LE MATEMATICHE
Vol. XLVII (1992) – Fasc. II, pp. 281-294

GROUP ASSOCIATIONSCHEMES AND SCHUR RINGS

UDO OTT

1. Introduction.

One of the major problems of finite geometry and algebraic combinatorics is to provide insight into the action of a group acting as an automorphism group on a finite combinatorial structure. In practice the choice of the appropiate tool for investigating this general problem depends on the knowledge of the action of the group: one distinguishes groups with large stabilizers, and groups with trivial stabilizers. In the first case, the adequate techniques are taken from group theory and have very often been successsfully applied. But if there is no natural way of introducing proper subgroups of the given group authomorphisms difficulties arise in finding an appropiate method in group theory. This is especially true in the case of regular groups of automorphisms. However, in this case a powerful method is given in the frame of *association schemes.*

2. Definition of Group Association Schemes.

A number of questions about the combinatorial structure of a group G and its modules are related to the study of various partitions of the group. A *partition* on G is a partition

$$\mathscr{P} = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_r\}$$

of G such that

(1) $$\Lambda_1 = \{1\}$$

$$\Lambda_2, \ldots, \Lambda_\tau \neq \emptyset, \tag{2}$$

and such that for each i there is a j with

$$\Lambda_i^{-1} = \{x^{-1} \mid x \in \Lambda_i\} = \Lambda_j. \tag{3}$$

A *group association scheme* G is a finite group with a partition $\mathscr{P}$ on G such that for any element $z \in \Lambda_k$ the number $a_{i,j}^k(z)$ of pairs $(x, y) \in \Lambda_i \times \Lambda_j$ satisfying the equation $xy = z$ is independent of the choice of the element z in Λ_k. These integers are denoted by $a_{i,j}^k$. Clearly, we have $a_{i,j}^k \geq 0$. The number of components of the partition is called the rank of the group association scheme.

There are two important types of group association schemes: primitive and imprimitive . A group association scheme G is called *primitive* if $\{1\}$ and G are the only subgroups of G represented by the union of certain components of the partition. In the contrary case, we say that the group association scheme is *imprimitive.*

A powerful method to develop combinatorial properties of group association schemes is the theory of algebras. The idea is to attach to each component of the partition a certain element in the group algebra $\mathbf{F}G$ of G over the field $\mathbf{F}$. By definition the group algebra $\mathbf{F}G$ consists of all formal linear combinations

$$\alpha = \sum_{g \in G} a_g g$$

with $a_g \in \mathbf{F}$ for $g \in G$. For a component Λ_i of the group association scheme we set

$$\lambda_i = \sum_{g \in \Lambda_i} g.$$

One verifies easily that

$$\lambda_i \lambda_j = \sum_k a_{i,j}^k \lambda_k.$$

In other words, the elements $\lambda_1, \ldots, \lambda_\tau \in \mathbf{F}G$ form a base of an τ-dimensional subalgebra of $\mathbf{F}G$, the so-called *Schur ring* of the group association scheme over $\mathbf{F}$, denoted by $\mathbf{S}$.

To analyze the combinatorial structure of a group association scheme we need also the definition of an automorphism $f : G \longrightarrow G$ of the group association scheme: this is a bijection f of G leaving all the relations given by the components of the partition invariant. This mean that

$$xy^{-1} \in \Lambda_i \Longleftrightarrow f(x)\, f(y)^{-1} \in \Lambda_i$$

for $i = 1, \ldots, \tau$. Clearly, a group element $g \in G$ induces the automorphism

$$\rho_g : \begin{cases} G \longrightarrow G \\ x \longmapsto \rho_g(x) = xg \end{cases}.$$

Remarks. There is a general theory of association schemes and we refer the reader to Bannai [1] for a complete introduction to this field of interest. The historical source of the notion of Schur rings is the theory of permutation groups and a discussion of Schur's work may be found in Wielandt [12]. We present the most important example in 3.1.

3. Examples.

3.1 Permutation Groups with Regular Subgroups.

Let G be a finite group acting transitively on the set Ω. Assume that G admits a subgroup H that is sharply transitive on Ω, i.e. only the identity element of H fixes points in Ω.
Choose an element ω of Ω and let

$$\Omega_1 = \{\omega\}, \Omega_2, \ldots, \Omega_\tau$$

be the orbits of the stabilizer

$$G_\omega = \{g \in G \mid \omega^g = \omega\}.$$

Our aim will be to show that

$$\mathscr{P} : \Lambda_i = \{h \in H \mid \omega^h \in \Omega_i\},$$

$i = 1, \ldots, \tau$, induces a group association scheme on H. The proof rests upon the fact that there is a natural bijection from the set $\mathscr{E}$ of orbits of G on $\Omega \times \Omega$ onto the set $\mathscr{F} = \{\Omega_i \mid i = 1, \ldots, \tau\}$ of orbits of G_ω on Ω, which is given by the map

$$\Gamma : \begin{cases} \mathscr{E} \longrightarrow \mathscr{F} \\ \Theta \longmapsto \Theta_\omega = \{\alpha \mid (\omega, \alpha) \in \Theta\} \end{cases}.$$

We set $\Theta_k = \Gamma^{-1}(\Omega_k)$.

Since H is sharply transitive on Ω, it is obvious that $\mathscr{P}$ satisfies the Equations (1), (2). In order to show that also the Equation (3) is true we need the argument that if Θ is an orbit of G on $\Omega \times \Omega$ then also $\Theta^* = \{(\chi, \psi) \mid (\psi, \chi) \in \Theta\}$

is an orbit. Now, $(\omega, \omega^h) \in \Theta$, $h \in H$ is equivalent to $(\omega, \omega^{h^{-1}}) \in \Theta^*, h \in H$, whence the Equation (3) is fulfilled.

Suppose next that $(\omega, \omega^z) \in \Theta_k$, $z \in H$ and $(\omega, \omega^x) \in \Theta_i$, $(\omega, \omega^y) \in \Theta_j$ with $x, y \in H$ and $xy = z$. Setting $x = zy^{-1}$ we observe that $(\omega^y, \omega^z) \in \Theta_i$. Thus the number of pairs $(x, y) \in \Lambda_i \times \Lambda_j$ satisfying the relation $xy = z$ equals the number of points χ in Ω such that $(\omega, \chi) \in \Theta_j$ and $(\chi, \omega^z) \in \Theta_i$. Since the stabilizer G_ω acts transitively on the set of elements ψ such that $(\omega, \psi) \in \Theta_k$ this number is clearly independent of $z \in \Lambda_k$. This proves that $\mathscr{P}$ defines a group association scheme for H.

We will apply this concept in Section 6 for transitive groups of prime degree to present a particular short proof of the following theorem of Burnside.

Theorem 1 (Burnside). *Let G be a transitive group of prime degree p. Then G is doubly transitive or isomorphic to a group of affine transformations*

$$x \longmapsto ax + b$$

over the prime field $GF(p)$.

The proof of Burnside's theorem requires also that we can regard each element $g \in G_\omega$ as an automorphism of the group association scheme in the following way. Set

$$\omega^{hg} = \omega^{g^*(h)} \tag{4}$$

where $g^*(h) \in H$ is uniquely determined. Then g^* is a permutation of H. Furthermore, the relation $xy^{-1} \in \Lambda_i$ is equivalent to $\omega^{xy^{-1}} \in \Omega_i$, hence equivalent to $(\omega, \omega^{xy^{-1}}) \in \Theta_i$, which means that $(\omega^y, \omega^x) \in \Theta_i$.
By the same argument $(\omega^{yg}, \omega^{xg}) = (\omega^{g^*(y)}, \omega^{g^*(x)}) \in \Theta_i$ is equivalent to $g^*(x)g^*(y)^{-1} \in \Lambda_i$ for $g \in G_\omega$. Thus g^* is an automorphism, as required.

In other words, after identifying the set Ω with the group H via the correspondence $h \longleftrightarrow \omega^h$ each element $g \in G_\omega$ acts as an automorphism on the group association scheme H.

3.2 Sharply Flag-Transitive Groups on Generalized Polygons.

In this section we present a picture of non-abelian group association schemes related to generalized polygons. A treatment of the general background and the basic concepts of generalized polygons might be found in Kantor [4].

Let $\mathbf{G} = (\mathscr{P}, \mathscr{L}; I)$ denote a generalized n-gon with parameters $s, t \geq 1$. Furthermore, suppose that $\mathbf{G}$ admits a group G of automorphism acting sharply transitively on the set $\mathscr{F}$ of chambers of the geometry. Then we are able to

construct a group association scheme over G with the help of the *generating* components $\Lambda_0 = \{1\}$ and

$$\Lambda_1 = G_a \setminus \{1\}$$

$$\Lambda_2 = G_A \setminus \{1\},$$

where $\{A, a\}$ denotes a fixed chamber in $\mathscr{F}$. It is not difficult to see that

$$\underbrace{\Lambda_1\Lambda_2\Lambda_1\Lambda_2\ldots}_{n \text{ factors}} = \underbrace{\Lambda_2\Lambda_1\Lambda_2\Lambda_1\ldots}_{n \text{ factors}}. \tag{5}$$

The partition $\mathscr{P}$ consists then of Λ_0 and all the $2n-1$ products of the form

$$\underbrace{\ldots\Lambda_i\Lambda_j\ldots}_{\text{at most } n \text{ factors}}$$

where i, j is a permutation of 1,2.

We wish to point out that the Schur ring of this group association scheme is isomorphic to the Hecke algebra of the geometry (refer to Ott [9]).

Conjecture 1. *Suppose that* $n = 3$. *Then we have* $s = t \in \{1, 2, 8\}$.

3.3 Difference Sets with -1 as Multiplier and Partial Addition Sets. Here we assume that G is a group association scheme of rank $\tau = 3$. From the relation

$$\lambda_2^2 = a\lambda_1 + b\lambda_2 + c\lambda_3 \tag{6}$$

we deduce that the group association scheme is uniquely determined by a nontrivial subset $\Delta = \Lambda_2$ of G satisfying:

1. $1 \notin \Delta$;
2. $\Delta^{-1} = \Delta$ or $\Delta^{-1} = G \setminus (\Delta \cup \{1\})$;
3. there are integers b and c such that each element $1 \neq g \in G$ admits exactly b or c representations of the form $g = xy$ with $x, y \in \Delta$ depending on respectively whether g is in Δ or not.

Clearly, property 2 implies that $a = |\Delta|$ or $a = 0$. In the first case the group association scheme is known as a group with a *partial addition set* (refer to Ma [8]). Moreover, such a partial addition set is known to be a *difference set with* -1 as multiplier in the special case that b equals c. Thus partial addition sets and difference sets with -1 as multiplier are special cases of group association schemes of rank $\tau = 3$. We should mention that in the literature the subset $G \setminus \Delta$ is also called a difference set, but without loss of generality one can assume that $1 \notin \Delta$.

Conjecture 2. *Suppose that G is an abelian difference set with -1 as multiplier and let p be a prime divisor of the order $n = |\Lambda_2| - c$ of this association scheme. Then we have $p \in \{2, 3, 5\}$.*

4. Schur's Multiplier Theorem.

In this section we present Schur's fundamental theorem on *multipliers*, which provide a useful method for certain questions concerning the existence of group association schemes.
Let $G, \mathscr{P}$ be a group association scheme of rank τ and $\mathbf{S}$ its Schur ring over the field $\mathbf{F}$. For what follows it will be convenient to introduce the following terminology: let m be an integer and Λ be a subset of G. Then $\Lambda^{[m]}$ denotes the subset

$$\Lambda^{[m]} = \{x^m \mid x \in \Lambda\}.$$

Similarly for

$$\lambda = \sum_{g \in G} a_g g$$

we set

$$\lambda^{[m]} = \sum_{g \in G} a_g g^m.$$

The integer m is called a *multiplier* of the group association scheme if whenever Λ_i is a component of $\mathscr{P}$ then so is $\Lambda_i^{[m]}$. In the special case

$$\Lambda_i^{[m]} = \Lambda_i$$

for $i = 1, \ldots, \tau$ the multiplier is called *rational.*

Remark. In the literature another slightly different definition of multipliers appears, in which a multiplier is rational, as for istance in the case of difference sets with -1 as multiplier.

With these preliminaries we can now state Schur's result on multipliers:

Theorem 2 (Schur). *Let $G, \mathscr{P} = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_\tau\}$ be an abelian group association scheme. Then every integer relatively prime to the group order is a multiplier.*

Proof. The entire calculation depends on the well-known property that over the ring $\mathscr{Z}$ of integers every coset of the form $m + \mathscr{Z}|G|$ contains a prime, provided the integers m and $|G|$ are relatively prime. Thus we may assume that $m = p$

is a prime not dividing the group order. Then we choose the field $\mathbf{F} = GF(p)$ and by using our assumption we observe that

$$\lambda^p = \lambda^{[p]} \in \mathbf{S}$$

for every element $\lambda \in \mathbf{S}$. Let g be an element in Λ_i. Clearly, there is an integer j such that $g^p \in \Lambda_j$. We need to show that $\Lambda_i^{[p]} = \Lambda_j$. For the proof of this equation we may assume that $|\Lambda_i| \leq |\Lambda_j|$; eventually we have to look at a prime q with $pq \equiv 1\ (mod|G|)$. The last statement is equivalent to the equation

$$\lambda_i^p = \lambda_i^{[p]} = \lambda_j.$$

Of course, there are elements $a_s \in \mathbf{F}, s = 1, \ldots, \tau$, such that

$$\lambda_i^p = \sum_{s=1}^{\tau} a_s \lambda_s. \tag{7}$$

We conclude that $a_s = 0$ or $a_s = 1$ for all $1 \leq s \leq \tau$, hence $a_j = 1$. Since $|\Lambda_i| \leq |\Lambda_j|$, this forces that λ_i^p to be equal to λ_j, the theorem is proved. □

It is obvious that on the basis of this result one can derive many standard applications. For instance, as an almost immediate corollary we have

Corollary 1 (Ghinelli-Smit [2]; Hughes, van Lint, Wilson [11]). *Let G be an abelian difference set with -1 as multiplier. Then every integer relatively prime to the group order is a rational multiplier.*

Another application:

Corollary 2. *Let G be an abelian partial addition set. Then every square of an integer relatively prime to the group order is a rational multiplier.*

In the non-abelian case there is no general result known about the existence of multipliers. We infer from Section 3.2 that there are examples having only the multiplier $m = -1$ (up to congruence). The smallest example here is the Frobenius group of order 21. On the other hand, the symmetric group is a group association scheme with respect to the partition into conjugacy classes for which each integer relatively prime to the group order is a rational multiplier.
Using elementary properties of modular representation theory Ghinelli-Smit and Löwe are able to generalize corollary (2):

Theorem 3 (Ghinelli-Smit, Löwe [6]). *Let G be a partial addition set, whose components are invariant under inner automorphisms of the group. Then every square of an integer relatively prime to the group order is a rational multiplier.*

Finally we would like to mention an application of Wielandt:

Theorem 4 (Wielandt [12]). *Assume that G is a primitive abelian group association scheme of composite order. Then G does not contain cyclic Sylow subgroups.*

Again, as a corollary we obtain almost immediately

Corollary 3 (Hughes, van Lint, Wilson [11]). *An abelian difference set with -1 as multiplier does not contain cyclic Sylow subgroup.*

In the terminology of partial addition sets:

Corollary 4. *Assume that G is a primitive abelian partial addition set of composite order. Then G does not contain cyclic Sylow subgroups.*

5. Divisibility Conditions.

As we mentioned earlier, the source of the notion of a group association scheme is the theory of transitive permutation groups with sharply transitive subgroups. Sometimes it happens that under this assumption the size of each component divides the group order. Of course, in general this is not true. Therefore the question arises under which circumstances a prime dividing the length of a component divides also the group order. A first approach to this question is given by the radical of the symmetric bilinear form on the Schur ring defined to be the restriction of the standard bilinear form

$$(\alpha, \beta) = \text{trace}\,(\alpha\beta)$$

on the group algebra, were the trace (γ) of γ is the trace of the induced right multiplication on the group algebra. In particular, we have

$$(g, h) = \begin{cases} |G| & gh = 1 \\ 0 & gh \neq 1 \end{cases}.$$

One easily checks that

$$(\lambda_i, \lambda_j^{[-1]}) = \begin{cases} |G||\Lambda_i| & i = j \\ 0 & i \neq j \end{cases}. \tag{8}$$

The *radical, rad* $(\mathscr{S})$, of $\mathscr{S}$ ist the set of all elements γ in $\mathscr{S}$ which are orthogonal to $\mathscr{S}$, hence we have

$$rad\,(\mathscr{S}) = \{\gamma \in \mathscr{S} \mid (\gamma, \mathscr{S}) = 0\}.$$

The important fact about the radical is that since $(\alpha\beta, \gamma) = (\beta, \gamma\alpha)$ and $(\alpha\beta, \gamma) = (\alpha, \beta\gamma)$ it is an ideal in $\mathbf{S}$.

Lemma 1. *Assume that $G, \mathscr{P}$ is a group association scheme and that the field* **F** *has characteristic p not dividing the group order. Then a base of $rad(\mathscr{S})$ consists of all elements λ_i for which p divides $|\Lambda_i|$.*

Proof. Clearly, by Equation (8) the congruence $|\Lambda_i| \equiv 0 \,(mod\, p)$ implies that $\lambda_i \in rad(\mathscr{S})$. Suppose now that

$$\alpha = \sum_{i=1}^{\tau} a_i \lambda_i \in rad(\mathscr{S}).$$

It follows that

$$0 = (\alpha, \lambda_i^{[-1]}) = a_i |G|\, |\Lambda_i|.$$

However, we have $|G| \not\equiv 0 \,(mod\, p)$. We conclude at once that $a_i = 0$ or $|\Lambda_i| \equiv 0 \,(mod\, p)$, which proves the lemma. □

Using the fact that the radical is an ideal in the Schur ring we obtain

Corollary 5. *Assume that $G, \mathscr{P}$ is a group association scheme and that the field* **F** *has characterstic p not dividing the group order. Then the linear span of all the elements λ_i such that p divides $|\Lambda_i|$ is an ideal in the Schur ring.*

In the contrary case where p divides the group order there is also the following basic lemma and a short proof might be found in Wielandt [12]:

Lemma 2. *Assume that $G, \mathscr{P}$ is an abelian primitive group association scheme and that the field* **F** *has characteristic p dividing the group order. Then we have*

$$\lambda_i^p = \lambda_i^{[p]} = |\Lambda_i|\, 1.$$

Since a subalgebra of a commutative semisimple algebra is itself semisimple we obtain, by using the theorem of Maschke, the following theorem.

Theorem 5. *Assume that $G, \mathscr{P}$ is an abelian group association scheme and that the field* **F** *has characteristic p not dividing the group order. Then the Schur ring is semisimple.*

We would like to mention that in the non-abelian case this theorem is not true. For istance, the Schur ring of the group association scheme for the Frobenius group of order 21 described in Section 3.2 is not semisimple over a field of characteristic 2.

We present a standard applications for froup association schemes of rank $\tau = 3$:
Here the defining Equation (6) can be written in the form

$$\lambda_2^2 = (a-c)1 + (b-c)\lambda_2 + c\sum_{g\in G} g = n1 + d\lambda_2 + c\gamma, \tag{9}$$

where

$$\sum_{g\in G} g = \gamma.$$

If the odd prime p divides $|G|$ and if $b \equiv c\,(mod\,p)$ then the Equation (9) regarded as an equation over $GF(p)$ yelds:

$$\lambda_2^p = n^{\frac{p-1}{2}}\lambda_2 + x\gamma \tag{10}$$

for a suitable integer x With the help of Lemma 2 we derive the following theorem.

Theorem 6. *Assume that $\{1\} \cup \Lambda_2$ is not a subgroup of the abelian group association scheme. Suppose that there is a prime divisor p of $|G|$ such that $b \equiv c\,(mod\,p)$. Then p divides n.*

By using Schur's multiplier theorem and Theorem 5 the same equation results in

Theorem 7. *Assume that the group association scheme is abelian. Suppose that there is a prime divisor p of n such that $b \equiv c\,(mod\,p)$. Then p divides $|G|$.*

Again, one can formulate these theorems for partial addition sets or difference sets with -1 as multiplier. In the last case, for instance , one gets the result

Theorem 8 (Ghinelli-Smit [2]). *Assume that G is an abelian difference set with -1 as multiplier. Then an odd prime divides $|G|$ if and only if it divides n.*

For partial addition sets in the non-abelian case only the following divisibility condition is known

Theorem 9 (Löwe [5]). *Suppose that a strongly regular graph with parameters (v,k,λ,μ) admits a regular group G of automorphisms. Assume that the discriminant $\delta = (\lambda-\mu)^2 + 4(k-\mu)$ is a square. Let $\mathscr{C} \neq \{1\}$ be a conjugacy class in G. Then*

$$2\sqrt{\delta}\ divides\ \left(\frac{2v\,|\mathscr{C}\cap\Delta|}{|\mathscr{C}|} + v\left((\lambda-\mu) - \sqrt{\delta}\right)\right).$$

This result is also the base for studying regular groups on generalized quadrangles (compare Ghinelli-Smit [3]).

6. A Fundamental Problem in Finite Geometry and the Theorem of Burnside.

We conclude our outline with a very short proof of Burnside's theorem. Apart from the fact that a transitive group of prime degree leads to an abelian group association scheme the main idea of the argument has its roots in a

6.1 The Problem

Let A denote a finite affine plane of order n and let Λ be a set of n points. A basic problem is to identify this subset as a line provided certain properties are fulfilled. In fact, a natural condition is the assumption that the set of lines carrying at least two points of Λ does not have many *slopes* (a *slope* is a point at infinity). We speak of these points as the slopes of Λ. In particular, we have the following conjecture

Conjecture 3. *Let A be an affine plane of prime order p and let Λ be a set of p points with at most $(p-1)/2$ slopes. Then Λ is a line.*

The answer to this problem turns out to be of fundamental importance in a variety of problems. In the case of a desarguessian plane $\mathscr{A} = AG(2,p)$ this conjecture is true and easily proved with the help of

Theorem 10 (Rédei [10]). *Let $f : GF(p) \longrightarrow GF(p)$ be a function such that its difference quotient takes at most $(p-1)/2$ values. Then $f(x) = ax + b$ for suitable elements $a, b \in GF(p)$.*

For completeness we sketch here the short proof of Lovász and Schrijver [7]: denote by U the set of values of the difference quotient of f. In the spirit of Fourier transforms we look at the polynomial

$$f_j^*(x) = \sum_{y \in GF(p)} (xy - f(y))^j \tag{11}$$

for $j \geq 1$.
Since the equation $xy_1 - f(y_1) = xy_2 - f(y_2)$ is equivalent to

$$x = \frac{f(y_1) - f(y_2)}{y_1 - y_2}$$

we conclude that $f_j^*(x) = 0$ for all $x \notin U$ provided that $j \leq p-2$. Certainly f_j^* has degree smaller then j for $1 \leq j \leq p-2$ and consequentely $f_j^* = 0$ for $1 \leq j \leq (p-1)/2$.
It is well known that each function f on $GF(p)$ can be represented as a polynomial

$$f(x) = c_0 + c_1 x + \cdots + c_d x^d$$

of degree $d \leq p-1$. Assuming that f is not linear we have that $d \geq 2$. Moreover, we may assume that $f(0) = 0$, which forces $c_0 = 0$. Let $p-1 = ad+b$ with $a > 0$ and $0 \leq b < d$. It follows from $d \geq 2$ that $a+b \leq (p-1)/2$, hence $f_{a+b}^* = 0$. Now a straightforward computation of the coefficient x^b in f_{a+b}^* yields a contradiction:

$$\begin{aligned} 0 &= \binom{a+b}{b} \sum_{y \in GF(p)} y^b f(y)^a \\ &= \binom{a+b}{b} \sum_{y \in GF(p)} (c_d^a y^{ad+b} + \cdots + c_1^a y^{a+b}) \\ &= \binom{a+b}{b} \sum_{y \in GF(p)} c_d^a y^{p-1} \\ &= -\binom{a+b}{b} c_d^a \end{aligned}$$

6.2 The Proof.
Now let G be transitive subgroup of the symmetric group S_p on p letters. Since p divides $|G|$ and p^2 does not divide S_p we deduce that G contains a p-Sylow subgroup P of order p. Clearly P must act sharply transitive on the point set. Hence Section 3.1 applies. We identify the set of points with P and then P itself with the additive group of $GF(p)$. Hence P consists of all the permutations of the form $x \mapsto x+b$.

Let $\Lambda_1 = \{0\}, \Lambda_2, \ldots, \Lambda_\tau$ be the group association scheme on P induced by the action of the stabilizer G_0. Assuming that G does not act doubly transitively we obtain $\tau \geq 3$. By Schur's multiplier theorem we conclude that the permutations

$$x \mapsto ax$$

for $a \neq 0$ permute the components of the partition. In other words, the multiplicative group $GF(p)^*$ of $GF(p)$ acts on the set of components. Moreover,

since $GF(p)^*$ is transitive on $GF(p) \setminus \{0\}$ we see immediately that this group is transitive on the components Λ_i for $i \geq 2$. But then it follows that there is a subgroup U (the stabilizer of this action) of $GF(p)^*$ such that the components Λ_i for $i \geq 2$ are the cosets of U in $GF(p)^*$. Moreover, by our assumption we have $|U| \leq (p-1)/2$.

From Section 3.1 we know that each permutation $g \in G_0$ as a permutation of $GF(p)$ is an automorphism of the group association scheme. Hence the relation $x - y \in aU$ is equivalent to $g(x) - g(y) \in aU$. Thus we obtain

$$\frac{g(x) - g(y)}{x - y} \in U$$

for all $x \neq y$. Since $g(0) = 0$ the theorem of Rédei implies then that $g(x) = ax$ for a suitable $a \in GF(p)$, which proves the theorem of Burnside.

REFERENCES

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I,* Benjamin/Cummings Pub. Co., Menlo Park, Calif., 1984.

[2] D. Ghinelli-Smit, *A new result on difference sets with -1 as multiplier,* Geom. Ded. 23 (1987), pp. 309-317.

[3] D. Ghinelli-Smit, *Regular groups on generalized quadrangles and nonabelian difference sets with multiplier -1,* Geom. Ded. 41 (1992), pp. 165-174.

[4] W.M. Kantor, *Generalizes polygons, scabs and gabs. In L.A. Rosati, editor,* Buildings and the Geometry of Diagrams, volume LNM 1181, Berlin, Heidelberg, New York, Tokio, 1986. Springer.

[5] St. Loewe, *Groups, strongly regular graphs, and quotient sets,* Ars Comb., 24B (1987), pp. 31-34.

[6] St. Loewe and D. Ghinelli-Smit, *On multipliers of partial addition sets,* Geom. Ded., 40 (1991), pp. 53-58.

[7] L. Lovász and A. Schrijver, *Remarks on a theorem of Rédei,* Studia Scientiarum Math. Hung., 16 (1981), pp. 449-454.

[8] S.L. Ma, *On association schemes, Schur rings, strongly regular graphs and partial addition sets,* Ars. Comb., 27 (1989), pp. 211-220.

[9] U. Ott, *Some remarks on representation theory in finite geometry. In D. Jungnickel and A. Aigner, editors,* Geometries and Groups, volume LNM 893, pages 68-110, Berlin, Heidelberg, New York, Tokio, 1981. Springer.

[10] L. Rédei, *Lückenhafte Polynome über endlichen Körpen,* Birkhäuser, Basel.

[11] D.R. Hughes, J.H. van Lint and R.M. Wilson, *Announcement at the 7th British Combinatorial Conference,* Cambridge, 1979.

[12] H. Wielandt, *Finite Permutation Groups,* Academic Press, New York, 1964.

Institute of Geometry
Technical University of Braunschweig
Germany