RANK 3 PERMUTATION GROUPS WITH A REGULAR NORMAL SUBGROUP.

by

RAYMOND HILL

A Thesis submitted for the Degree of Doctor of Philosophy at the University of Warwick.

University of Nottingham,
September, 1971.

ABSTRACT

A (p,n) group G is a permutation group (on a set Ω) which possesses a regular normal elementary abelian subgroup of order p^n. The set Ω may be identified with a vector space V on which G_o, the stabilizer of a point in G, acts as a subgroup of the general linear group GL(n,p). By a line of a subset Δ of V, we mean the intersection of Δ with a one-dimensional subspace of V. The main result (Theorem 1.3.2) concerns (*) - groups, the term we give to rank 3 (p,n) groups in which the stabilizer of a point is doubly-transitive on the lines of a suborbit. The essence of the problem is that of finding those subgroups of PGL (n,p) which have two orbits on the projective space PG (n - 1,p) and act doubly - transitively on one of them.

The notion of rank of a permutation group is discussed in 1.1, while in 1.2 we outline D.G.Higman's combinatorial treatment of rank 3 groups.

Associated with each permutation group having a regular subgroup is a certain S - ring, an algebraic structure which is basic to our theory. In 2.1 we define parameters of a rank 3 S - ring which coincide with those of any associated rank 3 group. Hence (*) - group with given parameters may be classified by finding all S - rings with the same parameters and then finding the associated (*) - groups. To assist in this task the concepts of the residual S-ring and the automorphism group of an S-ring are introduced. Also of great value is Tamaschke's notion of the dual S-ring, which is adapted to our use in 2.2.

In 3.1 we see how the imposition of conditions of transitivity on a suborbit of a rank 3 (p,n) group leads to information about the parameters. In 3.3 the various relations connecting the parameters of a (*)-group are combined to yield specific sets of parameters, all of which are found in §4 to admit rank 3 S-rings. From results concerning the uniqueness of these S-rings, certain finite simple groups are characterised as their automorphism groups, and the proof of the main theorem is completed. A number of results are obtained as by-products in §4, notably the answer to a question raised by Wielandt and a new representation of the simple group PSL(3,4) as a subgroup of $PO^{-}(6,3)$, leading to an interesting presentation of a recently-discovered balanced block design.

§5 is devoted to rank 3 (p,n) groups in which the transitivity condition on G_o is replaced by the condition that the associated block design is balanced.

TABLE OF CONTENTS

PREFACE

The author wishes to express his thanks to Professor J.A.Green for the invaluable advice and encouragement he has given during the preparation of this work. He would also like to thank Mrs. Angela Fullerton for her excellent typing of the manuscript. The financial support of the Science Research Council is gratefully acknowledged.

§ 1. INTRODUCTION. In this section we introduce most of our notation and some of the results to be used later on.

§ 1.1 Permutation Groups.

Let Ω be a finite set of arbitrary elements which we call points and denote by lower case Greek letters. A permutation on Ω is a 1-1 mapping of Ω into itself. We denote the image of the points $\alpha \in \Omega$ under the permutation g by $(\alpha)g$, or by αg where confusion will not arise. We define the product gh of two permutations g and h on Ω by $(\alpha)gh = (\alpha g)h$, hence reading products from left to right. With respect to this operation the set of all permutations of Ω is a group, the symmetric group on Ω, denoted by $S(\Omega)$. By a permutation group G on Ω we mean a subgroup of $S(\Omega)$. For such a group, we define an equivalence relation $\sim$ on Ω as follows: for any two points α and β of Ω, $\alpha \sim \beta$ if $\beta = \alpha g$ for some $g \in G$. The equivalence classes of $\sim$ on Ω are called the orbits of G on Ω. If G has just one orbit G is said to be transitive on Ω.

For any element $\alpha \in \Omega$ we let G_α denote the subgroup $\{g \in G \quad \alpha g = \alpha\}$ of G, called the stabilizer of α.

The following theorem is basic to the theory of permutation groups.

<u>Theorem 1.1.1.</u> Let G be a permutation group on Ω. If $\alpha \in \Omega$ and Δ is the orbit containing α, then the order $|\Delta|$ of Δ is equal to the index $|G:G_\alpha|$ of G_α in G.

<u>Proof</u>

We define a map θ from the set of right cosets of G_α in G to the set Δ by

$$(G_\alpha g)\theta = \alpha g$$

It is easy to show that θ is well-defined and is a bijection.

G is said to be <u>k-transitive</u> on Ω if for every two ordered k-tuples $(\alpha_1,\ldots,\alpha_k)$ and $(\beta_1,\ldots,\beta_k)$ of points of Ω (with $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$ for $i \neq j$) there exists $g \in G$ such that $\alpha_i g = \beta_i$, $i = 1,\ldots,k$. Thus 1-transitivity is the same as transitivity. The next theorem follows easily from the definition.

<u>Theorem 1.1.2.</u> Let G be transitive on Ω and $\alpha \in \Omega$. Then G is $(k+1)$-transitive on Ω if and only if G_α is k-transitive on $\Omega - \alpha$.

The notion of rank is designed to deal with those transitive groups which are not 2-transitive; we say G has <u>rank r</u> on Ω if G is transitive on Ω and G_α has r orbits (including $\{\alpha\}$). Thus the rank 2 groups are precisely the 2-transitive groups. The orbits of G_α and their orders are called <u>suborbits</u> of G and <u>subdegrees</u> of G respectively. We deduce from the following lemma that the rank and subdegrees of a transitive permutation group are well-defined.

Lemma 1.1.3. Let G be a permutation group on Ω. Let $\alpha \in \Omega$ and $g \in G$. Then

(i) $G_{\alpha g} = g^{-1} G_\alpha g$

(ii) If Δ is an orbit of G_α then

$\Delta g = \{ \delta g : \delta \in \Delta \}$ is an orbit of $G_{\alpha g}$.

Proof

(i) If $h \in g^{-1} G_\alpha g$, then $h = g^{-1} k g$ for some $k \in G_\alpha$.

Now $(\alpha g) g^{-1} k\, g = \alpha k g = \alpha g$

i.e. $h \in G_{\alpha g}$

Thus $g^{-1} G_\alpha g \leq G_{\alpha g}$ and similarly

$g \; G_{\alpha g} g^{-1} \leq G_\alpha$.

Hence $g^{-1} G_\alpha g = G_{\alpha g}$.

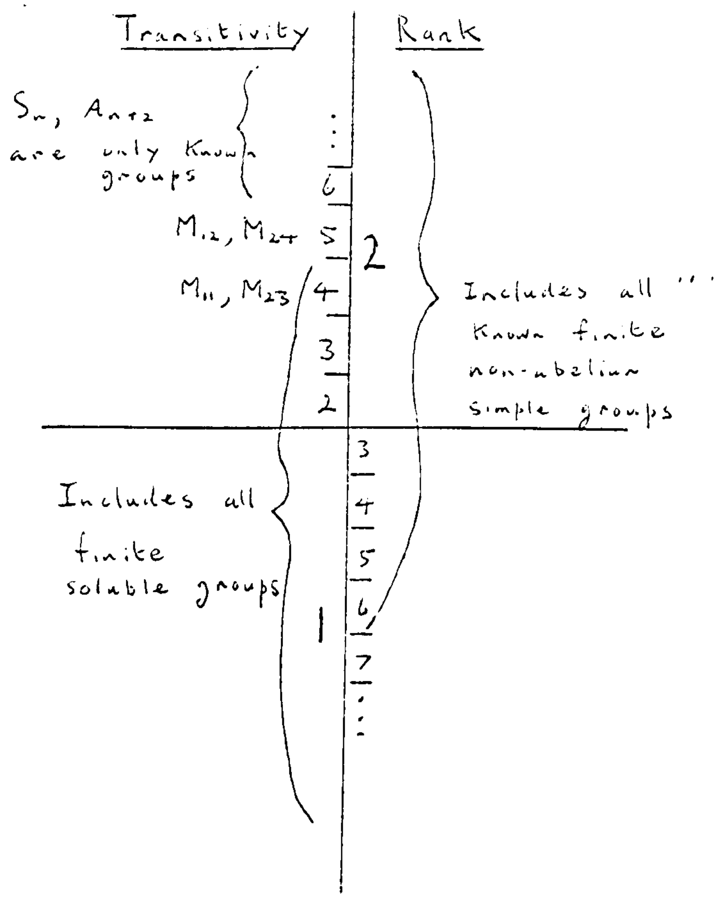
(ii) is a straightforward consequence of (i).

If G is transitive on Ω, 1.1.3(ii) shows that the rank and subdegrees of G are independent of the choice of α.

Diagram 1 shows how transitivity and rank each cover the range of non-trivial transitive permutation groups.

Since the representation of a group G on the right cosets of a subgroup H ($(Hx)g = Hxg$ for $x, g \in G$) is transitive, all abstract groups appear at least once in this table. We see that soluble groups generally have a lower degree of transitivity than non-abelian simple groups. The doubly transitive soluble groups were found by Huppert in 1957 [14], the only 3-transitive among these being S_3 and S_4.

Diagram 1.



S_n is n-transitive on n points, while A_n is (n-2)-transitive on n points; for if $(\alpha_1, \dots, \alpha_{n-2})$ and $(\beta_1, \dots, \beta_{n-2})$ are ordered (n-2)-tuples, one of the two permutations

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \cdots & \beta_{n-2} & \beta_{n-1} & \beta_n \end{pmatrix}, \begin{pmatrix} \alpha_1 & \cdots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \cdots & \beta_{n-2} & \beta_n & \beta_{n-1} \end{pmatrix}$$

is even. The only other known 4-transitive groups are the Mathieu groups M_{11}, M_{23} (4-transitive), M_{12} and M_{24} (5-transitive).

Groups of low rank are of interest since all known finite simple groups occur as such. Indeed the classical finite simple groups all have representations of rank ≤ 5, while 13 of the 18 sporadic finite simple groups (known in 1970) have rank 3 representations.

§ 1.2 Rank 3 Groups - Higman Designs.

Permutation groups of rank 3 received little attention until 1964 when D.G. Higman [10] tackled them from a combinatorial point of view. Higman's treatment was not applicable to rank 2 groups, but he later [12] generalized some of the work to groups of arbitrary rank ≥ 3. We will now describe how Higman associated with each rank 3 group a certain block design, having the given group as a collineation group. For the rest of § 1.2, we suppose that $|\Omega| = n$ and that G is a rank 3 permutation group on Ω with subdegrees k and ℓ. For $\alpha \in \Omega$, let $\Delta(\alpha)$ and $\Gamma(\alpha)$ denote the orbits of length k and ℓ respectively of G_α. By 1.1.3(ii) we may suppose that

(1.2.1): $\Delta(\alpha g) = \Delta(\alpha)g$, for all $\alpha \in \Omega$, $g \in G$

Now let $\lambda = |\Delta(\alpha) \cap \Delta(\beta)|$ for $\beta \in \Delta(\alpha)$

and $\mu = |\Delta(\alpha) \cap \Delta(\gamma)|$ for $\gamma \in \Gamma(\alpha)$.

Lemma 1.2.2. λ and μ are independent of the choice of $\beta \in \Delta(\alpha)$ and $\gamma \in \Gamma(\alpha)$.

Proof. Let $\beta_1, \beta_2 \in \Delta(\alpha)$.

Then $\beta_1 g = \beta_2$ for some $g \in G_\alpha$.

$$(\Delta(\alpha) \cap \Delta(\beta_1))g = \Delta(\alpha)g \cap \Delta(\beta_1)g$$
$$= \Delta(\alpha g) \cap \Delta(\beta_1 g) \quad \text{by (1.2.1)}$$
$$= \Delta(\alpha) \cap \Delta(\beta_2) .$$

Hence $\left|\Delta(\alpha) \cap \Delta(\beta_1)\right| = \left|\Delta(\alpha) \cap \Delta(\beta_2)\right|$. This shows that λ and similarly μ are well-defined.

Thus with a rank 3 group G we associate a block design $\mathcal{B}$, with parameters (k, ℓ, λ, μ), whose points are the elements of Ω and whose blocks are the sets $\Delta(\alpha)$, one for each $\alpha \in \Omega$. We call $\mathcal{B}$ a first Higman design. By a second Higman design we mean the design $\mathcal{B}'$ whose points are again the points of Ω and whose blocks are the sets $\alpha \cup \Delta(\alpha)$, one for each $\alpha \in \Omega$. (1.2.1) shows that G is a collineation group of these designs. Both kinds of Higman design are symmetric partially-balanced incomplete block designs (symmetric since the number of points is the same as the number of blocks; partially-balanced since the number of points in the intersection of any 2 blocks is one of two fixed integers). In a symmetric balanced incomplete block design, the number of points in the intersection of any 2 blocks is a constant, so we see that:

(1.2.3): A first Higman design is balanced $\Longleftrightarrow \mu = \lambda$.

(1.2.4): A second Higman design is balanced $\Longleftrightarrow \mu = \lambda + 2$.

Higman showed that certain relations hold among the parameters (k, ℓ, λ, μ):

Lemma 1.2.5. (Lemma 5 of [10])

$$\mu\ell = k(k - 1 - \lambda) .$$

Proof. Fix an element α of Ω. We count the number N of ordered pairs (β, γ) with $\beta \neq \alpha$ and $\gamma \in \Delta(\alpha) \wedge \Delta(\beta)$. There are k elements β in $\Delta(\alpha)$ for each of which $|\Delta(\alpha) \wedge \Delta(\beta)| = \lambda$, and there are ℓ elements β in $\Gamma(\alpha)$ for each of which $|\Delta(\alpha) \wedge \Delta(\beta)| = \mu$.

Hence $$N = \lambda k + \mu\ell .$$

On the other hand we have k choices for γ and for each of these we have $k-1$ choices for β.

Hence $\lambda k + \mu\ell = k(k-1)$ and the result follows.

As in § 29 of [22] we denote by G^* the (complex) permutation representation of G, and let $f_1, \ldots, f_s$ denote the degrees of the irreducible constituents of G^*. It follows from § 29 of [22] that if G has rank 3, then $s = 3$ and we may take $f_1 = 1$. By considering the eigenvalues of the incidence matrix of the block design $\mathcal{B}$ associated with G, Higman showed that

(1.2.6): $$\left\{ \begin{matrix} f_2 \\ f_3 \end{matrix} \right\} = \frac{2k + (\lambda - \mu)(k + \ell) \mp \sqrt{d}(k + \ell)}{\mp 2\sqrt{d}} \quad \text{if } |G| \text{ is even}$$

while $f_2 = f_3 = k$ if $|G|$ is odd.

$(d = (\lambda - \mu)^2 + 4(k - \mu))$.

From this Higman immediately derived further numerical conditions on the parameters:

Lemma 1.2.7. (Lemma 7 of [10])

If $|G|$ is even then either

I $k = \ell$, $\mu = \lambda+1 = k/2$ and $f_2 = f_3 = k$, or

II $d = (\lambda-\mu)^2 + 4(k-\mu)$ is a square, and

(i) if n is even, $\sqrt{d}$ divides $2k+(\lambda-\mu)(k+\ell)$ and $2\sqrt{d}$ does not, while

(ii) if n is odd, $2\sqrt{d}$ divides $2k+(\lambda-\mu)(k+\ell)$.

One way of finding rank 3 groups is to find block designs with parameters satisfying the conditions of Lemmas 1.2.5 and 1.2.7 and then see if the pointsof the design admit a rank 3 collineation group. Since we have 4 parameters for a Higman design and only 2 conditions on them, it makes sense to try to classify rank 3 groups satisfying conditions which give further information about the parameters (preferably, two more relations). As a simple example, we will now find all primitive rank 3 groups in which G_α is 2-transitive on both $\Delta(\alpha)$ and $\Gamma(\alpha)$. We first give necessary and sufficient conditions on the parameters for a rank 3 group to be primitive.

Lemma 1.2.8. Suppose G is a rank 3 group with $k \leq \ell$.

Then G is primitive if and only if $\mu \neq 0$

if and only if $\lambda \neq k-1$.

Proof. See p.148 of [10].

The following lemma of Higman (see (2.6) of [11]) shows how the double transitivity of G_α gives information about the parameters.

Lemma 1.2.9. Suppose G is a primitive rank 3 group on Ω with Δ and Γ chosen so that $k \leq \ell$.

(i) If G_α is 2-transitive on $\Delta(\alpha)$, then $\lambda = 0$

(ii) If G_α is 2-transitive on $\Gamma(\alpha)$, then $\mu = k-\ell+1$.

Proof. (i) Let $\beta \in \Delta(\alpha)$. Since $G_{\alpha,\beta}$ is transitive on $\Delta(\alpha) - \beta$

$$\Delta(\alpha) - \beta \leq \Delta(\beta) \quad \text{or} \quad \Delta(\alpha) - \beta \leq \Gamma(\beta) .$$

and hence $|\Delta(\alpha) \wedge \Delta(\beta)| = 0$ or k-1 respectively.

But $\lambda \neq k-1$ by 1.2.8, and so we have $\lambda = 0$.

(ii) is proved similarly.

Theorem 1.2.10. Suppose G is a primitive rank 3 group in which G_α is 2-transitive on both Δ and Γ. Then $|\Omega| = 5$ and $G \cong D_{10}$, the dihedral group of order 10.

Proof. Choose Δ and Γ such that $k \leq \ell$. By 1.2.9, $\lambda = 0$ and $\mu = k-\ell+1$. Since $\mu > 0$ by 1.2.8, we must have $\mu = 1$ and $k = \ell$, whence $k = k(k-1)$ by 1.2.5. This gives $k = 2$ and the parameters are thus (2,2,0,1). By 1.1.1, G is a subgroup of S_5 of order 5.2 = 10. Since S_5 contains no elements of order 10, the only possibility is that G is isomorphic to D_{10}. It is easily checked that the representation of D_{10} on the cosets of a subgroup of order 2 has the required form.

In Table 2 we list some investigations carried out in recent years which have yielded more interesting rank 3 groups.

TABLE 2.

Conditions	Possible degree and parameters	Groups	Proved by
G_α is 2-transitive on Δ and $\mu = 1$.	(1) 5,(2,2,0,1) (2) 10,(3,6,0,1) (3) 50,(7,42,0,1) (4) 3250,(57,3192,0,1)	D 10 A_5 or S_5 $U_3(5)$ or $[U_3(5)]C_2$ No known groups	D.G.Higman obtained the parameters and groups in [10],1964. He showed that the list of groups for (1), (2), (3) is complete in [11] 1966.
G_α is 2-transitive on Δ and rank 3 on Γ. ($\mu > 1$)	(1) 16,(5,10,0,2) (2) 100,(22,77,0,6) (List may not be complete)	$[V_{16}]A_5$ or $[V_{16}]S_5$ HS or $[HS]C_2$	Margaret S. Smith (1969-70)
G_α is isomorphic to PSL(2,q), where $k = q+1$ and $\ell = \frac{q^2+q}{2}$	(1) 16,(5,10,0,2) (2) 56, (10,45,0,2)	$[V_{16}]$ A_5 PSL (3,4)	Stephen Montague [16],1970.

Some of the notation in Table 2 requires explanation. The notation for the classical groups is standard, U meaning unitary and PSL projective special linear. By $[H]K$ we mean a semidirect product of H by K. V_{16} denotes an elementary abelian subgroup of order 16. HS denotes the Higman-Sims simple group, which was discovered in 1967 [13] as a rank 3 extension of the Mathieu group M_{22}.

We leave Table 2 with the observation that a classification of rank 3 groups in which G_α has rank 3 on both Δ and Γ would be of interest, for the new simple group of McLaughlin has such a representation.

The primitive soluble rank 3 groups have recently been classified by Foulser [6] and Dornhoff [5]. They are of the form $[V]G_\alpha$ where V is an elementary abelian regular normal subgroup of G and one of the following holds.

(i) $V = q^n$ and G is isomorphic to a subgroup of the group of semilinear transformations on the field $GF(q^n)$. In this case G_α has a simple structure, being a subgroup of a metacyclic group.

(ii) G_α is an imprimitive linear group with a subgroup of index 2 given by Huppert's classification of double-transitive soluble groups.

(iii) G has one of the degrees 7^2, 13^2, 17^2, 19^2, 23^2, 29^2, 31^2, 47^2, 3^4, 7^4, 2^6 or 3^6.

We also shall be concerned with rank 3 groups which contain a regular normal elementary abelian subgroup, and our main task will be an attempt to find such groups which have a high degree of transitivity on a suborbit. The problem is more fully stated in § 1.3.

§ 1.3 (p,n) groups.

Before defining a (p,n) group, we briefly describe groups which have a regular normal subgroup. By a regular group G we mean a transitive group on a set Ω in which $G_\alpha = \{1\}$ for every $\alpha \in \Omega$.

Suppose G is a permutation group on Ω and that G has a normal regular subgroup H. We distinguish a point α of Ω and associate with every point w of Ω that uniquely determined permutation $h \in H$ for which $(\alpha)h = w$. By virtue of this bijection of Ω onto H we can regard G as a permutation group on H; to the permutation $g \in G$ corresponds the permutation $\binom{h}{(h)g}$, where $(h)g$ is uniquely specified by the formula

$$(\alpha)(h)g = (\alpha)hg .$$

Thus, for each $h \in H$,

$$\begin{aligned} (h)k &= hk, \quad \text{for } k \in H \\ (h)g &= g^{-1}h\,g, \quad \text{for } g \in G_\alpha \end{aligned} \tag{1.3.0}$$

Since the distinguished point α of Ω corresponds to 1 in H we now write G_1 instead of G_α. The structure of G is given by:

Theorem 1.3.1. If G contains a regular normal subgroup H, then G is isomorphic to the semi-direct product $[H]G_1$.

Proof. Since H is regular, $H \wedge G_1 = \{1\}$. By 1.1.1, $|G| = |H|\,|G_1|$ and so $G = HG_1$. Since H is normal in G, the result follows.

Thus the action of G on H is determined by that of H and G_1, and by (1.3.0) we know that H acts in its regular representation (i.e. on itself by right multiplication) while G_1 acts automorphically on H.

If a permutation group G contains a regular normal elementary abelian subgroup H of order p^n (for some prime p) then, for brevity, we call it a <u>(p,n) group</u>.

A well-known theorem due to Galois (See e.g. [22], p.28) tells us that any primitive soluble group is a (p,n) group for some prime p and integer n. As we mentioned in § 1.2, all primitive soluble rank 3 groups have already been classified. We therefore venture the question: are there any interesting non-soluble rank 3 (p,n) groups?. Of course a (p,n) group is soluble if and only if G_1 is soluble. As we observed in § 1.2, high transitivity generally corresponds to non-solubility, and so we will impose conditions of high transitivity of G_1 on a suborbit Δ. (Because we have identified Ω with H, we now have $H = \{1\} \cup \Delta \cup \Gamma$ in a rank 3 (p,n) group). Since G_1 acts automorphically on H, the stabilizer $G_{1,h}$ of a further point h also stabilizes h^t for all integers t. We therefore define an equivalence relation on a suborbit Δ by $h_1 \sim h_2$ if $h_1 = h_2^t$, for some t with $0 < t < p$, and we call the equivalence classes the <u>lines</u> of Δ. We denote the line containing h by $\underline{h}$, and the set of lines of Δ by $\underline{\Delta}$. For (p,n) groups it is more natural to consider the transitivity of G_1 on $\underline{\Delta}$ rather than on Δ. The main theorem we shall prove is:

Theorem 1.3.2. Suppose G is a primitive rank 3 (p,n) group in which G_1 is 2-transitive on the lines of a suborbit. Let D denote the central subgroup $\{g \in G_1 : (h)g = h^t$ for all $h \in H$, some integer $t\}$ of G_1. Then the degree of G, the parameters of G, and G_1/D are respectively

(i)	3,	(1,1,0,0),	the cyclic group C_3 *
(ii)	5,	(2,2,0,1),	D_{10} *
(iii)	p^2 (any prime p),	$(2(p-1),(p-1)^2,p-2,2)$,	$D_{2(p-1)}$
(iv)	5^2,	(12,12,5,6),	S_3
(v)	7^2,	(24,24,11,12),	A_4
(vi)	p^4 (any prime p),	$((p^2+1)(p-1),\ p(p^2-1)(p-1),p-2,\ p(p-1)$,	$P\Gamma L(2,p^2)$
(vii)	3^5,	(22,220,1,2),	M_{11}
(viii)	3^6,	(112,616,1,20),	-
or (ix)	p^n,	where $p \neq 2$ and $n \geq 13$.	

Notes. (1) This result, which will follow from various results in the sequel, will shortly be restated, in perhaps a more natural way, in terms of linear groups.

(2) Assuming the existence of an automorphism group satisfying the hypotheses of the theorem, we will show that there exists a unique block design having each of the above sets of parameters. The groups listed arise from the full automorphism groups of these designs and, in some cases, suitable subgroups also have the required properties. In case (viii) the full automorphism group does not have the required transitivity properties but is nevertheless worthy of study since it gives rise to an interesting representation of the simple group PSL(3,4).

* For (i),(ii) only, the groups listed are in fact G, not G_1/D.

(3) It seems unlikely that possibility (ix) occurs, but our methods appear to be insufficient to confirm this for $p \neq 2$. However they give an algorithm for finding all possible sets of parameters of such (p,n) groups for a given integer n, and the lower bound on n can be increased as far as one is prepared to go (the manipulations become increasingly arduous as n increases).

The next lemma shows how rank 3 (p,n) groups fall into two types.

Lemma 1.3.3. Suppose G is a rank 3 (p,n) group with suborbits $\{1\}$, Δ and Γ, and parameters (k,ℓ,λ,μ). Then either

(i) $|\underline{h}| = p-1$, for all $h \in \Delta$, in which case $k = (p-1)|\underline{\Delta}|$
($|\underline{h}|$ denotes the number of points in the line $\underline{h}$, $|\underline{\Delta}|$ the number of lines in $\underline{\Delta}$)

or (ii) $k = \ell$ and $|\underline{h}| = \frac{p-1}{2}$ for all $h \in \Delta$, in which case $k = (p-1)/2.\,|\underline{\Delta}|$

Proof. Suppose (i) is not true. Then there exists $h \in \Delta$ and an integer t such that $h^t \in \Gamma$. By the transitivity of G_1 on Γ any element of Γ has the form $(h^t)g$ for some $g \in G_1$. But $(h^t)g = ((h)g)^t$ and $(h)g \in \Delta$. Thus $\Gamma = \{h^t : h \in \Delta\}$. The map from Δ to Γ given by $h \rightarrow h^t$ is a bijection, and hence (ii) holds.

Definition 1.3.4. For reasons which will become apparent in § 2.1 we say that a rank 3 (p,n) group is rational or irrational according as (i) or (ii) is satisfied in 1.3.3.

It is perhaps easier to visualize (p,n) groups if we translate to the language of lineargroups over vector spaces. The regular normal elementary abelian subgroup H, written additively, can be regarded as the vector space $V(n,p)$ of dimension n over the field $GF(p)$ of p elements. G_1 can then be regarded as a subgroup of the general linear group $GL(n,p)$. We now write G_o instead of G_1, its orbits on $V(n,p)$ being $\{0\}$, Δ and Γ . The group D of Theorem 1.3.2 consists of scalar multiples of the identity matrix, and if G is rational, then $G_o = G_o/D$ is a subgroup of $PGL(n,p)$ acting on the projective space $PG(n-1,p)$ with two orbits $\underline{\Delta}$ and $\underline{\Gamma}$ (It is easy to see that the lines defined on page 13 can now be regarded as the points of $PG(n-1,p)$). Since the irrational groups arising in Theorem 1.3.2 are not of great interest (they will be classified in § 3.1) the essence of the theorem can be restated as:

<u>Theorem 1.3.5</u>. A subgroup of $PGL(n,p)$ acting on the projective space $PG(n-1,p)$ with two orbits, double transitive on one of them, is one of the groups given by (iii)...(ix) of Theorem 1.3.2.

In the next section we consider (p,n) groups from yet another point of view - that of S-rings.

§ 2. S-RINGS.

§ 2.1 Definition and basic results.

The theory of S-rings (after I.Schur, who introduced them in [17], 1933) is useful in the investigation of those permutation groups which contain a regular subgroup of the same degree.

As in [22] we begin our discussion of S-rings by defining an S-module over a group H. Let CH denote the group ring of H over the field C of complex numbers i.e. CH is the set of formal linear combinations $\eta = \sum_{h \in H} c_h h$ $(C_h \in C)$ with the obvious multiplication defined by that in H. Those ring elements $\eta = \Sigma\, C_h h$ for which the coefficients C_h have only the values 0 and 1 are called simple quantities. Suppose $\tau_1, \ldots, \tau_r$ are simple quantities of CH such that $\sum_{i=1}^{r} \tau_i = \sum_{h \in H} h$. Then the subset of CH spanned by the τ_i (i.e. the set of linear combinations $\sum_{i=1}^{r} c_i \tau_i$, $c_i \in C$) is called an S-module over H with basis $\{\tau_1, \ldots, \tau_r\}$.

We shall be particularly interested in the following kind of S-module. Let G be a permutation group containing a regular subgroup H (not necessarily normal) and, as in § 1.3, identify the points of Ω with those of H. Let $\Delta_1, \ldots, \Delta_r$ be the orbits of G_1 on H and, for $i = 1, \ldots, r$, let $\hat{\Delta}_i$ denote the simple quantity $\sum_{h \in \Delta_i} h$ of the group ring CH. Then $\{\hat{\Delta}_1, \ldots, \hat{\Delta}_r\}$ is a basis for an S-module over H, called by Wielandt the transitivity module of G_1 over H and denoted by $C(H, G_1)$.

Definition 2.1.1. An S-ring over H is an S-module over H which is at the same time a subring of the group ring CH, and which in addition contains the identity element 1 as well as every quantity $\Sigma\, c_h h^{-1}$ whenever it contains $\Sigma\, c_h h$.

Given any subset Δ of H we let $\hat{\Delta}$ denote the simple quantity $\sum_{h \varepsilon \Delta} h$ of CH .

Definition 2.1.2. An S-ring $\mathcal{S}$ over H is called primitive if K = 1 and K = H are the only subgroups of H for which $\hat{K} \varepsilon \mathcal{S}$ holds.

S-rings are fundamental to the study of permutation groups which have a regular subgroup in view of the following important theorem of Schur.

Theorem 2.1.3. Suppose G is a permutation group containing H as a regular subgroup. Then the transitivity module $C(H,G_1)$ is an S-ring over H.

Proof. See pp. 61-63 of [22].

With the help of this theorem we will be able to get information about possible groups G solely through consideration of the subgroup H.

Let $\mathcal{S}$ be an S-ring with basis $\tau_1, \ldots, \tau_r$. We call r the rank of $\mathcal{S}$ and the integers $n_1, \ldots, n_r$, where n_i is the number of group elements whose formal sum is τ_i, the subdegrees of $\mathcal{S}$. It is clear that when $\mathcal{S}$ is a transitivity module $C(H,G_1)$, the rank and subdegrees of $\mathcal{S}$ and of the permutation group G coincide. Furthermore we have

Theorem 2.1.4. (24.12 of [22]). A permutation group G with regular subgroup H is primitive if and only if $C(H,G_1)$ is a primitive S-ring.

When $\tau = \Sigma c_h h$ is a simple quantity in CH, we define τ^m to be the simple quantity $\Sigma c_h h^m$.

Definition 2.1.5. If $\mathcal{S}$ is an S-ring in which $\tau_i^m = \tau_i$ for every simple basis quantity τ_i and for all integers m such that $(m, |H|) = 1$, then $\mathcal{S}$ is called (by Tamaschke [19]) a rational S-ring.

If $\mathcal{S}$ is a transitivity module associated with a rank 3 (p,n) group G then it is easy to see that $\mathcal{S}$ is rational if and only if G is rational in the sense of definition 1.3.4. We now give a necessary and sufficient condition for a rank 3 S-module over an elementary abelian group to be a rational S-ring.

Theorem 2.1.6. Let $\mathcal{S}$ be an S-module over an elementary abelian p-group H with simple basis quantities 1, $\hat{\Delta}$ and $\hat{\Gamma}$. ($H = \{1\} \cup \Delta \cup \Gamma$). Then $\mathcal{S}$ is a rational S-ring if and only if the following three conditions hold.

(i) $|\Delta \wedge \Delta x|$ = some fixed integer λ for all $x \in \Delta$.

(Δx denotes the subset $\{ax: a \in \Delta\}$ of H)

(ii) $|\Delta \wedge \Delta y|$ = some fixed integer μ for all $y \in \Gamma$.

(iii) If $x \in \Delta$, then $x^t \in \Delta$ for $t = 1,\dots,p-1$.

Proof. Suppose $\mathcal{S}$ is a rational S-ring. Let $k = |\Delta|$, $\ell = |\Gamma|$. Since $\mathcal{S}$ is a ring, there are integers λ and μ such that $\hat{\Delta}\hat{\Delta} = \lambda\hat{\Delta} + \mu\hat{\Gamma} + k.1$. For any $x \in \Delta$,

$$\lambda = |\{(a,b) \in \Delta \times \Delta : ab = x\}|$$

$= |\{a \in \Delta : a^{-1}x \in \Delta\}| = |\Delta \wedge \Delta x|$, since $a \in \Delta$ implies $a^{-1} \in \Delta$ if $\mathcal{S}$ is rational. Thus (i), and similarly (ii), hold. (iii) follows immediately from the fact that $\mathcal{S}$ is rational.

Conversely suppose (i), (ii) and (iii) hold. To prove $\mathcal{S}$ is an S-ring it is sufficient to show that $\hat{\Delta}\hat{\Delta}$, $\hat{\Gamma}\hat{\Gamma}$ and $\hat{\Delta}\hat{\Gamma}$ belong to $\mathcal{S}$. Using the reverse argument to that in the first part of the proof, it is easily shown that $\hat{\Delta}\hat{\Delta} = \lambda\hat{\Delta} + \mu\hat{\Gamma} + k.1$ and similarly that $\hat{\Gamma}\hat{\Gamma} = (\ell-k+\lambda+1)\hat{\Delta} + (\ell-k+\mu-1)\hat{\Gamma} + \ell.1$ and $\hat{\Delta}\hat{\Gamma} = (\ell-k+\lambda+1)\hat{\Delta} + \mu\hat{\Gamma}$. This completes the proof.

The next lemma shows that λ and μ correspond with the intersection numbers of a rank 3 (p,n) group G when $\mathcal{S} = C(H,G_1)$.

<u>Lemma 2.1.7</u>. If G is a rank 3 (p,n) group with parameters (k,ℓ,λ,μ) then $\lambda = |\Delta \wedge \Delta x|$ where $x \in \Delta$ and $\mu = |\Delta \wedge \Delta y|$ where $y \in \Gamma$.

<u>Proof</u>. By definition $\lambda = |\Delta(\alpha) \wedge \Delta(\beta)|$, for $\beta \in \Delta(\alpha)$. Hence $\lambda = |\Delta(\alpha) \wedge \Delta(\alpha)g|$, where $g \in G_1$ with $\alpha g = \beta$. If G is a (p,n) group over H we take $\alpha = 1$ and regard $\Delta = \Delta(1)$ as a subset of H. H acts regularly on itself. Thus, if $x \in \Delta$, $x : 1 \longrightarrow x$ and $\lambda = |\Delta \wedge \Delta x|$. The required value of μ is obtained in the same way.

For a rational rank 3 S-ring $\mathcal{S}$ over H we have now defined a set of parameters (k,ℓ,λ,μ) which are the same as those of a rank 3 group G when $\mathcal{S} = C(H,G_1)$. It follows from the equation $\hat{\Delta}\hat{\Delta} = \lambda\hat{\Delta} + \mu\hat{\Gamma} + k.1$ (in proof of 2.1.6) that $k^2 = \lambda k + \mu\ell + k$, which shows that Higman's relation of Lemma 1.2.5 holds for a rational rank 3 S-ring $\mathcal{S}$ without any assumption that $\mathcal{S}$ is a transitivity module.

§ 2.2 Dual S-rings.

O. Tamaschke [19 and 20] has carried out an extensive ring-theoretical investigation of the class of S-rings over H which lie in the centre of the group ring CH - he calls them central S-rings. We will be interested only in abelian groups H, over which S-rings are automatically central. Of great value to us will be Tamaschke's notion of the dual S-ring and also his numerical relations connecting the subdegrees and character degrees of a permutation group which has a regular subgroup.

Rather than discuss the dual of an S-ring over H in full generality, we will make a definition more convenient for our particular use; that is, when H is an elementary abelian p-group. It is easy to check that Tamaschke's definition is the same as ours for such a group.

For the rest of this section H denotes an elementary abelian p-group of order p^n, and $\mathcal{S}$ an S-ring over H with simple basis quantities $\tau_1,\ldots,\tau_r$. We write $H = H_1 \times \ldots \times H_n$ where H_i is a cyclic group of order p generated by h_i. The set $H^{\#}$ of (complex) characters of H can be identified with a group, which is isomorphic to H, in the following way. We define characters $x_1,\ldots,x_n$ by $(h_j)x_i = w$ if $i = j$

$= 1$ if $i \neq j$, where

w is a primitive p th. root of unity. The set of characters of H can then be written $H^{\#} = \{x_1^{i_1}\ldots x_n^{i_n}: i_k = 0,1,\ldots,p-1\}$ where $(h_1^{j_1}\ldots h_n^{j_n})x_1^{i_1}\ldots x_n^{i_n} = w^{i_1j_1+\cdots i_nj_n}$. With multiplication defined by $(x_1^{i_1}\ldots x_n^{i_n})(x_1^{j_1}\ldots x_n^{j_n}) = x_1^{i_1+j_1}\ldots x_n^{i_n+j_n}$, it is easy to check that $H^{\#}$ is an elementary abelian group of order p^n generated by $x_1,\ldots,x_n$. A character x in $H^{\#}$ can be defined to act on the ring CH by $(\Sigma\, c_h h)x = \Sigma\, c_h(hx)$, and in particular x acts on the simple basis quantities $\tau_1,\ldots,\tau_r$ of $\mathcal{S}$. We define an equivalence relation on $H^{\#}$ by $x \sim \psi$ if and only if $(\tau_k)x = (\tau_k)\psi$ for $k = 1,\ldots,r$. Let $T_1,\ldots,T_{r^{\#}}$ be the equivalence classes of $\sim$, and let $\tau_k^{\#}$ be the simple quantity $\hat{T}_k = \sum_{x\in T_k} x$ of $CH^{\#}$. Then $\tau_1^{\#},\ldots,\tau_{r^{\#}}^{\#}$ generate an S-module $\mathcal{S}^{\#}$ over $H^{\#}$, which we call the dual S-module to $\mathcal{S}$. From Theorem 1.10 of [19] we obtain

<u>Theorem 2.2.1</u>. If $\mathcal{S}$ is an S-ring of rank r over an elementary abelian group H, then:

(i) the dual S-module $\mathcal{S}^{\#}$ is an S-ring over $H^{\#}$.

(ii) $\mathcal{S}^{\#\#}$ is isomorphic to $\mathcal{S}$.

(iii) $r = r^{\#}$ i.e. rank $\mathcal{S}$ = rank $\mathcal{S}^{\#}$.

(iv) the map $\mathcal{S} \longmapsto \mathcal{S}^{\#}$ is a bijection from the set of S-rings of rank r over H to itself (identifying $H^{\#}$ with H).

Definition 2.2.2. $\mathcal{S}^{\#}$ is called the dual S-ring to $\mathcal{S}$.

Tamaschke showed that interesting numerical relations hold between the subdegrees, $n_1,\ldots,n_r$, of a central S-ring and those, $n_1^{\#},\ldots,n_r^{\#}$, of its dual:

Theorem 2.2.3. (c.f. 2.18 of [19]) Let $\mathcal{S}$ be a central S-ring of rank r over a group H. Then

(a) the rational numbers $q = |H|^{r-2} \prod_{i=1}^{r} \frac{n_i}{n_i^{\#}}$ and

$$q^{\#} = |H|^{r-2} \prod_{i=1}^{r} \frac{n_i^{\#}}{n_i}$$ are both integers.

(b) if $\mathcal{S}$ is also rational in the sense of definition 2.1.5, q and $q^{\#}$ are both squares.

Corollary 2.2.4. (c.f. 2.20 of [19]) If $|H|$ is a power of a prime p and $\mathcal{S}$ is rational, then q and $q^{\#}$ are not only squares but also powers of p.

Proof. Observing that $qq^{\#} = |H|^{2(r-2)}$, the result follows immediately from 2.2.3.

Suppose now that G is a group with regular subgroup H and transitivity module $C(H,G_1)$. Let $D_1,\ldots,D_s$ be the different irreducible representations appearing in the permutation representation G^* of G. Let ζ_i be the character corresponding to D_i, f_i the degree of D_i, and e_i the multiplicity of D_i in G^* $(i = 1,\ldots,s)$. By Theorems 28.8, 29.3 and 29.4 of [22], if $C(H,G_1)$ is central, then every $e_i = 1$ and s is equal to the rank r of $C(H,G_1)$. Moreover Tamaschke has proved:

Theorem 2.2.5. (c.f. 7.6 of [20]) Suppose $C(H,G_1)$ is a central S-ring over H with basis $\tau_1,\ldots,\tau_r$. Then the basis $\tau_1^{\#},\ldots,\tau_r^{\#}$ of $\mathcal{S}^{\#}$ coincides with the set of characters $\zeta_1,\ldots,\zeta_r$ in their action on H.

Corollary 2.2.6. If $C(H,G_1)$ is central, the subdegrees of $C(H,G_1)^{\#}$ are $f_1,\ldots,f_r$.

We now see that Corollary 2.2.4 represents an improvement (when $\mathcal{S} = C(H,G_1)$) on the following more general theorem of Frame.

Theorem 2.2.7. (c.f. 30.1 of [22]) Let G be a transitive group of degree n with subdegrees n_i, and let f_i, e_i be the degrees and multiplicities respectively of the absolutely irreducible constituents of the permutation representation G^* of G .

(A) If all the $e_i = 1$, then the rational number

$$q' = n^{r-2} \prod_{i=1}^{r} \frac{n_i}{f_i}$$ is an integer.

(B) If the irreducible constituents of G^* all have rational characters, then q' is a square.

By 2.2.6, if $\mathcal{S}$ of Theorem 2.2.3 is a central transitivity module $C(H,G_1)$, then q of 2.2.3 is the same as q' of 2.2.7. Let us now see how Tamaschke's theory ties in which that of Higman's for the particular case of rational rank 3 (p,n) groups.

Lemma 2.2.8. Suppose G is a rank 3 group with regular subgroup H. Let q be that integer given by Theorem 2.2.3 with $\mathcal{S} = C(H,G_1)$. Let d be as in 1.2.7. Then if $C(H,G_1)$ is central, d = q .

Proof. Since $q = q'$ if $C(H,G_1)$ is central,

$$\frac{d}{q} = \frac{d}{q'} = [(\lambda-\mu)^2 + 4(k-\mu)]\, \frac{f_2 f_3}{|H|\, k\ell} .$$

Using the values of f_2 and f_3 given by 1.2.6,

$$\frac{d}{q} = \frac{(k+\ell)(k^2+\ell k-\mu\ell-k\lambda) - k^2}{|H|\, k\ell} \quad \text{if } |G| \text{ is even},$$

$$\frac{(\lambda-\mu)^2 + 4(k-\mu)}{|H|} \quad \text{if } |G| \text{ is odd}.$$

$$= \frac{(k+\ell)(k+\ell k) - k^2}{|H|\, k\ell} \quad \text{if } |G| \text{ even, using 1.2.5,}$$

$$\frac{2k+1}{|H|} \quad \text{if } |G| \text{ odd, for then } \lambda = \mu = \frac{k-1}{2} \text{ by}$$

Corollary 1, p.148 of [10].

$$= \frac{k + \ell + 1}{|H|} \quad \text{in either case}$$

$$= 1 .$$

Immediately from 2.2.4 and 2.2.8 we get

Corollary 2.2.9. If G is a rational rank 3 (p,n) group, then d is the square of a power of p.

§ 2.3 S-rings over $V(n,p)$.

Since we will find it more convenient to write an elementary abelian p-group H additively and regard it as the vector space $V = V(n,p)$, we now convert our notation. To avoid confusion of + signs when we look at the group ring CV, we use $\dot{+}$ or $\dot{\Sigma}$ for formal sums, reserving + for vector addition in the additive group V. By an S-ring over V we simply mean an S-ring over an elementary abelian p-group with the notation changed as just described. The group $H^{\#}$ of characters of H may now be regarded as the dual space $V^{\#}$ in its usual meaning; i.e. $V^{\#}$ is the space of linear maps from V to GF(p). If we let the standard basis $\varepsilon_1, \dots, \varepsilon_n$ in V correspond to the generators $h_1, \dots, h_n$ of H, we define a basis $x_1, \dots, x_n$ in $V^{\#}$ by $(\varepsilon_j)x_i = \delta_{ij}$ (instead of $(h_j)x_i = w^{\delta_{ij}}$, as before; δ_{ij} denotes the 'Kronecker delta'). A dual S-ring over $V^{\#}$ is now defined in exactly the same way as in § 2.2.

For the rest of this section G denotes a (p,n) group in which the regular normal elementary abelian subgroup is written additively as V. Thus G is the semidirect product $[V]G_o$ as described in § 1.3, G_o being the stabilizer of 0 and regarded as a subgroup of GL(n,p). The transitivity module is now written $C(V,G_o)$.

Let $\mathcal{S}$ be any S-ring over V with simple basis quantities $\tau_1, \dots, \tau_r$. An element g of GL(n,p) acts on CV in the obvious way: $(\dot{\sum\limits_{v \in V}} c_v v)g = \dot{\Sigma}\, c_v((v)g)$. If $(\tau_i)g = \tau_i$ for i = 1,...,r, we say that g is an <u>automorphism</u> of $\mathcal{S}$, and define <u>Aut $\mathcal{S}$</u> to be the full automorphism group of $\mathcal{S}$ in GL(n,p). If G is a (p,n) group, $G_o \leq \mathrm{Aut}(C(V,G_o))$. On the other hand, for any S-ring $\mathcal{S}$, we have $\mathcal{S} \leq C(V, \mathrm{Aut}\,\mathcal{S})$ with equality if and only if $\mathcal{S}$ is the transitivity module of some (p,n) group of the same rank. Thus the rank 3 (p,n) groups with given parameters (k,ℓ,λ,μ) are given by those S-rings $\mathcal{S}$, with the same parameters, for which $\mathcal{S} = C(V, \mathrm{Aut}\,\mathcal{S})$.

We now show that an S-ring over V and its dual have the same automorphism group. If $G_o \leq GL(n,p)$, let G_o' denote the group of matrices $\{A : A' \varepsilon G_o\}$ (A' denotes the transpose of A). Of course G_o' is isomorphic to G_o.

<u>Theorem 2.3.1</u>. (i) If $\mathcal{S}$ is an S-ring over V, then Aut $\mathcal{S}$ is isomorphic to Aut $\mathcal{S}^{\#}$. (ii) If G is a (p,n) group, $C(V,G_o)^{\#}$ is isomorphic to $C(V^{\#},G_o')$. In other words the dual to $C(V,G_o)$ is that S-ring generated by simple quantities $\hat{\Delta}_1^{\#},\ldots,\hat{\Delta}_r^{\#}$ where the $\Delta_i^{\#}$ are the orbits of G_o' on $V^{\#}$.

<u>Proof</u>. (i) Let $\alpha = \Sigma\, d_j\varepsilon_j \;\varepsilon\, V$, $x = \Sigma\, z_i x_i \;\varepsilon\, V^{\#}$, and $A \;\varepsilon\; \mathrm{Aut}\,\mathcal{S}$. Suppose (a_{ij}) is the matrix of A with respect to the basis $\varepsilon_1,\ldots,\varepsilon_n$. Then

$$(\alpha)(xA') = (\alpha A)x \qquad \ldots (1),$$

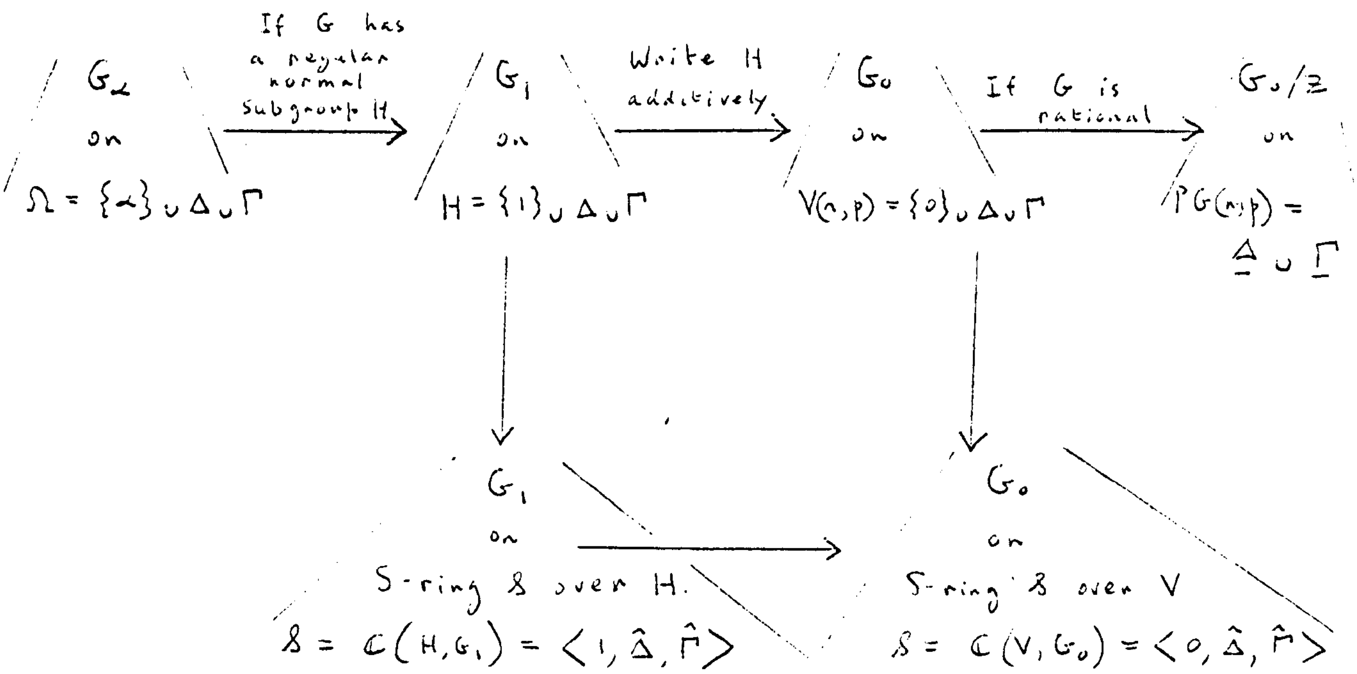
for $(\alpha)(xA') = (\Sigma\, d_k\varepsilon_k)(\Sigma\, a_{ij}z_jx_i) = \Sigma\, a_{ij}d_kz_j\,\delta_{ik}$
$= \Sigma\, a_{ij}d_iz_j = \Sigma\, a_{ij}d_iz_k\,\delta_{jk} = \Sigma\, a_{ij}d_iz_k\varepsilon_jx_k$
$= (\Sigma\, a_{ij}d_i\varepsilon_j)(\Sigma\, z_kx_k) = (\alpha A)x$.

Suppose $\hat{\Delta}_i = \dot{\Sigma}_{\alpha\varepsilon\Delta_i}\, \alpha$ is a simple basis quantity of $\mathcal{S}$. Since $A \;\varepsilon\; \mathrm{Aut}\,\mathcal{S}$, $(\hat{\Delta}_i)A = \hat{\Delta}_i$. By (1), $(\hat{\Delta}_i)\,xA' = (\hat{\Delta}_i)x$, for all i, x. Hence $xA' \sim x$ for all $x \;\varepsilon\; V^{\#}$, where $\sim$ is as in the definition of the dual S-ring (See p. 22), and it therefore follows that $A' \;\varepsilon\; \mathrm{Aut}\,\mathcal{S}^{\#}$.

Thus, if $A \in \mathrm{Aut}\,\mathcal{S}$, $A' \in \mathrm{Aut}\,\mathcal{S}^{\#}$; but by the same token, if $A' \in \mathrm{Aut}\,\mathcal{S}^{\#}$, $A = A'' \in \mathrm{Aut}\,\mathcal{S}^{\#\#} = \mathrm{Aut}\,\mathcal{S}$. Hence $A \in \mathrm{Aut}\,\mathcal{S}$ if and only if $A' \in \mathrm{Aut}\,\mathcal{S}^{\#}$, and $A \longmapsto (A^{-1})'$ gives the required isomorphism. (ii) is proved similarly.

By Corollary 2.2.6 the orbit lengths of G_0' on $V^{\#}$ are $f_1,\ldots,f_r$. We often have $\{f_1,\ldots,f_r\} = \{n_1,\ldots,n_r\}$ and indeed $C(V,G_0)$ isomorphic to its dual $C(V^{\#},G_0')$, though we will see in § 4 that this is not always the case.

We conclude this section with a diagram to illustrate the different ways in which we can now look at a rank 3 (p,n) group.



§ 3. PARAMETERS OF RANK 3 (p,n) GROUPS.

§ 3.1 Rank 3 (p,n) groups with high transitivity of G_o on a suborbit.

In this section we prove some results analogous to 1.2.9, showing how the imposition of conditions of transitivity on the suborbits of a rank 3 (p,n) group gives information about the intersection numbers λ and μ.

As in § 2.3, we regard the regular subgroup of a (p,n) group G additively as the vector space V. Thus $G = [V]G_o$, where G_o is regarded as a subgroup of GL(n,p). If $\alpha \in V$ and $g \in G_o$, we let αg denote the vector $(\alpha)g$ of V. To avoid confusion of notation, therefore, we write the elements of $[V]G_o$ as ordered pairs (α,g), where (α,g) : $\beta \longmapsto (\alpha+\beta)g$, for $\alpha,\beta \in V$, $g \in G_o$. Multiplication is given by $(\alpha,g)(\beta,h) = (\alpha+\beta g^{-1}, gh)$.

Lemma 3.1.1. If $x \in GL(n,p)$, then $[V]G_o$ and $[Vx]x^{-1}G_ox$ are isomorphic as permutation groups on V and Vx respectively ($Vx = \{\alpha x : \alpha \in V\}$).

Proof. It is a trivial verification that $(\alpha,g) \longmapsto (\alpha x, x^{-1}gx)$ gives the required isomorphism.

If G_o has orbits $\Delta_1,\ldots,\Delta_r$ on V, then $x^{-1}G_ox$ has orbits $\Delta_1 x,\ldots,\Delta_r x$ on Vx. Since we are interested in finding permutation groups only up to isomorphism we can use 3.1.1

to obtain the Δ_i in some canonical form.

We now consider our main problem, mentioned in § 1.3; that of finding the rank 3 (p,n) groups G in which G_o is doubly transitive on the lines of a suborbit. We will now dispense with the case where G is irrational (see definition 1.3.4).

<u>Theorem 3.1.2</u>. Suppose G is an irrational rank 3 (p,n) group with suborbits Δ and Γ, and suppose that G_o is doubly transitive on $\underline{\Delta}$. Then G is isomorphic to the cyclic group C_3 of order 3 or the dihedral group D_{10} of order 10.

<u>Proof</u>. Since G is irrational, $V = 0 \cup \Delta \cup \Gamma$, where

$$\Gamma = \{t\alpha : \alpha \in \Delta\} \text{ for some } t \in GF(p) \smallsetminus 0 .$$

<u>Case 1</u>. n = 2. Then $G_o \leq GL(2,p)$ and G_o is 2-transitive on the $(p^2-1)/(p-1)$ lines in $\underline{\Delta}$. By Theorems 1.1.1 and 1.1.2, $|G_o|$ is divisible by $(p+1)p$ and in particular p divides $|G_o|$. Since $GL(2,p)$ has order $(p^2-1)(p-1)p$, G_o must contain a Sylow p-subgroup P of GL(2,p). Because Sylow subgroups are conjugate, by Lemma 3.11 we may take P to be any Sylow p-subgroup of GL(2,p). Wetake $P = \{\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} : a \in GF(p)\}$. Then the vectors $(0,1), (1,1), \ldots, (p-1,1)$ all belong to the same orbit of P and therefore of G_o. Hence there exist field elements $b_1, \ldots, b_{\frac{p-1}{2}}$ and $c_1, \ldots, c_{\frac{p-1}{2}}$ such that

$$\Delta = \{b_1(1,0), \quad c_1(0,1), \quad \ldots, \; c_1(p-1,1),$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$
$$b_{\frac{p-1}{2}}(1,0), \; c_{\frac{p-1}{2}}(0,1), \; \ldots, \; c_{\frac{p-1}{2}}(p-1,1)\}$$

By Lemma 2.1.7, $\lambda = |\Delta \wedge \Delta + \alpha|$ for $\alpha \in \Delta$, and $\mu = |\Delta \wedge \Delta + \beta|$ for $\beta \in \Gamma$. We choose a and b in GF(p) such that $\alpha = a(1,0) \in \Delta$ and $\beta = b(1,0) \in \Gamma$. In this case both λ and μ are greater than or equal to $\frac{(p-1)p}{2}$, for the elements of Δ of the form $c_i(x,1)$ belong to both $\Delta + \alpha$ and $\Delta + \beta$. Since $k = \ell$, by 1.2.5, $\mu = k - 1 - \lambda$. Hence $(p^2-1)/2 = k = \mu + \lambda + 1 \geq p(p-1) + 1$, and this cannot occur for any prime p.

<u>Case 2</u>. $n > 2$. Assuming such a group G exists, then by restricting the action of G_o to any 2-dimensional subspace of V we get the conditions of Case 1 and hence a contradiction.

<u>Case 3</u>. $n = 1$. Since GL(1,p) is cyclic of order p-1, the only possibilities are $(p-1)/2 = 1$ or 2 and hence $p = 3$ or 5. Thus $G = [C_3]\,1$ or $[C_5]C_2$; i.e. G is isomorphic to C_3 or D_{10}.

The rational groups satisfying the hypotheses of Theorem 1.3.2 are of rather more interest, and we will be occupied with them for most of the sequel. For short we define a <u>(*)-group</u> to be a rational rank 3(p,n) group in which G_o is doubly transitive on the lines of a suborbit. Our problem now, therefore is to classify primitive (*)-groups, or, putting it another way, to prove Theorem 1.3.5. We make a start in:

Theorem 3.1.3. Let G be a (*)-group with parameters (k, ℓ, λ, μ). Then $\lambda = r(k/(p-1)-1) + p-2$, where either (i) $r+1 = p$ and G is imprimitive or (ii) $r+1$ divides $p-1$.

Proof. As usual, G_o is regarded as a subgroup of $GL(n,p)$ acting on $V = V(n,p)$. We may assume that the group S of all scalar matrices is contained in G_o, for G_oS has the same orbits as G_o and hence the parameters of $[V]G_o$ and of $[V]G_oS$ are the same. Let $\alpha_1 \in \Delta$. By 2.1.7, $\lambda = |\Delta \cap \Delta + \alpha_1|$. The vectors $2\alpha_1, 3\alpha_1, \ldots, (p-1)\alpha_1$ lie in $\Delta \cap \Delta + \alpha_1$; so $\lambda \geq p-2$. Suppose $\lambda \neq p-2$. Then there exists α_2 in Δ such that α_1 and α_2 are linearly independent and $\alpha_1 + \alpha_2 \in \Delta$. We let $\langle\alpha, \beta, \gamma, \ldots\rangle$ denote the subspace of V spanned by the vectors α, β, $\gamma, \ldots$. It is now more convenient to look at the lines of Δ.
Let $\underline{\Delta} = \{\underline{\alpha_1}, \underline{\alpha_2}, \ldots, \underline{\alpha}_m\}$ where $m = k/(p-1)$. Suppose $\underline{\langle\alpha_1, \alpha_2\rangle} \cap \underline{\Delta} = \{\underline{\alpha_1}, \underline{\alpha_2}, \underline{\alpha_1 + t_1\alpha_2}, \ldots, \underline{\alpha_1 + t_r\alpha_2}\}$, where $t_1 = 1$ and $t_i \in GF(p) \setminus 0$, $i = 2, \ldots, r$. The integer r is independent of the choice of α_1 and α_2 since G_o is 2-transitive on $\underline{\Delta}$. The double transitivity of G_o on $\underline{\Delta}$ also implies that for each $i \geq 2$, there exists $g_i \in G_o$ such that $(\underline{\alpha_1})g_i = \underline{\alpha_1}$ and $(\underline{\alpha_2})g_i = \underline{\alpha}_i$. Since $S \leq G_o$, we may assume $(\alpha_1)g_i = \alpha_1$ and $(\alpha_2)g_i = a_i\alpha_i$ for some $a_i \in GF(p) \setminus 0$. Hence $(\alpha_1 + t_j\alpha_2)g_i = \alpha_1 + t_ja_i\alpha_i$. We will show that

$$\Delta \wedge \Delta + \alpha_1 = \{\alpha_1 + t_j a_i \alpha_i \ : \ i = 2,\ldots,m \ ; \ j = 1,\ldots,r\} \cup$$
$$\{a\alpha_1 \ : \ a = 2,\ldots,p-1\} \qquad \ldots (1),$$

and hence that $\lambda = r(m-1) + p-2$ as required. Let the right hand side of (1) be the set X. It is easy to see that X is contained in $\Delta \wedge \Delta + \alpha_1$ and that the given elements of X are all distinct. Suppose $\alpha \in \Delta \wedge \Delta + \alpha_1$. If α is a scalar multiple of α_1 then $\alpha \in X$. Suppose $\alpha = \alpha_1 + b\alpha_i$ for some $i > 1$, $b \in GF(p) \setminus 0$. Then $(\alpha)g_i^{-1} = \alpha_1 + a_i^{-1}b\alpha_2 \in \Delta \wedge \langle\alpha_1, \alpha_2\rangle$. Hence $a_i^{-1}b = t_j$ for some $j \in \{1,\ldots,r\}$. Hence $b = a_i t_j$ and $\alpha = \alpha_1 + a_i t_j \alpha_i \in X$. Thus (1) is true and since $m = k/(p-1)$ we have proved the first part of the theorem.

It remains to prove the assertions about the integer r. Let L be the subgroup of G_o which fixes α_1 and also $\langle\alpha_1, \alpha_2\rangle$ as a set. Let L_1 be the subgroup which fixes every point of $\langle\alpha_1, \alpha_2\rangle$. Then L/L_1 is isomorphic to a subgroup of $\{\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} : a \in GF(p),\ b \in GF(p) \setminus 0\}$ and therefore has order dividing $p(p-1)$. Since G_o is 2-transitive on $\underline{\Delta}$, L/L_1 acts transitively on $\{\underline{\alpha_2}, \underline{\alpha_1 + t_1\alpha_2}, \ldots, \underline{\alpha_1 + t_r\alpha_2}\}$. Hence, by 1.1.1, $r+1$ divides $p(p-1)$ ... (2).

By definition, $\lambda \leq k$, which in this case implies that $r(m-1) + p-2 \leq m(p-1)$ and hence that $r \leq p-1$. Now $r = p-1$ if and only if $\lambda = k-1$, in which case G is imprimitive by 1.2.8. If $r < p-1$, then p cannot divide $r+1$ and we deduce from (2) that $r+1$ divides $p-1$. This completes the proof.

Before continuing our treatment of (*)-groups, we first consider some situations where even more stringent conditions of transitivity are imposed. Let G be a linear group acting transitively on some subset Δ of $V(n,p)$. Then we say that G is <u>near-2-transitive</u> on Δ if G_α is transitive on $\Delta \setminus \underline{\alpha}$ for any $\alpha \in \Delta$ ($\underline{\alpha}$ denotes the set $\{\alpha, 2\alpha, \ldots, (p-1)\alpha\}$); i.e. if the orbits of G_α on Δ are $\{\alpha\}$, $\{2\alpha\}, \ldots, \{(p-1)\alpha\}$, and $\Delta \setminus \underline{\alpha}$. Clearly if G is near-2-transitive on Δ, then G is 2-transitive on $\underline{\Delta}$. We define G to be <u>near-3-transitive</u> on Δ if G_α is near-2-transitive on $\Delta \setminus \underline{\alpha}$ for any $\alpha \in \Delta$.

<u>Theorem 3.1.4</u>. Suppose G is a primitive rank 3 (p,n) group in which G_o is near-2-transitive on a suborbit. Then G is isomorphic to C_3 or D_{10}, or $\lambda = p-2$.

<u>Proof</u>. If G is irrational we deduce from 3.1.2 that G is isomorphic to C_3 or D_{10}. So we suppose that G is a primitive rational (p,n) group. By 2.1.7, $\lambda = |\Delta \cap \Delta + \alpha|$ for $\alpha \in \Delta$. Clearly $\Delta \cap \Delta + \alpha$ contains $\{2\alpha, \ldots, (p-1)\alpha\}$. Suppose also that β belongs to $\Delta \cap \Delta + \alpha$, but that β does not belong to $\underline{\alpha}$. Let δ be any element of $\Delta \setminus \underline{\alpha}$. Since G_o is near-2-transitive, there exists $g \in G_o$ such that $\alpha g = \alpha$ and $\beta g = \delta$. Since $\beta - \alpha \in \Delta$, $(\beta - \alpha)g = \delta - \alpha \in \Delta$. Hence $\delta \in \Delta \cap \Delta + \alpha$ for all $\delta \in \Delta \setminus \alpha$. Therefore $\lambda = k-1$, which by 1.2.8 implies that G is imprimitive - a contradiction. Hence no such β exists and $\lambda = p-2$.

<u>Theorem 3.1.5.</u> Suppose G is a primitive rank 3 (p,n) group in which G_0 is near-3-transitive on Δ. Then $G = C_3$ or D_{10}, or $\lambda = p-2$ and $\mu = 2$.

<u>Proof.</u> By Theorem 3.1.4, it is necessary to prove only the assertion about μ when G is rational. By 2.1.7, $\mu = |\Delta \cap \Delta + \gamma|$ for $\gamma \in \Gamma$. G is primitive; so by 1.2.8, $\mu \neq 0$. Let $\alpha \in \Delta \cap \Delta + \gamma$. Then $\alpha - \gamma \in \Delta$ and, since G is rational, $\gamma - \alpha$ is also in Δ. But $-\alpha$ lies in Δ if G is rational, and so $\gamma - \alpha \in \Delta \cap \Delta + \gamma$. $\gamma - \alpha$ and α are distinct, for otherwise $\gamma = 2\alpha$ and $\gamma \in \Gamma$ while $\alpha \in \Delta$. Hence $\mu \geq 2$. Suppose $\mu > 2$. Then there exists $\beta \in \Delta \cap \Delta + \gamma$ with $\beta \neq \alpha$ or $\gamma - \alpha$. Let δ be any element of $\Delta \setminus \{\alpha, \gamma - \alpha\}$. Since G_0 is near-3-transitive on Δ, there exists $g \in G_0$ such that $\alpha g = \alpha$, $(\gamma - \alpha)g = \gamma - \alpha$, and $\beta g = \delta$. Then $(\gamma - \beta)g = (\gamma - \alpha)g + \alpha g - \beta g = \gamma - \delta$. Thus $\gamma - \delta \in \Delta$ and hence $\delta \in \Delta \cap \Delta + \gamma$ for all $\delta \in \Delta$. Hence $\mu = k$ which, by Corollary 3, p.149 of [10], is a contradiction to the primitivity of G. Thus $\mu = 2$ as required.

It is not difficult to classify all groups satisfying the hypotheses of Theorem 3.1.5 (without having the possibility of some group of large order as in (ix) of 1.3.2). They are given by cases (i), (ii), (vi) (for $p = 2$ only) and (vii) of Theorem 1.3.2. We do not give a proof of this assertion now since it will follow later when we find all (*)-groups in which $\mu = 2$.

Another subclass of ($*$)-groups is given by:

<u>Theorem 3.1.6</u>. Suppose G is a primitive rank 3(p,n) group in which G_o is 3-transitive on the lines of a suborbit. Then $n \leq 2$ or $\lambda = p-2$.

<u>Proof</u>. If G is irrational, then $n \leq 2$ by Theorem 3.1.2. Suppose G is rational and $\lambda \neq p-2$. As in Theorem 3.1.4, there exist linearly independent α and β such that $\alpha-\beta \in \Delta$. Suppose there exists γ belonging to Δ but not to $\langle\alpha,\beta\rangle$. Since G_o is 3-transitive on $\underline{\Delta}$, there exists $g \in G_o$ such that $\alpha g = a\alpha$, $\beta g = b\beta$, $(\alpha+\beta)g = c\gamma$, for some a, b, c $\in GF(p)$. But $c\gamma = (\alpha+\beta)g = \alpha g+\beta g = a\alpha+b\beta \in \langle\alpha,\beta\rangle$ contradicting the choice of γ. Hence Δ is contained in $\langle\alpha,\beta\rangle$. It follows from Proposition 23.7 of [22] that if $\underset{\sim}{G}$ is primitive then the elements of Δ generate V(n,p). Hence $n \leq 2$ and the theorem is proved.

Finally we prove a lemma about the intersection numbers of rational rank 3 (p,n) groups in general, which though very simple, serves a useful purpose in immediately showing that certain sets of parameters (which satisfy the Higman-Tamaschke conditions) cannot admit S-rings of the desired type.

<u>Lemma 3.1.7</u>. Let G be a rational rank 3 (p,n) group with parameters (k,ℓ,λ,μ). If p = 2, then λ and μ are both even. If $p \neq 2$, then λ is odd and μ is even.

Proof. $\lambda = |\Delta \cap \Delta + \alpha|$, $\alpha \in \Delta$. Suppose $\beta \in \Delta \cap \Delta + \alpha$, $\beta \not\in \underline{\alpha}$. Then since G is rational, $\alpha - \beta$ also belongs to $\Delta \cap \Delta + \alpha$. Because $\beta \not\in \underline{\alpha}$, β and $\alpha - \beta$ are distinct. Hence $\Delta \cap \Delta + \alpha$ contains p-2 points of $\underline{\alpha}$ and the remaining points occur in pairs. Hence λ is odd if p is odd, even if p = 2.

$\mu = |\Delta \cap \Delta + \gamma|$, $\gamma \in \Gamma$. If $\beta \in \Delta \cap \Delta + \gamma$, then $\gamma - \beta$ belongs to $\Delta \cap \Delta + \gamma$ and since β, $\gamma - \beta$ are distinct, the points of $\Delta \cap \Delta + \gamma$ occur in pairs. Thus μ is even for any prime p.

§ 3.2 Residual S-rings and Extensions.

We saw in § 2 that corresponding to a rank 3 (p,n) group G is an S-ring $\mathcal{S} = C(V, G_0)$ with the same parameters. We recall that if $\mathcal{S}$ has basis $0, \hat{\Delta}, \hat{\Gamma}$, where $V = 0 \cup \Delta \cup \Gamma$ then $k = |\Delta|$, $\ell = |\Gamma|$, $\lambda = |\Delta \cap \Delta + \alpha|$ for $\alpha \in \Delta$, and $\mu = |\Delta \cap \Delta + \gamma|$ for $\gamma \in \Gamma$. The notion of a residual S-ring $\mathcal{S}_1$ of $\mathcal{S}$, which is well-defined only when $\mathcal{S}$ is rational and λ is as in 3.1.3, will be useful for two reasons: (1) as we shall see in § 4, we can prove the uniqueness of an S-ring with given parameters by proving (a) that the residual S-ring $\mathcal{S}_1$ is unique and (b) that $\mathcal{S}_1$ has a unique extension (an S-ring $\mathcal{S}$ is called an extension of $\mathcal{S}_1$ if $\mathcal{S}_1$ is the residual of $\mathcal{S}$); (2) we obtain further restrictions on the possible parameters of a (*)-group in the next theorem, in which also the residual is defined.

Theorem 3.2.1. Let G be a $(*)$-group with suborbits 0, Δ and Γ, and let $\mathcal{S}$ be the corresponding transitivity module, regarded as an S-ring over $V = V(n,p)$. By 3.1.1, we may assume $(0,\ldots,0,1)$ belongs to Δ. Let
$\Delta_1 = \{(a_1,\ldots,a_{n-1}) \in V(n-1,p)\colon\ (a_1,\ldots,a_n) \in \Delta$, some $a_n \in GF(p)\} \setminus \{0\}$. Let Γ_1 be the set $V(n-1,p) \setminus (\Delta_1 \cup 0)$ and $\mathcal{S}_1$ the S-module with basis 0, $\hat{\Delta}_1$, $\hat{\Gamma}_1$. Then $\mathcal{S}_1$ is either (i) a rank 2 S-ring over $V(n-1,p)$ (if Γ_1 is empty) or (ii) a rank 3 S-ring over $V(n-1,p)$ with parameters
$k_1 = (k-p+1)/(r+1)$, $\ell_1 = p^{n-1}-1-k_1$,
$\lambda_1 = [\mu(p-r-1) + (r+1)(\lambda-2p+2)]/(r+1)^2$, $\mu_1 = \mu p/(r+1)^2$,
where r is given by the value of λ obtained in Theorem 3.1.3. We call $\mathcal{S}_1$ the <u>residual S-ring</u> of $\mathcal{S}$, and $\mathcal{S}$ an <u>extension</u> of $\mathcal{S}_1$.

<u>Proof</u>. Suppose (i) is not true. By Theorem 2.1.6, it is sufficient to prove that λ_1 and μ_1 are well-defined; i.e. that $|\Delta_1 \cap \Delta_1+\alpha|$ is dependent only on whether α belongs to Δ_1 or Γ_1. Define a map $\theta : \Delta \setminus \underline{(0,\ldots,0,1)} \to \Delta_1$ by $((a_1,\ldots,a_n))\theta = (a_1,\ldots,a_{n-1})$. From the definition of r in the proof of 3.1.3 (taking $\alpha_1 = (a_1,\ldots,a_n)$, and $\alpha_2 = (0,\ldots,0,1)$) we get $|(a_1,\ldots,a_{n-1})\theta^{-1}| = r+1$. Since (i) is not true there exists $\xi = (x_1,\ldots,x_{n-1}) \in \Gamma_1$. By definition of Δ_1, $(x_1,\ldots,x_{n-1},z) \in \Gamma$ for all $z \in GF(p)$. Now $\mu_1 = |\Delta_1 \cap \Delta_1+\xi|$ = the number of ordered pairs (α_1,β_1) in $\Delta_1 \times \Delta_1$ such that $\alpha_1+\beta_1 = \xi$. Let $X = \{(x_1,\ldots,x_{n-1},z)\colon z \in GF(p)\}$, a subset of Γ, and let $M = \{(\alpha,\beta) \in \Delta\times\Delta\colon \alpha+\beta \in X\}$.

We calculate $|M|$ in two different ways. For each $z \in GF(p)$, there are μ pairs $(\alpha,\beta) \in \Delta \times \Delta$ with $\alpha+\beta = (x_1,\ldots,x_{n-1},z)$. Hence $|M| = \mu p$. On the other hand, for each of the μ_1 pairs $(\alpha\theta, \beta\theta) \in \Delta_1 \times \Delta_1$ satisfying $\alpha\theta + \beta\theta = \xi$, the $(r+1)^2$ pairs in $(\alpha\theta)\theta^{-1} \times (\beta\theta)\theta^{-1}$ are all in M. Since every pair (α,β) in M lies in $(\alpha\theta)\theta^{-1} \times (\beta\theta)\theta^{-1}$, we get $|M| = (r+1)^2\mu_1$. Thus $\mu_1 = \mu p/(r+1)^2$.

We now find λ_1. Let $\eta = (y_1,\ldots,y_{n-1})' \in \Delta_1$ and define $Y = \{(y_1,\ldots,y_{n-1},z) : z \in GF(p)\}$; $N = \{(\alpha,\beta) \in \Delta \times \Delta : \alpha+\beta \in Y\}$. We calculate $|N|$ in two different ways. Since $(0,\ldots,0,1) \in \Delta$, there are $r+1$ elements z of $GF(p)$ such that $(y_1,\ldots,y_{n-1},z) \in \Delta$. Hence $|N| = (r+1)\lambda + (p-r-1)\mu$. On the other hand, for each of the λ_1 pairs $(\alpha\theta, \beta\theta)$ in $\Delta_1 \times \Delta_1$ satisfying $\alpha\theta + \beta\theta = \eta$, the $(r+1)^2$ pairs in $(\alpha\theta)\theta^{-1} \times (\beta\theta)\theta^{-1}$ are all in N. The only other pairs in N are the $2(r+1)(p-1)$ pairs (α,β) in which α or β belongs to $\underline{(0,\ldots,0,1)}$. Thus $|N| = \lambda_1(r+1)^2 + 2(r+1)(p-1)$ and hence $\lambda_1 = (\mu(p-r-1) + (r+1)(\lambda-2(p-1))/(r+1)^2$. (As a check, we can deduce this value of λ_1, given $\mu_1 = \mu p/(r+1)^2$, from the equation $\mu_1 \ell_1 = k_1(k_1-1-\lambda_1)$). μ_1 and λ_1 are well-defined since they have been determined independently of the choice of ξ in Γ_1 and η in Δ_1 respectively.

Combining this theorem with some earlier results, we get further restrictions on λ.

Theorem 3.2.2. Suppose G is a $(*)$-group of degree p^n. Then one of the following holds: (i) G is imprimitive (ii) $\lambda = p-2$ or (iii) $n = 2$.

Proof. Let $\mathcal{S} = C(V,G_0)$ and let $\mathcal{S}_1$ be the residual of $\mathcal{S}$.

Case 1: $\mathcal{S}_1$ has rank 3. By 3.2.1, $(r+1)^2$ divides μp, for μ_1 is an integer. Suppose G is primitive and $r \neq 0$. Then by 3.1.3, $r+1$ divides $p-1$ ... (a), and hence $r+1$ does not divide p. Thus $(r+1)^2$ divides μ. Since λ_1 is an integer, 3.2.1 and (a) imply that $r+1$ divides $\lambda-2(p-1)$. Hence $r+1$ divides $\lambda = r(m-1) + p-2$, where $m = k/p-1$, ... (b). Now $\underline{\Delta}$ is the union of $(\underline{0,\ldots,0,1})$ with disjoint sets $(\underline{\alpha})\theta^{-1}$, $\underline{\alpha} \in \underline{\Delta}_1$, each containing $r+1$ elements (θ is as in the proof of 3.2.1). Hence $r+1$ divides $m-1$. From this and (b), we infer that $r+1$ divides $p-2$ ... (c). But (a) and (c) give a contradiction to $r \neq 0$. Thus $r = 0$ and $\lambda = p-2$ if G is primitive.

Case 2: $\mathcal{S}_1$ is a rank 2 S-ring; i.e. $\Delta_1 = V(n-1,p) \setminus 0$, and $k_1 = p^{n-1}-1$. By 3.2.1, $k = (p^{n-1}-1)(r+1) + p-1$. Thus $m = (p^{n-1}-1)(r+1)/(p-1) + 1$ ... (e). $\ell = p^n-1-k = (p^{n-1}-1)(p-r-1)$. By 3.1.3, $\lambda = r(m-1) + p-2$. μ can now be computed from the formula $\mu\ell = k(k-1-\lambda)$, and it turns out that $\mu = (r+1)m$. Substituting the above values of parameters k, ℓ,λ,μ in '$d = (\lambda-\mu)^2 + 4(k-\mu)$' gives $d = (m+p-2-r)^2$. Using (e) we obtain

$$(p-1)^2 d = p^2(p^{n-2}r + p^{n-2} + p-r-2)^2 \quad \ldots \text{(f)}.$$

By 2.2.9, d is a p-power. If $n > 2$, (f) implies that $p^{n-2}r + p^{n-2} + p-r-2$ is divisible by p. Since $r \leq p-1$, we must have $r = p-2$. But then $\mu = k$, which implies that G is imprimitive. If $n = 1$, then $r+1 = p$; otherwise the right-hand side of (f) is not an integer. This again leads only to imprimitive groups with $\lambda = k-1$. We are left with the possibility that $n = 2$. In that case $(p-1)^2 d = p^2(p-1)^2$ and hence $d = p^2$. This gives no restriction on the choice of $m = r+2$, and in our next theorem, which classifies all rational rank 3 S-rings over $V(2,p)$, we will see that for any m with $1 \leq m \leq \frac{p+1}{2}$, there is a rank 3 S-ring for which the residual is defined.

We will find all ($*$)-groups with $n = 2$ in § 4.1 by appealing to a theorem of Dickson (p.213 of [15]) which classifies all subgroups of $PSL(2,p)$.

The following is an immediate corollary to 3.2.1 and 3.2.2.

<u>Corollary 3.2.3</u>. Suppose G is a primitive ($*$)-group of degree p^n and $\mathcal{S}$ the corresponding S-ring. Then, if $n > 2$, the residual S-ring has parameters $(k-p+1,\ p^{n-1}-p-k-2,\ \mu p-\mu-p,\ \mu p)$.

<u>Theorem 3.2.4</u>. For any integer m with $1 \leq m \leq (p+1)/2$, there is a rational rank 3 S-ring over $V = V(2,p)$ with parameters

$$(k,\ell,\lambda,\mu) = (m(p-1),\ (p+1-m)(p-1),\ p+m^2-3m,\ m(m-1))$$

Moreover, any rational rank 3 S-ring over V has these parameters for some m.

<u>Proof</u>. The result will follow if we show that any partition of the lines of V into two sets $\underline{\Delta}$ and $\underline{\Gamma}$ gives an S-ring, with simple basis quantities $0, \hat{\Delta}, \hat{\Gamma}$, having the above parameters. For $m = |\underline{\Delta}| = 1$ this is trivially verified. Suppose $m \geq 2$ and let $\underline{\Delta}$ be any set of m lines of V. We must show that $\lambda = |\Delta \wedge \Delta + \delta|$ is independent of δ in Δ. We may choose a basis $\{\alpha, \beta\}$ of V such that

$$\underline{\Delta} = \{\underline{\alpha}, \underline{\beta}, \underline{\alpha + t_1\beta}, \ldots, \underline{\alpha + t_r\beta}\}$$

and

$$\lambda = |\Delta \wedge \Delta + \alpha|.$$

Clearly $$|\Delta \wedge (\underline{\alpha} + \alpha)| = p-2,$$

while $$|\Delta \wedge (\underline{\beta} + \alpha)| = r = m-2 .$$

It is easy to show that, for each $i = 1, \ldots, m-2$, the vector $a(\alpha + t_i\beta) + \alpha$ ($a \in GF(p) \setminus 0$) belongs to Δ if and only if $a = -1$ or $a = t_j/(t_i - t_j)$ for some $j \in \{1, \ldots, i-1, i+1, \ldots, m-2\}$.

Hence

$$\lambda = p-2+m-2+(m-2)^2 = p+m^2-3m .$$

In a similar way we can show that

$$\mu = m(m-1) .$$

Hence, by 2.1.6, the S-module with basis $0, \hat{\Delta}$ and $\hat{\Gamma}$ ($\Gamma = V(2,p) \setminus (0 \cup \Delta)$) is an S-ring.

§ 3.3 Possible parameters of (*)-groups.

We now have several conditions which must be satisfied by the parameters of a (*)-group. For convenience we collect them together below, adapting them to get equations (A) ... (F). The rest of the section will be devoted to the task of finding all integer solutions of these equations.

Suppose G is a primitive (*)-group of degree p^n and parameters $k, \ell, \lambda, \mu, d, f_2, f_3$ defined as in § 1.2. Then

$$p^n = k + \ell + 1 \qquad \text{... (A)}$$

By 2.2.8 and 2.2.9, there exists a positive integer t such that

$$p^{2t} = p^n k\ell/f_2f_3 \qquad \text{... (B),}$$

and
$$p^{2t} = (\lambda-\mu)^2 + 4(k-\mu) \qquad \text{... (C).}$$

By 1.2.5, $\mu\ell = k(k-1-\lambda)$, which becomes, using (A):

$$\mu(p^n-k-1) = k(k-1-\lambda) \qquad \text{... (D).}$$

Eliminating k from (C) and (D) we can rearrange terms to get:

$$[\mu^2+2\mu(-p^t-\lambda-3) + (\lambda+p^t)(\lambda+2+p^t)][\mu^2+2\mu(p^t-\lambda-3) + (\lambda-p^t)(\lambda+2-p^t)] = 16\mu(p^n-p^{2t}) \qquad \text{... (E)}$$

By 3.2.2,

$$\lambda = p-2 \text{ or } n > 2 \qquad \text{... (F)}$$

For $\lambda = p-2$, (E) becomes:

$$[\mu^2+2\mu(-p^t-p-1) + (p-2+p^t)(p+p^t)][\mu^2+2\mu(p^t-p-1) + (p-2-p^t)(p-p^t)] = 16\mu(p^n-p^{2t}) \qquad \text{... (E').}$$

<u>Lemma 3.3.1.</u> If $\lambda = p-2$, p^{2t-1} divides μp^n.

<u>Proof.</u> The result is clear for $2t-1 \le n$, so we suppose $2t-1 > n$. Then, by (B), p^{2t-n} divides $k\ell$, and since

$k+\ell+1 = p^n$, p^{2t-n} divides either k or ℓ .

(i) If p^{2t-n} divides k, then by (D) p^{2t-n} divides μ and hence p^{2t} divides μp^n.

(ii) If p^{2t-n} divides ℓ, then by (A) p^{2t-n} divides p^n-k-1 and so by (D)

$$p^{2t-n} \text{ divides } k-1-\lambda = k-p+1 .$$

Hence

$$p^{2t-n} \text{ divides } (p^n-k-1) + (k-p+1) = p^n-p.$$

Hence $2t-n \leq 1$ and p^{2t-1} divides p^n .

In both cases (i) and (ii) we deduce that p^{2t-1} divides μp^n .

<u>Lemma 3.3.2</u>. p^t divides $\mu^2 - 2(p+1)\mu + p(p-2)$.

<u>Proof</u>. By 3.3.1, p^{2t-1} divides the left-hand side of (E'). Hence p^t divides at least one of the two factors in this expression. Whichever this factor is, the result follows.

We let y be that integer given by:

$$\mu^2 - 2(p+1)\mu + p(p-2) = yp^t \qquad \ldots \text{ (G)}.$$

(E') and (G) give

$$(y-2\mu+2p-2+p^t)(y+2\mu-2p+2+p^t) = 16\mu(p^{n-2t}-1) \quad \ldots \text{ (H)} .$$

<u>Lemma 3.3.3</u>. If $\lambda = p-2$, then (i) $\mu \leq k/(p-1)$, (ii) $\mu \leq p^t-p+2$.

<u>Proof</u>. (i) $\mu = |\Delta \cap \Delta+\gamma|$ where $\gamma \in \Gamma$. Suppose $\alpha \in \Delta \cap \Delta+\gamma$. Then $\alpha = \beta+\gamma$, some $\beta \in \Delta$. Suppose also that

$a\alpha \in \Delta \wedge \Delta + \gamma$ for some $1 \neq a \in GF(p) \setminus 0$. Then $a\alpha = \delta + \gamma$, some $\delta \in \Delta$. Hence $(a-1)\alpha = \delta - \beta$ belongs to $\Delta \wedge \Delta + \delta$. But since $\lambda = p-2$,

$$\Delta \wedge \Delta + \delta = \{2\delta, \ldots, (p-1)\delta\}$$

and so α is a multiple of δ. Hence $\gamma = a\alpha - \delta$ is also a multiple of δ, giving a contradiction to $\gamma \in \Gamma$. We have thus shown that at most one point of each line of Δ lies in $\Delta \wedge \Delta + \gamma$, $\gamma \in \Gamma$. i.e. $\mu \leq k/(p-1)$.

(ii) From (C) and (F),

$$p^{2t} = (p-2-\mu)^2 + 4(k-\mu) .$$

Using (i),

$$p^{2t} \geq (p-2-\mu)^2 + 4(p-2)\mu = (p-2+\mu)^2 .$$

Hence $p^t \geq p-2+\mu$ and (ii) is proved.

Note. The left-hand side of (G) factorizes into linear factors (in μ) with integer coefficients if and only if $4p+1$ is a square, which is true if and only if $p = 2$. This seems to be the reason why the case $p = 2$ is easier to deal with, and our next theorem shows that we can find all possible parameters of $(*)$-groups when $p = 2$.

Theorem 3.3.4. Let G be a primitive $(*)$-group of degree 2^n. Then the parameters of G are $(5,10,0,2)$.

Proof. By 3.3.2, 2^t divides $\mu(\mu-6)$. But by 3.3.3, $\mu \leq 2^t$. Hence

$$\mu = 2^t,\ 2^{t-1},\ 2^{t-1}+6 \text{ or } 6 .$$

If $n = 2$, $k = 1$ and hence G is imprimitive. Hence $n > 2$ and $\lambda = 0$ by 3.2.2.(E') becomes:

$$[\mu^2+2\mu(-2^t-3) + 2^t(2+2^t)][\mu^2 + 2\mu(2^t-3) - 2^t(2-2^t)] = 16\mu(2^n-2^{2t}) \quad \ldots (E'')$$

Case 1. $\mu = 2^t$. By (C) $\mu = k$, which gives a contradiction to G primitive by Corollary 3, p.149 of [10].

Case 2. $\mu = 2^{t-1}$. (E'') gives

$$(2^{t-2}-1)(7.2^{t-2}-5) = 8(2^n-2^{2t}) .$$

The only possibility is that $t = 2$ which yields $n = 4$, $\mu = 2$, $k = 5$ and $\ell = 10$.

Case 3. $\mu = 2^{t-1}+6$. (E'') gives

$$2^n(2^{t-2}+3) = 9(2^{4t-9}-2^{3t-6} + 5.2^{2t-5}) .$$

If $t \geq 3$, comparing the highest power of 2 dividing each side, $n = 2t-5$. Then

$$2^{t-2} + 3 = 9(2^{2t-4} - 2^{t-1}) + 5 .$$

Clearly the right-hand side is greater than the left for $t > 3$, while $t = 3$ leads to $\mu = 10$, $k = 1$, contradicting $\mu \leq k$. Putting $t = 1$ or 2 gives an immediate contradiction.

Case 4. $\mu = 6$. (E'') gives

$$3.2^{n-2t+3} = 2^{2t-2}+1 .$$

Clearly we can have only $n = 2t-3$, which implies $2t-2 = 1$, contradicting the fact that t is an integer. This completes the proof.

It often happens that $2t = n$ for rank 3 (p,n) groups (it follows from (E) that $2t = n$ if and only if $\{k,\ell\} = \{f_2,f_3\}$, bearing in mind that $k+\ell = f_1+f_3$). We find that for (*)-groups in which $n = 2t$ or $n = 2t+1$ our equations are easier to manipulate:

Theorem 3.3.5. A necessary condition for the existence of a primitive (*)-group with $p \neq 2$, $\lambda = p-2$ and with (i) $n = 2t$ or (ii) $n = 2t+1$ is respectively that (i) $4p^t+4p+1$ is a square or $t = 1$, or (ii) $4p^{t+1}+4p+1$ is a square.

Proof. Consider first a polynomial in μ of the following form.

$$P(\mu) = (\mu^2+a\mu+b)(\mu^2+c\mu+d) - e\mu \ .$$

If $P(\mu)$ is the product $(\mu^2+x\mu+b)(\mu^2+y\mu+d)$ of two second-degree polynomials then, comparing coefficients of powers of μ,

(1) $a+c = x+y$,

(2) $bc+ad-e = by+dx$,

(3) $ac = xy$.

Solving (1) and (2) for x and y, and using (3), it is found that $P(\mu)$ is such a product if and only if $e = 0$ or $e = (c-a)(b-d)$. Taking $P(\mu)$ to be the left hand side minus the right hand side of equation (E) gives the condition

$$16(p^n-p^{2t}) = 0 \quad \text{or} \quad 16(p^n-p^{2t}) = 16p^{2t}(\lambda+1) \ .$$

With $\lambda = p-2$, the second condition is equivalent to $n = 2t+1$. Thus $n = 2t$ or $2t+1$ is a necessary and sufficient condition for (E') to have the form $Q(\mu)\ R(\mu) = 0$ where Q and R are second-degree polynomials. If $n = 2t$, (E') becomes:

$$\mu^2 + 2\mu(-p^t-p-1) + (p-2+p^t)(p+p^t) = 0 \qquad \text{or}$$

$$\mu^2 + 2\mu(p^t-p-1) + (p-2-p^t)(p-p^t) = 0 \ .$$

If $n = 2t + 1$, then

$$\mu^2 + 2\mu(p^t-p-1) + (p-2+p^t)(p+p^t) = 0 \qquad \text{or}$$

$$\mu^2 + 2\mu(-p^t-p-1) + (p-2-p^t)(p-p^t) = 0 \ .$$

Solving these equations, if $n = 2t$ then

$$\mu = p+1+p^t \pm (4p^t+4p+1)^{1/2}$$

or

$$\mu = p+1-p^t \pm (-4p^t+4p+1)^{1/2} ,$$

while if $n = 2t+1$ then,

$$\mu = p+1-p^t \pm (-4p^{t+1}+4p+1)^{1/2} \qquad \text{or}$$

$$\mu = p+1+p^t \pm (4p^{t+1}+4p+1)^{1/2}$$

Lemma 3.3.3 tells us which signs we must take. If $n = 2t$,

$$\mu = p+1+p^t-(4p^t+4p+1)^{1/2}$$

or $\mu = 2$ and $t = 1$ (we discount $\mu = 0$ since G is primitive).

If $n = 2t+1$,

$$\mu = p+1+p^t-(4p^{t+1}+4p+1)^{1/2}.$$

<u>Corollary 3.3.6</u>. Let G be a primitive ($*$)-group with $p > 2$, $\lambda = p-2$ and either (i) $n = 2t$ or (ii) $n = 2t+1$. Then the parameters (k,ℓ,λ,μ) of G are respectively:

(i) $\left(\tfrac{1}{2}(p^t+1)(x-3),\ \tfrac{1}{2}(p^t+1)(2p^t-x+1),\ p-2,\ p+1+p^t-x\right)$,

where $x^2 = 4p^t+4p+1$, or

(ii) $\left(\tfrac{1}{2}[p^t(x-2p-1) + x-3],\ p^{2t+1}-k-1,\ p-2,\ p+1+p^t-x\right)$,

where $x^2 = 4p^{t+1}+4p+1$.

<u>Proof</u>. The values of μ were found in 3.3.5. k is obtained from (C) and then ℓ from (A).

<u>Note.</u> It can be shown that the sets of parameters of 3.3.6 satisfy all the numerical conditions we have found. Thus, for $n = 2t$ ($t > 1$) or $n = 2t+1$, the condition of 3.3.5 that $4p^s + 4p + 1$ is a square, $s = t$ or $t + 1$, is 'sufficient' in the sense that our present knowledge will yield no stronger necessary condition. Indeed we shall see that for all known cases when $4p^s + 4p + 1$ is a square, a rank 3 S-ring exists with the appropriate parameters.

We now turn our attention to the question: when is $4p^s + 4p + 1$ equal to x^2, for some integer x? We observe that there are solutions $s = 2$, $x = 2p+1$ for all p and that t cannot be even and greater than 2, for if so,

$$(2p^{s/2})^2 < 4p^s + 4p + 1 < (2p^{s/2} + 1)^2 .$$

Unfortunately, the general problem seems to be intractible by known number-theoretic means. It is interesting that a problem of exactly the same nature was encountered by Montague [16] in his search for rank 3 extensions of $PSL(n,q)$. His condition was that

$$p^s + p^{s-1} + \dots + p+1 = x^2$$

for some integer x. He used a computer to show that for $p \leq 12,000$ and $1+p+\dots+p^s \leq 10^9$, the only solutions are $(p,s) = (3,4)$ and $(7,3)$. Without resorting to such means, we can get a similar result by finding what x has to be modulo p^s. In our case, for example we get:

<u>Lemma 3.3.7.</u> The only integer solutions (p,s,x) of

$$4p^s + 4p + 1 = x^2$$

with p an odd prime and $s \leq 10$ are $(p,2,\pm(2p+1))$ for any p and $(3,3,\pm 11)$.

Proof. Case $s = 1$: $8p+1 = x^2$ and so $x = \pm 1$ modulo p. i.e. $x = \pm (ap+1)$, some integer a, and hence $a^2p+2a = 8$ which is easily seen to have no solution with p prime.

Case $s = 2$: $x = \pm(2p+1)$ gives two solutions for every p. There cannot be more than 2 solutions for a given p, so we are done in this case.

Case $s = 3$:

$$x^2 = 4p^3 + 4p + 1 \qquad \ldots (1)$$

$x = \pm(ap+1)$ for some integer a. Equating coefficients of p in (1), $a \equiv 2$ modulo p. Hence

$$x = \pm (bp^2 + 2p + 1),$$

some integer b. Equating coefficients of p^2 in (1) gives $b = -2$ modulo p. Hence

$$x = \pm (cp^3 - 2p^2 + 2p + 1) .$$

Equating coefficients of p^3 in (1) gives $c = 4$ modulo p. We see that x^2 is greater than $4p^3 + 4p + 1$ unless $(p,c) = (3,1)$, which yields the solutions

$$(p,s,x) = (3,3,\pm 11).$$

As we remarked earlier, we need consider only odd s for $s > 2$.

Case $s = 5$: As for $s = 3$,

$$x = \pm(ap^5 - 10p^4 + 4p^3 - 2p^2 + 2p + 1)$$

where $a = 28$ modulo p. It is easy to see that x^2 is greater than $4p^5 + 4p + 1$ for any such a and p.

Cases $s = 7$ and $s = 9$ are eliminated in similar fashion.

Corollary 3.3.8. Let G be a primitive (*)-group with $\lambda = p-2$ and either $n = 2t$ or $n = 2t+1$. Then the degree p^n of G is p^2 (any odd prime p), p^4 (any prime p), 3^5 or 3^6, or $n \geq 21$. The respective sets of parameters are as in cases (iii), (vi), (vii), (viii) and (ix) of Theorem 1.3.2.

Proof. (a) $p > 2$. (i) $n = 2t$. If $x^2 = 4p^t + 4p + 1$, for an integer x, then by 3.3.7,

$$(p,t,x) = (p,2,2p+1) \text{ or } (3,3,11),$$

(we take the positive values of x since, by 3.3.6, x must be greater than 3 for k to be positive).

(ii) $n = 2t+1$. If $x^2 = 4p^{t+1} + 4p + 1$, for an integer x, then by 3.3.7,

$$(p,t,x) = (p,1,2p+1) \text{ or } (3,2,11).$$

But by 3.3.6 the former gives $\mu = 0$, and since G is primitive we discard this. For the latter solution, 3.3.6 gives the required parameters with $p^n = 3^5$.

(b) $p = 2$. By 3.3.4 we get the $n = 4$ case only with parameters as required.

We now return to the general case (n not necessarily 2t or 2t+1) and show that for low t we get no further (*)-groups. We need the following lemma.

Lemma 3.3.9. In a (*)-group, with $p > 2$, n is greater than or equal to 2t-2.

Proof. This is immediate from 3.3.1 and 3.3.2, p^t being the highest power of p dividing μ.

<u>Theorem 3.3.10.</u> Suppose G is a $(*)$-group with $\lambda = p-2$. Then if $n \leq 12$ the only possible sets of parameters are those given by 3.3.8.

<u>Proof.</u> By 3.3.4 it is sufficient to consider $p > 2$ and by 3.3.9 to consider only $t \leq 7$.

Given t, our method is to find μ modulo p^t by means of Lemma 3.3.2. Lemma 3.3.3 then gives the possible values of μ. It is then not difficult to check whether the resulting parameters fulfil conditions (A)...(F). Thus we have an algorithm for finding possible parameters with given n (or t). We have worked this through for $t \leq 7$, though we give details up to only $t = 5$, which amply demonstrates our method.

By 3.3.2,

$$\mu^2 - 2(p+1)\mu + p(p-2) = 0 \text{ modulo } p^t.$$

Thus $\mu = 0$ or 2 modulo p. We consider the two cases separately.

<u>Case 1</u>: $\mu = 2$ modulo p. The following table gives possible values of μ obtained from the above congruence.

t	μ (modulo p^t)	a (given by 3.3.3)
1	a, $a = 2 \bmod p$	2
2	$ap+2$, $a = 3 \bmod p$	0 if $p=3$, 3 if $p>3$
3	ap^2+3p+2, $a = -2 \bmod p$	$p-2$
4	ap^3-2p^2+3p+2, $a = 4 \bmod p$	1 if $p=3$, 4 if $p>3$
5	$ap^4+4p^3-2p^2+3p+2$, $a =-10 \bmod p$	-1 if $p = 3$, 0 if $p=5$, 4 if $p=7$, $p-10$ if $p>7$.

We now find which of these values of μ lead to parameters satisfying our conditions.

$t = 1$: By (C), $k = 2(p-1)$ and hence

$$(k,\ell,\lambda,\mu) = (2(p-1),\ (p-1)^2,\ p-2,\ 2).$$

$t = 2$: If $p = 3$ and $\mu = 2$, then by (C), $k = 22$ which gives

$$(k,\ell,\lambda,\mu) = (22,220,1,2)\ .$$

If p is prime > 3, then $\mu = 3p+2$, which, being odd, we discard by Lemma 3.1.7.

$t = 3$: $$\mu = p^4 - 2p^3 + 3p + 2.$$

From (G) we get

$$y = p^3 - 4p^2 + 8p - 6,$$

(H) becomes

$$(p-3)(p^3-2p^2 + 3p) = \mu(p^{n-6}-1)\ .$$

Clearly the only possibility is $p = 3$, $n = 6$. This gives

$$(k,\ell,\lambda,\mu) = (112,616,1,20).$$

$t = 4$: If $p = 3$, we again get $\mu = 20$. From (C), $k = 1570$. From

$$\mu\ell = k(k-1-\lambda)\ ,$$

$\ell = 121088$. Hence

$$k+\ell+1 = 124659 = 3^8.19 \neq 3^n,\ \text{any } n.$$

If $p > 3$, μ is odd and the case is dismissed as for $t = 2$.

$t = 5$: μ is odd if $p = 5$ or 7. Suppose $p = 3$. As in the $t = 4$ case we get $\mu = 20$, $k = 14692$, $\ell = 10805967$ and hence

$$k+\ell+1 = 3^9.61 \neq 3^n,\ \text{any } n\ .$$

For $p > 7$ we get a contradiction by proceeding as in the $t = 3$ case.

Cases $t = 6$ and 7 can be resolved in a similar way, and we could continue indefinitely in this way.

<u>Case 2</u>: $\mu = 0$ modulo p. Since the method is exactly the same as in Case 1, we omit the details, merely pointing out that for $t \leq 7$, only $t = 2$ yields possible parameters, these being as in case (vi) of 1.3.2, with $\mu = p^2-p$.

§ 4. CLASSIFICATION OF (*)-GROUPS.

§ 4.0 General Remarks; Orthogonal Groups.

In § 3 we showed that a primitive (*)-group has degree p^2, p^4, 3^5, 3^6, or p^n with $n > 12$. In § 4 we will complete the proof of our main theorem, 1.3.2, by finding all primitive (*)-groups having parameters as given by Theorems 3.2.4 and 3.3.10. By Theorem 3.2.2 either $\lambda = p-2$ or $n = 2$, and these two cases require different treatments. In § 4.1 we find (*)-groups of degree p^2, and in 4.2, 4.3 and 4.4 those of degree p^4, 3^5 and 3^6 respectively.

For each of the last three degrees our method will follow the same pattern. We will first prove the existence and uniqueness of an S-ring with the given parameters by

(1) proving the existence and uniqueness of the residual S-ring $\mathcal{S}_1$,

(2) constructing an extension $\mathcal{S}$ in a unique way.

The final step is

(3) to find the automorphism group Aut $\mathcal{S}$ (defined in § 2.3) of $\mathcal{S}$.

Then the semidirect product [V] Aut $\mathcal{S}$ is a (*)-group if Aut $\mathcal{S}$ has two orbits on $V - 0$ and is doubly-transitive on the lines of one of them. It turns out that these conditions are fulfilled except for degree 3^6 and even then Aut $\mathcal{S}$ is a group of some interest.

We now look at steps 1 and 2 more closely, outlining our method of proof. We denote by $A(p)$, B, and C those parameters, given by 3.3.10, of (*)-groups of degree p^4, 3^5 and 3^6 respectively. The residual S-ring has parameters given by Corollary 3.2.3. Denoting these parameters by $A_1(p)$, B_1 and C_1 respectively we list below the parameters of S-rings (corresponding to (*)-groups) and their residuals.

	degree	k	λ	μ
$A(p)$	p^4	$(p^2+1)(p-1)$	$p-2$	$p(p-1)$
$A_1(p)$	p^3	$p^2(p-1)$	$p^2(p-2)$	$p^2(p-1)$
B	3^5	11.2	1	2
B_1	3^4	10.2	1	6
C	3^6	56.2	1	20
C_1	3^5	55.2	37	60

In § 4.2 we will see that there is a unique S-ring having parameters $A_1(p)$ and that an extension $\mathcal{S}$ (assuming it admits a suitable automorphism group) with parameters $A(p)$ is unique. We show in § 4.3 that $A(3)$ admits a unique S-ring without any assumption about its automorphism group. But $B_1 = A(3)$ and hence the residual in the p^4 case is also unique. It follows from 1.2.6 and 2.2.6 that an S-ring with parameters C_1 is the dual to an S-ring with parameters B, and hence is unique. In § 4.4 we show that the extension is unique under certain assumptions about its automorphism group.

Orthogonal Groups.

Since orthogonal groups over finite fields will arise in § 4.2 and in § 4.4, we give a brief description of them here. The discussion will concern only fields of characteristic not equal to 2.

Let $V = V(n,F)$ denote a vector space of dimension n over the field F. We call a map Q from $V \times V$ into F a quadratic form over V if

(i) $(\alpha,\beta)Q = (\beta,\alpha)Q$ for $\alpha, \beta \in V$.

(ii) $(a\alpha,\beta)Q = a(\alpha,\beta)Q$ for $a \in F$, $\alpha,\beta \in V$.

(iii) $(\alpha+\beta,\gamma)Q = (\alpha,\gamma)Q + (\beta,\gamma)Q$ for $\alpha,\beta,\gamma \in V$.

We say that an element g of $GL(n,F)$ is an isometry of V with respect to Q if

$$(\alpha g,\beta g)Q = (\alpha,\beta)Q$$

for all α and $\beta \in V$. The group of isometries of V with respect to Q is called the orthogonal group of Q. If $\alpha_1,\ldots,\alpha_n$ is a basis of V then the matrix A, whose i,j th coefficient is $(\alpha_i,\alpha_j)Q$, is called the matrix of Q with respect to this basis. Q is said to be non-singular if A is. If we change basis via $\beta_j = \Sigma\, s_{ij}\alpha_i$, then the matrix of Q with respect to $\beta_1,\ldots,\beta_n$ is $S'AS$, where S is the non-singular matrix with coefficients s_{ij}.

Theorem 4.0.1. Let $V = V(2n,p)$ and suppose Q is a non-singular quadratic form over V. Then a basis may be chosen for V such that Q has matrix

$$A_1 = \begin{bmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{bmatrix} \quad \text{or} \quad A_2 = \begin{bmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 1 & 0 \\ & & & & & 0 & -g \end{bmatrix}$$

where g is a non-square. The two forms are not equivalent; we call them forms of type 1 and 2 respectively, and the corresponding orthogonal groups are denoted by $O^+(2n,p)$ and $O^-(2n,p)$.

Given any quadratic form with matrix B there is a non-singular matrix S such that $B = S'AS$ where A is one of the matrices A_1 and A_2 of 4.0.1. Hence $\det B = \det A(\det S)^2$. But $\det A_1 = (-1)^n$ while $\det A_2 = g.(-1)^n$, and so a quadratic form for n even is of type 1 or 2 according as the determinant of its matrix is a square or a non-square.

We shall be mainly concerned with the latter of the two types. We state some facts about $O^-(n,p)$ in the next theorem. A vector α of V is called <u>isotropic</u> (with respect to Q) if $(\alpha,\alpha)Q = 0$.

<u>Theorem 4.0.2</u>. Let Q be a quadratic form of type 2. Then

(i) the number of isotropic vectors is $(p^n+1)(p^{n-1}-1) + 1$.

(ii) the order of $PO^-(2n,p)$ is $p^{n(n-1)}(p^2-1)(p^4-1)\ldots(p^{2n-2}-1)(p^n+1)$.

($PO^-(2n,p)$ denotes the projective orthogonal group; in this case it is $O^-(2n,p)$ factored out by the subgroup $\{I,-I\}$, where I is the identity matrix).

The proofs of results mentioned above may be found in [1] or [4].

§ 4.1 (*)-groups of degree p^2.

In Theorem 3.2.4 we found that rank 3 S-rings exist over $V(2,p)$ for any k which is a multiple of $p-1$, and in 3.2.2 that, unlike the case $n \neq 2$, the imposition of an automorphism group doubly-transitive on $\underline{\Delta}$ leads to no further restrictions on the parameters. The reason is that residual S-rings are well-defined for all rational rank 3 S-rings over $V(2,p)$, and they are all the same, for there is only one rational S-ring over $V(1,p)$. We must therefore adopt a different approach for this case. Since Dickson has essentially determined all subgroups of $PGL(2,p)$, we simply consider all possibly doubly-transitive representations of these.

Theorem 4.1.1. Suppose G is a primitive (*)-group of degree p^2.

Then G_o/Z is isomorphic to one of

(i) the dihedral group $D_{2(p-1)}$ for any prime $p \neq 2$.

(ii) the symmetric group S_3, with $p = 5$.

(iii) the alternating group A_5, with $p = 7$.

(Z denotes the centre of $GL(2,p)$; i.e. the scalar multiples of the identity matrix).

Proof. We first show that p is not 2 and that p does not divide $|G_o|$.

If $p = 2$, then $k+\ell = 3$ and assuming $k \leq \ell$, we have $k = 1$ and hence $\mu = 0$, contradicting G primitive.

Suppose p divides $|G_o|$. Then there is an orbit of G_o on Ω containing p lines. Hence $|\Delta| = 1$ and $|\Gamma| = p$. But then $\Delta \cup O$ is a subspace of V and hence G is imprimitive - a contradiction. Since PGL(2,p) has order $p(p^2-1)$ it follows that $|G_o/Z|$ divides p^2-1.

We first consider the special cases $|\Delta| \leq 2$. If $|\Delta| = 1$, then G is imprimitive. If $|\Delta| = 2$ we choose a basis for V(2,p) such that $\Delta = \{(\underline{1,0}), (\underline{0,1})\}$. This case is special because there are elements of PGL(2,p) which fix both lines of Δ but not the remaining lines of PG(1,p). If $\mathcal{S}$ is the S-ring with simple basis quantities $0, \hat{\Delta}, \hat{\Gamma}$, with Δ as above, then

$$\text{Aut}\,\mathcal{S} = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} : a,b,c,d \in GF(p)\}.$$

It is easily checked that [V] G_o, with $G_o = \text{Aut}\,\mathcal{S}$, is a (*)-group and that G_o/Z is isomorphic to the dihedral group $D_{2(p-1)}$ with generators and relations

$$\langle A = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \text{ modulo } Z,\ B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ modulo } Z : B^{-1}AB = A^{-1} \text{ modulo } Z\rangle,$$

where a is a generator of the multiplicative group $GF(p) \sim 0$.

We now examine the complete list of subgroups of PSL(2,p) found by Dickson (See Huppert's book [15], p.213). By Dickson's Theorem, the only subgroups of PSL(2,p) ($p \neq 2$) with order dividing p^2-1 are

(1) cyclic groups of order z, where z divides $(p \mp 1)/2$.

(2) dihedral groups of order 2z, with z as in (1).

(3) A_4, if $p > 3$.

(4) S_4, if $p^2-1 \equiv 0$ modulo 16 and $p > 3$.

(5) A_5, if $p^2-1 \equiv 0$ modulo 5.

We wish to find subgroups of PGL(2,p) which have two orbits on PG(1,p) and which are 2-transitive on one of them. Such a subgroup must be one of (1) to (5) or contain such a group with index 2. It is not difficult to show case by case that the latter possibility does not occur, though we omit the details. We now consider 2-transitive representations of groups (1) to (5).

Case (1) Since a transitive abelian group is regular (See e.g. 4.4 of [22]), the only doubly-transitive cyclic groups are C_1 and C_2. We have already considered $|\underline{\Delta}| = 1$ or 2, and so no (*)-groups arise from this case.

Case (2) We have already seen how $D_{2(p-1)}$ gives (*)-groups for all primes $p \neq 2$, with $|\underline{\Delta}| = 2$. Suppose D_{2z} acts 2-transitively on a set $\underline{\Delta}$ with $|\underline{\Delta}| > 2$. By 9.6 of [22], D_{2z} is primitive on $\underline{\Delta}$ and hence by 8.8 of [22], the normal cyclic subgroup of order z is transitive. But by 4.4 of [22], transitive abelian groups are regular, and hence $|\underline{\Delta}| = z$. By Theorem 1.1.1, $z(z-1)$ divides $2z$, and so z is less than or equal to 3. We have already dealt with $|\underline{\Delta}| \leq 2$, and we need consider only $z = 3$. Now D_6 acts transitively on $\underline{\Gamma}$, where $|\underline{\Delta}| + |\underline{\Gamma}| = p+1$. Hence $|\underline{\Gamma}|$ is a divisor of 6, and it is easy to see that the only possibility is that $p = 5$ and $|\underline{\Delta}| = |\underline{\Gamma}| = 3$. We may choose a basis of $V = V(2,5)$ such that

$$\underline{\Delta} = \{(\underline{1,0}),\ (\underline{0,1}),\ (\underline{1,1})\}.$$

We indeed get a (*)-group in this case with

$$G_o = <\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 1 & 1 \end{pmatrix} >,$$

and G_o/Z is isomorphic to D_6 (i.e. to S_3).

Case (3) A_4 is 2-transitive only on 4 letters. Hence

$$|\Delta| = 4 \text{ and } |\Gamma| \text{ divides } |A_4| = 12 .$$

Since $|\Delta| + |\Gamma| = p+1$, we can have only $p = 7$. With

$$\Delta = \{(\underline{1,0}), (\underline{0,1}), (\underline{1,1}), (\underline{1,3})\},$$

we get a (*)-group $[V]G_o$, where G_o/Z is isomorphic to A_4. G_o is generated by $\begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 2 & 6 \end{pmatrix}$.

Case (4) Again the only possibility is $p = 7$ with Δ as in case (3). But G_o of (3) is the largest subgroup of PGL(2,7) which stabilizes Δ . Otherwise there would be a matrix $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$ in GL(2,7) which fixes $(\underline{1,1})$ and $(\underline{1,3})$. Clearly there is no such matrix.

Case (5) Suppose G_o/Z is isomorphic to A_5. Now A_5 acts 2-transitively on 5 or 6 letters. Hence

$$|\Delta| = 5 \text{ or } 6, \text{ and } |\Gamma| \text{ is a divisor of } 60.$$

Also

$$|\Delta| + |\Gamma| = p+1 \quad \text{and} \quad p^2-1 = 0 \text{ modulo } 5.$$

The only primes satisfying these conditions are

(a) $p = 11$, with $|\Delta| = |\Gamma| = 6$

(b) $p = 19$, with $|\Delta| = 5$, $|\Gamma| = 15$.

Suppose (a) occurs. The element $A = \begin{pmatrix} 0 & 1 \\ 10 & 3 \end{pmatrix}$ of GL(2,11) has order 5, and so by Lemma 3.1.1 we may assume that A belongs to G_o. The orbits of A on PG(1,p) are

$$\underline{\Delta}_1 = \{(\underline{1,0}), (\underline{0,1}), (\underline{1,8}), (\underline{1,1}), (\underline{1,7})\},$$

$$\underline{\Delta}_2 = \{(\underline{1,3}), (\underline{1,4}), (\underline{1,5}), (\underline{1,10}), (\underline{1,9})\},$$

$$\underline{\Delta}_3 = \{(\underline{1,2})\}, \qquad \underline{\Delta}_4 = \{(\underline{1,6})\}$$

We may assume $\underline{\Delta} = \underline{\Delta}_1 \cup \underline{\Delta}_3$ or $\underline{\Delta} = \underline{\Delta}_1 \cup \underline{\Delta}_4$.
If G_o is 2-transitive on $\underline{\Delta}$, then G_o contains an element which maps $(\underline{1,0})$ to $(\underline{0,1})$ and $(\underline{0,1})$ to $(\underline{1,0})$; i.e. G_o contains a matrix $B = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$ for some $a \in GF(p) \setminus 0$. If $\underline{\Delta} = \underline{\Delta}_1 \cup \underline{\Delta}_3$, then $\underline{\Delta}$ contains the lines $(\underline{1,a})$, $(\underline{8,a})$, $(\underline{7,a})$ and $(\underline{2,a})$; i.e. the lines $(\underline{1,a})$, $(\underline{1,7a})$, $(\underline{1,8a})$ and $(\underline{1,6a})$ belong to $\underline{\Delta}$. But this is not true for any a. We get a similar contradiction if $\underline{\Delta} = \underline{\Delta}_1 \cup \underline{\Delta}_4$. Hence (a) cannot occur.

In the same way it can be shown that (b) cannot occur either. This completes the proof of Theorem 4.1.1.

§ 4.2 <u>(*)-groups of degree p^4</u>.

In this section we find (*)-groups with parameters A(p) as defined in § 4.0. We will prove

<u>Theorem 4.2.1.</u> Let $\mathcal{S}$ be an S-ring which admits a (*)-group G with parameters A(p). Then a basis may be chosen for V(4,p) such that

(i) for $p = 2$, $\Delta = \{(1,0,0,0),\ (0,1,0,0),\ (0,0,1,0),$
$(0,0,0,1),\ (1,1,1,1)\}$

(ii) for $p \neq 2$, $\Delta = \{(x,y,z,w):\ wz = x^2+y^2+exy\}$,
where e^2-4 is a non-square in $GF(p)$, and $\frac{\text{Aut}\,\mathcal{S}}{Z}$ is isomorphic to

(i) the symmetric group S_5 for $p = 2$

(ii) $[PO^-(4,p)]C_2$, the projective orthogonal group of second type extended by a cyclic group of order 2, for $p \neq 2$.

(Z denotes the centre of $GL(4,p)$).

<u>Proof of (i).</u> We first prove the uniqueness of an S-ring with parameters $A(2) = (5,10,0,2)$. The S-ring is primitive since μ is not equal to 0 or k. By 23.7 of [22], the elements of Δ generate $V = V(4,2)$. Hence we may choose a basis of V such that the vectors $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ and $(0,0,0,1)$ belong to Δ. Let α be the remaining vector of Δ. If $\alpha = (1,1,0,0)$, then α belongs to $\Delta \cap \Delta + (1,0,0,0)$, contradicting $\lambda = 0$. Similarly α cannot be any other vector with exactly two zero coordinates. If $\alpha = (1,1,1,0)$, then $\Delta \cap \Delta + (1,1,0,0)$ contains four vectors, contradicting $\mu = 2$. Similarly α cannot be any other vector with exactly one zero coordinate. Hence the only possibility is $\alpha = (1,1,1,1)$. It is easily seen that with this α, any permutation of the five elements of Δ acts as a linear transformation, and hence Aut $\mathcal{S}$ is isomorphic to S_5.

We will prove Theorem 4.2.1 for $p \neq 2$ by a sequence of lemmas (1 to 10). The uniqueness of the residual S-ring is used to obtain the first three coordinates of the elements of Δ. Then by using the transitivity properties of the automorphism group and the fact that the dual S-ring also has rank 3, we determine the fourth coordinates. By Lemma 3.1.1, we wish to find Δ only up to change of basis. Assuming the existence of an S-ring with the required parameters, by suitable changes of basis we 'home in' on some unique canonical set which can easily be checked to yield an S-ring with the required parameters. Before starting the proof we prove a general lemma which will be useful.

<u>Lemma 4.2.2</u>. Suppose $\mathcal{S}$ is a rational rank 3 S-ring over $V(n,p)$ in which $\lambda = p-2$. If $\underline{\alpha}$, $\underline{\beta}$ and $\underline{\gamma}$ are distinct lines of Δ, then α, β and γ are linearly independent vectors.

<u>Proof</u>. If false, there are non-zero elements a and b of $GF(p)$ such that $\gamma = a\alpha + b\beta$. But then $\Delta \wedge \Delta + a\alpha$ contains γ as well as p-2 scalar multiples of α. This contradicts $\lambda = p-2$.

<u>Lemma 1</u>. Let G be a (*)-group with parameters $A(p)$. Then we may choose a basis of V such that

(i) $\underline{\Delta} = \{(\underline{0,0,0,1}), (\underline{x,y,1,f(x,y)}): x,y \in GF(p)\}$,

where f is a function from $GF(p) \times GF(p)$ to $GF(p)$,

(ii) $G_{o,\alpha}$ is isomorphic to a subgroup of K, where

$\alpha = (0,0,0,1)$ and K is the group

$$\left\{\begin{pmatrix} A & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} a & b \end{matrix} & c \end{pmatrix} : A \in GL(2,p),\ a,b,c \in GF(p),\ c \neq 0\right\}$$

Proof. (i) We choose a basis for V such that $\alpha = (0,0,0,1) \in \underline{\Delta}$. The residual S-ring is imprimitive, having parameters

$$A_1(p) = (p^2(p-1),\ p^2-1,\ p^2(p-2),\ p^2(p-1)),$$

in which $\mu_1 = k_1$. Hence we have

$$\Delta_1 \cap (\Delta_1 + \gamma) = \Delta_1$$

for any $\gamma \in \Gamma_1$, and so

$$(\Gamma_1 \cup 0) \cap (\Gamma_1 \cup 0) + \gamma = \Gamma_1 \cup 0$$

for any $\gamma \in \Gamma_1$. Hence $\Gamma_1 \cup 0$ is a 2-dimensional subspace of $V(3,p)$. By a suitable choice of basis, we may suppose

$$\Gamma_1 \cup 0 = \{(x,y,0) : x,y \in GF(p)\}.$$

Hence

$$\Delta_1 = \{(x,y,z) : x,y,z \in GF(p),\ z \neq 0\}$$

and therefore

$$\underline{\Delta} = \{\underline{(0,0,0,1)},\ \underline{(x,y,1,f(x,y))}\},$$

where f is a map from $GF(p) \times GF(p)$ to $GF(p)$. f is a well-defined function since if $(x,y,1,s)$ and $(x,y,1,t)$ belong to $\underline{\Delta}$ with $s \neq t$, then

$$(x,y,1,s) = (x,y,1,t) + (0,0,0,s-t),$$

giving a contradiction to $\lambda = p-2$, by Lemma 4.2.2.

(ii) $G_{o,\alpha}$ is isomorphic to a subgroup of $\mathrm{Aut}\,\mathcal{S}_1$, where $\mathcal{S}_1$ denotes the residual S-ring of $\mathcal{S}$. The i-th row of a matrix of $\mathrm{Aut}\,\mathcal{S}_1$, regarded as a vector, lies in the same orbit as $(0,\ldots,1,\ldots0)$, where the 1 is in the i-th place. Since $(1,0,0)$ and $(0,1,0)$ belong to Γ_1, while $(0,0,1)$ belongs to Δ_1, the result follows.

<u>Lemma 2</u>. A basis can be chosen such that $f(x,y) = 0$ if and only if $x = y = 0$.

<u>Proof</u>. We make use of the dual S-ring $\mathcal{S}^{\#}$, which was defined in § 2.2. Recall that $\hat{\Delta}$ denotes the formal sum $\sum_{S \in \Delta} \dot{S}$. If ϕ and ψ are elements of the dual space $V^{\#}$, then it is not difficult to see that since $\mathcal{S}$ is rational, $(\hat{\Delta})\phi = (\hat{\Delta})\psi$ if and only if ϕ and ψ take the same number of zeros on a complete set X of line representatives of Δ. In our case we take

$$X = \{(0,0,0,1),\ (x,y,1,f(x,y)\}:\ x,y \in GF(p)\}$$

Since $\mathcal{S}^{\#}$ has rank 3, an element of $V^{\#} \setminus 0$ takes one of two fixed values on $\hat{\Delta}$. We define $x_1,\ldots,x_4$ as in § 2.3 by

$$\epsilon_j x_i = \delta_{ij},$$

where $\varepsilon_j = (0,\ldots,1,\ldots0)$, the 1 being in the j-th place. Now x_3 takes one zero on X, while x_1 takes p+1 zeros on X. We use a counting argument. Consider the following subset of $V^{\#}$.

$$Y = \{i x_1 + j x_2 + k x_3 + x_4;\quad i,j,k \in GF(p)\}.$$

The total number of zeros taken by Y on X is p^4. Hence we must have p^3-p^2 elements of Y each taking p+1 zeros, and p^2 elementsof Y each taking one zero. Suppose $i_1x_1 + i_2x_2 + i_3x_3 + x_4$ takes just one zero. Then transforming in V by

$$\begin{bmatrix} 1 & 0 & 0 & i_1 \\ 0 & 1 & 0 & i_2 \\ 0 & 0 & 1 & i_3 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

we may assume that x_4 takes just one zero; i.e. exactly one of the f(x,y) is zero. Suppose f(a,b) = 0. Then transforming in V by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -a & -b & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

we may suppose that f(x,y) = 0 if and only if x = y = 0. (Note that neither of the above two transformations changes the form of X).

<u>Lemma 3</u>. $G_{o,\alpha}$ contains a subgroup P of order p^2.

<u>Proof</u>. Since G is a (*)-group, $G_{o,\alpha}$ is transitive on $\underline{\Delta} - \underline{\alpha}$.

But $|\underline{\Delta} - \underline{\alpha}| = p^2$ and so by 1.1.1, p^2 divides the order of $G_{o,\alpha}$.

Lemma 4. A Sylow p-subgroup S of K is non-abelian of exponent p and order p^3. S is isomorphic to

$$\langle A,B,C : CAC^{-1} = A,\ CBC^{-1} = AB,\ BAB^{-1} = A,\ A^p = B^p = C^p = 1\rangle.$$

(K is as in Lemma 1).

Proof. We take $S = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} : a,b,c \in GF(p)\right\}$.

Since S is a Sylow p-subgroup of GL(3,p) it is certainly a Sylow p-subgroup of K. Let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

It is a trivial verification that the given relations hold. The exponent is p (for $p \neq 2$), since

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 & 0 \\ pa & 1 & 0 \\ d & pc & 1 \end{pmatrix}$$

where $d = pb + \frac{p(p-1)}{2} ac$.

Lemma 5. If S is as in Lemma 4, then the subgroups of S of order p^2 are

$$P_t = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & ta & 1 \end{pmatrix} : a,b \in GF(p)\right\}$$

for $t = 0,1,\ldots,p-1$, and

$$P_\infty = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{pmatrix} : a,b \in GF(p)\right\}$$

Proof. Since S has exponent p, any subgroup of order p^2 is elementary abelian. Suppose P has generators $A^{i_1}B^{i_2}C^{i_3}$ and $A^{j_1}B^{j_2}C^{j_3}$, with A, B and C as in Lemma 4. Using the relations given in Lemma 4, we find that these two generators commute if and only if

$$i_2/i_3 = j_2/j_3 .$$

Hence $P = \langle A, B^iC^j\rangle$, for some i and j, not both zero. It easily follows that

$$P = P_t, \text{ where } t = j/i \text{ if } i \neq 0; \quad t = \infty \text{ if } i = 0.$$

Lemma 6. $G_{o,\alpha}$ contains a subgroup of the form

$$\left\{ \begin{pmatrix} 1 & 0 & 0 & h(x,y) \\ 0 & 1 & 0 & g(x,y) \\ x & y & 1 & f(x,y) \\ 0 & 0 & 0 & 1 \end{pmatrix} : x,y \in GF(p) \right\}$$

where f, g and h are functions from $GF(p) \times GF(p)$ to $GF(p)$.

Proof. By Lemmas 1,3,4 and 5, we may assume that P (of Lemma 3) consists of matrices of the form $\begin{pmatrix} A & & & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$, where the matrices A comprise a subgroup Q of $GL(3,p)$, with

$$Q = P_o, P_1, \ldots, P_{p-1} \text{ or } P_\infty .$$

Now P_t is conjugate to P_s for t and s non-zero, for

$$U^{-1}P_t\,U = P_s ,$$

where $U = \begin{pmatrix} t & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & s^{-1} \end{pmatrix}$.

It is therefore sufficient to consider cases $Q = P_o$, P_1 or P_∞.

(i) $Q = P_o$. Then

$$P = \left\{ \begin{pmatrix} 1 & 0 & 0 & h(x,y) \\ x & 1 & 0 & g(x,y) \\ y & 0 & 1 & f(x,y) \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad : \quad x,y \in GF(p) \right\}$$

By Lemma 2, $(0,0,1,0) \in \Delta$, and so the third row of any matrix in G_o may be regarded as a vector in Δ . P is generated by matrices

$$A = \begin{pmatrix} 1 & 0 & 0 & a_1 \\ 0 & 1 & 0 & b_1 \\ 1 & 0 & 1 & c_1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 & 0 & a_2 \\ 1 & 1 & 0 & b_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

for some $a_1, b_1, c_1, a_2, b_2 \in GF(p)$. The group P is elementary abelian, and so $AB = BA$. This implies that

$$a_1 = a_2 = 0 .$$

We now get

$$A^i = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & ib_1 \\ i & 0 & 1 & ic_1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Hence $(i,0,1,ic_1) \in \Delta$ for all $i \in GF(p)$. But any three such vectors are linearly dependent, contradicting $\lambda = p-2$, by Lemma 4.2.2.

(ii) $Q = P_1$: as in (i) we get a contradiction.

Thus $Q = P_\infty$, and P has the required form.

Lemma 7. Δ is as in the statement of Theorem 4.2.1 and the group $O^-(4,p)$ is contained in Aut $\mathcal{S}$, where $\mathcal{S}$ is the S-ring with basis quantities 0, $\hat{\Delta}$ and $\hat{\Gamma}$.

Proof. By Lemma 6, G_0 contains a subgroup generated by

$$A = \begin{pmatrix} 1 & 0 & 0 & a_1 \\ 0 & 1 & 0 & b_1 \\ 1 & 0 & 1 & c_1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 & 0 & a_2 \\ 0 & 1 & 0 & b_2 \\ 0 & 1 & 1 & c_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The third row of the matrix $A^x B^y$ is $(x,y,1,f(x,y))$, where

$$f(x,y) = xya_2 + \frac{y(y-1)}{2} b_2 + yc_2 + \frac{x(x-1)}{2} a_1 + xc_1 ,$$

and since $(0,0,1,0)$ belongs to Δ, a set of line representatives of Δ is

$$X = \{(0,0,0,1),\ (x,y,1,f(x,y)) : x,y \in GF(p)\} .$$

The vectors with $y = 0$ in X are

$$\{(x,0,1,\ \frac{a_1}{2} x^2 + x(c_1 - \frac{a_1}{2}))\}$$

If $a_1 = 0$, then any three of these are linearly dependent and so we must have

$$a_1 \neq 0 .$$

Since $f(1 - \frac{2c_1}{a_1}, 0) = 0$ we have by Lemma 2,

$$a_1 = 2c_1 .$$

Now consider those vectors in X with $x = ky$, some $k \in GF(p)$.

$$f(ky,y) = y^2(ka_2 + \frac{b_2}{2} + \frac{k^2 a_1}{2}) + y(- \frac{b_2}{2} + c_2) .$$

As above, we require the coefficient of y^2 to be non-zero and that of y to be zero. Hence

$$b_2 = 2c_2 \text{ and } k^2 a_1/2 + ka_2 + b_2/2 \neq 0 .$$

This last inequality holds for all k if and only if

$$a_2^2 - a_1 b_2 \text{ is not a square in } GF(p).$$

Writing a, b and c for c_1, c_2 and a_2 respectively, we now have

$$\triangle = \{(x,y,z,w) : wz = ax^2 + by^2 + cxy\},$$

where $c^2 - 4ab$ is not a square.

Consider the quadratic form Q defined by

$$((x_1,y_1,z_1,w_1),(x_2,y_2,z_2,w_2))Q = 2ax_1x_2 + 2by_1y_2 + cx_1y_2$$
$$+ cx_2y_1 - w_1z_2 - w_2z_1 .$$

The matrix of Q is

$$\begin{bmatrix} 2a & c & 0 & 0 \\ c & 2b & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

Since det A = c^2-4ab is a non-square, Q is a quadratic form of type 2. Hence $\triangle$ consists precisely of the non-zero isotropic vectors of Q. If we choose a basis for V such that the matrix of Q is

$$\begin{bmatrix} 2 & e & 0 & 0 \\ e & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

where e^2-4 is a non-square, then we get $\triangle$ as in the statement of Theorem 4.2.1.

Thus $O^-(4,p)$ is contained in the automorphism group of $\mathcal{S}$, the S-ring with basis $0, \hat{\Delta}, \hat{\Gamma}$. So also is Z, the centre of $GL(4,p)$. The semi-direct product $[V]Z.O^-(4,p)$ is not a (*)-group, for the orbits of $Z.O^-(4,p)$ on $V(4,p)$ are

$$\Delta = \{\alpha : (\alpha,\alpha)Q = 0\}$$

$$\Gamma' = \{\alpha : (\alpha,\alpha)Q \text{ is a square}\} \text{ and}$$

$$\Gamma'' = \{\alpha : (\alpha,\alpha)Q \text{ is a non-square}\}$$

We shall see in Lemma 10 that $Z.O^-(4,p)$ is contained in Aut $\mathcal{S}$ as a subgroup of index 2 and that $O^-(4,p)$ has an outer automorphism which maps vectors of Γ' to vectors of Γ''.

<u>Lemma 8</u>. $\left|\dfrac{\text{Aut }\mathcal{S}}{Z}\right| \leq 2(p^2+1)p^2(p^2-1)$

<u>Proof</u>. This will follow from Theorem 1.1.1 if we show that the stabilizer of three lines of $\underline{\Delta}$ in Aut $\mathcal{S}$ has at most order 2. We choose a basis of V such that Δ is as in the statement of 4.2.1. Suppose Zg is an element of $\dfrac{\text{Aut }\mathcal{S}}{Z}$ which fixes the lines $(\underline{0,0,1,0})$, $(\underline{0,0,0,1})$ and $(\underline{1,0,1,1})$. We may choose the coset representative g such that

$$(0,0,1,0)g = (0,0,a,0),\ (0,0,0,1)g = (0,0,0,b) \text{ and}$$
$$(1,0,1,1)g = (1,0,1,1),$$

for some a and b in $GF(p) \setminus 0$. Then

$$(1,0,0,0)g = (1,0,1-a,1-b)$$

and

$$g = \begin{pmatrix} 1 & 0 & 1-a & 1-b \\ h & i & j & k \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & b \end{pmatrix}$$

for some h, i, j, k ε GF(p). Using the fact that the vector $(x,y,1,x^2+y^2+exy)g$ is isotropic for all x and y in GF(p), it is straightforward, though tedious, to show that

$$a = b = 1,\ j = k = 0, \text{ and } (h,i) = (0,1) \text{ or } (-1,e) .$$

Since we have only two solutions for the matrix g, the proof is completed.

Lemma 9. There is an element s of GF(p) (for $p \neq 2$) such that both $-s$ and $1+4s$ are non-squares.

Proof. If $p \neq 2$, $s \mapsto -s$ and $s \mapsto 1+4s$ are both bijections of GF(p) onto GF(p). Since exactly half of the non-zero elements of GF(p) are squares, for the lemma to be false we require that for any t ε GF(p),

$$-t \text{ is a square if and only if } 4t+1 \text{ is a non-square} \quad \ldots(1)$$

Suppose $p \neq 5$. Then $-t = 4t+1$ if $t = -1/5$, contradicting (1), and so the lemma is true for $p \neq 5$. If $p = 5$, then we may take $s = 3$.

Lemma 10. $\dfrac{\mathrm{Aut}\,\mathcal{S}}{Z}$ is isomorphic to an extension of $PO^-(4,p)$ by a cyclic group of order 2.

Proof. We have already shown that $\dfrac{\mathrm{Aut}\,\mathcal{S}}{Z}$ contains $PO^-(4,p)$. By Theorem 4.0.2, $PO^-(4,p)$ has order $p^2(p^2+1)(p^2-1)$ and if we show that Aut $\mathcal{S}$ contains an element of PGL(4,p) not lying in $PO^-(4,p)$, then the result will follow by Lemma 8. We now find it convenient to change the basis of V so that the matrix of Q is

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & -2s & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

where s is chosen such that $-s$ and $4s+1$ are non-squares. Since $\det A = 1+4s$, Q is indeed equivalent to our earlier form. Now consider the element Zg of $PGL(4,p)$, where

$$g = \begin{pmatrix} 0 & 1 & 0 & 0 \\ s & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -s \end{pmatrix}$$

Then

$$(x,y,z,w)g = (sz,x+y,z,-sw).$$

Hence if $\alpha = (x,y,z,w)$, then

$$(\alpha,\alpha)Q = 2(x^2-sy^2+xy-wz)$$

whereas

$$(\alpha g,\alpha g)Q = -2s(x^2-sy^2+xy-wz) .$$

Since $-s$ is a non-square, g does not belong to $PO^-(4,p)$. But if $(\alpha,\alpha)Q = 0$, then $(\alpha g,\alpha g)Q = 0$, and hence $g \in \mathrm{Aut}\,\mathcal{S}$.

This completes the proof of Theorem 4.2.1.

Let $\mathcal{S}$ be the S-ring given by 4.2.1. We will show that for all primes p (including 2), the permutation group $\frac{\mathrm{Aut}\,\mathcal{S}}{Z}$ acting on $\underline{\Delta}$ is isomorphic to $P\Gamma L(2,p^2)$ acting on $PG(1,p^2)$. We first define the group $P\Gamma L(2,p^2)$.

By a <u>semi-linear transformation</u> of a vector space V over a field F we mean a bijection T from V onto V such that for some automorphism t of F, we have for all $\alpha,\beta \in V$, $a \in F$,

$$(\alpha+\beta)T = \alpha T + \beta T, \quad (a\alpha)T = at(\alpha T) .$$

It is shown in (10.6.9) of [18] that the set of semilinear transformations of V is a group, denoted by $\Gamma L(V)$, containing the group of linear transformations GL(V) as a normal subgroup, and that $\Gamma L(V)/GL(V)$ is isomorphic to the automorphism group of F. We let $P\Gamma L(V)$ denote the group $\frac{\Gamma L(V)}{Z}$, where Z denotes the group of linear maps of the form

$$\alpha T = a\alpha$$

for all $\alpha \in V$, some $a \in F$.

If F is $GF(p^2)$, then its automorphism group has order 2. Hence the order of $P\Gamma L(2,p^2)$ is $2(p^2+1)p^2(p^2-1)$.

Theorem 4.2.3. Let $\mathcal{S}$ be as in 4.2.1. Then $\frac{\operatorname{Aut}\mathcal{S}}{Z}$ acting on Δ is isomorphic to $P\Gamma L(2,p^2)$ acting on $PG(1,p^2)$.

Proof. (i) $p = 2$. Since $P\Gamma L(2,4)$ acts on 5 points of $PG(1,4)$, and has the same order as the symmetric group S_5, we must have the required isomorphism.

(ii) $p \neq 2$. We let Q be the quadratic form over $V(4,p)$ with matrix as in the proof of Lemma 10. Now the polynomial x^2-x-s is irreducible over $GF(p)$, since $1+4s$ is a non-square. Thus

$$GF(p^2) = \{a\lambda + b \; : \; a,b \in GF(p)\} ,$$

where λ is the primitive (p^2-1)-th root of unity in $GF(p^2)$, satisfying the equation

$$\lambda^2 - \lambda - s = 0 .$$

We have

$$\Gamma L(2,p^2) = [GL(2,p^2)]\langle\tau\rangle,$$

where τ is the map which sends (α,β) to (α^p,β^p) for all $(\alpha,\beta) \in V(2,p^2)$.

We get a permutation isomorphism θ as follows.

θ : $\underline{\Delta} \to PG(1,p^2)$ is defined by

θ : $(\underline{0,0,0,1}) \mapsto (\underline{1,0})$

and $(\underline{x,y,1,x^2-y^2s+xy}) \to (\underline{y\lambda+x,1})$,

for all $x,y \in GF(p)$, while

θ : $[PO^-(4,p)]C_2 \to P\Gamma L(2,p^2)$

is given by its action on the following generators (the 4×4 and 2×2 matrices should be read modulo the centres of $GL(4,p)$ and $GL(2,p^2)$ respectively).

$$\theta : \begin{bmatrix} 0 & 1 & 0 & 0 \\ s & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -s \end{bmatrix} \mapsto \begin{bmatrix} \lambda & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mapsto \tau, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \mapsto \tau\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We omit the straightforward verification that θ is a permutation isomorphism.

We now consider certain subgroups of the two isomorphic groups above. From now on our discussion holds only for

$p \neq 2$. By $SL(2,p^2)$ we mean the group of linear transformations of $V(2,p^2)$ which have determinant 1, and by $PSL(2,p^2)$ the quotient of this group by the subgroup of scalar matrices. By $P\Omega^-(4,p)$ we mean a certain normal subgroup of index 2 in $PO^-(4,p)$. The precise definition may be found in [1] or [+]. It is well known that $PSL(2,p^2)$ and $P\Omega^-(4,p)$ are isomorphic groups (See e.g. [1]). The restriction of θ above to $PSL(2,p^2)$ gives such an isomorphism. We now see how the larger groups on each side of the isomorphism correspond. One might expect the outer automorphisms of $PO^-(4,p)$ and $PGL(2,p^2)$ to correspond; this is not in fact the case. From the definition of θ we see that $(\tau)\theta^{-1}$ belongs to $PO^-(4,p)$, whereas θ maps the outer automorphism of $PO^-(4,p)$ to $Z\begin{pmatrix}\lambda & 0\\ 0 & 1\end{pmatrix}$, which belongs to $PGL(2,p^2)$. We thus have the following isomorphisms:

$$
\begin{tikzcd}[column sep=small]
 & {[PO^-(4,p)]C_2} \arrow[dl, dash] \arrow[dr, dash] & & & & P\Gamma L(2,p^2) \arrow[dl, dash] \arrow[dr, dash] & \\
{[P\Omega^-(4,p)]C_2} \arrow[dr, dash] & & PO^-(4,p) \arrow[dl, dash] \arrow[r, "\theta"] & {} & PGL(2,p^2) \arrow[dr, dash] & & {[PSL(2,p^2)]\langle\tau\rangle} \arrow[dl, dash] \\
 & P\Omega^-(4,p) & & & & PSL(2,p^2) &
\end{tikzcd}
$$

We now prove some further facts of interest about our S-rings with parameters $\Lambda(p)$.

A <u>Steiner system</u> $S(t,k,v)$ denotes a block design which has v points, k points lying in each block, with any set of t points lying in exactly one block.

Theorem 4.2.4. If $\mathcal{S}$ is as in 4.2.1, then Aut $\mathcal{S}$ is an automorphism group of the Steiner system $S(3,p+1,p^2+1)$.

Proof. As the points of the design we take the elements of $\underline{\Delta}$, where Δ is as in 4.2.1. As blocks we take subsets of $\underline{\Delta}$ generated by three lines, i.e. the blocks are the sets $\underline{\Delta \wedge \langle\alpha,\beta,\gamma\rangle}$, for distinct $\underline{\alpha}$, $\underline{\beta}$, $\underline{\gamma} \in \underline{\Delta}$. Since $\underline{\Delta}$ admits a 3-transitive automorphism group G_o, G_o act transitively on the blocks and hence each contains the same number of points. The block containing $(\underline{0,0,1,0})$, $(\underline{0,0,0,1})$ and $(\underline{1,0,1,1})$ is

$$\{(\underline{0,0,0,1}),\ (\underline{x,0,1,x^2}) : x \in GF(p)\} .$$

Hence $k = p+1$ and we have the required design.

The number of blocks in the design is $p(p^2+1)$ which we observe is the same as the number of points of $\underline{\Gamma}$. We show in our next theorem that the representation of Aut $\mathcal{S}$ is the same in each case.

Theorem 4.2.5. The permutation representations of Aut $\mathcal{S}$ on $\underline{\Gamma}$ and of Aut $\mathcal{S}$ on the blocks of the associated Steiner system are isomorphic.

Proof. (i) $p = 2$. Recall that in this case we may take

$$\underline{\Delta} = \{(1,0,0,0),\ (0,1,0,0),\ (0,0,1,0),\ (0,0,0,1),\ (1,1,1,1)\}.$$

The blocks of $S(3,3,5)$ are simply all subsets of three vectors (for $p = 2$, vectors and lines are the same thing). We define a map ϕ from the set of blocks to Γ by

$$(B)\phi = \sum_{\alpha \in B} \alpha$$

for each block B. By the linearity of Aut $\mathcal{S}$ on V, it follows that the action of Aut $\mathcal{S}$ on the two sets is the same.

(ii) $p \neq 2$. In this case Γ is the set of non-isotropic lines under $PO^-(4,p)$. For each $\alpha \in \Gamma$, we let $\alpha^\perp$ denote the set

$$\{\beta \in V : (\alpha,\beta)Q = 0\} .$$

Then $\alpha^\perp$ is a three-dimensional subspace such that

$$V = \langle\alpha\rangle + \alpha^\perp .$$

Let $\Gamma^\perp = \{\alpha^\perp : \alpha \in \Gamma\}$. Since $PO^-(4,p)$ and its outer automorphism preserve zero scalar products, Aut $\mathcal{S}$ has the same action on Γ as on $\Gamma^\perp$. It can easily be shown that for a quadratic form over $V(3,p)$ there are $p+1$ isotropic lines. Hence under Q restricted to $\alpha^\perp$, $\alpha^\perp$ contains $p+1$ isotropic lines and these must form a block of the Steiner system. The result now follows.

We conclude this subsection with a conjecture. We have proved that an S-ring $\mathcal{S}$ with parameters $A(p)$ is unique under certain assumptions about Aut $\mathcal{S}$. Looking at small primes suggests that such assumptions are unnecessary. More generally we can show that an S-ring with parameters $A(p)$ is unique provided the following combinatorial result holds.

<u>Conjecture 4.2.6</u>. Let θ be a permutation of the non-zero elements $\{1,\dots,p-1\}$ of $GF(p)$, with $(1)\theta = 1$. Then a necessary and sufficient condition for the set

$$X = \{(1,x,(x)\theta) : x = 1,\dots,p-1\}$$

to have the property that any three vectors of X are linearly independent is that $(x)\theta = x^{-1}$ for all $x \in GF(p)\setminus 0$.

§ 4.3 (*)-groups of degree 3^5.

Theorem 4.3.1. There is a unique S-ring $\mathcal{S}$ over $V(5,3)$ having parameters $B = (22, 220, 1, 2)$. $\frac{\text{Aut } \mathcal{S}}{Z}$ is isomorphic to the Mathieu group M_{11}, and $[V]Z.M_{11}$ is a (*)-group.

The proof is broken down into Lemmas 1, 2 and 3.

Lemma 1. The residual S-ring $\mathcal{S}_1$ over $V(4,3)$ with parameters B_1 is unique.

Proof. We found in § 4.0 that the residual S-ring $\mathcal{S}_1$ has parameters

$$B_1 = (20, 60, 1, 6) = A(3).$$

In § 4.2 we showed that an S-ring $\mathcal{S}$ with parameters $A(p)$ is unique for all p, with the assumption that $\mathcal{S}$ admits a suitable automorphism group. For p = 3, we prove the uniqueness without such an assumption. Suppose

$$V(4,p) = 0 \cup \Delta_1 \cup \Gamma_1$$

where $\mathcal{S}_1$ has basis quantities 0, $\hat{\Delta}_1$ and $\hat{\Gamma}_1$. By Lemmas 1 and 2 of § 4.2 (which did not assume knowledge of Aut $\mathcal{S}$), a basis of $V(4,p)$ may be chosen such that

$$\underline{\Delta}_1 = \{\underline{(0,0,0,1)}, \underline{(x,y,1,f(x,y))} : x,y \in GF(3)\}$$

where f is a function from $GF(3) \times GF(3)$ to $GF(3)$, which has the property that

(1) $f(x,y) = 0$ if and only if $x = y = 0$.

Let $\chi_1, \chi_2, \chi_3, \chi_4$ generate $V^{\#}$ as in § 2.3, and let

$$X_1 = \{(0,0,0,1), (x,y,1,f(x,y)) : x,y \in GF(3)\}$$

be a set of line representatives of Δ_1. χ_1 takes four zeros on X_1, while χ_3 takes one zero. Hence, as in Lemma

2 of § 4.2, every element of $V^{\#}$ takes either one or four zeros on X_1. It follows from (1) that $x_3 + x_4$ and $2x_3 + x_4$ take a total of eight zeros and hence take four each. Thus

$$\{f(x,y) : x,y \in GF(p)\} = \{0,1,1,1,1,2,2,2,2\} \quad \ldots (2)$$

with $f(0,0) = 0$. Suppose (x_1, y_1) and (x_2, y_2) satisfy

$$f(x_1, y_1) = f(x_2, y_2) = \cancel{2}\, 1$$

Transforming by

$$\begin{pmatrix} x_1 & y_1 & 0 & 0 \\ x_2 & y_2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1}$$

we may suppose that

$$f(1,0) = f(0,1) = 1 .$$

(Note: when we transform in V, i.e. change basis, we must make sure that the form of X_1 remains the same, only the unknown $f(x,y)$ undergoing any change). We now have in Δ_1 the elements (0,0,1,0), (0,0,0,1), (1,0,1,1) and (0,1,1,1). But

$$2(0,0,1,0) + 2(1,0,1,1) = (2,0,1,2),$$

and so by Lemma 4.2.2, (2,0,1,2) belongs to Γ_1. Hence $f(2,0) = 1$, and similarly $f(0,2) = 1$. We now have four of the $f(x,y)$ equal to 1, and by (2) the remaining $f(x,y)$ must all be equal to 2. Thus $\Delta_1 = X_1 \cup 2X_1$, where

$$X_1 = \{(0,0,1,0), (0,0,0,1), (1,0,1,1), (2,0,1,1), (0,1,1,1), (0,2,1,1), (1,1,1,2), (2,2,1,2), (1,2,1,2), (2,1,1,2)\}$$

i.e. Δ_1 consists of those points (x,y,z,w) satisfying

$$wz = x^2 + y^2 .$$

<u>Lemma 2</u>. An S-ring $\mathcal{S}$ over $V(5,3)$ with parameters B is unique.

<u>Proof</u>. By Lemma 1 there are elements a_{ij} in $GF(p)$ such that a set of line representatives of Δ is

$$
\begin{aligned}
X = \{&(0,0,0,0,1)\\
&(0,0,0,1,0)\\
&(0,0,1,0,0)\\
&(1,0,1,1,a_{10})\\
&(2,0,1,1,a_{20})\\
&(0,1,1,1,a_{01})\\
&(0,2,1,1,a_{02})\\
&(1,1,1,2,a_{11})\\
&(2,2,1,2,a_{22})\\
&(1,2,1,2,a_{12})\\
&(2,1,1,2,a_{21})\}
\end{aligned}
$$

Transforming in V by

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & -a_{10}\\
0 & 1 & 0 & 0 & -a_{01}\\
0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$

we may suppose

$$a_{10} = a_{01} = 0 .$$

Now x_1 takes five zeros on X, while x_4 takes two zeros. Since the dual S-ring has rank 3, every element of $V^{\#}$ takes two or five zeros on X. Now

$$(X)x_5 = \{1,0,0,0,0,a_{20},a_{02},a_{11},a_{22},a_{12},a_{21}\}.$$

Hence x_5 takes five zeros and so just one more a_{ij} is zero.

We may suppose a_{20} is non-zero; for if $a_{20} = 0$ we transform by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Transforming by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

if necessary, we may suppose that

$$a_{20} = 1 .$$

We now have

$$(X)\, x_3 + x_4 + x_5 = \{1,1,1,2,2,0,2 + a_{02}, a_{11}, a_{22}, a_{12}, a_{21}\}.$$

Since exactly one of the unknown a_{ij} is zero, $x_3 + x_4 + x_5$ takes two zeros on X, and so we must have

$$a_{02} = 2 .$$

Hence just one of a_{11}, a_{22}, a_{12}, a_{21} is zero, and we consider these four cases separately, making use of the fact that the following sets have two or five zeros.

(i) $(X)x_1 + x_5 = \{1,0,0,1,0,0,2,1+a_{11},2+a_{22},1+a_{12},2+a_{21}\}$

(ii) $(X)x_2 + x_5 = \{1,0,0,0,1,1,1,1+a_{11},2+a_{22},2+a_{12},1+a_{21}\}$

(iii) $(X)x_4 + x_5 = \{1,1,0,1,2,1,0,2+a_{11},2+a_{22},2+a_{12},2+a_{21}\}$.

<u>Case 1</u>. $a_{11} = 0$. By (ii), $a_{22} = a_{12} = a_{21} = 1$ or 2. By (i), the latter holds to give five zeros in $(X)\chi_1 + \chi_5$. But then $(X)\chi_2 + \chi_5$ has just one zero. Hence this case can not occur.

<u>Case 2</u>. $a_{22} = 0$. Transforming by

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

we get case 1 and hence a contradiction.

<u>Case 3</u>. $a_{12} = 0$. As in case 1 we get

$$a_{21} = a_{11} = a_{22} = 2 .$$

This does not lead to a contradiction.

<u>Case 4</u>. As in Case 2, we can change basis to get case 3.

Hence we may choose a basis for V such that an S-ring $\mathcal{S}$ over V(5,3) with parameters B has simple basis quantities 0, $\hat{\Delta}$ and $\hat{\Gamma}$, where $\Delta = X \cup 2X$, with

$$X = \{(0,0,0,0,1),\ (0,0,0,1,0),\ (0,0,1,0,0),$$
$$(1,0,1,1,0),\ (2,0,1,1,1),\ (0,1,1,1,0),$$
$$(0,2,1,1,2),\ (1,1,1,2,2),\ (2,2,1,2,2),$$
$$(1,2,1,2,2),\ (2,1,1,2,0)\}$$

<u>Lemma 3</u>. Let $\mathcal{S}$ be the S-ring over V(5,3) with parameters B. Then $\frac{\text{Aut}\,\mathcal{S}}{Z}$ is isomorphic to the Mathieu group M_{11}.

<u>Proof.</u> Let $\alpha = (0,0,0,0,1)$. The stabilizer $(\mathrm{Aut}\,\mathcal{S})_\alpha$ is isomorphic to a subgroup of Aut $\mathcal{S}_1$. Given an automorphism A_1 of $\mathcal{S}_1$ (A_1 represented by a matrix in $GL(4,3)$), we must find whether we can choose $a, b, c, d, e \in GF(3)$ such that

$$A = \begin{bmatrix} & & & & a \\ & & & & b \\ & A_1 & & & c \\ & & & & d \\ 0 & 0 & 0 & 0 & e \end{bmatrix}$$

is an automorphism of $\mathcal{S}$. For example, consider the matrix

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

of Aut $\mathcal{S}_1$. If A_1 'extends' to A, then since the third and fourth rows of A may be regarded as elements of Δ, we have (we take Δ as given by Lemma 2)

$$c = 0 \quad \text{and} \quad d = 0 .$$

Now $(1,0,1,1,0)A = (0,1,1,1,a)$ belongs to Δ and so

$$a = 0$$

Also $(0,1,1,1,0)A = (1,0,1,1,b)$, and so

$$b = 0 .$$

Since $(2,0,1,1,1)A = (0,2,1,1,e)$, we have

$$e = 2 .$$

It is easy to check that the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

does indeed fix Δ as a set, and hence belongs to Aut $\mathcal{S}$. We can show similarly that the matrices of

$$\mathrm{Aut}\,\mathcal{S}_1 = [PO^-(4,3)]C_2$$

which extend as above are precisely those lying in $P\Omega^-(4,3)$. Hence $(\mathrm{Aut}\,\mathcal{S})_{\underline{\alpha}}$ is isomorphic to $P\Omega^-(4,3)$, and therefore has order 10.9.8, acting sharply 3-transitively on the ten points of $\underline{\Delta} \setminus \underline{\alpha}$.

It will now follow that Aut $\mathcal{S}$ is sharply 4-transitive on $\underline{\Delta}$ if we find an element of Aut $\mathcal{S}$ which does not fix $(\underline{0,0,0,0,1})$. In finding such an element we also demonstrate a technique which we have found very useful for finding automorphisms of a given S-ring over a vector space. Because of the desired high transitivity of Aut $\mathcal{S}$, it is likely that there is an automorphism which fixes several points of $\underline{\Delta}$. In this case we guess that there is a matrix B in Aut $\mathcal{S}$ satisfying

$$(0,0,0,1,0)B = (0,0,0,1,0),\ (0,0,1,0,0)B = (0,0,2,0,0)$$

$$(1,0,1,1,0)B = (1,0,1,1,0) \text{ and } (0,0,0,0,1)B = (0,1,1,1,0)$$

Suppose

$$(0,1,1,1,0)B = \alpha,$$

for some $\alpha \in \Delta$. Now

$$(0,2,1,1,2) = 2(0,1,1,1,0) - (0,0,0,1,0) - (0,0,1,0,0) + 2(0,0,0,0,1)$$

and hence

$$(0,2,1,1,2)B = 2\alpha + (0,2,1,0,0).$$

(0,2,1,0,0) belongs to Γ , and since $\mu = 2$, we have

$$|\Delta \cap \Delta + (0,2,1,0,0)| = 2 .$$

In fact, $\Delta \wedge \Delta + (0,2,1,0,0) = \{(1,0,2,2,2), (2,2,2,1,1)\}$ Hence $\alpha = (1,0,2,2,2)$ or $(2,2,2,1,1)$. We now know the action of B on five independent vectors and hence can find its matrix. With the latter value of α, it turns out that B does not belong to Aut $\mathcal{S}$. But with the former we get

$$B = \begin{bmatrix} 1 & 0 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

which is easily checked to stabilize Δ as a set and hence belongs to Aut $\mathcal{S}$.

We now have that $\frac{\text{Aut}\,\mathcal{S}}{Z}$ is sharply 4-transitive on the eleven points of $\underline{\Delta}$, and hence has order $11.10.9.8 = 7920$. The fact that $\frac{\text{Aut}\,\mathcal{S}}{Z}$ is isomorphic to the Mathieu group M_{11} follows from Theorem 5.8.1 of [8], where it is shown that M_{11} is the only 4-transitive group on 11 letters, in which the stabilizer of 4 points has odd order. Alternatively we can show that $\frac{\text{Aut}\,\mathcal{S}}{Z}$ is M_{11} by means of the characterization of M_{11} as the automorphism group of the Steiner system S(4,5,11) (See [23]). This Steiner system with automorphism group Aut $\mathcal{S}$ arises in this case as in Theorem 4.2.4. The points are those of $\underline{\Delta}$, the blocks those subsets $\underline{\Delta \wedge W}$, where W is any 4-dimensional subspace of V(5,3) having four linearly independent vectors in Δ.

The proof of Lemma 3, and hence of Theorem 4.3.1, is now completed.

From the 3-transitive group $P\Omega^{-}(4,p)$ on 10 points of

PG(3,3), we have constructed a 4-transitive group on 11 points of PG(4,3). We now consider the more general situation: given a subset Δ_1 of V(n-1,p) admitting a linear group t-transitive on Δ_1, does there exist a subset Δ of V(n,p) admitting a subgroup of GL(n,p) which is (t+1)-transitive on Δ and such that $(0,\ldots,0,1) \in \Delta$ and

$\Delta_1 = \{(x_1,\ldots,x_{n-1}):(x_1,\ldots,x_n) \in \Delta$, some $x_n \in GF(p)\} \setminus \{0\}$?

(c.f. definition of the residual S-ring). We call Δ an <u>extension</u> of Δ_1.

<u>Theorem 4.3.2.</u> Let Δ_1 be that subset Δ of V(4,p) given by Theorem 4.2.1. Then

(i) for p = 2, there is an infinite sequence of extensions.

(ii) for p = 3, we can extend twice only.

(iii) for p > 3, extensions do not exist.

<u>Proof.</u> (i) p = 2: for any $n \geq 2$, let Δ be the set

$$\{(1,0,\ldots 0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1),(1,1,\ldots,1)\}.$$

Any permutation of the n+1 points of Δ acts linearly on Δ. Thus we can extend indefinitely, getting automorphism groups S_5, S_6, $S_7,\ldots$ acting on V(n,2) for n = 4,5,6,...

(ii) p > 2: If there is a subgroup of PGL(5,p) acting 4-transitively on p^2+2 points, then $(p^2+2)(p^2+1)p^2(p^2-1)$ divides the order of PGL(5,p). This implies that

$$p^2+2 \text{ divides } (p^5-1)(p^2-1)(p^3-1)$$

and hence that

$$p^2+2 \text{ divides } 3^2(2p-17) .$$

This is clearly not true for p > 3, but is for p = 3. Indeed we have already seen that an extension exists for p = 3;

we get M_{11} acting 4-transitively on 11 points of $PG(4,3)$. It can be shown in a similar way (we omit the lengthy proof) that a further extension exists: a set of 12 points of $PG(5,3)$ acted on 5-transitively by the Mathieu group M_{12}. This representation of M_{12} was constructed in a different way by Coxeter [2]. It can be shown that there is no further extension to a 6-transitive group on 13 points.

Let $G = [V]G_o$, where G_o is the subgroup of $GL(n,p)$ as given by the above extensions. We give the ranks $r(p)$ of such permutation groups G below

$n =$	4	5	6	7	8	9	10	. . .
$r(2)$:	3	4	4	5	5	6	6	. . .
$r(3)$:	3	3	4					
$r(5)$:	3							
$r(7)$:	3							
⋮	⋮							

We look at the case $(p,n) = (3,6)$ more closely. It is not difficult to find the orbits of M_{12} on $PG(5,3)$; there are three of them, containing 12, 132 and 220 points. Hence $[V(6,3)]Z.M_{12}$ is a rank 4 group with subdegrees 1, 24, 264 and 440. We now consider the corresponding S-ring and its dual. Recall that if the S-ring $\mathcal{S}$ is the transitivity module $C(V,G_o)$, then its dual $\mathcal{S}^{\#}$ is $C(V^{\#},G_o')$, where G_o' consists of the transposes of matrices in G_o (See Theorem 2.3.1) The following diagram gives the orbit lengths of M_{12}, M_{11} and $PSL(2,11)$ in their actions as $\frac{G_o}{Z}$ and $\frac{G_o'}{Z}$ on the lines of $V(6,3)$ and $V(6,3)^{\#}$ respectively.

$\frac{G_o}{Z}$	line orbits under $\frac{G_o}{Z}$										line orbits under $\frac{G_o'}{Z}$									
M_{12}	12 Δ		132				220				12		132				220			
M_{11}	1	11	22		110		220				12		66		66		55	165		
PSL(2,11)	1	11	11	11	55	55	55	55	55	55	1	11	11	55	11	55	55	55	55	55

The orbit lengths on the left were found directly by finding the orbits of G_o on $V(6,3)$. Those on the right could be obtained similarly by finding the orbits of G_o' on $V(6,3)^{\#}$. However, it is easier to find them by means of the results of Tamaschke (2.2.3 and 2.2.4). Consider first the rank 4 group $[V]Z.M_{12}$. Let the n_i and f_i be as defined in 2.2.7. Then

$$\{n_1,n_2,n_3,n_4\} = \{1,24,264,440\}$$

By Theorems 2.2.4 and 2.2.6

$$3^{12}.\frac{24.264.440}{f_2\ f_3\ f_4} \quad \text{is the square of a 3-power,}$$

where

$$f_2 + f_3 + f_4 = 24 + 264 + 440.$$

It is easy to show that the only possibility is

$$\{f_2,f_3,f_4\} = \{n_2,n_3,n_4\}$$

The action of the subgroup M_{11} of M_{12} is obtained by fixing a line in the orbit Δ (See diagram). Since $[V(5,3)]Z.M_{11}$ is a rank 3 group with subdegrees 1, 22, 220, we have by 2.2.4,

$$3^5.\frac{22.220}{f_2 f_3} \quad \text{is the square of a 3-power,}$$

where

$$f_2 + f_3 = 242.$$

The only possibility is

$$\{f_2, f_3\} = \{110,\ 132\}.$$

(This could also be obtained from Higman's formula (1.2.6)). We may assume that f_2 and f_3 for this case are f_2 and f_3 of the rank 6 group $[V(6,3)]Z.M_{11}$. It can now be shown, using 2.2.4, that for this group

$$\{f_2, f_3, f_4, f_5, f_6\} = \{24,\ 132,\ 132,\ 110,\ 330\}$$

Hence we get the line orbit lengths as in the diagram. Similarly, the subgroup of M_{11} isomorphic to $PSL(2,11)$ has orbits as shown.

The permutation group $[V(6,3)]Z.M_{11}$ is of particular interest for several reasons.

(1) It gives rise to nine distinct permutation representations of M_{11}, including the 3-transitive representation of degree 12.

(2) It gives one of the few examples we know of an S-ring over a vector space in which the subdegrees of $\mathcal{S}$ are different from those of $\mathcal{S}^{\#}$.

(3) It gives an answer to the following question raised by Wielandt (p.93, [22]): in a permutation group, if the n_i are all different, does it follow that the f_i are all different? In this case

$$\{n_1, \ldots, n_6\} = \{1,\ 2,\ 22,\ 44,\ 220,\ 440\},$$

while

$$\{f_1, \ldots, f_6\} = \{1,\ 24,\ 132,\ 132,\ 110,\ 330\}.$$

§ 4.4. The 3^6 case.

In this section $\mathcal{S}$ will denote an S-ring over V(6,3) with parameters

$$C = (2.56,\ 2.308,\ 1,\ 20),$$

and $\mathcal{S}_1$ its residual. In § 4.0, we saw that $\mathcal{S}_1$ has parameters

$$C_1 = (2.55,\ 2.66,\ 37,\ 60).$$

Theorem 4.4.1. An S-ring $\mathcal{S}_1$ over V(5,3) with parameters C_1 is unique. $\dfrac{\mathrm{Aut}\ \mathcal{S}_1}{Z}$ is isomorphic to the Mathieu group M_{11}.

Proof. We proved earlier (Theorem 4.3.1) that an S-ring over V = V(5,3) with parameters

$$B = (22,\ 220,\ 1,\ 2)$$

is unique. It is isomorphic to the transitivity module $C(V,\ G_o)$ where G_o/Z is isomorphic to the group M_{11}. By (1.2.6) the corresponding rank 3 group $G = [V]G_o$ has

$$\{f_1, f_2, f_3\} = \{1,\ 110,\ 122\},$$

and by 2.2.6, these are the subdegrees of $C(V,\ G_o)^{\#}$. Hence if $\mathcal{S}_1$ has parameters C_1, $\mathcal{S}_1^{\#}$ has parameters B and so is isomorphic to $C(V,\ G_o)$. Thus $\mathcal{S}_1 = \mathcal{S}_1^{\#\#}$ is unique and by 2.3.1, $\dfrac{\mathrm{Aut}\ \mathcal{S}_1}{Z}$ is isomorphic to $\dfrac{\mathrm{Aut}\ \mathcal{S}_1^{\#}}{Z}$, i.e. to M_{11}.

From the uniqueness of the residual S-ring $\mathcal{S}_1$, no doubt a unique extension could be constructed as in Theorem 4.3.1. However, this would be an arduous task with $|\Delta|$ so large as 56, and since we will construct an S-ring with parameters C by other means, we will content ourselves with the following more modest result about the uniqueness of Aut $\mathcal{S}$

Theorem 4.4.2. Suppose $\mathcal{S}$ is a rank 3 S-ring over V(6,3) with parameters C and basis O, $\hat{\Delta}$, $\hat{\Gamma}$. If $\mathcal{S}$ admits an automorphism group G_o transitive on Δ and such that the minimal normal subgroup of $\frac{G_o}{Z}$ is simple, then G_o/z is isomorphic to either PSL(3,4) or [PSL(3,4)]C_2 .

Note. Suppose G = [V]G_o is a (*)-group with parameters C. Then G_o/Z is 2-transitive on $\underline{\Delta}$. Let N/Z be a minimal normal subgroup of G_o/Z. By a Theorem of Burnside (12.4 of [22]) every non-regular minimal normal subgroup of a doubly transitive group is elementary abelian and hence has degree p^n for some prime p. But in our case the degree of G_o/Z on $\underline{\Delta}$ is 56, which is not a prime power, and so N/Z is non-regular and hence primitive and simple. Since primitive groups are transitive this shows that the (*)-group G will be given by Theorem 4.4.2. In fact the theorem shows that (*)-groups with parameters C do not exist and this is why we weaken the conditions on Aut $\mathcal{S}$ so as to trap an S-ring with the required parameters.

Proof of 4.4.2. The stabilizer of a point of $\underline{\Delta}$ in G_o/Z is isomorphic to a subgroup of $\frac{\text{Aut}\,\mathcal{S}_1}{Z}$ which by 4.4.1 is isomorphic to M_{11}. By Theorem 1.1.1 we get

(A): 56 divides $|N/Z|$ divides $|G/Z|$ divides 56.11.10.9.8.

M. Hall has shown that any unknown simple group of order less than 1,000,000 must have one of twenty-one possible orders, and condition (A) ensures that $|N/Z|$ can be none of these. The only known simple groups whose order satisfies (A) are

(1) the Mathieu group M_{22} of order 56.11.10.9.8.

(2) the alternating group A_7 of order 56.5.9.

(3) the alternating group A_8 of order 56.10.9.4.

(4) the projective special linear group of dimension 3 over GF(4), denoted by PSL(3,4), of order 56.10.9.4.

Case (1). If N/Z is isomorphic to M_{22}, then the stabilizer $(N/Z)_{\alpha}$ ($\alpha \in \Delta$) has order 11.10.9.8 and hence is isomorphic to M_{11}, being a subgroup of the same order. But it is known that M_{11} is not a subgroup of M_{22}, and so this case cannot occur.

Case (2). By examination of the character table of A_7, we find that no set of permutation characters and subdegrees of this group fulfils the conditions of Frame's Theorem, 2.2.7, for A_7 to have a transitive representation on 56 points.

Case (3). A_8 does have a representation on 56 points, namely its natural action on the unordered triples of 8 symbols. But the stabilizer of a triple contains an element of order 15, which gives a contradiction, since M_{11} contains no elements of order 15.

Case (4). Suppose N/Z is isomorphic to PSL(3,4). From Frame's result (2.2.7) and examination of the character table of PSL(3,4) we find that the only possible representation of PSL(3,4) on 56 points is one of rank 3 with subdegrees 1, 10, 45 and associated character degrees f_1, f_2, f_3 = 1, 20, 35. We will see later that this case occurs.

Now consider possible orders of G_o/Z satisfying (A).

(a) Suppose $|G_o/Z| = 56.11.10.9.8$. Let $\alpha \in \Delta$.
Then $(G_o/Z)_{\underline{\alpha}}$ is isomorphic to M_{11}, and $(N/Z)_{\underline{\alpha}}$ is a proper normal subgroup of $(G_o/Z)_{\underline{\alpha}}$, contradicting the simplicity of M_{11}.

(b) Suppose $|G_o/Z| = 56.11.10.9.4$. Then $(G_o/Z)_{\underline{\alpha}}$ is isomorphic to a subgroup of M_{11} of index 2, again contradicting the simplicity of M_{11}.

(c) There remain only the possibilities that G_o/Z has order 56.10.9.8 or 56.10.9.4 and hence is isomorphic to PSL(3,4) or an extension of this group by C_2.

In our next theorem we exhibit an S-ring satisfying the hypotheses of Theorem 4.4.2. This result arose out of a suggestion by B. Fischer that since the number of isotropic lines of V(6,3) under $O^-(6,3)$ is 112, the desired suborbit $\underline{\Delta}$ might consist of half of the isotropic lines.

Theorem 4.4.3. There exists an S-ring $\mathcal{S}$, with parameters C, whose automorphism group is isomorphic to [PSL(3,4)]C_2.

Proof. Since the details of the proof run into many pages we give only an outline. By Theorem 4.0.2, the orthogonal group $O^-(6,3)$ has 224 isotropic points(i.e. 112 isotropic lines). Let I denote the set of isotropic points. We guess that under the action of some subgroup M of $O^-(6,3)$, I splits into two orbits each with 112 points, and that one of these orbits, Δ, gives a simple basis quantity $\hat{\Delta}$ for a rank 3 S-ring $\mathcal{S}$ over V(6,3). Since we require that M be transitive on 56 lines we may assume M contains an element of order 7.

<u>Step 1</u>: Find an element of order 7 lying in an orthogonal group $O^-(6,3)$.

Let T be the element

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}$$

of $GL(6,3)$. T has order 7. We will find a quadratic from Q with matrix A such that T is an isometry with respect to Q (these terms were defined in § 4.0). By taking various pairs α, β of basis vectors and using

$$(\alpha T, \beta T)Q = (\alpha,\beta)Q$$

we get equations connecting the coefficients of A which can be solved to give, for example

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

A has determinant 1 and so by 4.0.1 the quadratic form Q with matrix A has type 2.

<u>Step 2</u>: Find the set I of isotropic vectors of $O^-(6,3)$; i.e. vectors $(x_1,\ldots,x_6)$ which satisfy

$$\sum_{i=1}^{6} x_i^2 + 2\sum_{i=1}^{5} x_i x_{i+1} = 0 .$$

We list them as orbits of the 7-cycle T; i.e. in subsets $X_1, X_2, \ldots, X_{32}$ of the form

$$\{\alpha, \alpha T, \alpha T^2, \ldots, \alpha T^6\}$$

in such a way that $X_1 \cup X_2 \cup \cdots \cup X_{16}$ is a complete set of line representatives of I. We then have

$$\underline{I} = \underline{X_1} \cup \cdots \cup \underline{X_{16}} .$$

We take, for example,

$$X_1 = \{(2,1,0,0,0,0),\ (0,2,1,0,0,0),\ (0,0,2,1,0,0),\ (0,0,0,2,1,0),\ (0,0,0,0,2,1),\ (2,2,2,2,2,1),\ (2,1,1,1,1,1)\}$$

and $X_{17} = \{2\alpha : \alpha \in X_1\}$, and so on.

Step 3: Find all possible $\underline{\Delta}$.

We consider subsets of $\underline{I}$ which are unions of precisely 8 of the 16 $\underline{X_i}$. Since we require that $\hat{\Delta}$ be a simple basis quantity for a rank 3 S-ring with $\lambda = 1$, Δ satisfies the condition given by 4.2.2, that

(1) if α and β are linearly independent vectors in Δ , then $\alpha+\beta$ does not belong to Δ .

The possible sets $\underline{\Delta}$ for which (1) holds are obtained with little difficulty. For example, if we suppose X_1 above is a subset of Δ , then the X_i which contain the isotropic vectors

$$(2,1,0,2,1,0) = (2,1,0,0,0,0) + (0,0,0,2,1,0)$$

and

$$(2,1,0,1,2,0) = (2,1,0,0,0,0) + (0,0,0,1,2,0)$$

cannot be subsets of Δ . By repeated use of this sort of argument we find that there are just four different unions of eight $\underline{X}_i$ which satisfy (1), and it is readily seen that these are equivalent under suitable changes of basis (which leave the set I unchanged). We thus get an essentially unique set Δ with

$$\left| \Delta \wedge \Delta + \alpha \right| = 1, \quad \text{for all } \alpha \in \Delta.$$

A set of line representatives of Δ is

X = {(2,1,0,0,0,0), (0,2,1,0,0,0), (0,0,2,1,0,0),
(0,0,0,2,1,0), (0,0,0,0,2,1), (2,2,2,2,2,1), (2,1,1,1,1,1),
(2,0,1,0,1,0), (0,2,0,1,0,1), (2,2,1,2,0,2), (1,0,0,2,0,1),
(2,0,2,2,1,2), (1,0,1,0,0,2), (1,2,1,2,1,1),
(1,1,2,0,0,0), (0,1,1,2,0,0), (0,0,1,1,2,0), (0,0,0,1,1,2),
(1,1,1,1,2,2), (1,2,2,2,2,0), (0,1,2,2,2,2),
(1,1,0,2,0,1), (2,0,0,2,1,2), (1,0,1,1,0,2), (1,2,1,2,2,1),
(2,0,1,0,1,1), (2,1,2,0,2,0), (0,2,1,2,0,2),
(1,1,0,2,0,2), (1,2,2,1,0,1), (2,0,1,1,0,2), (1,0,1,2,2,1),
(2,0,2,0,1,1), (2,1,2,1,2,0), (0,2,1,2,1,2),
(1,1,1,2,0,0), (0,1,1,1,2,0), (0,0,1,1,1,2), (1,1,1,2,2,2),
(1,2,2,2,0,0), (0,1,2,2,2,0), (0,0,1,2,2,2),
(1,1,2,2,0,0), (0,1,1,2,2,0), (0,0,1,1,2,2), (1,1,1,2,2,0),
(0,1,1,1,2,2), (1,1,2,2,2,0), (0,1,1,2,2,2),
(2,1,1,0,1,2), (1,0,2,2,1,2), (1,2,1,0,0,2), (1,2,0,2,1,1),
(2,0,1,2,1,0), (0,2,0,1,2,1), (2,2,1,2,0,1)}

Since we find also that

$$\left| \Delta \wedge \Delta + \gamma \right| = 20,$$

for all $\gamma \in \Gamma$, where $\Gamma = V(6,3) \setminus \Delta \cup 0$, it follows from 2.1.6 that $0, \hat{\Delta}, \hat{\Gamma}$ generate an S-ring with parameters C.

Step 4: Find Aut $\mathcal{S}$.

We already know that, by our construction, the matrix T belongs to Aut $\mathcal{S}$. By means of a more complex version of the technique described in the proof of Lemma 3 of § 4.3, we find also the following matrices belonging to Aut $\mathcal{S}$.

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 1 & 2 & 0 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 2 & 0 & 1 & 2 & 0 \\ 2 & 0 & 0 & 1 & 2 & 0 \\ 2 & 1 & 1 & 0 & 2 & 0 \\ 1 & 2 & 0 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 2 & 2 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 1 & 0 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Let G_0 be the subgroup $\langle T,A,B,C,D\rangle$ of $GL(6,3)$, and let $\alpha = (2,1,0,0,0,0)$. Then

$$G_{0,\underline{\alpha}} = \langle A.B,C,D\rangle \ .$$

G_0 is transitive on $\underline{\Delta}$ and has rank 3 with subdegrees 1, 10, 45, for the orbits of $G_{0,\underline{\alpha}}$ on $\underline{\Delta}$ are $\{\underline{\alpha}\}$, $\underline{\Delta}_2$ and $\underline{\Gamma}_2$, where a set of line representatives of Δ_2 is

$\{(0,0,0,2,1,0),\ (1,0,0,2,0,1),\ (0,0,0,2,2,1),$
$(2,0,0,2,1,2),\ (2,1,0,1,2,2),\ (0,1,0,2,0,2),\ (0,0,0,0,1,2),$
$(1,1,0,2,0,2),\ (2,2,0,1,0,2),\ (0,2,0,1,2,1)\}.$

We see that

$$\Delta_2 = \{ \delta \in \Delta : (\delta, \alpha)Q = 0\}$$

while

$$\Gamma_2 = \{ \delta \in \Delta : (\delta, \alpha)Q \neq 0\}$$

Let $\beta = (0,0,0,2,1,0)$ and $\delta = (1,0,0,2,0,1)$. The orbits of $\langle B,C,D \rangle$ on $\underline{\Delta_2}$ are $\{\underline{\beta}\}$ and $\underline{\Delta_2} \setminus \underline{\beta}$, and those of $\langle C,D \rangle$ on $\underline{\Delta_2}$ are $\{\underline{\beta}\}$, $\{\underline{\delta}\}$ and $\underline{\Delta_2} \setminus \{\underline{\beta}, \underline{\delta}\}$. By Theorem 1.1.1, the order of G_o/Z is 56.10.9.8. By Theorem 4.1.1 the order of $\frac{\mathrm{Aut}\,\mathcal{S}}{Z}$ is a divisor of 56.11.10.9.8. If $\frac{\mathrm{Aut}\,\mathcal{S}}{Z}$ contains an element of order 11, then the group is doubly transitive on $\underline{\Delta}$; but it can be shown that no element of $(\mathrm{Aut}\,\mathcal{S})_{\underline{\alpha}}$ maps a point in Δ_2 to one in Γ_2 . Hence G_o is the full automorphism group Aut $\mathcal{S}$ of $\mathcal{S}$.

<u>Step 5</u>: Identify Aut $\mathcal{S}$.

To identify the group G_o/Z we first consider the stabilizer of the point $\underline{\alpha}$. We observed earlier that one of the orbits $\underline{\Delta_2}$ of G_o on $\underline{\Delta}$ consists of those lines of Δ which are orthogonal to $\underline{\alpha}$. We see also that the vectors of Δ_2 span a 4-dimensional subspace $\langle \Delta_2 \rangle$ of V(6,3). We can show by 2.1.6 that $\hat{\Delta}_2$ is a simple basis quantity for a rank 3 S-ring over V(4,p) with parameters A(3). Since we have already proved the uniqueness of such an S-ring, the results of § 4.2 imply that

$(G_o/Z)_{\underline{\alpha}}$ is isomorphic to PGL(2,9).

It is shown in [16] that a rank 3 extension of this group with subdegrees 1,10,45 is unique and isomorphic to $[\mathrm{PSL}(3,4)]C_2$. This completes our proof.

<u>Note</u>: We have shown that PSL(3,4) acts on 56 points of PG(5,3) as a rank 3 permutation group with parameters

$$(k,\ell,\lambda,\mu) = (10,\ 45,\ 0,\ 2).$$

Since $\mu = \lambda+2$, the associated second Higman design (defined on Page 6) is balanced. This gives solutions for design numbers 51 and 52 (listed as having no known solutions) in M. Hall's table (p.294 of [9]). Since the publication of Hall's book, the above rank 3 representation of PSL(3,4) on 56 pointshas been found independently by Wales [21] and Montague [16]. Our construction gives the further information that the 56 points may be chosen in PG(5,3) on which PSL(3,4) acts as a subgroup of $PO^{-}(6,3)$. It seems likely that the geometry of this situation might be explored to good effect.

§ 5. Rank 3(p,n) groups with a balanced symmetric block design.

This section was motivated by the following remark of D.G. Higman (p.153, [10]): "It would be interesting to determine rank 3 groups, in addition to the symplectic groups, whose associated designs are balanced symmetric; at present we know only the orthogonal groups $O_{2m+1}(q)$, $m \geq 2$, q odd" We found a further example of such a group in § 4.4 with parameters (10, 45, 0, 2). In § 5 we search for rank 3 (p,n) groups with balanced block designs. The results of Higman and Tamaschke are sufficient to restrict the possible sets of parameters to two infinite series, for which we will exhibit corresponding series of rank 3 (p,n) groups.

We recall the following results about the parameters (k,ℓ,λ,μ) of a rank 3 (p,n) group (See 1.2.5, 1.2.7 and 2.2.9).

(a) $k + \ell + 1 = p^n$

(b) $\mu\ell = k(k-1-\lambda)$

(c) $d = (\lambda-\mu)^2 + 4(k-\mu)$

(d) $d = p^{2r}$, some integer r.

(e) p^r divides $2k + (\lambda-\mu)(k+\ell)$, but $2p^r$ does not.

We saw in § 1.2 that the first Higman design is balanced if $\lambda = \mu$, the second if $\lambda + 2 = \mu$.

<u>Theorem 5.1.</u> Suppose G is a rank 3 (p,n) group.

(i) If the first Higman design of G is balanced (i.e. $\lambda = \mu$) then p = 2 and

$$(k,\ell,\lambda) = (2^{r-1}(2^r \pm 1),\ 2^{2r-1} \mp 2^{r-1} - 1,\ 2^{r-1}(2^{r-1} \pm 1)).$$

(ii) If the second Higman design of G is balanced (i.e. $\lambda = \mu - 2$) then we get parameters for the same designs as in (i) with Δ and Γ interchanged.

Proof. (i) With $\lambda = \mu$, (c) becomes

$$d = 4(k-\mu),$$

and so (d) gives

$$p = 2 .$$

Hence, from (c) and (d)

$$k-\mu = 2^{2r-2} .$$

From (e), we see that

2^r divides 2k but does not divide 4k,

and hence we get

$$k = a\ 2^{r-1} \qquad \ldots (f)$$

and

$$\mu = 2^{r-1}(a-2^{r-1}) \qquad \ldots (g)$$

for some odd integer a.

(a), (b), (f) and (g) give

$$(a-1)(a+1) = 2^{n-r+1}(a-2^{r-1}) \qquad \ldots (h)$$

Hence 2^{n-r} divides a-1 or a+1, and since k is strictly less than 2^n-1, we have

$$a = 2^{n-r} \pm 1 \quad \text{or} \quad a = 2^{n-r+1} - 1.$$

If $a = 2^{n-r+1} - 1$, then (h) gives

$$2^{r-1} = 1 \ ; \quad \text{i.e. } r = 1 .$$

But then

$$k = 2^n - 1$$

contradicting (a), for ℓ is strictly positive. Hence

$$a = 2^{n-r} \pm 1$$

and (h) implies that

$$n = 2r.$$

(f) now gives

$$k = 2^{r-1}(2^r \pm 1)$$

while (g) gives

$$\mu = \lambda = 2^{r-1}(2^{r-1} \pm 1) .$$

(ii) is proved similarly.

We now show that Theorem 5.1 is the best result possible by showing that for each set of parameters given by it, there is a group satisfying the hypotheses. We consider orthogonal groups over the field GF(2) of 2 elements (in § 4.0, we discussed orthogonal groups only for $p \neq 2$).

Let V be the vector space V(2r,2). We define quadratic forms over V as in Chapter 8 of [3]. There are two of them up to change of basis, denoted by Q_o and Q_1, and defined as maps from V to GF(2) as follows. For $\alpha = (x_1, x_2, \ldots, x_{2r})$

$$(\alpha)Q_o = x_1x_2 + x_3x_4 + \ldots + x_{2r-1}x_{2r}$$

and

$$(\alpha)Q_1 = (\alpha)Q_o + x_1^2 + x_2^2 .$$

We define the orthogonal group $O^{(i)}(2r,2)$ to be the group

$$\{T \in GL(2r,2) : (\alpha T)Q_i = (\alpha)Q_i\}$$

for $i = 0$ and 1. Let $G^{(i)}(2r)$ be the semi-direct product $[V(2r,2)]O^{(i)}(2r,2)$. Then $G^{(i)}(2r)$ is rank 3 with suborbits

$$\{0\},\ \Delta^{(i)} = \{\alpha : (\alpha)Q_i = 1\},\ \Gamma^{(i)} = \{\alpha : (\alpha)Q_i = 0,\ \alpha \neq 0\}.$$

It is not difficult to show that

$$|\Delta^{(0)}| = 2^{r-1}(2^r-1) ,$$

while

$$|\Delta^{(1)}| = 2^{r-1}(2^r+1),$$

and hence that $G^{(0)}(2r)$ and $G^{(1)}(2r)$ are two series of rank 3 groups having parameters asgiven by Theorem 5.1.

These rank 3 representations were found independently by Rudvalis [not yet published], who has also made some further observations of interest. He showed that the first and second Higman designs of $G^{(0)}(2r)$ are respectively equivalent to the second and first Higman designs of $G^{(1)}(2r)$. Thus, for each r, the two designs are essentially the same having an automorphism group which contains both $O^{(0)}(2r,2)$ and $O^{(1)}(2r,2)$. Rudvalis shows that these two groups (as subgroups of GL(2r,2)) generate the symplectic group Sp(2r,2). Hence [V]Sp(2r,2) is an automorphism group of the rank 3 design, although it acts doubly transitively on the points of the design. This gives an example of a design associated with a rank 3 S-ring $\mathcal{S}$ in which the automorphism group of the design is larger than Aut $\mathcal{S}$.

REFERENCES

1. ARTIN, E., Geometric Algebra, Interscience, New York, 1957.
2. COXETER, H.S.M., 'Twelve points in PG(5,3) with 95040 self-transformations', Proc. Roy. Soc. (A) 247, 279-293 (1958).
3. DICKSON, L.E., Linear Groups, Dover, New York, 1958.
4. DIEUDONNÉ, J., La Géométrie des Groupes Classiques, Berlin/Göttingen/Heidelberg; Springer, 1955.
5. DORNHOFF, L., 'The rank of primitive solvable permutation groups', Math. Zeit. 109, 205-210 (1969).
6. FOULSER, D.A., 'Solvable primitive permutation groups of low rank', Trans. Am. Math. Soc. 143, 1-54 (1969).
7. FRAME, J.S., 'The degrees of the irreducible components of simply transitive permutation groups', Duke Math. J. 3, 8-17 (1937).
8. HALL, M., The Theory of Groups, Macmillan, New York, 1959.
9. HALL, M., Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.
10. HIGMAN, D.G., 'Finite permutation groups of rank 3', Math. Zeit. 86, 145-156 (1964).
11. HIGMAN, D.G., 'Primitive rank 3 groups with a prime subdegree', Math. Zeit. 91, 70-86 (1966).
12. HIGMAN, D.G., 'Intersection matrices for finite permutation groups', Journal of Algebra 6, 22-42 (1967).

13. HIGMAN, D.G. and SIMS, C.S., 'A simple group of order 44,352,000', Math. Zeit. 105, 110-113 (1968).

14. HUPPERT, B., 'Zweifach transitive, auflösbare Permutationsgruppen', Math. Zeit. 68, 126-150 (1957).

15. HUPPERT, B., Endliche Gruppen I, Berlin-Heidelberg-New York, Springer, 1967.

16. MONTAGUE, S., 'On rank 3 groups with a multiply transitive constituent', J. Alg. 14, 506-522 (1970).

17. SCHUR, I., 'Zur Theorie der einfach transitiven Permutationsgruppen', S.B. Preuss. Akad. Wiss., Phys.-Math. Kℓ. 598-623 (1933).

18. SCOTT, W.R., Group Theory, Prentice-Hall, New Jersey, 1964.

19. TAMASCHKE, O., 'Zur Theorie der Permutationsgruppen mit regulärer Untegruppe I', Math. Zeit. 80, 328-352 (1963).

20. TAMASCHKE, O., 'Zur Theorie der Permutationsgruppen mit regularer Untergruppe II', Math. Zeit. 80, 443-465 (1963).

21. WALES, D., 'Uniqueness of the graph of a rank 3 group', Pac. J. Math. 30.1, 271-277 (1969).

22. WIELANDT, H., Finite Permutation Groups, Academic Press, New York, 1964.

23. WITT, E., 'Die 5-fach transitiven Gruppen von Mathieu', Abhandl. Math. Sem. Univ. Hamburg 12, 256-264 (1937).