (G, X_k) are known? Some of the techniques in chapters 2 and 3 (in particular the integration operator ${}^c\circ\, \partial \,\circ^c$) may be used to produce a partition of X_{k+1} whose classes consist of unions of (G, X_{k+1})-orbits. Details of this will be given in a forthcoming paper. In general we can not expect to produce the exact orbits of (G, X_{k+1}) as the examples of groups shows that are 2-homogeneous but not 3-homogeneous. For $k \geqq 4$ however, k-homogeneous groups are, except for some groups of degree $\leqq 33$, also $(k+1)$-homogeneous and therefore contain the alternating group. This is one of the consequences of the classification of all finite simple groups. Any progress on the determination of the (G, X_{k+1})-orbits in general will provide a better understanding of the rare occurrence of multiply homogeneous groups.

Notation. We use the standard definitions and notation of Wielandt's book [17] with the exception that the use of Greek characters is avoided. For a subset x of S and any group G on S G_x denotes the setwise stabilizer of x while $G_{(x)}$ is the subgroup of G fixing each element of x. The constituent of G on x is denoted by $G^x = G_x/G_{(x)}$.

II. The set algebra RX and its dual. Let $S = \{s_1, s_2, \ldots, s_n\}$ be a finite set and let X be the lattice of all subsets of S. For an arbitrary field R we consider formal sums v over sets in X with coefficients in R, $v = \sum v_x \cdot x$ where x is in X and v_x in R. The set of these sums forms a vector space which we will denote by RX. A multiplication may be defined in RX by the following rule: If $v = \sum v_x \cdot x$ and $w = \sum w_y \cdot y$, then $v \cup w := \sum_{x,y} v_x \cdot w_y \cdot (x \cup y)$ where $x \cup y$ is the union of the sets x and y. Straight forward verifications show that $(RX, +, \cup)$ is an associative, distributive and commutative algebra which we shall call the *set algebra* of S over R. RX may also be considered as the set of polynomials in $R[s_1, s_2, \ldots, s_n]$ where each s_i occurs with degree at most one. The above defined $\cup$-multiplication agrees with the usual multiplication of polynomials if we calculate modulo the ideal IP generated by the polynomials of the form $s_i^2 - s_i$ for $i = 1, \ldots, n$. This remark shows that RX is isomorphic to the factor algebra $R[s_1, s_2, \ldots, s_n]/IP$ and X is a set of idempotent elements in RX.

The partial derivatives $\partial/\partial s_i =: \partial_i$ on $R[s_1, s_2, \ldots, s_n]$ become linear transformations on RX given by $\partial_i(x) = 0 \cdot \emptyset$ if s_i is not contained in $x \in X$ otherwise $\partial_i(x) = \{s \mid s \text{ in } x,\ s \neq s_i\}$. In combinatorial analysis the duality between s and $\partial/\partial s$ is an important concept (compare G.-C. Rota, page 7 in [12]), for this reason we call ∂_i the *dual point* of s_i. The product $\partial_1 \cdot \partial_2 \cdot \ldots \cdot \partial_r$ as linear transformations on RX

is commutative and since $\partial_i \cdot \partial_i = 0$, we may call $\partial_1 \cdot \partial_2 \cdot \ldots \cdot \partial_r$ the *dual set* of $\{s_1, s_2, \ldots, s_r\}$. Let D be the set of all dual sets in this sense and let RD denote the vectorspace generated by the transformations in D. It is easy to verify that RD is an associative, distributive and commutative algebra over R which is isomorphic to $R[\partial_1, \partial_2, \ldots, \partial_n]/NP$ where NP is the ideal generated by the polynomials ∂_i^2, $i = 1, \ldots, n$. Here D is a set of nilpotent elements. We gather our remarks in:

Proposition 2.1. *For a finite set $S = \{s_1, s_2, \ldots, s_n\}$ with subset lattice X, the set algebra RX for an arbitrary field R is isomorphic to $R[s_1, s_2, \ldots, s_n]/IP$. The algebra of dual sets RD is isomorphic to $R[\partial_1, \partial_2, \ldots, \partial_n]/NP$. Both algebras have dimension 2^n.*

In the following we shall determine the rank (as linear transformations on RX) of various elements in RD. The rank of a dual point clearly is 2^{n-1} but it is less obvious what the rank of a sum of dual points may be. Of particular interest is the symmetric polynomial

$$\partial = \partial_1 + \partial_2 + \partial_3 + \cdots + \partial_n$$

and its powers. In the remainder of this chapter we determine the rank of these transformations.

Let $u = \sum u_x \cdot x$ and $v = \sum v_y \cdot y$ be elements in RX. We shall say u and v are *disjoint* if there is partitioning of S into disjoint subsets S' and S'' such that $u_x = 0$ if $x \cap S'' \neq \emptyset$ and $v_y = 0$ if $y \cap S' \neq \emptyset$. We obtain the following "product rule" for disjoint elements:

Lemma 2.2. *If u and v are disjoint elements in RX and if ∂ is the sum over all distinct dual points, then*

$$\partial^m(u \cup v) = \sum_{i=0}^{m} \binom{m}{i} \cdot (\partial^{m-i}(u)) \cup (\partial^i(v)).$$

Here the binomial coefficient is to be taken in R and ∂^0 is the identity map.

Proof. Since u and v are disjoint, $u \cup v$ is the product of u and v as polynomials in $R[s_1, \ldots, s_n]$ and here the product rule is valid. □

Now suppose $S' \cup S'' = S$ is a partition of S where $|S'| = k$ and $|S''| = l$. For any $i \leqq k$ let u_i be the sum over all subsets of S' of size i and similarly, for $j \leqq l$ let v_j be the sum over all subsets of S'' of size j.

Lemma 2.3. *Let $k \geqq l$ and $m = k - l$. Then the equation $\partial^m(w) = (m + j)! \cdot (u_{l-j} \cup v_j)$ has a solution w_j for every $j \leqq l$. This solution is given inductively by*

$$w_j = j! \cdot (u_{k-j} \cup v_j) - \sum_{i=1}^{m} \binom{l-j+i}{l-j} \cdot \binom{m}{i} \cdot i! \cdot w_{j-i}$$

where $w_0 = u_k$ and $w_{j-i} = 0$ for j less than i.

Proof. We show that the w_j defined above satisfies the equation. Since $\partial \cdot \partial \cdot \ldots \cdot \partial(u_i)$ and $\partial \cdot \partial \cdot \ldots \cdot \partial(v_j)$ are disjoint, lemma 2.2 applies and therefore we obtain

$$\partial^m(w_j) = j! \cdot \sum_{i=1}^{m} \binom{m}{i} \cdot (\partial^{m-i}(u_{k-j})) \cup (\partial^i(v_j)) - \sum_{i=1}^{m} \binom{l-j+i}{l-j} \binom{m}{i} \cdot i! \cdot (m+j-i)! \cdot (u_{l-j+i} \cup v_{j-i}).$$

We calculate the ith term in the first sum: Since

$$\partial^{m-i}(u_{k-j}) = i! \binom{m-i+j}{m-i} \cdot (m-i)! \cdot u_{k-j-m+i} \quad \text{and} \quad \partial^i(v_j) = \binom{l-j+i)}{l-j} \cdot i! \cdot v_{j-i},$$

we obtain $\binom{l-j+i}{l-j} \cdot \binom{m}{i} \cdot (m-i+j)\,! \cdot (u_{l-j+i} \cup v_{j-i})$ as the ith term in the first sum. For $i = 0$ we have $(m+j)! \cdot (u_{l-j} \cup v_j)$, the right hand side of the original equation and for positive i the corresponding term is removed by the second sum. This completes the proof of lemma 2.3. □

For $k \leqq n$ let X_k be the family of k-element subsets of S. We identify $X_0 = \{\emptyset\}$ and $X_1 = S$. If RX_k denotes the corresponding subspace of RX, then $RX = \oplus RX_k$ becomes a graded vectorspace and ∂ is a homogeneous transformation of degree -1.

Theorem 2.4. *Let S be a set of n elements and k, l, m integers such that $0 \leqq l \leqq k \leqq n$ and $m = k - l$. Let R be a field of characteristic zero or bigger than k. Then ∂^m: $RX_k \to RX_l$ is injective if and only if $k + l \geqq n$; ∂^m is surjective if and only if $k + l \leqq n$.*

We formulate this result also for incidence matrices: Let $I(l, k, n)$ be the $(0, 1)$-matrix whose rows are indexed by X_l and whose columns are indexed by X_k such that the x, y-entry equals 1 if and only if $x \subseteq y$. Since $I(l, k, n)$ is, apart from a constant, the matrix of ∂^m, we obtain the following

Corollary 2.5. *The incidence matrix $I(l, k, n)$ has maximal rank for $l \leqq k \leqq n$ over any field of characteristic zero or bigger than k.*

Proof. In the case $k + l \leqq n$, we show that any x in X_l is an image under ∂^m. Put $S' = x$ and let S'' be a subset of S of size k disjoint from S'. By lemma 2.3 there is some w_l in RX_k satisfying $\partial^m(w_l) = k! \cdot x$. By assumption on the characteristic of R, $k! \neq 0$ and therefore ∂^m is surjective.

If $l + k \geqq n$, we add new points to S in order to obtain a set S^* of size $n^* = l + k$. Let ∂^* be the sum over all duals of points in S^* and X^* the lattice of subsets of S^*. By the first part, the map ∂^{*m}: $RX_k^* \mapsto RX_l^*$ is surjective and since the dimension of the two spaces is the same, this map is also injective. Consider the inclusion map *inc*: $RX_k \mapsto RX_k^*$ and the projection *proj*: $RX^* \mapsto RX$ given by $proj(x) = x$ if x is in X and $proj(x) = 0$ otherwise. The composition $\partial^{*m} \cdot inc$ is injective and since Kernel $(proj) \cap$ Image$(\partial^{*m} \cdot inc) = 0$, the same is true for $proj \cdot \partial^{*m} \cdot inc = \partial^m$. Note that the assumption on char R is essential: $I(1, 2, 3)$ has rank 2 over the field of 2 elements. □

In X we consider the map ${}^c\colon X \to X$ which sends any subset x onto its complement ${}^cx$ in S. This mapping extends to an involutory linear transformation of RX.

Theorem 2.6. *Let V be a subspace of RX such that $\partial V \subseteq V$ and ${}^cV \subseteq V$ and let $V_k = RX_k \cap V$. Then V_k uniquely determines V_l for any $l \leqq k$, $l + k \leqq n$ or $l \geqq k$ and $l + k \geqq n$ by $V_l = \partial^{k-l}(V_k)$ or $V_l = \partial^{n-k-l}({}^cV_k)$. In particular $V = \bigoplus V_k$ is completely determined by V_{n^*} where n^* is the integer $(n-1)\cdot\frac{1}{2} \leqq n^* \leqq n\cdot\frac{1}{2}$.*

Proof. By assumption we have ${}^c(V_l) = V_{n-l}$ and therefore it suffices to assume $l \leqq k$. Since V is ∂-invariant, we have the chain of homomorphisms

$$\partial^{(n-2l)}\colon\ V_{n-l} \to \cdots \xrightarrow{\partial} V_k \xrightarrow{\partial} \cdots \xrightarrow{\partial} V_l\,.$$

By theorem 2.4 this map is injective and since the image and pre-image spaces have the same dimension, also surjective. Therefore $V_l = \partial^{k-l}(V_k)$ is determined as the image of V_k under the map ∂^{k-l}. □

III. Partitions. Let S be again a finite set of size n and X_k the system of k-element subsets. For each $k \leqq n$ we consider a partition P_k of X_k into classes $P_{k,1}, \ldots, P_{k,i}, \ldots$ and the partition $P = \bigcup_{k=1}^{n} P_k$ of the whole of X. To each partition P_k we associate the subspace RP_k of RX_k which is spanned by the vectors $p_{k,i} = \sum x$, x in $P_{k,i}$. Thus $RP = \bigoplus RP_k$ is a subspace of RX representing P. Conversely, we call a subspace V of RX a partition space if $V = RP$ for some partition P of X. The following observation is fundamental:

Proposition 3.1. *The partitions of X and the partition subspaces of RX are in one-one correspondence.*

Proof. Observe that a partition P is finer than or equal to P' if and only if $RP \supseteq RP'$. Therefore $RP = RP'$ if and only if $P = P'$. □

Definition. A partition P of X is a *C-D-partition* or *generalized orbits* if the following two conditions are satisfied for each $k = 0, 1, \ldots, n$:

C: If $P_{k,i}$ is an arbitrary class in P_k, then

$${}^c(P_{k,i}) = \{{}^cx \mid x \text{ in } P_{k,i}\} \text{ is a union of classes in } P_{n-k}.$$

D: For any y in X_{k-1} and any class $P_{k,i}$ let $l(y)$ be the number of sets in $P_{k,i}$ that contain y. Then $l(y)$ only depends on the class that contains y.

In [14] we have met a similar situation in the case of tactical decompositions; it can be shown that P is a C-D-partition if and only if (P_k, P_l) is a tactical decomposition for every $k \leqq l \leqq n$.

Proposition 3.2. *A partition P satisfies C if and only if ${}^c(RP) \subseteq RP$ and D is satisfied if and only if $\partial(RP) \subseteq RP$ for some field R of characteristic zero or bigger than n.*

Proof. Let $p = \sum x$ be the sum over all sets in some class $P_{k,i}$; the vectors of this type form a basis of RP_k and ${}^c p = \sum {}^c x$ is contained in RP_{n-k} if and only if $\{{}^c x \mid x \text{ in } P_{k,i}\}$ is a union of classes in P_{n-k}. Similarly,

$$v = \partial(p) = \sum \partial(x) = \sum_{x \in P_{k,i}} \sum_{x \supset y \in X_{k-1}} y = \sum_j \sum_{y \in P_{k-1,j}} v_y \cdot y .$$

Then v is contained in RP_{k-1} if and only if $v_y = v_{y'}$ whenever y and y' belong to the same class $P_{k-1,j}$. By assumption on the characteristic of R this is equivalent to D. □

Our next theorem shows that C-D-partitions P are determined by P_{n^*}, this is a consequence of the above proposition and theorem 2.6.

Theorem 3.3. *Let S be a set of size n and X_k the family of k-subsets of S. Let P_k be a partition of X_k for $k = 0, 1, \ldots, n$ such that $P = \cup P_k$ is a C-D-partition of $X = \cup X_k$. Then P_k uniquely determines P_l for any $l \leqq k$, $l + k \leqq n$ or $l \geqq k$, $l + k \geqq n$. In particular P is uniquely determined by P_{n^*} where n^* is the integer $(n-1)\frac{1}{2} \leqq n^* \leqq n \cdot \frac{1}{2}$.*

Proof. Let R be a field of characteristic zero. In view of proposition 3.2 and theorem 2.6, the vectorspaces RP_l and RP are completely determined. Therefore, by proposition 3.1, the partitions P_l and P are determined by RP_l and RP respectively. □

In the following we shall suppose that an arbitrary partition Q_{n^*} of X_{n^*} is given and we shall investigate under what circumstances there is a C-D-partition P of X for which $P_{n^*} = Q_{n^*}$. If $Q_{n^*,1}, \ldots, Q_{n^*,i}, \ldots$ are the classes of Q_{n^*}, let q_i be the sum over all sets in $Q_{n^*,i}$. For any element $v = \sum v_x \cdot x$ in RX_k we define the level surfaces of v: $lev_r(v) = \{x \mid x \text{ in } X_k, v_x = r\}$ for any r in R. This is used to define the level surfaces of Q_{n^*} in X_k:

$$Lev(Q_{n^*}, k) = \{lev_r(\partial^{n^*-k}(q_i)) \mid r \text{ in } R, i = 1, \ldots\} \quad \text{if} \quad k \leqq n^*$$

and

$$Lev(Q_{n^*}, k) = \{{}^c L \mid L \text{ in } Lev(Q_{n^*}, n-k)\} \quad \text{for} \quad k \geqq n^* .$$

For each $k = 0, 1, \ldots, n$ we consider the coarsest partition P_k of X_k which is as fine as $Lev(Q_{n^*}, k)$, that is, if L is a family of k-sets in $Lev(Q_{n^*}, k)$ and $P_{k,i}$ any class of P_k, then $P_{k,i} \cap L = \emptyset$ or $P_{k,i}$ and the number of classes in P_k is minimal with this respect. Clearly $P_{n^*} = Q_{n^*}$ since Q_{n^*} is a partition itself.

Theorem 3.4. *Let Q_{n^*} be a partition of X_{n^*}, $(n-1) \cdot \frac{1}{2} \leqq n^* \leqq n \cdot \frac{1}{2}$, and let P be the partition of X defined above. Then P is a C-D-partition if and only if the number of classes in P_k is equal to the dimension of the space $\partial^{n^*-k}(RQ_{n^*})$ for all $k \leqq n^*$ and some field R of characteristic zero.*

Proof. If P is a C-D-partition with $P_{n^*} = Q_{n^*}$, by theorem 2.6 $RP_k = \partial^{n^*-k}(RP_{n^*})$ and the dimension of the latter space is the number of classes in P_k.

Conversely, let RL_k be the vectorspace spanned by the vectors l where l is the sum over some level surface in $Lev(Q_{n^*}, k)$. Then ${}^c(RL_k) = RL_{n-k}$ and

$$RL_k \supseteq \partial^{n^*-k}(RQ_{n^*}) \quad \text{or} \quad \supseteq {}^c(\partial^{n^*+k-n}(RQ_{n^*}))\,,$$

according to $k \leqq n^*$ or $k > n^*$. By the construction of P, we have $RP_k \supseteq RL_k$ for all k and by the assumption on the dimensions, we obtain that

$$RP_k = RL_k = \partial^{n^*-k}(RQ_{n^*}) \quad \text{or} \quad = {}^c(\partial^{n^*+k-n}(RQ_{n^*}))\,.$$

This implies $\partial(RP_k) \subseteq RP_{k-1}$ and since ${}^c(RP_k) = {}^c(RL_k) = RL_{n-k} = RP_{n-k}$, P is a C-D-partition by proposition 3.2. □

IV. The Theorem of Livingstone and Wagner. In this chapter we will derive some important conclusions for permutation groups from our results on partitions. Let G be an arbitrary permutation group on the finite set S. The G-action on S leads to an action of G on the subset lattice X. This in turn extends naturally to linear transformations on RX by defining

$$g\colon\ v = \sum v_x \cdot x \to v^g = \sum v_x \cdot x^g$$

where $x^g = \{s^g \mid s \in x\}$. Note that this operation of G on RX is compatible with the $\cup$-multiplication defined in chapter II. The partitioning of X into G-orbits is denoted by

$$X(G) = \{\{x^g \mid g \in G\} \mid x \in X\}$$

and $RX(G)$ is the partition space corresponding to $X(G)$. The subspace of $RX(G)$ corresponding to $X_k(G)$, the G-orbits on X_k, is denoted by $RX_k(G)$, in accordance with the notation in chapter III. The following is elementary and can easily be verified.

Proposition 4.1. *For any group G on the finite set S, the partitioning $X(G)$ into orbits is a C-D-partition in the sense of chapter III. $RX(G)$ is the centralizer algebra*

$$\{v \mid v^g = v \text{ for all } g \text{ in } G\}$$

which is invariant under the maps ^{c} and ∂.

Representation algebras of this type and similar constructions have been considered in Siemons [13], and Wielandt [19, 20].

The main result of this paragraph is an important improvement of the theorem of Livingstone and Wagner [10] which asserts $|X_k(G)| \geqq |X_{k-1}(G)|$ for any group G on S and $2k \leqq n$. (Proofs for this theorem can also be found in Wielandt [18] and Cameron [3].) The following is an immediate consequence of 3.3:

Theorem 4.2. *Let S be a set consisting of n elements and k an integer $\leqq n$. Let $X_k(G)$ be the family of orbits of some permutation group G on the k-subsets of S. Then $X_k(G)$ uniquely determines $X_l(G)$, independently of the group G, for any $l \leqq k$, $l + k \leqq n$ or $l \geqq k$, $l + k \geqq n$. In particular $X(G)$ is determined by $X_{n^*}(G)$ where n^* is the integer $(n-1) \cdot \frac{1}{2} \leqq n^* \leqq n \cdot \frac{1}{2}$.*

In the proof of theorem 2.6 we have seen that $RX_l(G) = \partial^{k-l}(RX_k(G))$ for $l \leqq k$, $l + k \leqq n$ for any field of characteristic zero. Therefore we obtain an expression for the number $|X_l(G)| = \dim RX_l(G)$ of G-orbits on the l-subsets of S:

Corollary 4.3. *For $l \leqq k$, $l + k \leqq n$ the number of G-orbits on X_l is given by*

$$|X_l(G)| = |X_{n-l}(G)| = |X_k(G)| - \dim(\text{Kernel}(\partial^{k-l}) \cap RX_k(G))$$

where R is a field of characteristic zero.

Theorem 4.4. *Let G and H be groups on S and k an integer $\leqq \frac{1}{2} \cdot |S|$ so that the following holds: For any g in G and any k-subset x there is some h in H so that $x^g = x^{h^*}$ Then for any subset y of size $\leqq k$ and any $g \in G$ there is some h^* in H so that $y^g = y^{h^*}$.*

Proof. The hypothesis is equivalent to the assumption that every G-orbit on X_k is contained in some H-orbit. Therefore $RX_k(G) \supseteq RX_k(H)$ for any field of characteristic zero. If y has size l and $m = k - l$, by theorem 2.6, $\partial^m(RX_k(G)) = RX_l(G)$ and a similar relation holds for $RX_k(H)$. Therefore $RX_l(G) \supseteq RX_l(H)$ and this is equivalent to the conclusion of the theorem. □

We now consider the following question. Suppose an *arbitrary* permutation on X_k is given, say as permutation matrix G_k. When is G_k induced by a permutation G_1 on S when acting on X_k in the natural way?

Apparently this is the case if and only if for any $x \in X_k$ we obtain $I \cdot G_k(x) = G_1 \cdot I\ (x)$ where I is the incidence matrix of points in k-sets. If the equation holds we obtain $G_1 = I \cdot G_k \cdot I^-$ for any right-inverse I^- of I (see corollary 2.5). Conversely suppose $G_1 = I \cdot G_k \cdot I^-$ is a permutation matrix independent of the particular choice of I^- as a right-inverse. Then $I \cdot G_k \cdot M = 0$ whenever $I \cdot M = 0$. Taking $M = (1 - I^- \cdot I)$, we obtain

$$0 = I \cdot G_k \cdot (1 - I^- \cdot I) = I \cdot G_k - I \cdot G_k \cdot I^- \cdot I = I \cdot G_k - G_1 \cdot I\,.$$

Since permutation matrices are the orthogonal (0, 1)- matrices we have the following:

Theorem 4.5. *Let G_k be a permutation matrix on X_k and let I be the incidence matrix of points in k-sets. Then G_k is induced by a permutation G_1 on S if and only if IG_kI^- is an orthogonal (0, 1)-matrix independent of the choice of I^- as a right-inverse of I, and $G_1 = IG_kI^-$.*

A corresponding result may easily be formulated for the more general question: When does G_k induce a permutation on X_l? Theorem 4.2 may be considered as a consequence of 4.5 if one observes that the partitioning into orbits corresponds to a linear operator $x \to \sum_{g \in G} x^g$ which commutes with the inclusion map (Proposition 3.2).

V. Orbit equivalence. In this section we consider the equivalence relation of permutation groups on S having the same orbits on the subset lattice of S:

Definition. Let G and H be two groups on the set S consisting of n elements. G is *k-orbit equivalent* to H, $G \approx_k H$, if $X_k(G) = X_k(H)$. The *k-closure* $G^{(k)}$ of G is the largest group on S with $X_k(G^{(k)}) = X_k(G)$. G is *orbit equivalent* to H, $G \approx_* H$, if $X(G) = X(H)$, and the *closure* G^* is the largest group on S with $X(G^*) = X(G)$.

Using this terminology we obtain as a corollary to 4.2 the following theorem:

Theorem 5.1. *If $G \approx_k H$ are permutation groups of degree n, $k \leqq n^*$ where*

$$(n-1)\cdot\tfrac{1}{2} \leqq n^* \leqq n\cdot\tfrac{1}{2},$$

then $G \approx_l H$ for any $l \leqq k$ and $G \approx_* H$ if and only if $G \approx_{n^*} H$. Furthermore,

$$G \subseteqq G^* \subseteqq \cdots \subseteqq G^{(l)} \subseteqq G^{(l-1)} \subseteqq \cdots \subseteqq G^{(1)}$$

for $l \leqq n^*$ and G is l-homogeneous if and only if $G^{(l)}$ is the symmetric group.

For infinite sets Bercov and Hobby [1] have proved the same result using a form of Ramsey's theorem. (Their proof does not apply in the finite case). We note that their result may also be proved independently of Ramsey's theorem by extending the techniques of Chapter II to infinite dimensional set algebras. In theorem 5.1 k-homogeneity can in general not be replaced by k-transitivity as the example of the symmetric and alternating groups shows. For $5 \leqq k \leqq n^*$, however, k-homogeneity and k-transitivity are equivalent and for $2 \leqq k \leqq 4$ the same is true apart from some well-understood exceptions, see Kantor, theorem 1 in [9].

In the following theorem we show that the primitivity of G is reflected in the orbit algebra $RX(G)$:

Theorem 5.2 (Rudio's Lemma). *Let G be a group on S of degree n. Then G is primitive on S if and only if ${}^c\!\circ\, \partial_j \circ^c \circ\, \partial_i \colon RX(G) \mapsto RX$ is a monomorphism for all $i \neq j$ in $\{1, \ldots, n\}$.*

If $G \approx_k H$ for some $k \geqq 2$, $k \leqq n-2$, then both groups have the same blocks of imprimitivity. In particular, H is primitive if and only if G is primitive on S.

Rudio's Lemma (1888, see theorem 8.1 in [17], compare also [16]) asserts a separation property: A group G is primitive on a finite set S if and only if for any pair s, s' of distinct points and any subset $x \neq S, \emptyset$ of S, there is a group element g such that $s \in x^g \not\ni s'$.

Proof of 5.2. Let R be any field and let s_i, s_j be two distinct points of S and let ∂_i, ∂_j be their dual points. The map ${}^c\!\circ\, \partial_j \circ^c \circ\, \partial_i$ interchanges s_i with s_j in any set x that contains s_i but not s_j and maps x onto zero in all other cases. For this reason it will be sufficient to show that none of the canonical basis vectors of $RX(G)$ is mapped onto zero in order that ${}^c\!\circ\, \partial_j \circ^c \circ\, \partial_i$ is injective.

According to Rudio's Lemma, a subset x is a block of imprimitivity for G if and only if ${}^c\!\circ\, \partial_j \circ^c \circ\, \partial_i(x^g) = 0$ for all g in G and some pair $i \neq j$. Hence x, $2 \leqq |x| \leqq n-2$, is a block of imprimitivity if and only if ${}^c\!\circ\, \partial_j \circ^c \circ\, \partial_i(q) = 0$ for the basis vector q of $RX(G)$ that consists of all G-images of x. If x has size 1 or $n-1$, the assumption ${}^c\!\circ\, \partial_j \circ^c \circ\, \partial_i(q) \neq 0$ for all $i \neq j$ is equivalent to the transitivity of G on S.

For the second part of the proof we can assume $G \approx_2 H$. We call a subset Q of X_2 an equivalence relation in X_2 provided $\{s, s'\}$ and $\{s, s''\} \in Q$ always implies that $\{s', s''\}$ is contained in Q. Let q be the sum over all sets in Q. It is easy to see that Q is an equivalence relation if and only if either $\partial_i(q) = \partial_j(q)$ or $\partial_i(q)$ and $\partial_j(q)$ are disjoint for all i and j. If Q is a G-invariant equivalence relation, $(\partial_i(q))^g = \partial_{i^g}(q)$ for all g in G and therefore $\{\partial_i(q) \mid i = 1, \ldots, n\}$ corresponds to a partitioning of S into blocks of imprimitivity. Since $G \approx_2 H$, both groups have the same block systems, each corresponding to an equivalence relation in $X_2(G) = X_2(H)$. □

We remark that the theorem suggests a notion of primitivity for arbitrary C-D partitions on X. Defining a partition P to be primitive if for all $i \neq j$ the map ${}^c\circ \partial_j \circ {}^c \circ \partial_i$ is a monomorphism on RP, we have seen in the proof of 5.2 that P is primitive if and only if P_2 contains no equivalence relations except possibly the two trivial relations.

Lemma 5.3. *Let G be a group on S of degree n and $k \leqq \frac{1}{2}n$. Then the index $|G^{(k)} : G|$ is equal to $|G_x^{(k)} : G_x|$ for any subset x of size $l \leqq k$ or $l \geqq n - k$. In particular, the order of $G^{(k)}$ divides $|G : G_x| l!\,(n - l)!$.*

Proof. We can assume that $|x| = l \leqq k$ and, by theorem 5.1, $G^{(k)} \approx_l G$. Therefore the G-orbit and the $G^{(k)}$-orbit of x are the same. Hence $|G^{(k)} : G_x^{(k)}| = |G : G_x|$. For the remainder observe that $G_x^{(k)}$ is a subgroup of the direct product of the symmetric groups on x and ${}^c x$. □

Theorem 5.4. *Let G and H be orbit equivalent groups of degree n. If p is a prime, $2p > n + 1$, then p divides the order of G if and only if it divides the order of H.*

Proof. In lemma 5.3 we take $l = p - 1$; therefore $|G^* : G|$ and $|H^* : H|$ divide $(p - 1)! \cdot (n - p + 1)!$ and hence are coprime to p. Since $H^* = G^*$ the required property follows. □

Theorem 5.5. *Let G and H be transitive and orbit equivalent groups of degree n and let p, $n - 3 \geqq p \geqq (n + 1) \cdot \frac{1}{2}$, be a prime dividing the order of G. Then both groups contain the alternating group of degree n unless $n = 9$ in which case G and H are among the groups $PSL(2, 8)$, $P\Gamma L(2, 8)$, $\mathrm{Alt}(9)$, $\mathrm{Sym}(9)$.*

Proof. First we show that G is primitive on S: Let $g \in G$ be an element of order p displacing the points $\{s_1, \ldots, s_p\} = y$. A block of imprimitivity for G would have to contain y or otherwise be disjoint from y. The first assumption contradicts the fact $p > n\frac{1}{2}$ while the transitivity of G excludes the second possibility. Hence both G and H are primitive by theorem 5.2. As a consequence of Jordan's theorem (see theorem 13.9 in [17]), G contains the alternating group of degree n. If $p > (n + 1) \cdot \frac{1}{2}$, p divides the order of H by theorem 5.4 and hence $H \supseteq \mathrm{Alt}(n)$.

In the remaining case $p = (n + 1) \cdot \frac{1}{2} \geqq 5$ does not divide the order of H so that H is not (p)-transitive. On the other hand $H \approx_* G$ which implies that H is k-homogeneous for every $k \leqq n$. The assumption that H is $(p - 1)$-transitive contradicts

lemma 9 in [10]. Hence we may apply theorem 2b in [10] and conclude $n = 9$, $p = 5$ and $H = PSL(2, 8)$ or $P\Gamma L(2. 8)$. □

The group $P\Gamma L(2, 8)$ is the largest non-trivial group which is k-homogeneous for all $k \leqq n$. The only other groups with this property are the Frobenius group of order 20 ($n = 5$), $G = PGL(2, 5)$ ($n = 6$) and $G \supseteq PGL(2, 8)$ with $n = 9$. (See for instance § 1 of Livingstone and Wagner [10]). Hence, $G \approx_* \mathrm{Alt}(n)$ implies $G \supseteq \mathrm{Alt}(n)$ unless G is one of these exceptions.

In the general case the orbit equivalence relation for permutation groups seems to be close to the equality relation. A possible approach in this direction would be to compare the constituents of orbit equivalent groups. The following example shows that the equality of constituents does not imply equality for the whole group: If $G = \mathrm{Alt}(S)$ and x is a subset of size $\geqq 2$ and $\leqq n - 2$ then $G^x = \mathrm{Sym}(x)$ and $G^{^c x} = \mathrm{Sym}({}^c x)$. However, we have the following

Proposition 5.6. *Let $G \approx_* H$ be groups on S with $G \subseteq H$ and suppose x is a subset of S with the property that 1 is the only permutation in H fixing every point of x. Then $G = H$ if and only if $G^x = H^x$.*

Proof. Let h be in H; then there exists some g in G so that $x^g = x^h$ and thus $g^{-1}h \in H_x$. If $G^x = H^x$ choose an element g' in G which agrees with $g^{-1} \cdot h$ on x. Then $g' \cdot h^{-1} \cdot g$ fixes every point of x and hence must be the identity. This shows that h is contained in G. □

We now turn to the more general problem of k-closure. This equivalence relation has a natural interpretation in the context of geometrical groups. The full automorphism group of an (undirected) graph on the vertex set S, for instance, is 2-closed since this group can be characterized as the largest group on S that preserves the family of 2-subsets representing the edges of the graph. Likewise, if $\mathscr{P}$ is an affine or projective plane (or indeed any $2 - (n, k, 1)$-design) then $\mathscr{P}$ is fully determined by the subset of X_3 representing the family of collinear point tripels. Therefore the automorphism group of $\mathscr{P}$ is 3-closed.

Let C be a subgroup of $G^{(k)}$ containing G for some $k \leqq \frac{1}{2} \cdot n$ and let p be a prime dividing the order of C. If P' is a Sylow-p-subgroup of C, then $\{x\}$ is contained in $X(P')$ for some subset x of S if and only if x is a union of point orbits of P' and hence $\{x\} \in X(P)$ for any subgroup P of P'. In the opposite direction we prove

Lemma 5.7. *Let P be a Sylow-p-subgroup of G for some prime p and let x be a set of size l for which $\{x\}$ is contained in $X(P)$. Then for any k, $l \leqq k$ and $l + k \leqq n$ or $l \geqq k$ and $l + k \geqq n$ and any given p-subgroup P' of $C \subseteq G^{(k)}$ there is some g in G so that $\{x^g\} \in X(P')$.*

Proof. By theorem 5.1 $C \approx_l G$ and therefore $d = |G : G_x| = |C : C_x|$ is prime to p. Hence let P^* be a Sylow-p-subgroup of C contained in C_x. (This implies $\{x\} \in X(P^*)$). There is some h in C such that $(P^*)^h$ contains the given group P'. This implies $\{x^h\} \in X(P^{*h}) \subseteq X(P')$ and hence we can choose some $g \in G$ so that $\{x^g\} = \{x^h\}$ is contained in $X(P')$. □

Theorem 5.8. *Let G be a group on S of degree n and let $G \subseteq C \subseteq G^{(k)}$ for some $k \leqq \frac{1}{2} \cdot n$. Suppose p is a prime dividing the order of C but not the order of G. Let P' be a Sylow-p-subgroup of C with fixed point set S'. Then the size of S' is bigger than or equal to* $\min(p-1, k)$ *and the G-orbits on X_l are in one-one correspondence to the orbits of $C^{S'}$ on the l-subsets of S' for every $l \leqq \min(p-1, k)$.*

Proof. Let x be a set of size $l \leqq \min(p-1, k)$. Since G has order prime to p, by lemma 5.7 there is some $g \in G$ so that $\{x^g\} \in X(P')$. Since $l < p$, x^g must be a union of points fixed by P'. Hence $x^g \subseteq S'$ and every G-orbit on X_l contains a subset of S' for any $l \leqq \min(p-1, k)$.

It remains to show that if $x, y \subseteq S'$ such that $x^g = y$ for some $g \in G$, then there is some a in $C_{S'}$ with $x^a = y$. In this case it is clear that P' and $(P')^g$ are Sylow-p-subgroups of $C_{(y)}$. Hence there is some h in $C_{(y)}$ so that $a = gh$ is contained in the normalizer of P' in $C_{(y)}$. Therefore $x^{g \cdot h} = y^h = y$ and $(S')^a = S'$, i.e. $a \in C_{S'}$. This shows that the sets of any G-orbit on X_l contained in S' are precisely one $C_{S'}$-orbit. □

References

[1] R. D. BERCOV and C. R. HOBBY, Permutation groups on unordered sets. Math. Z. **115**, 165–168 (1970).

[2] R. E. BLOCK, On the orbits of collineation groups. Math. Z. **96**, 33–49 (1967).

[3] P. CAMERON, Transitivity of permutation groups on unordered sets. Math. Z. **148**, 127–139 (1976).

[4] P. CAMERON, P. M. NEUMANN and J. SAXL, An interchange property in finite permutation groups. Bull London Math. Soc. **11**, 177–183 (1979).

[5] P. DEMBOWSKI, Verallgemeinerungen von Transitivititätsklassen endlicher projektiver Ebenen. Math. Z. **69**, 59–89 (1958).

[6] C. HERING, On codes and projective designs. Kyoto University Mathematics Research Institute, Seminar Notes **344**, 20–60 (1979).

[7] D. HUGHES, Collineations and generalised incidence matrices. Trans. Amer. Math. Soc. **86**, 284–296 (1957).

[8] W. M. KANTOR, On incidence matrices of finite projective and affine spaces. Math. Z. **124**, 315–318 (1972).

[9] W. M. KANTOR, k-homogeneous groups. Math. Z. **124**, 261–265 (1972).

[10] D. LIVINGSTONE and A. WAGNER, Transitivity of finite permutation groups on unordered sets. Math. Z. **90**, 393–403 (1965).

[11] C. PRAEGER and J. SAXL, On the orders of primitive permutation groups. Bull. London Math. Soc. **12**, 303–307 (1980).

[12] G.-C. ROTA, Finite Operator Calculus. New York-London 1975.

[13] I. J. SIEMONS, On doubly homogeneous groups. Proc. Royal Irish Acad. (in print).

[14] I. J. SIEMONS, Orbits in finite incidence structures. Geom. Dedicata (in print).

[15] H. WIELANDT, Abschätzungen über den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad. Schr. Math. Sem. Inst. angew. Math. Universität Berlin, **2**, 151–174 (1934).

[16] H. WIELANDT, Gedanken für eine allgemeine Theorie der Permutationsgruppen. Rend. Sem. Mat. Torino **21**, 31–39 (1962).

[17] H. WIELANDT, Finite permutation groups. New York 1964.

[18] H. WIELANDT, Endliche K-Homogene Permutationsgruppen. Math. Z. **101**, 142 (1967).
[19] H. WIELANDT, Permutation groups through invariant relations and invariant functions. Lecture Notes, Ohio State Univ. 1969.
[20] H. WIELANDT, Allgemeine Methoden in der Theorie der Permutationsgruppen. In: Permutations, Acte du Collogue 1972, Paris.

Eingegangen am 25. 2. 1981

Anschrift des Autors:

Johannes Siemons
Department of Mathematics
University College Cork
Ireland
and
Rittnertstr. 53
D-7500 Karlsruhe 41