ACADEMIC PAPERBACKS*

EDITED BY Henry Booker, D. Allan Bromley, Nicholas DeClaris, W. Magnus, Alvin Nason, and A. Shenitzer

---

BIOLOGY

Design and Function at the Threshold of Life: The Viruses HEINZ FRAENKEL-CONRAT
The Evolution of Genetics ARNOLD W. RAVIN
Isotopes in Biology GEORGE WOLF
Life: Its Nature, Origin, and Development A. I. OPARIN
Time, Cells, and Aging BERNARD L. STREHLER
The Spread of Cancer JOSEPH LEIGHTON

ENGINEERING

A Vector Approach to Oscillations HENRY BOOKER
Dynamic Programming and Modern Control Theory RICHARD BELLMAN and ROBERT KALABA
Hamilton's Principle and Physical Systems B. R. GOSSICK

MATHEMATICS

Finite Permutation Groups HELMUT WIELANDT
Complex Numbers in Geometry I. M. YAGLOM
Elements of Abstract Harmonic Analysis GEORGE BACHMAN
Geometric Transformations (in two volumes) P. S. MODENOV and A. S. PARKHOMENKO
Introduction to p-Adic Numbers and Valuation Theory GEORGE BACHMAN
Linear Operators in Hilbert Space WERNER SCHMEIDLER
The Method of Averaging Functional Corrections: Theory and Applications A. Yu. LUCHKA
Noneuclidean Geometry HERBERT MESCHKOWSKI
Quadratic Forms and Matrices N. V. YEFIMOV
Representation Theory of Finite Groups MARTIN BURROW
Stories about Sets N. Ya. VILENKIN
Commutative Matrices D. A. SUPRUNENKO and R. I. TYSHKEVICH

PHYSICS

Crystals: Their Role in Nature and in Science CHARLES BUNN
Elementary Dynamics of Particles H. W. HARKNESS
Elementary Plane Rigid Dynamics H. W. HARKNESS
Mössbauer Effect: Principles and Applications GUNTHER K. WERTHEIM
Potential Barriers in Semiconductors B. R. GOSSICK
Principles of Vector Analysis JERRY B. MARION

*Most of these volumes are also available in a cloth bound edition.

Finite Permutation Groups

By

HELMUT WIELANDT

University of Tübingen
Tübingen, Germany

Translated from the German by

R. BERCOV

ACADEMIC PRESS New York San Francisco London

A Subsidiary of Harcourt Brace Jovanovich, Publishers

ACADEMIC PRESS INC.
111 Fifth Avenue, New York, New York 10003

United Kingdom Edition published by
ACADEMIC PRESS, INC. (LONDON) LTD.
24/28 Oval Road, London NW1 7DX

LIBRARY OF CONGRESS CATALOG CARD NUMBER: 64-18217

PRINTED IN THE UNITED STATES OF AMERICA

79 80 81 82 9 8 7 6 5 4 3

Dedicated to the memory of

ISSAI SCHUR

Preface

In addition to the theory of abstract groups, which has been especially advanced in recent decades, the historically older theory of permutation groups deserves and finds increasing interest. It is true that every abstract group is isomorphic to a permutation group, so that with respect to algebraic structure there is no difference between abstract groups and permutation groups. A specific treatment of permutation groups is nevertheless justified for several reasons. In the first place, certain concepts play a dominant role for permutation groups (such as fixed points and transitivity) which do not appear in the theory of abstract groups. This is connected with the fact that in every permutation group certain subgroups are distinguished in a natural way (see §3). In addition, permutation groups are a handy aid in the construction of abstract groups, and moreover they appear in various mathematical disciplines where they find useful applications, e.g., in Galois theory (group of an equation) and function theory (monodromy group).

A knowledge of the basic facts of both the theory of abstract finite groups and the theory of permutation groups will be assumed throughout; a knowledge of Frobenius' theory of group characters will be assumed in the last chapter. These fundamentals can be found, e.g., in the books by W. Burnside,

M. Hall, or A. Speiser mentioned in the Bibliography. Since no knowledge of the extensive apparatus of modular characters and p-blocks shall be assumed we shall not go into the important results of R. Brauer (1943) and his school. Thus, this is by no means a complete treatment of the subject. Our aim is to bring together some rather elementary theorems on permutation groups which either no longer appear in current textbooks or have not yet appeared in textbooks at all [no monograph on permutation groups seems to have been published after W. A. Manning's book (1921)]. The first half of the book, after the introduction of a suitable notation, deals primarily with older theorems (by C. Jordan and others) on multiply transitive groups, and the second half with more recent results of W. A. Manning, I. Schur, J. S. Frame, and others on simply transitive groups. Some unpublished material has been included, e.g., Theorem 18.2 and §26.

These lectures had been given in a less complete form at the University of Tübingen during the winter semester 1954-5. Important progress on some of the problems treated here has been made in the meantime. Hence I have inserted a number of references to recent results in the English translation, and the Bibliography has been extended.

I wish to express my thanks to Dr. J. André who in 1955 prepared the lecture notes in German, and to Dr. R. Bercov who originally undertook the translation of the first half to satisfy part of the language requirement for the degree of Doctor of Philosophy at the California Institute of Technology, and agreed in 1961 to complete the translation. My thanks are also due to G. Glauberman who helped in reading the proofs and made useful comments.

HELMUT WIELANDT

Tübingen

CHAPTER I

Fundamental Concepts

§1. Notation

Let Ω be a finite set of arbitrary elements which we denote by lower case Greek letters and call *points*. We denote subsets of Ω by capital Greek letters: $\Delta \subseteq \Omega$. If Δ is a proper subset of Ω, we write $\Delta \subset \Omega$. The empty set $\emptyset$ will always be regarded as a subset of Ω. By $|\Delta|$ we denote the number of points in Δ (in short: the *length* of Δ). Throughout, we put $|\Omega| = n$. We can then take the natural numbers $1, 2, \cdots, n$ as the "points":

$$\Omega = \{1, \cdots, n\}.$$

A *permutation on* Ω is a one-to-one mapping of Ω onto itself. Permutations will be denoted by lower case Latin letters, as will elements of abstract groups. We denote the image of the point $\alpha \in \Omega$ under the permutation p by α^p. We write

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1^p & 2^p & \cdots & n^p \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha^p \end{pmatrix}.$$

We define the *product* pq of two permutations p and q on Ω by the formula $\alpha^{pq} = (\alpha^p)^q$; hence we read products from left to right and not from right to left as is often customary. pq is again a permutation on Ω. With respect to the operation

just mentioned, all the permutations on Ω form a group, the *symmetric group* S^Ω. The unit element of this group, the *identity permutation* 1, leaves all the points of Ω fixed and is characterized by this property. If p takes the point α into β, then p^{-1}, the *permutation inverse* to p, takes the point β into α.

In addition to the method of writing permutations just indicated, the *cyclic form* is especially convenient. It can be recalled by the following example:

$$\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&4&6&7\end{pmatrix} = (123)\,(45)\,(6)\,(7) = (123)\,(45).$$

The last expression exhibits the *reduced form* in which the single point cycles are omitted. The identity permutation 1, which has only single point cycles, is denoted in the reduced form by a single such cycle, e.g., $1 = (1)$. Each permutation can be decomposed uniquely, except for order, into disjoint cycles. For example, the *cycle decomposition* of $(123)\,(234)$ is $(13)\,(24) = (24)\,(31) = \cdots$.

A *transposition* t is a permutation which interchanges two points and fixes the rest, and thus is a two-point cycle: $t = (\alpha\beta)$ with $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$. Every permutation p may be written as a product of transpositions: $p = (\alpha_1\beta_1) \cdots (\alpha_s\beta_s)$. This decomposition is not uniquely determined, but s is uniquely determined modulo 2 by p. We call p *even* if $s \equiv 0\,(2)$, otherwise *odd*. The even permutations on Ω form a group A^Ω, the *alternating group* on Ω. A^Ω is a normal subgroup of S^Ω of index 2 if $n \geq 2$. By the way, the even permutations on Ω can be characterized as the commutators $sts^{-1}t^{-1}$ where s and t run over S^Ω (Ore, 1951).

If p and s are two permutations on Ω, p and $s^{-1}ps$ are called *conjugate* or *similar*. The cyclic form of $s^{-1}ps$ is obtained by replacing each point α in the cyclic form of p by α^s.

We will denote subsets of S^Ω (*complexes*) by capital Latin letters, particularly the subgroups of S^Ω, the *permutation*

groups on Ω. The permutation group generated by a complex K, i.e., the intersection of all subgroups of S^Ω which contain K, is denoted by $\langle K \rangle$.

By the *degree* of a permutation group $G \neq 1$, we mean the number of points actually moved by G, and therefore not fixed by all $g \in G$. For example, the degree of S^Ω is equal to n if $n > 1$. The degree of a permutation $g \neq 1$ is the degree of the cyclic group $\langle g \rangle$, i.e., the number of points in the reduced form of g. We call the smallest of the degrees of the elements $g \neq 1$ of G the *minimal degree* of G. In the literature on permutation groups this has been called the *class* of G, but we wish to avoid this ambiguous expression.

By $|G|$ we denote the order of G (i.e., the number of permutations contained in G) and by $|G : H|$ the index $|G| : |H|$ of a subgroup H of G. In addition, we introduce the following symbols:

$H \leq G$ denotes:	H is a subgroup of G.
$H < G$ denotes:	H is $\neq G$ and a subgroup of G.
$H \lhd G$ denotes:	H is a normal subgroup of G.
$H \lhd G$ denotes:	H is $\neq G$ and a normal subgroup of G.
$H \cong G$ denotes:	H is isomorphic to G.
$H \overset{\sim}{\rightarrow} G$ denotes:	G is a homomorphic image of H.

By the *normalizer* $\mathbf{N}(H)$ of H in G, we mean the largest subgroup of G in which H is normal. $\mathbf{N}(H)$ consists of all $g \in G$ with $gH = Hg$. The *centralizer* $\mathbf{Z}(H)$ of H in G consists of all $g \in G$ for which $gh = hg$ holds for all $h \in H$.

If $\Delta \subseteq \Omega$ and $K \subseteq S^\Omega$ we denote by Δ^K the set of all δ^k with $\delta \in \Delta$ and $k \in K$. For example, $\Omega^K = \Omega$, $\emptyset^K = \emptyset$, and $|\Delta^p| = |\Delta|$.

Exercise 1.1. Cycles of even degree are odd permutations.

Exercise 1.2. The order of a permutation is the least common multiple of the degrees of the cycles in its cyclic form.

§2. The Transitive Constituents G^{Δ}

Let G be a permutation group on Ω, in short: $G \leq S^{\Omega}$. We say that a set $\Delta \subseteq \Omega$ is a *fixed block* of G or is fixed by G if $\Delta = \Delta^G$. Then each $g \in G$ induces a permutation on Δ which we denote by g^{Δ}. We call the totality of g^{Δ}'s formed for all $g \in G$ the *constituent* G^{Δ} of G on Δ (for example, $G = G^{\Omega}$). G^{Δ} is a permutation group on Δ. Obviously the mapping $g \to g^{\Delta}$ is a homomorphism: $G \supseteq G^{\Delta}$. If this mapping is an isomorphism, that is, $| G^{\Delta} | = | G |$, then the constituent G^{Δ} is called *faithful.*

Clearly the intersection and union of two fixed blocks of G are again fixed by G, and for every set $\Gamma \subseteq \Omega$ the smallest fixed block of G containing Γ is Γ^G.

Every group G on Ω has the trivial fixed blocks $\emptyset$ and Ω. If it has no others it is called *transitive.* Otherwise it is called *intransitive.* Accordingly, a constituent G^{Δ} is transitive precisely when Δ is a minimal fixed block ($\Delta \neq \emptyset$). In this case Δ is called an *orbit* or *set of transitivity* of G.

It is easily seen that the orbits of G partition Ω:

Lemma 2.1. *Each point $\alpha \in \Omega$ lies in exactly one orbit Δ of G, $\Delta = \alpha^G$. Two points α and β lie in the same orbit if and only if $\beta = \alpha^g$ for some $g \in G$.*

Examples. S^{Ω} is always transitive, even if $| \Omega | = 1$. A^{Ω} is transitive only for $n > 2$. The points which appear in the same cycle of the cyclic form of a permutation p constitute an orbit of $\langle p \rangle$.

Lemma 2.2. *If Δ is an orbit of G and $s \in S^{\Omega}$, then Δ^s is an orbit of $s^{-1}Gs$.*

§3. The Subgroups G_{Δ}

Let $G \leq S^{\Omega}$ and $\Delta \subseteq \Omega$. Those permutations of G which

leave each point of Δ *individually* fixed form a subgroup G_Δ of G. If Δ consists of a single point α we write $G_\Delta = G_\alpha$. Accordingly, we have

$$G_\emptyset = G, \qquad G_{\Gamma\cup\Delta} = G_\Gamma \cap G_\Delta = (G_\Gamma)_\Delta,$$
$$G_{\alpha\beta} = G_{\beta\alpha}, \qquad G_\Delta = \bigcap_{\alpha\in\Delta} G_\alpha \ (\Delta \neq \emptyset).$$

It is easily proved that:

Proposition 3.1. *For each* $g \in G$ *and* $\Delta \subseteq \Omega$, $g^{-1}G_\Delta g = G_{\Delta^g}$. *In particular, if* Δ *is fixed by* G, *then* $G_\Delta \trianglelefteq G$, $G/G_\Delta \cong G^\Delta$.

If $\alpha^G = \beta^G$, *then* G_α *and* G_β *are conjugate in* G.

We prove a basic theorem:

Theorem 3.2.

$$|\, G_\alpha \,|\, |\, \alpha^G \,| = |\, G \,|.$$

Proof. We determine the length $|\, \alpha^G \,|$ of the orbit α^G. We have $\alpha^h = \alpha^r$ if and only if $hr^{-1} \in G_\alpha$, i.e., $h \in G_\alpha r$. Therefore there are precisely as many points α^h as there are distinct right cosets $G_\alpha r$. However, this number is $|\, G : G_\alpha \,|$ and therefore

$$|\, \alpha^G \,| = |\, G \,| : |\, G_\alpha \,|,$$

as asserted.

Proposition 3.3. $|\, G : G_{\alpha\beta} \,| = |\, \alpha^G \,|\, |\, \beta^{G_\alpha} \,| = |\, \beta^G \,|\, |\, \alpha^{G_\beta} |$.

This formula shows, for instance, that in a transitive group G the length of that orbit of G_β which contains α equals the length of the orbit of G_α which contains β.

Proof. Application of 3.2 shows that

$$|\, G \,| = |\, G_\alpha \,|\, |\, \alpha^G \,| = |\, G_{\alpha\beta} \,|\, |\, \beta^{G_\alpha} \,|\, |\, \alpha^G \,|.$$

The following two theorems are further applications of 3.2.

Theorem 3.4. *Let p be a prime number, p^m a divisor of $|\alpha^G|$, and P a Sylow p-subgroup of G. Then p^m is also a divisor of $|\alpha^P|$.*

Proof. Repeated application of 3.2 shows that p^m is a divisor of

$$|\alpha^G|\,|G_\alpha : P_\alpha| = |G : G_\alpha|\,|G_\alpha : P_\alpha| = |G : P_\alpha| = |G : P|\,|P : P_\alpha| = |G : P|\,|\alpha^P|.$$

From this it follows that p^m divides $|\alpha^P|$ since $(|G : P|, p) = 1$.

Theorem 3.4′. *Every shortest orbit ψ of P in α^G has length p^m if p^m is the highest power of p dividing $|\alpha^G|$.*

Proof. By 3.2 the length of each orbit of P is a power of p. Now p^m divides $|\psi|$ by 3.4, and p^{m+1} does not divide $|\psi|$ since otherwise p^{m+1} would be a divisor of $|\alpha^G|$ which was supposed not to be the case. Thus $|\psi| = p^m$.

The following set of theorems, 3.5–3.7, goes back to Jordan (1873).

Theorem 3.5. *Let the subgroup $U \leq G_\alpha$ be conjugate in G_α to every group V which lies in G_α and is conjugate to U in G. Let N be the normalizer of U in G. If G is transitive on Ω, N is transitive on the set Φ of all points left fixed by U.*

Proof. By 3.1, $\Phi^N = \Phi$. By assumption $\alpha \in \Phi$. If β is an arbitrary element of Φ, then there exists, because of the transitivity of G, some $g \in G$ with $\alpha = \beta^g$. We now form the group $V = g^{-1}Ug$ which leaves α fixed. By assumption there exists an $h \in G_\alpha$ with $h^{-1}Vh = U$. The element $n = gh$ lies in N and takes β into α. Therefore N is transitive on Φ.

The assumption made on U holds particularly for G_α itself and by the Sylow theorems it holds also for every Sylow subgroup of G_α. Therefore we have the following two theorems.

Theorem 3.6. *In a transitive group G, the normalizer of G_α is transitive on the points left fixed by G_α.*

Theorem 3.7. *In a transitive group G, the normalizer of every Sylow subgroup U of G_α is transitive on the points left fixed by U.*

It should be mentioned that an important generalization of Theorem 3.6 has been given by W. A. Manning (1918):

Theorem 3.6′. *Let G be transitive on Ω, let $\alpha \in \Gamma \subseteq \Omega$, and let Δ be the set of all points left fixed by G_Γ. Let those groups $g^{-1}G_\Gamma g$ $(g \in G)$ which are contained in G_α make up k different sets $\mathfrak{S}_1, \cdots, \mathfrak{S}_k$ of conjugates under G_α. Then the normalizer of G_Γ in G has exactly k transitive constituents on Δ; their degrees are proportional to the numbers of groups contained in $\mathfrak{S}_1, \cdots, \mathfrak{S}_k$.*

This theorem contains 3.6 as the special case $\Gamma = \alpha$. It might be worthwhile to look for an analogous generalization of 3.5.

Groups G_Δ which are transitive on the remaining points $\Omega - \Delta$ possess a remarkable property which will be useful to us later:

Theorem 3.8. *Let $\Gamma, \Delta \subseteq \Omega$ and let G be transitive on Ω. In addition, let G_Γ be transitive on $\Omega - \Gamma$ and G_Δ transitive on $\Omega - \Delta$. If $|\Gamma| \leq |\Delta|$, then there exists $g \in G$ such that $g^{-1}G_\Delta g \leq G_\Gamma$.*

Proof. If $\Gamma = \emptyset$ or $\Delta = \Omega$, then $G_\Gamma = G$ or $G_\Delta = 1$, and the conclusion is trivial. Now let $\Gamma \neq \emptyset$ and $\Delta \neq \Omega$ which implies $\Delta \neq \emptyset$ and $\Gamma \neq \Omega$. Because of the transitivity of G, we may assume that the nonempty sets $\Omega - \Gamma$ and $\Omega - \Delta$ have at least one point in common (since if this is not the case in the beginning, we consider in place of G_Δ an appropriate conjugate $s^{-1}G_\Delta s$). The group $\langle G_\Gamma, G_\Delta \rangle = H$ is then transitive on $\Omega - (\Gamma \cap \Delta)$. If now (a) this set is smaller

than Ω we can get the conclusion by induction; if on the other hand it is (b) equal to Ω, then $\Gamma \cap \Delta = \emptyset$, and since $\Omega - \Gamma$ and $\Omega - \Delta$ have a point in common, we have $|\Gamma| + |\Delta| < |\Omega|$. This implies that $\Omega - \Gamma$ and $\Omega - \Delta^t$ have at least one point in common, for every $t \in G$. Hence, if we choose $t \in G$ with $\Gamma \cap \Delta^t \neq \emptyset$, we come back, by replacing G_Δ by $t^{-1}G_\Delta t$, to case (a).

We mention the following theorems as exercises.

Exercise 3.9. *If G is transitive, then the total number of single point cycles of all elements of G is equal to the order of G. In short: in a transitive group each element leaves on the average exactly one point fixed* (Proof: 3.2).

Exercise 3.10. *If a group has exactly k orbits, then each element of the group leaves on the average k points fixed.*

Exercise 3.11. *In each transitive group of degree $n > 1$ there is an element of degree n* (Jordan, 1872. Proof: 3.9).

Exercise 3.12. *In each permutation group whose order is divisible by a given prime number p, there are elements whose cycle decomposition contains a p-cycle: $s = (\alpha_1, \alpha_2, \ldots, \alpha_p) \ldots$* (Proof: Sylow's theorem).

Exercise 3.13. *The order of a permutation group G is odd if and only if the degrees of all transitive constituents of G and the degrees of all transitive constituents of each G_α ($\alpha \in \Omega$) are odd* (Proof: 3.12, 3.3; 3.2).

§4. Regular and Semiregular Groups

A permutation group G on Ω is called *semiregular* if, for each $\alpha \in \Omega$, $G_\alpha = 1$; and G is called *regular* if it is semiregular and transitive. Accordingly, every regular group is also semiregular and subgroups as well as constituents of semiregular groups are semiregular. 1 is semiregular. In the

case of semiregular groups, the degree and minimal degree coincide.

Proposition 4.1. *All orbits of a semiregular group G have the same length, namely, $|G|$.*

Proof. 3.2. From 4.1 and 3.2 it further follows that:

Proposition 4.2. *The order of a semiregular group is a divisor of its degree. A transitive group is regular if and only if its order and degree are equal.*

Proposition 4.3. *If the centralizer Z of G in S^Ω is transitive, then G is semiregular.*

Proof. Let $\alpha, \beta \in \Omega$. There exists $z \in Z$ with $\alpha^z = \beta$. By 3.1, $G_\alpha = z^{-1}G_\alpha z = G_{\alpha^z} = G_\beta$. Since β is arbitrary, it follows that $G_\alpha = 1$.

Proposition 4.4. *Every Abelian group G transitive on Ω is regular. G is its own centralizer in S^Ω.*

Proof. G is regular by 4.3, since the centralizer Z of G contains the transitive group G. By the same argument Z is regular and therefore $|Z| = |\Omega| = |G|$. On the other hand, $Z \geq G$, hence $Z = G$.

Exercise 4.5. The centralizer of every semiregular group is transitive.

Exercise 4.5′. If G is transitive on Ω, the centralizer Z of G in S^Ω is semiregular, and $|Z|$ equals the number of fixed points of G_α (Kuhn, 1904).

Examples of regular groups are obtained in the regular representations of arbitrary abstract groups. We take the elements of G as "points" to be permuted. To each $g \in G$ we assign (Jordan, 1870, p. 60) the permutations

$$g^* = \begin{pmatrix} x \\ xg \end{pmatrix} \quad \text{and} \quad {}^*g = \begin{pmatrix} x \\ g^{-1}x \end{pmatrix}.$$

These correspondences establish isomorphisms between G and the regular and transitive permutation groups G^* and ${}^*G$ on G consisting of all the g^* and ${}^*g$, respectively, which we call the *right regular* and *left regular* representations of G, respectively. As an application, we prove the following theorem on abstract groups.

Theorem 4.6. *If* $|G| = 2u$ *with* u *odd, then* G *contains a normal subgroup of order* u.

Proof. G contains an element a of order 2. From this it follows that a^* is a product of u transpositions and is therefore an odd permutation. Hence G^* contains odd permutations, and therefore the subgroup N^* consisting of all the even permutations of G^* is a normal subgroup of index 2. The desired normal subgroup of G is then the subgroup of G to which N^* corresponds.

§5. Frobenius Groups

By a *Frobenius group* we mean a transitive permutation group of degree n, which has minimal degree $n - 1$. In other words, these are the nonregular transitive groups G with $G_{\alpha\beta} = 1$ for $\alpha \neq \beta$. These important groups have been investigated repeatedly. An extensive account is given by de Séguier (1912, pp. 94–137, 209–215). The principal result is a theorem of Frobenius (1902):

Theorem 5.1. *In a Frobenius group of degree* n, *the elements of degree* n *together with* 1 *form a regular group* R. *This is a characteristic subgroup of* G.

Remarks. The proof of this theorem has to date been given only with the help of the theory of group characters.

A short formulation due to E. Witt is reproduced in Speiser (1937, p. 202).

Thompson (1959, 1960) proved a long-standing conjecture:

Theorem 5.1′. *The characteristic subgroup R mentioned in* 5.1 *is nilpotent, that is, R is the direct product of its Sylow subgroups.*

Wielandt (1958) proved a generalization of 5.1:

Theorem 5.1″. *Let G be any transitive group. Define G_α^* to be that subgroup of G_α which is generated by all $G_{\alpha\beta}$, $\beta \neq \alpha$. Then there is a unique transitive normal subgroup G^* of G such that $G^* \cap G_\alpha = G_\alpha^*$.*

The structure of the possible factor groups $G/R \cong G_\alpha$ is known to some extent (Zassenhaus, 1935a; Vincent, 1947). It is these finite groups which have a faithful representation by matrices over a field such that only the unit matrix has 1 as an eigenvalue.

As an exercise we mention:

Exercise 5.2. *Assume that the intransitive group G has degree n and minimal degree $n - 1$. If no transitive constituent of G has degree* 1, *then they all are faithful and all except one are regular* (Frobenius, 1902).

§6. Blocks

Let G be a permutation group on Ω. We call a subset ψ of Ω a *block* of G if for each $g \in G$ the image set ψ^g either coincides with ψ or has no point in common with ψ. Obviously, the whole set Ω, the empty set $\emptyset$, and the sets $\{\alpha\}$ consisting of only one point are blocks of every G on Ω. We call these *trivial blocks*. In addition, every fixed block in the sense of §2 is a block. If $U \leq G$, then every block of G is also a block of U.

Proposition 6.1. *If ψ and ψ' are blocks of G, then their intersection $\psi \cap \psi'$ is also a block of G.*

For if $\Delta = \psi \cap \psi'$ has a nonempty intersection with Δ^g for some $g \in G$, then so do ψ with ψ^g and ψ' with ψ'^g. Therefore the fact that ψ and ψ' are blocks implies that

$$\Delta^g = \psi^g \cap \psi'^g = \psi \cap \psi' = \Delta.$$

Hence Δ is also a block.

Proposition 6.2. *If $g \in G$, $U \leq G$, and ψ is a block of U, then ψ^g is a block of $g^{-1}Ug$.*

Proof. Let $u \in U$. If $\psi^{g \cdot g^{-1}ug} \cap \psi^g \neq \emptyset$, it follows by application of g^{-1} that $\psi^u \cap \psi \neq \emptyset$, hence since ψ is a block of U, $\psi^u = \psi$. Application of g now shows that $\psi^{g \cdot g^{-1}ug} = \psi^g$.

From this it follows that if ψ is a block of G then for each $g \in G$, ψ^g is also a block of G. Two such blocks are called *conjugate*. Any two conjugate blocks are equal or disjoint. The totality of all blocks conjugate to a block ψ of G form a *complete block system*. All blocks of a complete block system have the same length. If G is transitive on Ω, the union of the members of a complete block system of G is Ω. Hence:

Proposition 6.3. *The length of a block of a transitive group G divides the degree of G.*

To conclude this section we give two exercises.

Exercise 6.4. *For any two different points $\alpha, \beta \in \Omega$, let $\psi_{\alpha\beta}$ be the intersection of all blocks of G which contain α and β. (By 6.1, $\psi_{\alpha\beta}$ is also a block of G.) Let all $\psi_{\alpha\beta} \neq \Omega$. Further, let every $\psi_{\alpha\beta}$ contain only trivial proper subblocks. Then $G_{\alpha\beta} = 1$.*

Exercise 6.5. *The blocks of the group G which is generated by the cycle $(1\ 2\ 3 \cdots n)$ are the residue classes* mod *d where d runs over the divisors of n.*

§7. Imprimitive Groups

In this section we assume that G is transitive. A transitive group is called imprimitive if there is at least one nontrivial block ψ (i.e., $\psi \neq \emptyset, \{\alpha\}, \Omega$). Such a block is usually referred to in the literature as a *set of imprimitivity*. We establish a sufficient condition for the imprimitivity of a transitive group.

Proposition 7.1. *If the transitive group G contains an intransitive normal subgroup N different from 1, then G is imprimitive. The orbits of N form a complete block system of G.*

Proof. If ψ is an orbit of N, then ψ^g ($g \in G$) is by 2.2 an orbit of $g^{-1}Ng = N$. Thus G can only permute the pairwise disjoint orbits of N among each other. These therefore form blocks of G. Because $N \neq 1$, they contain more than one point, because of the intransitivity of N they are proper subsets of Ω, and because of the transitivity of G they are conjugate.

We note some obvious facts.

Proposition 7.2. *Let $\bar{\Omega} = \{\psi_1, \cdots \psi_k\}$ be a complete nontrivial block system of the imprimitive group G, and let $\bar{g}$ be the permutation on $\bar{\Omega}$ induced by g,*

$$\bar{g} = \begin{pmatrix} \psi_1 & \cdots & \psi_k \\ (\psi_1)^g & \cdots & (\psi_k)^g \end{pmatrix}.$$

Then the $\bar{g}$ form a permutation group $\bar{G}$ on $\bar{\Omega}$ and the mapping $g \to \bar{g}$ is a homomorphism of G onto $\bar{G}$.

The kernel N of this homomorphism consists of those permutations of G which take each of the blocks ψ_i ($i = 1, \cdots, k$) into itself. $\bar{G}$ is transitive on $\bar{\Omega}$. The blocks ψ_i are fixed sets but not necessarily orbits of N.

In this way imprimitive permutation groups are reduced to transitive groups of smaller degree.

The following theorem enables us to construct blocks of transitive groups.

Theorem 7.3. *If $\Delta \subseteq \Omega$ and $\alpha \in \Omega$, then $\psi = \cap_{x \in \Delta^g} \Delta^g$ is a block of the transitive group G.*

Proof. Let $h \in G$ and $\psi \cap \psi^h \neq \emptyset$. First let $\alpha \in \psi^h$. Then $\alpha \in \Delta^g$ implies $\alpha \in \Delta^{gh}$, hence we have $\psi \subseteq \psi^h$. Because $|\psi| = |\psi^h|$, we have $\psi = \psi^h$.

Now let $\beta \in \psi \cap \psi^h$. Because of the transitivity of G, there is a $k \in G$ with $\alpha^k = \beta$. Therefore α is in $\psi^{k^{-1}}$ and $\psi^{hk^{-1}}$ as well as in ψ. From what was just shown, we have $\psi = \psi^{k^{-1}} = \psi^{hk^{-1}}$. By application of k it follows that $\psi = \psi^h$. Hence ψ is a block of G.

The following theorem gives a necessary and sufficient condition that a group be imprimitive.

Theorem 7.4. *Let $\alpha \in \Omega$. The transitive group G on Ω is imprimitive if and only if there is a group Z which lies properly between G_α and G, i.e., for which $G_\alpha < Z < G$ holds.*

Proof. (a) Let G be imprimitive and ψ a nontrivial block of G. Let Z be the set of those $z \in G$ for which $\psi = \psi^z$. Z is clearly a subgroup of G, and indeed a proper subgroup because $\psi \subset \Omega$ and G is transitive. Let $\alpha \in \psi$. Because ψ is a block it follows from $\alpha^g = \alpha$ that $\psi^g = \psi$. Therefore $G_\alpha \leq Z$. Because $|\psi| > 1$ there is a $\beta \neq \alpha$ in ψ and because of the transitivity of G an $h \in G$ with $\alpha^h = \beta$. We conclude that $h \in Z$ by the above argument, but $h \notin G_\alpha$, hence $G_\alpha < Z$.

(b) Let Z be given with $G_\alpha < Z < G$. We put $\psi = \alpha^Z$. First we show that ψ is a block. Let $\beta \in \psi \cap \psi^g$ with $g \in G$. Then $\beta = \alpha^z = \alpha^{z'g}$ (with $z, z' \in Z$). Therefore $z'gz^{-1} \in G_\alpha < Z$, i.e., $g \in Z$. Thus $\psi^g = \psi$ and ψ is a block. Because $G_\alpha < Z$, ψ does not consist of α alone. We have shown that $\psi = \psi^g$ holds only for $g \in Z$. Since $Z < G$ there is a $g \in G$

with $\psi \neq \psi^g$, and therefore $\psi \neq \Omega$. Hence ψ is a nontrivial block, G is imprimitive.

The following theorem may be proved in the same way as 7.4.

Theorem 7.5. *The lattice of groups between G_α and G is isomorphic to the lattice of blocks of G which contain α.*

Theorem 7.6. *Let G be a regular group on Ω, whose degree n is not a prime. Then G is imprimitive.*

Proof. By 4.2, $|G|$ is not a prime. Hence for $\alpha \in \Omega$ there is a proper subgroup between G and $G_\alpha = 1$. By 7.4, G is imprimitive.

§8. Primitive Groups

Let it again be assumed that G is transitive. In accordance with the definition of imprimitive groups in §7, we call G *primitive* if G has only trivial blocks.

From 7.3, it follows for a primitive G, that $\alpha = \cap_{\alpha \in \Delta^g} \Delta^g$ if $\Delta \subset \Omega$ and $\alpha \in \Omega$. From this we have the useful theorem:

Theorem 8.1. *Let $\emptyset \subset \Delta \subset \Omega$. If G is primitive on Ω, then for any two distinct α and β in Ω, there exists $g \in G$ with $\alpha \in \Delta^g$ and $\beta \notin \Delta^g$.*

This fact has been stated in a less precise form by Rudio (1888). A refinement of 8.1 will be pointed out later (8.10).

The following theorem is an immediate consequence of 7.4.

Theorem 8.2. *Let $\alpha \in \Omega$, $|\Omega| > 1$. A transitive group G on Ω is primitive if and only if G_α is a maximal subgroup of G.*

We now give some sufficient conditions for the primitivity of a permutation group.

Theorem 8.3. *A transitive group of prime degree is primitive.*

Proof. By 6.3, the length of each block of a transitive group divides the degree, hence in our case each block is trivial.

Theorem 8.4. *Let G be transitive on Ω. In addition, let $U \leq G$ and let Δ be an orbit of U. If U^Δ is primitive on Δ and $|\Omega| < 2|\Delta|$, then G is primitive on Ω.*

Proof. Let ψ be a block of G, and let $\alpha \in \psi$. We want to show that ψ is trivial. ψ is also a block of U. Now $\alpha^U = \Delta$ is a fixed block of U, hence by 6.1, $\Delta \cap \psi$ is a block of U and therefore also of U^Δ. It contains α. Because of the primitivity of U^Δ, $\Delta \cap \psi$ is trivial, therefore $=\Delta$ or $=\alpha$.

If $\Delta \cap \psi = \Delta$, then $\Delta \subseteq \psi$, hence $\psi = \Omega$ because $|\psi|$ divides $n = |\Omega|$ and $|\psi| \geq |\Delta| > n/2$.

Now let $\Delta \cap \psi = \alpha$. For each $g \in G$, $\Delta \cap \psi^g$ is a block of U^Δ. If it is equal to Δ, we conclude as before that $\psi^g = \Omega = \psi$. We now assume that the block $\Delta \cap \psi^g$ consists of at most one point for all $g \in G$. (There are no other possibilities because of the primitivity of U^Δ.) The number of different ψ^g's is therefore $\geq |\Delta| > n/2$. Since this number is a divisor of n, it is equal to n. Hence it follows that $|\psi| = 1$.

In any case, ψ is a trivial block, hence G is primitive.

Proposition 8.5. *Let the transitive group G on Ω be generated by its subgroups C and D, i.e., $G = \langle C, D \rangle$. Let C be primitive on $\Gamma \subset \Omega$ and $C \leq G_{\Omega-\Gamma}$, and let D be primitive on $\Delta \subset \Omega$ and $D \leq G_{\Omega-\Delta}$. Then G is primitive on Ω.*

Proof. The transitivity of G implies $\Gamma \cup \Delta = \Omega$ and $\Gamma \cap \Delta \neq \emptyset$. From this we conclude that $|\Gamma| > n/2$ or $|\Delta| > n/2$. The theorem now follows from 8.4.

Proposition 8.6. *If G is primitive on Ω and α and β are different points of Ω, then either $G_\alpha \neq G_\beta$ or G is a regular group of prime degree.*

Proof. (a) Let $G_\alpha \neq 1$. Let Φ be the set of those points of Ω which are left fixed by every permutation of G_α. By 3.6, $\mathbf{N}(G_\alpha) = N$ is transitive on Φ. *If* G_α were equal to G_β for $\beta \neq \alpha$, then we would have $N > G_\alpha$, and therefore by the assumed primitivity of G (by Theorem 8.2) we would have $N = G$. Hence it would follow that $\Phi = \Omega$ and $G_\alpha = 1$ in contradiction to assumption (a).

(b) If $G_\alpha = 1$, then G is regular, hence $n = |\Omega|$ is by 7.6 a prime.

Proposition 8.7. *If G is primitive on Ω and α and β are different points of Ω, then $G = \langle G_\alpha, G_\beta \rangle$ or G is regular of prime degree.*

Proof. We assume that $\langle G_\alpha, G_\beta \rangle < G$. Since G is primitive, G_α is maximal by 8.2, hence $G_\beta \leq \langle G_\alpha, G_\beta \rangle = G_\alpha$. Since G_β is also maximal, $G_\beta = G_\alpha$. Hence we conclude by 8.6 that G is imprimitive (which is in contradiction with the assumption) or that it is regular of prime degree.

Theorem 8.8. *Every normal subgroup $\neq 1$ of a primitive group is transitive.*

Proof. 7.1. There is a partial converse of 8.8 which we mention as an exercise.

Exercise 8.8'. Let G contain a minimal normal subgroup $\neq 1$ which is transitive and Abelian. Then G is primitive.

We propose two more problems.

Exercise 8.9. If the degree of a primitive group is even and >2, then the order of the group is divisible by 4 (proof by 4.6).

Exercise 8.10. Let the group G of composite order be primitive on Ω. Let $\Gamma \subset \Omega$, $\Delta \subset \Omega$, $|\Gamma| = |\Delta| > 0$, and let α, β be any two distinct points of Ω. Then G contains an element g such that $\alpha^g \in \Gamma$ and $\beta^g \notin \Delta$ (Wielandt, 1956).

Remark. Primitive solvable groups have been investigated by Huppert (1955), and primitive groups with abelian normal subgroups by Itô (1955).

In conclusion, it should be pointed out that to each transitive group G on Ω there are certain primitive groups (in general of smaller degree) which we may call *primitive components* of G. They are obtained in the following way.

If ψ is a maximal block of G (different from Ω) and $\bar{\Omega}$ the complete block system containing ψ, then a transitive group $\bar{G}$ on $\bar{\Omega}$ is induced by G which is homomorphic to G (see 6.2). Since ψ is a maximal block of G, $\bar{G}$ is primitive on $\bar{\Omega}$. We call $\bar{G}$ a *first* (or *highest*) *primitive component* of G (note that $\bar{G}$ is not uniquely determined by G).

The group of all $g \in G$ which take ψ as a whole into itself may be denoted by G'. The constituent G'^{ψ} is transitive; this follows immediately from the fact that ψ is a block. We now proceed with G'^{ψ} as we did above with G and thus obtain a *second primitive component* of G. Continuing in this way, we obtain a *series* of *primitive components*.

From the maximality of ψ it follows by 8.2 that the subgroup G' is maximal in G. Likewise G'' is maximal in G', etc. These groups form a series of subgroups of G (otherwise arbitrary), which goes from G to G_1 (if from each block system occurring, the block is chosen which contains 1), and which cannot be refined. The number of primitive components in a series depends in general on the choice of the series. It might be worthwhile to investigate how suitable assumptions on the primitive components of G affect the permutation group structure of G.

CHAPTER II

Multiply Transitive Groups

§9. Multiple Transitivity

Let G be a permutation group on Ω and k a natural number with $1 \leq k \leq n = |\Omega|$. G is called *k-ply transitive* or *k-fold transitive* (on Ω) if for every two ordered k-tuples $\alpha_1, \cdots, \alpha_k$ and $\beta_1, \cdots, \beta_k$ of points of Ω (with $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$, for $i \neq j$) there exists $g \in G$ which takes α_i into β_i: $\alpha_i^g = \beta_i$ $(i = 1, \cdots, k)$. The transitivity introduced in §2 is the same as 1-fold transitivity. Every $(k+1)$-fold transitive group is also k-fold transitive. Every group having a k-fold transitive group as a subgroup is itself k-fold transitive.

The following two theorems follow easily from the definition.

Theorem 9.1. *Let G be transitive on Ω and $\alpha \in \Omega$. Then G is $(k+1)$-fold transitive on Ω if and only if G_α is k-fold transitive on $\Omega - \alpha$. If G is k-fold transitive on Ω and $\Delta \subseteq \Omega$ with $|\Delta| = d < k$, then G_Δ is $(k-d)$-fold transitive on $\Omega - \Delta$.*

Theorem 9.2. *Let G be k-fold transitive on Ω. In addition, let Γ and Δ be subsets of Ω, with $|\Gamma| = |\Delta| = k$. Then there exists $g \in G$ with $\Delta = \Gamma^g$ and $G_\Delta = g^{-1}G_\Gamma g$.*

Several of the theorems proved earlier for transitive groups

can be generalized without difficulty to multiply transitive groups. Thus it follows by repeated application of Theorem 3.2 that:

Theorem 9.3. *The order of a k-fold transitive group of degree n is divisible by* $n(n-1)\cdots(n-k+1)$. *The quotient is the order of any subgroup of the form* G_Δ *with* $|\Delta| = k$.

Jordan's method (see the proof of 3.5) yields the following theorem.

Theorem 9.4. *Let G be k-fold transitive on* Ω, *and let* $\Gamma \subseteq \Omega$, $|\Gamma| = k$. *Let the subgroup* $U \leq G_\Gamma$ *be conjugate in* G_Γ *to every group V which lies in* G_Γ *and which is conjugate to U in G. Then the normalizer* $\mathbf{N}(U)$ *is k-fold transitive on the set of the points left fixed by U* (Witt, 1937).

In the examination of multiply transitive groups with transitive subgroups of smaller degree, to be undertaken in §13, the following theorem will be useful.

Theorem 9.5. *Let* $\Delta \subset \Omega$, *G k-fold transitive on* Ω, $2 \leq k \leq |\Delta| + 1$, *and* G_Δ *transitive on* $\Omega - \Delta$. *Then the normalizer of* G_Δ *is* $(k-1)$*-fold transitive on* Δ.

Proof. We choose $\Gamma \subseteq \Delta$ with $|\Gamma| = k-1$. We observe that G_Γ is still transitive on $\Omega - \Gamma$. By 3.8, every group conjugate to G_Δ which lies in G_Γ is already conjugate to G_Δ in G_Γ. Now 9.4 yields the assertion with $U = G_\Delta$.

Multiple transitivity may be regarded as a strong form of primitivity, for from the definition it follows easily that:

Theorem 9.6. *Every doubly transitive group is primitive.*

The following theorem gives trivial examples of multiply transitive groups.

Theorem 9.7. *If* $|\Omega| = n$, *then the symmetric group* S^Ω *is* n*-fold transitive* ($n \geq 1$), *and the alternating group* A^Ω *is* ($n-2$)*-fold transitive* ($n \geq 3$).

Proof. The assertion about S^Ω is clear. The one about A^Ω holds for $n = 3$ and by 9.1 follows for n from its correctness for $n - 1$.

Remarks. Many, but not all, non-Abelian *simple* groups can be represented as doubly transitive permutation groups. A counter-example of order $2^6 \cdot 3^4 \cdot 5$ has been pointed out by Parker (1954).

The *solvable* multiply transitive groups have been determined by Huppert (1957). Apart from certain exceptions of degrees 3^2, 3^4, 5^2, 7^2, 11^2, 23^2, they may be described as groups of semilinear transformations $x \to as(x) + b$ where x and b run over a finite field F, a runs over a multiplicative group of non-zero elements of F, and s runs over an automorphism group of F.

Whereas there are numerous nontrivial doubly and triply transitive groups, only two nontrivial quadruply transitive groups and two nontrivial quintuply transitive groups are known; they were found in 1861 by Mathieu. Their degrees are 11, 23 and 12, 24, respectively. Structure and representations[1] of these groups are of great interest, for they and a subgroup of one of them are the five examples found to date of simple groups which do not fit into the known infinite series (de Séguier, 1912, pp. 147–171; Witt, 1937). It is not known if there are nontrivial k-fold transitive groups for $k \geq 6$. There are only estimates such as $k < 3 \log n$ (Wielandt, 1934; see also Parker, 1959; Parker and Nikolai, 1958). Wielandt (1960a) proved that there is no nontrivial eightfold transitive group if O. Schreier's conjecture ("the outer automorphism

[1] The representations af the Mathieu groups have been investigated by Frobenius (1904), Stanton (1951), and Todd (1959).

group of every simple finite group is solvable") is true. More precisely, he proved:

Theorem 9.8. *Let G be an eightfold transitive group which is neither symmetric nor alternating. Let H be a minimal normal subgroup of the largest subgroup of G which fixes five given points. H is simple and non-Abelian. Let A be the group of all automorphisms of H, and I the group of inner automorphisms of H. Then the outer automorphism group $B = A/I$ contains two subgroups C, D such that $C \lhd D$ and $D/C \cong A^5$, the simple group of order* 60.

The concept of k-fold transitivity may be strengthened or weakened in several ways. The most important we call *sharp k-fold transitivity*. G is called sharply k-fold transitive on Ω if for any two ordered k-tuples of the kind considered previously, there is *exactly one* $g \in G$ which takes the first into the second. These are the k-ply transitive groups in which every element is determined by its effect on any k points, and which therefore have order $n(n-1)\cdots(n-k+1)$ (see 9.3). For example, S^Ω is sharply n-fold transitive, and A^Ω sharply $(n-2)$-fold transitive. Outside of these, there are, as Jordan (1873) has shown,[1] no sharply k-fold transitive groups with $k \geq 6$, only one sharply quintuply transitive group ($n = 12$), and one sharply quadruply transitive group ($n = 11$), namely, the Mathieu groups.

There are sharply threefold transitive groups of degree $p^m + 1$ only (p prime), and indeed one such for m odd or $p = 2$, and two such for m even, $p > 2$ (Zassenhaus, 1934; Tits, 1952; Huppert, 1962).[2] In particular, the projective group of a line over a Galois field is sharply triply transitive.

[1] A generalization of this is given by Hall (1954).

[2] More generally, all doubly transitive groups have been determined which contain a permutation fixing exactly two points but no permutation, except 1, fixing more than two points (Feit, 1960; Itô, 1962a; Suzuki, 1962). They have degree $p^m + 1$ or 2^p (p prime).

Sharply doubly transitive groups are Frobenius groups, their degrees are prime powers (by 5.1 and 11.3). These groups have been investigated frequently, a report is given by de Séguier (1912, p. 97 ff.); the complete determination is due to Zassenhaus (1935). The sharply simply transitive groups are the regular groups. They have no special structure, since every abstract group can be faithfully represented as a regular permutation group (§4).

Tits (1952) deals with a weakened concept of sharp k-fold transitivity (also for $|\Omega| = \infty$). It is suited to projective groups of higher dimensions. A weakening of the concept of k-fold transitivity in which unordered k-tuples are used in place of ordered k-tuples is of importance for game theory (Neumann and Morgenstern, 1947, p. 258; Beaumont and Peterson, 1955). Bays (1952) deals with a concept of "primitivity for k-tuples."

In the following, two other modifications of multiple transitivity will be discussed, which will be used in §12 to deduce an improved form of the following classical theorem.

Theorem 9.9. *A normal subgroup $N \neq 1$ of a k-fold transitive group $G \neq S^\Omega$ of degree n ($k \geq 2$) is in general $(k-1)$-fold transitive. There are exceptions only in the case $n = 2^m$, $k = 3$, in which case N may be a regular elementary Abelian 2-group* (Jordan, 1870, p. 65; 1873, p. 69).

§10. Multiple Primitivity and Half-Transitivity

We call the group G on Ω *k-fold primitive* ($k = 1, 2, \ldots, n$) if it is k-fold transitive and the subgroups which leave $k-1$ points fixed are not only transitive on the rest (by 9.1) but even primitive. G is k-fold primitive on Ω with $k \geq 2$, if G is transitive and G_α is $(k-1)$-fold primitive on $\Omega - \alpha$. For example, S^Ω is n-fold primitive ($n > 1$); A^Ω is $(n-2)$-fold primitive ($n \geq 3$). From 9.6 it follows that:

Theorem 10.1. *Let $k = 1, 2, \ldots$. Every $(k+1)$-fold transitive group is k-fold primitive. Every k-fold primitive group is k-fold transitive and every group of which it is a subgroup is k-fold primitive.*

Whereas doubly primitive groups have appeared in the literature occasionally, the general concept does not yet seem to have been used systematically for an improved investigation of multiply transitive groups.

Another improvement is obtained through the following concept. We call a group G on Ω *half-transitive* or $\frac{1}{2}$*-fold transitive* if its orbits all have equal length >1. It is convenient to designate, in addition to these, the groups S^{Δ} with $|\Delta| = 1$ (consisting only of 1) as half-transitive since they are transitive. In addition, we call a group G on Ω $(k+\frac{1}{2})$*-fold transitive* $(k = 1, 2, \ldots, n-1)$ if G is transitive on Ω and G_α is $(k-\frac{1}{2})$-fold transitive on $\Omega - \alpha$ (the choice of the point α is without importance because of the transitivity). Obviously we have:

Theorem 10.2. *Let $k = 1, 2, \ldots$. Every k-fold transitive group is $(k-\frac{1}{2})$-fold transitive. Every $(k+\frac{1}{2})$-fold transitive group is k-fold transitive and each group of which it is a subgroup is k-fold transitive [however, not necessarily $(k+\frac{1}{2})$-fold transitive].*

This seemingly artificial concept of half-transitivity is justified by the following theorem (to be generalized in §12).

Theorem 10.3. *Every normal subgroup $N \neq 1$ of a transitive group G is half-transitive.*

Proof. The orbits of N are conjugate blocks of G by 7.1 and therefore have the same length.

Further examples of half-transitive groups are given by the semiregular groups $\neq 1$. Every Frobenius group is $\frac{3}{2}$-fold transitive.

The $\frac{3}{2}$-fold transitive groups have an important property:

Theorem 10.4. *Every $\frac{3}{2}$-fold transitive group is primitive or a Frobenius group.*

Proof. Let $n > 2$ and let G be $\frac{3}{2}$-fold transitive on Ω, i.e., let $G_1 = H$ have only orbits of length $m > 1$. Let us assume that G has a block of length k with $1 < k < n = |\Omega|$. Then the points $1, \ldots, n$ may be arranged in a matrix α_{ij} in such a way that every row ψ_i is a block of G with length k and, say, $\alpha_{11} = 1$.

ψ_1 is fixed by H, therefore $k \equiv 1(m)$, hence $(k, m) = 1$. For $i > 1$, ψ_i^H is fixed by H and does not contain 1. Therefore $|\psi_i^H|$ is divisible by m, but also by k, therefore by km. On the other hand, $|\alpha_{ij}^H| = m$, and therefore $|\psi_i^H| \leq km$. Thus it follows that $|\psi_i^H| = km$, and therefore $\alpha_{ij}^H \cap \alpha_{im}^H = \emptyset$ for $j \neq m$. This means that for $i > 1$, $\alpha_{ij}^H \cap \psi_i = \alpha_{ij}$. Now it follows that:

(a) If $\alpha \in \psi_i$ $(i > 1)$, then $H_\alpha = G_{1\alpha} \leq G_{\psi_i}$ since for $a \in H_\alpha$ we have

$$\alpha_{ij}^a = (\alpha_{ij}^H \cap \psi_i)^a = \alpha_{ij}^H \cap \psi_i^a = \alpha_{ij}^H \cap \psi_i = \alpha_{ij}.$$

(b) Under the hypothesis of (a), $G_{1\alpha} \leq G_{\psi_1}$, since 1 and α may be interchanged in the argument.

(c) Under the hypothesis of (a), $G_{1\alpha} = G_{1\alpha_{12}} = \cdots = G_{1\alpha_{1k}}$. For $G_{1\alpha} \leq G_{\psi_1} \leq G_{1\alpha_{12}}$, and $|G_{1\alpha}| = |G_{1\alpha_{12}}|$ by 3.2 because $|\alpha^{G_1}| = |\alpha_{12}^{G_1}| = m$.

(d) From (c) it follows that $G_{1\alpha_{12}} = 1$, since α is arbitrary except that $\alpha \notin \psi_1$.

(e) Now for any $\alpha \neq 1$, $G_{1\alpha} = 1$, since this is true by (d) if $\alpha \in \psi_1$, and by (b) if $\alpha \notin \psi_1$.

We have shown:

$\frac{3}{2}$-fold transitivity and imprimitivity of G imply that for $\alpha \neq 1$, $G_{1\alpha} = 1$. The minimal degree of G is therefore $\geq n - 1$, and since G cannot be regular because of the $\frac{3}{2}$-fold

transitivity (except if $n = 2$ in which case G is primitive) the minimal degree of G is exactly $n - 1$, and G is a Frobenius group.

Remark. All $\frac{5}{2}$-fold transitive groups G in which G_α is a Frobenius group on $\Omega - \alpha$ have been determined by Feit, Itô, and Suzuki; see footnote 2 on page 22.

§11. Regular Normal Subgroups of Multiply Transitive Groups

We investigate the question of how multiply transitive a group of automorphisms of a group N can be on $N - 1$.

Theorem 11.1. *Let A be a group of automorphisms of N regarded as a permutation group on $N - 1$.*

(a) *If A is transitive, then N is elementary Abelian,*

$$|N| = p^m.$$

(b) *If A is primitive, then in addition*

$$|N| = 2^m, \quad \text{or} \quad |N| = 3.$$

(c) *If A is $\frac{3}{2}$-fold transitive, the same assertion holds.*

(*d*) *If A is doubly primitive, then*

$$|N| = 4, \quad \text{or} \quad |N| = 3.$$

(e) *If A is $\frac{5}{2}$-fold transitive, $|N| = 4$.*

Proof. (a) A is transitive on $N - 1$. Hence all elements $n \neq 1$ have the same order; this is a prime number p, and therefore $|N| = p^m$. The center Z of N has an element other than 1, and is invariant under A. Because of the transi-

tivity of A, $Z = N$. Hence N is Abelian of type $(p, p, \ldots, p)$, i.e., *elementary Abelian.*

(b) If $n \neq 1$, then the set $\{n, n^{-1}\}$ is a block of A. Since A is primitive, this block is trivial, i.e., $= n$ or $= N - 1$. In the first case $p = 2$, in the other $|N| = 3$.

(c) If $p \neq 2$, there is an $n^{-1} \neq n \in N$. n^{-1} is also left fixed by A_n. This contradicts the assumption of $\frac{3}{2}$-fold transitivity unless $N - 1 = n + n^{-1}$, hence $|N| = 3$.

(d) Here we have at the outset $|N| \geq 3$. If $|N| \geq 4$, we have $|N| = 2^m$ by (b). We choose a subgroup of N of order 4. Let its elements be $1, l, m, n$. Obviously, l and m form a block of A_n. Since A_n was assumed primitive on $N - n - 1$, this block is trivial. Hence $|N| = 4$.

(e) Here we have $|N| \geq 4$. We determine l, m, n as in (d). l is left fixed by $A_{n,m}$, and therefore, because of the $\frac{5}{2}$-fold transitivity, $|N - 1 - n - m| = 1$, hence $|N| = 4$.

We can use these results to investigate regular normal subgroups of multiply transitive groups. The connection is made by the following theorem.

Theorem 11.2. *Let N be a regular normal subgroup of the group G on Ω. Let $\alpha \in \Omega$. In addition let A be the group of automorphisms which N undergoes under similarity transformations by the elements $g \in G_\alpha$, considered as a permutation group on $N - 1$. Then the permutation groups G_α on $\Omega - \alpha$ and A on $N - 1$ differ only in the designation of points; the "point" n of the second group corresponds to the point α^n of the first.*

Proof. Let $\gamma, \delta \in \Omega - \alpha$ and let $g \in G_\alpha$ take γ into δ. In addition let c and d be the corresponding "points" of $N - 1$, hence $c = (\alpha\gamma \cdots) \cdots$ and $d = (\alpha\delta \cdots) \cdots$. Then $g^{-1}cg = (\alpha\delta \cdots) \cdots \in N$, and therefore $= d$ by the regularity of N.

From 11.1 and 11.2 we have the following theorem.

Theorem 11.3. *Let N be a regular normal subgroup of a permutation group G of degree n. Then:*

(a) *If G is doubly transitive, N is elementary Abelian. In particular, $n = p^m$ for a prime p.*

(b) *If G is doubly primitive or $\frac{5}{2}$-fold transitive, $n = 2^m$ or $n = 3$.*

(c) *If G is triply primitive, $n = 3$ or $n = 4$.*

(d) *If G is $\frac{7}{2}$-fold transitive, $n = 4$.*

(e) *G is never $\frac{9}{2}$-fold transitive.*

Note. Quadruple primitivity of G does occur ($G = S^{\Omega}$, $|\Omega| = 4$).

We now turn to regular normal subgroups of primitive groups.

Proposition 11.4. *Every regular normal subgroup N of a primitive group G of degree $n > 1$ is a minimal normal subgroup of G.*

Proof. If there were an $M \lhd G$ with $1 < M < N$, then $G_\alpha < G_\alpha M < G$, in contradiction to Theorem 8.2. Conversely the following theorem, which goes back to Galois, holds.

Theorem 11.5. *Every solvable minimal normal subgroup N of a primitive group G is regular. N is elementary Abelian and is the only minimal normal subgroup of G. The degree of G is a power of a prime.*

Proof. The commutator group of N is normal in G and $< N$, hence equal to 1. Thus N is Abelian. By 8.8, N is transitive, therefore regular. The elements m^p, formed for all $m \in N$, for a fixed prime p dividing n, form a normal subgroup of G, which is properly contained in N; hence $m^p = 1$. N is elementary Abelian, hence n is a prime power. If there were a second minimal normal subgroup M of G, it would be

disjoint from N, therefore it would lie in the centralizer of N, which, by 4.4, equals N.

A further theorem of Galois states:

Theorem 11.6. *Let* $|\Omega| = p$, *a prime, and* G *transitive on* Ω. G *is solvable if and only if for* $\alpha \neq \beta$, $G_{\alpha\beta} = 1$.

Proof (due to Galois, without the use of the theorems of Sylow and Frobenius).

(a) Let $G_{\alpha\beta} = 1$ for all $\alpha \neq \beta$. G contains an element of degree p (Theorem 3.11), and since $G_{\alpha\beta} = 1$, this element generates a semiregular group P of degree p, hence a regular group of order p. G contains no subgroup Q of the same order p different from P for otherwise PQ would contain exactly p^2 different elements whereas the order of the whole group G is at most $p(p-1)$ since $G_{\alpha\beta} = 1$. Therefore $P \trianglelefteq G$. Since P is its own centralizer (4.4), G/P is isomorphic to a group of automorphisms of the cyclic group P. Therefore G/P is Abelian (even cyclic), thus G is solvable.

(b) Let G be solvable. We choose a minimal normal subgroup N of G. By 11.5, N is regular and $|N| = p$. By 11.2, G_α coincides, except for designation of points, with a group of automorphisms of N (regarded as a permutation group on $N - 1$) and is therefore semiregular on $\Omega - \alpha$.

As a supplement to 11.6, we mention the following theorem.

Theorem 11.7. *Every nonsolvable transitive group of prime degree is doubly transitive* (Burnside, 1911, p. 341).

Remark. There are several known values of p for which every nonsolvable transitive group is either the alternating or symmetric group: $p = 5$, 19 (Carmichael, 1937, p. 162), 47, 59 (de Séguier, 1912, p. 170).

In addition, we mention without proof the following theorem.

Theorem 11.8. *The regular normal subgroup of a primitive Frobenius group is elementary Abelian* (Frobenius, 1902, proof by 5.1 and 5.2).

We close with a problem.

Exercise 11.9. The symmetric group of degree 4 *is the only quadruply transitive group which contains a solvable normal subgroup* $\neq 1$.

§12. Nonregular Normal Subgroups of Multiply Transitive Groups

Theorem 12.1. *Let* $G \neq S^\Omega$ *be a* k*-fold transitive group on* Ω (k *an integer*). *In addition, let* $N \trianglelefteq G$, N *not regular, and* $N \neq 1$. *Then* N *is* $(k - \frac{1}{2})$*-fold transitive or sharply* $(k-1)$*-fold transitive.*

Proof. (a) $k = 1$. See 10.3.

(b) $k = 2$. Let $\alpha \in \Omega$, then $N_\alpha \trianglelefteq G_\alpha$. In addition, $N_\alpha \neq 1$, since N was assumed to be nonregular. Thus N_α is half-transitive, and N is $\frac{3}{2}$-fold transitive.

(c) $k = 3$. In this case N_α is a normal subgroup $\neq 1$ of the doubly transitive group G_α. If N_α is not regular, then N_α is $\frac{3}{2}$-fold transitive by (b), hence N is $\frac{5}{2}$-fold transitive. If, on the other hand, N_α is regular on $\Omega - \alpha$, then N is sharply doubly transitive.

(d) $k \geq 4$. We proceed by induction on k. G_α is $(k-1)$-fold transitive. In addition, we have $G_\alpha \neq S^{\Omega-\alpha}$ since $G \neq S^\Omega$. If $N_\alpha \neq 1$ is not regular, then N_α is $(k - \frac{3}{2})$-fold transitive or sharply $(k-2)$-fold transitive by the induction hypothesis, and therefore N is $(k - \frac{1}{2})$-fold transitive or sharply $(k-1)$-fold transitive. If, however, N_α is regular, then N is a Frobenius group. By 5.1 (theorem of Frobenius) there exists a regular $R \trianglelefteq N$. We even have $R \trianglelefteq G$. Since $k \geq 4$ it follows by

11.3(d) that $n = 4$. In this case, however, G would be S^Ω, which was excluded.

Note. We mention without proof that a sharply $(k-1)$-fold transitive normal subgroup does not occur in Theorem 12.1 for $G \neq S^\Omega$ and $k \geq 3$ (Wielandt and Huppert, 1958). Hence, by Theorems 12.1 and 10.4, a nonregular normal subgroup $N \neq 1$ of a k-fold transitive group is, as a rule, $(k-1)$-fold primitive. This statement has been made more precise by Itô (1958) who showed that there are no exceptions for $k > 2$, $G \neq S^\Omega$. The difficult proof of Itô's main lemma (Theorem 2) has been simplified by Feit (1960).

We now prove:

Theorem 12.2. *Let $G \neq S^\Omega$ be k-fold primitive on Ω, and let $N \neq 1$ be a nonregular normal subgroup of G. Then N is k-fold transitive.*

Proof. (a) $k = 1$. See 8.8.

(b) $k = 2$. Clearly $1 \neq N_\alpha \trianglelefteq G_\alpha$. Since G_α is primitive, N_α is transitive by 8.8; hence N is doubly transitive.

(c) $k \geq 3$. We proceed by induction on k. From $G \neq S^\Omega$ it follows that $G_\alpha \neq S^{\Omega-\alpha}$. If N_α is not regular, then N_α is $(k-1)$-fold transitive by the induction hypothesis, since G_α is $(k-1)$-fold primitive and we have $1 \neq N_\alpha \trianglelefteq G_\alpha$. Therefore N is k-fold transitive. If N_α were regular, i.e., if N were a Frobenius group, then it would follow as before from 11.3(c) that $n = 3$ or $n = 4$. In this case we would have $G = S^\Omega$, which contradicts the assumption.

Theorems 12.1 and 11.3 imply Theorem 9.9, mentioned earlier without proof, according to which a normal subgroup $N \neq 1$ of a k-fold transitive group $G \neq S^\Omega$ is in general $(k-1)$-fold transitive.

Theorem 12.2 contains the well-known theorem that the alternating group of degree $n \geq 5$ is simple: if $1 \neq N \trianglelefteq A^\Omega$,

it follows easily [e.g., from 11.3(c)] that N is not regular. A^{Ω} is $(n-2)$-fold primitive. By 12.2, N is $(n-2)$-fold transitive. This shows that $n!/2$ divides $|N|$, hence $N = A^{\Omega}$.

We conclude with three problems.

Exercise 12.3. Every nonregular, imprimitive normal subgroup $\neq 1$ of a doubly transitive group is a Frobenius group and contains an elementary Abelian characteristic subgroup (Burnside, 1911, p. 199; proof by 12.1, 10.4, 5.1, 11.3).

Exercise 12.4. Every nonregular minimal normal subgroup of a doubly transitive group is primitive and simple (Burnside, 1911, p. 202; proof by 12.3).

Exercise 12.5. If $N \trianglelefteq G$ and G is $\frac{3}{2}$-fold transitive, then N is transitive or semiregular (proof by 10.4).

§13. Primitive Groups with Transitive Subgroups of Smaller Degree

In this section we make the following general assumptions:

(1) G is primitive on Ω.

(2) Ω is divided into disjoint subsets Γ and Δ:

$$\Omega = \Gamma \cup \Delta \qquad \text{and} \qquad \Gamma \cap \Delta = \emptyset,$$

such that

$$1 < |\Gamma| < |\Omega| \qquad \text{and} \qquad 1 \leq |\Delta| < |\Omega|.$$

(3) G_{Δ} is transitive on Γ.

Under these assumptions we claim:

Theorem 13.1. *G is doubly transitive. If in addition G_{Δ} is primitive on Γ, then G is even doubly primitive* (Jordan, 1871).

We prove this theorem by induction on $|\Delta|$. For $|\Delta| = 1$, the assertion is trivial. Let $|\Delta| > 1$.

(a) First, we assume that $2|\Delta| < |\Omega|$. This implies $2|\Gamma| > |\Omega|$, and therefore for every $g \in G$ we have $\Gamma \cap \Gamma^g \neq \emptyset$. Let $\alpha, \beta \in \Delta$. Because of the primitivity of G there is some $g \in G$ with $\alpha \in \Delta^g$ and $\beta \notin \Delta^g$ by Theorem 8.1. Because $\Gamma \cap \Gamma^g \neq \emptyset$, $H = \langle G_\Delta, g^{-1}G_\Delta g\rangle$ is transitive on $\Gamma \cup \Gamma^g$, since G_Δ is transitive on Γ and $g^{-1}G_\Delta g$ is transitive on Γ^g. Further, $\bar{\Delta} = \Delta \cap \Delta^g$ is the set of all points which are left fixed by *every* element of H. Because $\alpha \in \bar{\Delta}$ we have $1 \leq |\bar{\Delta}|$, and because $\beta \notin \bar{\Delta}$ we have $|\bar{\Delta}| < |\Delta|$. We use the induction hypothesis and obtain the double transitivity of G. If G_Δ is primitive, then by 8.5, H is also primitive. The same induction argument shows the double primitivity of G.

(b) We now assume that $2|\Delta| \geq |\Omega|$. For $\alpha, \beta \in \Gamma$ there is, by 8.1, some $g \in G$ with $\alpha \in \Gamma^g$ and $\beta \notin \Gamma^g$. We have $\alpha \in \Gamma \cap \Gamma^g \neq \emptyset$ and again $H = \langle G_\Delta, g^{-1}G_\Delta g\rangle$ is transitive on $\Gamma \cup \Gamma^g$. From $2|\Gamma| \leq |\Omega|$ it follows that $\Gamma \cup \Gamma^g \subset \Omega$. Because $\Gamma^g \neq \Gamma$, we have $\Gamma \cup \Gamma^g \supset \Gamma$. Now we may again use the induction hypothesis as before, and obtain the double primitivity or double transitivity of G (according as G_Δ is primitive or not).

Remarks. (i) The proof shows even more than we have claimed, namely:

Theorem 13.1′. *Under assumptions* (1), (2), (3) *the normal closure H of G_Δ in G (that is, the group generated by all conjugates $g^{-1}G_\Delta g$, $g \in G$) is doubly transitive. If G_Δ is primitive on Γ, then H is doubly primitive on Ω.*

(ii) It would be interesting to know whether the following generalization of Theorem 13.1 is true: if G is primitive and G_α contains a subgroup $H \neq 1$ which possesses exactly k

orbits containing more than one point, then G_α possesses at most k orbits containing more than one point. Partial results in this direction have been obtained by Wielandt (1962a).

An application of Theorem 13.1 is the important theorem:

Theorem 13.2. *If G is primitive on Ω and G_Δ is primitive on $\Omega - \Delta = \Gamma$, and in addition, $1 < |\Gamma| = m < n = |\Omega|$, then G is $(n - m + 1)$-fold primitive* (Jordan, 1871).

We prove this theorem by induction on $n - m = |\Delta|$. For $n - m = 1$, the assertion is trivial. Now let $n - m > 1$. Let $\delta \in \Delta$. Then $\Gamma \subset \Omega - \delta$ holds and G is doubly primitive (by 13.1). G_δ is therefore primitive on $\Omega - \delta$, and by the induction hypothesis we have that G_δ is $(n - m)$-fold primitive. Since G is transitive, the assertion follows by 9.1.

In particular $(n - 1)$-fold transitivity of G follows for $m = 2$ and $(n - 2)$-fold transitivity for $m = 3$. Hence we have the following theorem.

Theorem 13.3. *A primitive group which contains a transposition is a symmetric group. A primitive group which contains a 3-cycle is either alternating or symmetric.*

For certain values of n, there exist groups G of degree n which contain transitive subgroups of degrees $< n - 2$ and are doubly but not triply transitive. These *Jordan groups* can be interpreted as automorphism groups of block designs (Hall, 1962). A Jordan group of degree n cannot contain transitive subgroups whose degrees are small compared to n. This is shown by the following theorem which we shall prove together with a refinement (13.5).

Theorem 13.4. *Let G be primitive on Ω and G_Δ transitive on $\Omega - \Delta = \Gamma$. In addition, let $1 < |\Gamma| \leq \frac{1}{2}|\Omega|$. Then G is triply transitive on Ω* (Marggraf, 1892).

Theorem 13.5. *If the hypotheses of* 13.4 *are satisfied, and* $|\Gamma| < \frac{1}{2}|\Omega|$, *then G is alternating or symmetric* (Marggraf, 1892).

For the proof we require two lemmas. Under the hypotheses of 13.1 we claim that:

Lemma 13.6. *There is a subset* Γ^* *of* Ω *with*

$$\Gamma \subset \Gamma^* \subset \Omega$$

such that $\Delta^* = \Omega - \Gamma^*$ *and* $\psi = \Gamma^* - \Gamma$ *have the following properties:*

(a) G_{Δ^*} *is transitive on* Γ^*.

(b) $|\psi|$ *is a proper divisor of* $|\Gamma|$ (*in particular we have* $|\psi| \leq \frac{1}{2}|\Gamma|$).

(c) *If we put* $N = \mathbf{N}(G_\Delta)$ *then* $N_{\Delta^*} = N \cap G_{\Delta^*}$ *is transitive on* ψ.

Proof. (a) There is a $g \in G$ with $\Gamma^g \neq \Gamma$ and $\Gamma^g \cap \Gamma \neq \emptyset$ for otherwise Γ would be a block of G and G would be imprimitive. From the permutations of G with this property we choose g so that $\Gamma \cup \Gamma^g = \Gamma^*$ consists of as few elements as possible. $\langle G_\Delta, g^{-1}G_\Delta g\rangle$ is transitive on Γ^* and is a subgroup of G_{Δ^*}. Therefore G_{Δ^*} is also transitive on Γ^*.

(b) $\psi = \Gamma^* - \Gamma$ is a block of G_{Δ^*}. To show this we form $\Gamma^* - (\psi \cap \psi^h) = \Gamma \cup \Gamma^h$ for $h \in G_{\Delta^*}$. Because $\Gamma^h \cup \Gamma \subseteq \Gamma^*$ and $\Gamma \cap \Gamma^g \neq \emptyset$, $\Gamma^h \cap \Gamma \neq \emptyset$ holds; because of the minimality of Γ^*, $\Gamma \cup \Gamma^h = \Gamma^*$ or $= \Gamma$, i.e., $\psi \cap \psi^h = \emptyset$ or $= \psi$. This means that ψ is a block. Because of the transitivity of G_{Δ^*}, Γ^* and hence also Γ is a sum of blocks conjugate to ψ. Because $\Gamma \cap \Gamma^g \neq \emptyset$ and $\Gamma \neq \Gamma^g$, Γ consists of at least two such blocks, thus we have $|\Gamma| = k|\psi|$ with $k \geq 2$, as was asserted. In particular, $|\psi| \leq \frac{1}{2}|\Gamma|$.

(c) Let $\alpha, \beta \in \psi$. Then there is an $h \in G_{\Delta^*}$ with $\alpha^h = \beta$. Because $\alpha \notin \Gamma$ we have $\beta \notin \Gamma^h$. Hence it follows from the

minimality property of $\Gamma \cup \Gamma^g$ formulated in (a), in a way exactly corresponding to what was done in (b), that $\Gamma^h = \Gamma$, hence $\Delta^h = \Delta$. Hence we conclude that $h^{-1}G_\Delta h = G_\Delta$, i.e., $h \in N$.

Lemma 13.7. *$N = \mathbf{N}(G_\Delta)$ is primitive on Δ.*

The proof will be carried out in several steps.

(a) N is transitive on Δ. This follows from 9.5 since G is doubly transitive by 13.1.

(b) Let $\alpha \in \Gamma$. Then $N = N_\alpha G_\Delta$, and therefore $(N_\alpha)^\Delta = N^\Delta$. To prove this, note $N_\alpha G_\Delta \leq N$. Now let $n \in N$. Since Γ is fixed by N, it follows that $\alpha^n = \beta \in \Gamma$. Because of the transitivity of G_Δ on Γ, there is an $h \in G_\Delta$ with $\alpha^h = \beta$. Then $n' = nh^{-1} \in N_\alpha$, and therefore $n = n'h \in N_\alpha G_\Delta$.

(c) The primitivity of N^Δ will now be proved separately for various ranges of $|\Delta|$. For $|\Delta| = 1$ it is trivial. Next let $2 \leq |\Delta| \leq \frac{1}{2}|\Omega|$. Under this additional assumption we even prove the double transitivity of N^Δ. Let α, β, and $\alpha', \beta' \in \Delta$ be given. We want an $n \in N$ with $\alpha^n = \alpha'$ and $\beta^n = \beta'$, i.e., an n of the form

$$n = \begin{pmatrix} \alpha & \beta & \cdots \\ \alpha' & \beta' & \cdots \end{pmatrix}.$$

Because of the double transitivity of G there exists $g \in G$ with $\alpha^g = \alpha'$ and $\beta^g = \beta'$. We now show the transitivity of $H = \langle G_\Delta, g^{-1}G_\Delta g \rangle$ on $\Gamma \cup \Gamma^g$. For this it suffices to prove that $\Gamma \cap \Gamma^g \neq \emptyset$. This relation is certainly fulfilled if $|\Delta| < \frac{1}{2}|\Omega|$. There remains only the case $|\Gamma| = |\Delta| = \frac{1}{2}|\Omega|$. $\Gamma \cap \Gamma^g = \emptyset$ implies $\Delta^g = \Gamma$, in contradiction to $\alpha' \in \Delta$. From 3.8 (applied to H instead of G and to Δ^g instead of Γ) the existence of an $h \in H$ with $g^{-1}G_\Delta g = h^{-1}G_\Delta h$ follows. Now $n = gh^{-1}$ has the desired properties.

(d) We now assume that $|\Delta| > \frac{1}{2}|\Omega|$, i.e., $|\Delta| > |\Gamma|$, and prove the primitivity of N^Δ by induction on $|\Delta|$. From

13.6(b) it follows that $|\psi| \leq \frac{1}{2}|\Gamma| < \frac{1}{2}|\Delta|$, and therefore $|\Delta^*| = |\Delta| - |\psi| > \frac{1}{2}|\Delta|$. Let $N^* = \mathbf{N}(G_{\Delta^*})$ and $\alpha \in \psi$. Then by (b) and by the induction hypothesis $(N_\alpha^*)^{\Delta^*} = (N^*)^{\Delta^*}$ is primitive on Δ^*. Let $n \in N_\alpha^*$. Because $\alpha \notin \Gamma \cup \Gamma^n$, and therefore $\Gamma \cup \Gamma^n \subset \Gamma^*$, we conclude from the minimality of Γ^* exactly as in 13.6(a) that $\Gamma = \Gamma^n$, and thus $\Delta^n = \Delta$. From this it follows that $N_\alpha^* \leq N$. Application of 8.4 to Δ and Δ^* now yields the primitivity of N^Δ on Δ.

After these preliminary remarks, we can now prove Theorems 13.4 and 13.5.

Proof of 13.4. Let $\alpha \in \Gamma$. By 13.7, $(N_\alpha)^\Delta = N^\Delta$ is primitive on Δ. The degree of $(N_\alpha)^\Delta$ is $|\Delta|$, and that of G_α is $|\Omega - \alpha| = |\Omega| - 1$, since by 13.1 G_α is transitive on $\Omega - \alpha$. From our assumption that $|\Gamma| \leq \frac{1}{2}|\Omega|$ it follows that

$$|\Delta| > \tfrac{1}{2}|\Omega - \alpha|.$$

The hypotheses of 8.4 are satisfied by G_α and $U = N_\alpha$, hence G_α is primitive on $\Omega - \alpha$. Let $\delta \in \Delta$. Since G_δ is similar to G_α, G_δ is primitive on $\Omega - \delta$. By 13.1, since $G_\Delta \leq G_\delta$, G_δ is doubly transitive on $\Omega - \delta$. Hence G is triply transitive.

Proof of 13.5. The theorem is trivial for $|\Omega| = 1$. Now let $|\Omega| = n > 1$. We proceed by induction on n. Introduce Δ^* and ψ as in 13.6. We distinguish two cases:

(a) $|\psi| > 1$. By 13.7 N^Δ is primitive on Δ. In addition, $|\psi| \leq \frac{1}{2}|\Gamma| < \frac{1}{2}|\Delta|$ holds by 13.6(b). Because $|\psi| > 1$, by applying 13.6(c) to N^Δ, Δ, and ψ (instead of G, Ω, and Γ) we can make use of the induction hypothesis and obtain with the help of 13.7(b) the relation $(N_\alpha)^\Delta = N^\Delta \geq A^\Delta$ for every $\alpha \in \Gamma$. Hence $|N_\alpha| \geq \frac{1}{2}|\Delta|!$. From

$$|N_\alpha^\Gamma| \leq (|\Gamma| - 1)! \qquad \text{and} \qquad N_\alpha^\Gamma \cong N_\alpha / N_\Gamma$$

it follows that

$$|N_\Gamma| \geq \frac{|N_\alpha|}{(|\Gamma|-1)!} \geq \frac{\frac{1}{2}|\Delta|!}{(|\Gamma|-1)!} \geq \tfrac{1}{2}|\Delta|(|\Delta|-1).$$

If $|\Delta| > 3$, the last expression in the above formula is $> |\Delta|$. In this case N_Γ is therefore not regular on Δ. On the other hand, $(N_\Gamma)^\Delta = N_\Gamma \neq 1$ is a normal subgroup of N^Δ, therefore of A^Δ or S^Δ. This is only possible, however, if $N_\Gamma \geq A^\Delta$. If $\alpha, \beta, \gamma \in \Delta$, then $(\alpha\beta\gamma) \in N \leq G$. By 13.3, $G \geq A^\Omega$.

Now let $|\Delta| \leq 3$. By assumption $|\Gamma| < |\Delta|$, therefore $n \leq 5$. Since by 13.4 G is already known to be triply transitive, it follows again that $G \geq A^\Omega$.

(b) $|\psi| = 1$. In this case G_{Δ^*} is doubly transitive by 13.6(a), and therefore primitive, on Γ^*. The $|\Delta|$-fold transitivity of G then follows from 13.2. Thus G permutes the points of Δ like S^Δ. From $g \in G$ and $\Delta^g = \Delta$ it follows that $g \in N$. Therefore $N^\Delta = S^\Delta \geq A^\Delta$. Now we conclude exactly as in (a) that $G \geq A^\Omega$.

We mention without proof that the hypothesis $|\Gamma| < \frac{1}{2}|\Omega|$ may be omitted in the statement of 13.5 unless $|\Omega| = 2^m$, $m > 2$. In this exceptional case a counterexample is provided by the normalizer, in S^Ω, of the regular Abelian group of order 2^m and type $(2, 2, \cdots, 2)$.

In addition we note without proof:

Theorem 13.8. *A primitive group of degree n, which contains a cycle of degree m with $1 < m < n$, is $n - m + 1$-fold transitive* (Marggraf, 1892).

Note. In the case $m = n$, G is doubly transitive if n is not a prime (Schur, 1933). The proof is based on entirely different methods (see Chapter IV).

A primitive group which contains a cycle of smaller prime

degree is by 13.2 multiply transitive. This result may be strengthened:

Theorem 13.9. *Let p be a prime and G a primitive group of degree $n = p + k$ with $k \geq 3$. If G contains an element of degree and order p, then G is either alternating or symmetric* (Jordan, 1873).

Proof. G contains, say, the cycle $(1, 2 \cdots p) = g$. Let Δ be the set of the remaining points $p + 1, \cdots, n$. Then $\langle g \rangle$ is a Sylow subgroup of G_Δ. By 13.2, G is k-fold transitive on Ω, consequently by 9.4 the normalizer N of $\langle g \rangle$ is k-fold transitive on Δ. Therefore $N^\Delta = S^\Delta$. By the argument of part (b) of the proof of 13.7 we have $(N_\alpha)^\Delta = S^\Delta$ for $\alpha \in \{1, 2, \cdots, p\}$. By 11.2, $N_\alpha^{\Omega - \Delta}$ is isomorphic to an automorphism group of $\langle g \rangle$ and is therefore Abelian. The commutator group $N'_\alpha = K$ of N_α has $K^{\Omega - \Delta} = 1$ and $K^\Delta = S'^\Delta = A^\Delta$ as constituents. Hence it contains a cycle c of order 3. From $c \in G$ and the primitivity of G it follows by 13.3 that $A^\Omega \leq G$.

Remark. Jordan (1873, 1875) has extended the investigation to elements of order p and degree qp ($q = 2, 3, \cdots$). W. A. Manning (1909, 1911, 1918, 1919) and Weiss (1928) have carried it on further. We mention some of their results.

Theorem 13.10. *Let p be a prime and G a primitive group of degree $qp + k$, which contains an element of order p and degree qp, but which is neither alternating nor symmetric. Then:*

from	$q = 1$	2	3	4	4	5	6	7	≥ 8
and	$p \geq 2$	5	5	7	5	7	11	11	$2q - 1$
it follows that	$k \leq 2$	2	3	4	5	6	6	8	$4q - 4$

This theorem can be used to obtain limits of transitivity. For instance, a group of degree 100 ($= 97 + 3$) or of degree 25 ($= 2 \cdot 11 + 3$) can be at most triply transitive if it does not contain the alternating group. For were such a group

quadruply transitive, then its order would be divisible by 97 or 11, respectively, and it would contain an element g of the same order, which contradicts Theorem 13.10.

It should be mentioned here that for $q > 4$ better transitivity limits are obtained from the following theorem of Miller (1915).

Theorem 13.11. *If $n = qp + k$, p prime, $p > q > 1$, $k > q$, then a permutation group of degree n which is neither alternating nor symmetric can be at most k-fold transitive.*

Another application can be made to the order of primitive groups which do not contain the alternating group. For it follows from 13.10 that such a group must possess Sylow subgroups which are appreciably smaller than the corresponding Sylow subgroups of S^Ω. Details are given in the next section.

§14. The Order of Primitive Groups

By the method indicated, W. A. Manning (1919) obtained the theorem:

Theorem 14.1. *Let G be primitive on Ω but not $A^\Omega \leq G$. Then the index $| S^\Omega : G |$ is divisible by $\prod_{q=1}^{\infty} \tau_q$. Here τ_q denotes the product of all prime numbers from the following intervals:*

$$q = 1: \qquad 2 \leq p < n - 2;$$

$$q = 2, 3, 4: \qquad q + 1 < p < \frac{n}{q} - 1;$$

$$q = 5: \qquad 5 < p < \frac{n - 6}{5};$$

$$q = 6: \qquad 5 < p < \frac{n - 10}{6};$$

$$q \geq 7: \qquad 2q - 2 < p < (n - 4q + 4)/q.$$

Vacuous products are set equal to 1.

We do not deal more closely with these arithmetical limits which are in practice not very convenient. We derive instead a handy result which is due to Bochert (1889):

Theorem 14.2. *Let G be primitive on Ω, not containing A^Ω. Let $|\Omega| = n$. Then*

$$|S^\Omega : G| \geq \left[\frac{(n+1)}{2}\right]!$$

Proof. (a) By assumption G contains no 3-cycle because of 13.3.

(b) Let $a, b \in G$ have exactly one point in common when written in reduced cyclic form. Then the commutator $aba^{-1}b^{-1}$ is a 3-cycle, as can be easily verified.

(c) Let S^Δ be the subgroup of S^Ω whose permutations permute the points of $\Delta \subseteq \Omega$ arbitrarily (i.e., as a symmetric group) but leave the remaining points individually fixed. Put $k = |\Delta|$. In addition, let $S^\Delta \cap G = 1$ (this is, e.g., always satisfied for $|\Delta| = 1$) and let k be chosen as large as possible with this property. We now wish to show that $k \geq n/2$. Let us assume the contrary, $k < n/2$. Then $S^{\Omega-\Delta} \cap G > 1$ because $|\Omega - \Delta| > k$. Let $a \neq 1$ be chosen from $S^{\Omega-\Delta} \cap G$. a moves (at least) one $\alpha \in \Omega - \Delta$, but no point from Δ. Likewise, because of the minimality of k there is in $S^{\Delta\cup\alpha} \cap G$ some $b \neq 1$. If α were left fixed by b, then we would have $b \in S^\Delta \cap G$, which cannot be. α is therefore moved by b, but no other point of $\Omega - \Delta$ is moved by b. There is therefore exactly one point, namely α, which is moved by a and b. By (b) $aba^{-1}b^{-1} \in G$ is a 3-cycle, which is not possible because of (a). This contradiction is avoided only if $k \geq n/2$.

(d) If $u, v \in S^\Delta$ belong to the same coset Gs, then $uv^{-1} \in S^\Delta \cap G$, i.e., $u = v$. Thus it follows that $|S^\Omega : G| \geq k!$.

From $k \geq n/2$ it now follows that $k \geq [(n+1)/2]$ since k is an integer. From this the theorem of Bochert follows.

Lower limits are easily found for the index of *nonprimitive* subgroups of S^Ω by determining the largest subgroup of S^Ω with given nontrivial blocks. It always has an obvious structure. Together with 14.2 this yields theorems of the following kind: Every proper subgroup of S^Ω except A^Ω has a large index in S^Ω. We mention as an example and exercise:

Exercise 14.3. Every subgroup of S^Ω with $|\Omega| \geq 5$ (except A^Ω and S^Ω) has index $\geq |\Omega|$ in S^Ω; equality holds only for the subgroups $S^{\Omega-\alpha}$ unless $|\Omega| = 6$.

§15. The Minimal Degree of Multiply Transitive Groups

We conclude the chapter on multiply transitive groups with a short report on the minimal degree, that is, the smallest of the degrees of the elements $\neq 1$. Bochert showed in an ingenious way that this minimal degree is a large part of the degree n in the case of multiply transitive groups. His results have been supplemented by W. A. Manning (1933) as follows.

Theorem 15.1. *Let G be a k-ply transitive group, neither alternating nor symmetric. Let n be its degree, m its minimal degree.*

If $k \geq$	2	3	4	5	6	8	25
then $m \geq$	$\frac{n}{3} - \frac{2\sqrt{n}}{3}$	$\frac{n}{3} - 1$	$\frac{n-1}{2}$	$\frac{n}{2}$	$\frac{3n}{5}$	$\frac{2n}{3}$	$\frac{25n}{31}$

Note. There is no $c > 0$ such that $m \geq cn$ for *all primitive* groups. However Jordan (1871) has shown that $m \to \infty$ as

$n \to \infty$. More precisely, the short proof of Jordan's result in de Séguier's book (1912, p. 58) shows that if G is a primitive group of minimal degree $m > 3$ and of degree n, then

$$n < \frac{m^2}{4} \log \frac{m}{2} + m \left(\log \frac{m}{2} + \frac{3}{2} \right).$$

There are therefore only finitely many primitive groups with a given minimal degree. The primitive groups with minimal degree $m \leq 15$ have been determined explicitly (see especially W. A. Manning, 1906–1929). Their degrees are all ≤ 49.

Burckhardt and Vogt (1909, p. 555) mention that there are no primitive groups with minimal degrees 9, 25, 49.

CHAPTER III

The Transitive Constituents of G_α

In this chapter, simply transitive permutation groups will be discussed. Let $\alpha \in \Omega$ and let G be transitive on Ω. We will be dealing with questions which in the case of multiply transitive groups become meaningless, in particular with the question of what relations exist between the different transitive constituents of G_α.

§16. Pairing of Constituents of G_α

The concept to be discussed here was originally introduced by Burnside (1901) in another way (from representation theory). We follow W. A. Manning (1927).

Let Γ be an orbit of G_α. We consider the set K of all $g \in G$ for which $\alpha \in \Gamma^g$ holds, and form the subset $\Gamma' = \alpha^K = \{\alpha^g \mid \alpha \in \Gamma^g\}$ of Ω. We call this process *reflection* of Γ by α.

Theorem 16.1. *Under reflection by α, an orbit Γ of G_α goes into another such orbit: Γ' is also an orbit of G_α.*

Proof. (a) Obviously $KG_\alpha \subseteq K$. Therefore

$$\Gamma'^{G_\alpha} = \alpha^{KG_\alpha} \subseteq \alpha^K = \Gamma'.$$

Since clearly $\Gamma'^{G_\alpha} \supseteq \Gamma'$, it follows that $\Gamma'^{G_\alpha} = \Gamma'$.

(b) Let $\beta', \gamma' \in \Gamma'$. Then $\beta' = \alpha^g$ and $\gamma' = \alpha^h$ for $g, h \in K$, thus $\alpha^{g^{-1}}, \alpha^{h^{-1}} \in \Gamma$. There exists $b \in G_\alpha$ with $\alpha^{g^{-1}b} = \alpha^{h^{-1}}$

since Γ is an orbit of G_α . $a = g^{-1}bh$ lies in G_α and takes β' into γ'. Proposition 16.1 now follows from (a) and (b).

Theorem 16.2. *Under double reflection of an orbit of G_α by α the original orbit is obtained: $(\Gamma')' = \Gamma$.*

It is sufficient to show that $(\Gamma')' \cap \Gamma \neq \emptyset$. Let $\gamma' \in \Gamma'$, i.e., $\gamma' = \alpha^g$ with $\alpha = \gamma^g$ for some $\gamma \in \Gamma$. From this it follows that $\gamma = \alpha^{g^{-1}}$ and $\alpha = \gamma'^{g^{-1}} \in \Gamma'^{g^{-1}}$, i.e., $\gamma \in (\Gamma')'$, thus $\gamma \in (\Gamma')' \cap \Gamma$ as asserted.

Definition. The Γ and Γ' which are associated with each other by Theorems 16.1 and 16.2 are called *paired* orbits; G_α^Γ and $G_\alpha^{\Gamma'}$ are called *paired constituents* of G_α .

Theorem 16.3. *Paired orbits have the same length.*

Proof. For each $\gamma \in \Gamma$ there are exactly $| G_\alpha |$ permutations in K (i.e., with $\alpha = \gamma^g$). Hence $| K | = | G_\alpha | \, | \Gamma |$. However, at most $| G_\alpha |$ permutations in K map α onto the same point, thus $| \Gamma' | = | \alpha^K | \geq | K | / | G_\alpha | = | \Gamma |$. By 16.2, $\Gamma' = \Gamma$.

We now wish to investigate when an orbit of G_α is paired with itself.

Theorem 16.4. *Let $\beta \in \Gamma$. Then $\Gamma = \Gamma'$ holds if and only if G contains an element g which exchanges α and β, i.e., whose cycle decomposition contains the transposition $(\alpha\beta)$.*

Proof. (a) Let $\Gamma = \Gamma'$. Choose an $h \in G$ with $\beta^h = \alpha$. Because $\Gamma = \Gamma'$, we have $\alpha^h \in \Gamma$. Since also $\beta \in \Gamma$, there is some $k \in G_\alpha$ such that $(\alpha^h)^k = \beta$. Now $g = hk$ exchanges α and β.

(b) If $g = (\alpha\beta) \cdots \in G$, we have $\beta \in \Gamma'$. Because $\Gamma \cap \Gamma' \neq \emptyset$ we have $\Gamma = \Gamma'$.

Theorem 16.5. *The group G_α has an orbit different from α and paired with itself if and only if G is of even order.*

Proof. (a) Let $\Gamma = \Gamma'$, $\alpha \notin \Gamma$ and $\beta \in \Gamma$. Then by 16.4 there exists $g = (\alpha\beta) \cdots \in G$. The order of g and hence that of G is therefore even.

(b) Let G contain an element g of order 2. Then some $(\beta\gamma)$ occurs in the cycle representation of $g : g = (\beta\gamma) \cdots$. Choose $s = (\beta\alpha \cdots) \cdots \in G$. Then $(\alpha\delta)$ with $\delta = \gamma^s$ occurs in the cycle decomposition of $s^{-1}gs$. Hence $\Gamma = \delta^{G_\alpha} = \Gamma'$ is an orbit of the desired kind.

Thus if G is of odd order, the number of orbits of G_α different from $\{\alpha\}$ with a given length is always even.

To conclude, we mention without proof a result which generalizes a theorem of Rietz (1904):

Theorem 16.6. *Let G be primitive on Ω, and let ψ be a fixed block of G_α such that for each orbit Γ of G_α, either Γ or Γ' is contained in ψ. Then the constituent G_α^ψ is faithful* (Wielandt, 1962a).

The proof relies on certain properties of *subnormal* subgroups of primitive groups G (i.e., of the groups which occur in composition series of G).

§17. The Degrees of the Transitive Constituents of G_α

We begin with a lemma:

Lemma 17.1. *Let H be an arbitrary (not necessarily transitive) permutation group. Let $\gamma \in \Omega$, $U \leq H$, and $|H : U| = i$. Then $|\gamma^U|$ is divisible by*

$$\frac{|\gamma^H|}{(|\gamma^H|, i)}.$$

Proof. Let $t = |\gamma^H|$. Then $t = |H : H_\gamma|$. Because $U \leq H$, t is a divisor of

$$|H : H_\gamma|\,|H_\gamma : U_\gamma| = |H : U_\gamma| = |H : U|\,|U : U_\gamma| = i|\gamma^U|.$$

Therefore $t/(t, i)$ is also a divisor of $i|\gamma^U|/(t, i)$. From $[t/(t, i), i/(t, i)] = 1$ it follows that $t/(t, i)$ divides $|\gamma^U|$ as was asserted. From 17.1 it follows immediately that:

Lemma 17.2.

$$\frac{1}{i}|\gamma^H| \leq \frac{|\gamma^H|}{(|\gamma^H|, i)} \leq |\gamma^U|$$

holds. Since $\gamma^H \supseteq \gamma^U$ we find:

Theorem 17.3. *$U \leq H$ and $(|\gamma^H|, |H : U|) = 1$ imply $|\gamma^U| = |\gamma^H|$.*

In what follows let G be transitive on Ω and let $\alpha \in \Omega$ be given. Let the lengths of the orbits of G_α, ordered according to increasing magnitude, be $1 = n_1 \leq n_2 \leq \cdots \leq n_k$. We assert:

Theorem 17.4. *If there exists an index $j > 1$ such that $n_j > n_2 n_{j-1}$, then G is imprimitive.*

Proof. Let Δ be the union of those orbits whose length is $< n_j$, and $\Gamma = \Omega - \Delta$. Then $\Gamma \neq \emptyset$, moreover $\Delta \neq \{\alpha\}$ since $n_j > n_2$. We choose an arbitrary $\delta \neq \alpha$ with $|\delta^{G_\alpha}| = n_2$ and consider $U = G_{\alpha\delta}$. For every $\gamma \in \Gamma$ we have

$$|\gamma^U| \geq \frac{|\gamma^{G_\alpha}|}{|G_\alpha : U|} \geq \frac{n_j}{n_2} > n_{j-1}$$

by 17.2. Hence $|\gamma^{G_\delta}| \geq |\gamma^U| > n_{j-1}$, therefore $\geq n_j$. We denote by Γ^* the set of those $\xi \in \Omega$ for which $|\xi^{G_\delta}| \geq n_j$ holds. We have shown $\Gamma^* \supseteq \Gamma$. As G_α, G_δ are similar,

$| \Gamma^* | = | \Gamma |$; hence $\Gamma^* = \Gamma$. We can now conclude that $\Gamma^{G_\delta} = \Gamma^{G_\alpha} = \Gamma = \Gamma^{\langle G_\alpha, G_\delta \rangle}$ and obtain $\langle G_\alpha , G_\delta \rangle < G$. By 8.7, G is imprimitive or regular. However, the latter possibility contradicts our hypothesis.

Theorem 17.5. *If there is an index $j > 1$ such that n_j and the maximal orbit length n_k are relatively prime, then G is imprimitive or a regular group of prime degree.* (Weiss, 1934).

Proof. Let Δ be the set of all $\xi \in \Omega$ for which $| \xi^{G_\alpha} | = n_k$ holds. Then $\emptyset \subset \Delta \subset \Omega$. Let $\beta \in \Omega$ be chosen so that $| \beta^{G_\alpha} | = n_j$. In addition put $H = G_\alpha$ and $U = G_{\alpha\beta}$. By 3.2, $| H : U | = | \beta^H |$. The hypotheses of 17.3 are satisfied, and for $\gamma \in \Delta$ we therefore have $| \gamma^{G_\beta} | \geq | \gamma^U | = | \gamma^H | = n_k$, hence $| \gamma^{G_\beta} | = n_k$. Hence if Δ^* denotes the set of those $\xi \in \Omega$ for which $| \xi^{G_\beta} | \geq n_k$ then $\Delta \subseteq \Delta^*$. Because of the similarity of G_α and G_β, we have $| \Delta | = | \Delta^* |$. This implies that Δ is a fixed block of G_α and G_β, hence of $\langle G_\alpha , G_\beta \rangle$. We now conclude the argument as in 17.4.

We note the following theorems without proof.

Theorem 17.6. *Let G be primitive, K a (not necessarily transitive) constituent of G_α, $K \neq G_\alpha^\alpha$. If all the transitive constituents of G_α not contained in K are primitive, then K is faithful* (W. A. Manning, 1927).

Theorem 17.7. *Let G be primitive but not doubly transitive. Let G_α have a doubly transitive constituent K on Γ of degree $t > 2$. Then G_α has a transitive constituent L of degree $m > t$ such that m is a divisor of $t(t-1)$. (In particular, the longest transitive constituent of G_α in a primitive group G which is not doubly transitive is never doubly transitive.) If, in addition, K is doubly primitive and $\Gamma = \Gamma'$, then either K is faithful or*

$m = t(t-1)$. *In the latter case L is imprimitive and has K as a first primitive component* (W. A. Manning, 1927, 1929).

Exercise 17.8. Each primitive group of degree 8 *is doubly transitive* (Proof by 17.5).

§18. The Structure of the Transitive Constituents of G_α in Primitive Groups G

Throughout this section let G be primitive, and let Γ be an orbit of G_α different from α.

Proposition 18.1. *Let the subgroup $V \neq 1$ of G leave a point fixed. Then there is a $g \in G$ with $g^{-1}Vg = U \leq G_\alpha$ and $U^\Gamma \neq 1$.*

Proof. Let $\gamma \in \Gamma$. Let Δ be the set of those $\xi \in \Omega$ for which $\xi^V = \xi$ holds. Δ is a proper and nonempty subset of Ω. By Theorem 8.1 there exists $g \in G$ with $\alpha \in \Delta^g$ and $\gamma \notin \Delta^g$. Now put $g^{-1}Vg = U$. Then $\alpha^U = \alpha$ holds, thus $U \leq G_\alpha$ and $\gamma^U \neq \gamma$. The latter fact implies $U^\Gamma \neq 1$.

Theorem 18.2. *If K is an (abstract) composition factor group of G_α (in the sense of the theorem of Jordan and Hölder), then there exists $U \leq G_\alpha$ such that K is a composition factor group of U^Γ.*

Proof. We choose $V \leq G_\alpha$ minimal such that K is still a composition factor group of V. By 18.1 we may choose $g \in G$ such that $U = g^{-1}Vg \leq G_\alpha$ and $U^\Gamma \neq 1$. Hence U_Γ is a proper normal subgroup of U. K appears as a composition factor group in U, but not in U_Γ because of the required minimality property. By the theorem of Jordan and Hölder K appears in $U/U_\Gamma \cong U^\Gamma$, as asserted.

This theorem allows numerous conclusions:

Theorem 18.3. *If G_α^Γ is solvable, then G_α is solvable.*

For were G_α not solvable, then G_α would contain a non-solvable composition factor group and by 18.2 G_α^Γ would also contain such a composition factor group. This contradicts the hypothesis.

Likewise the following theorem is obtained from 18.2.

Theorem 18.4. *If a prime p is a divisor of the order of G_α, then p also divides the order of G_α^Γ.*

[W. A. Manning gives another proof (1921, p. 83). The theorem was already known to Jordan (1870, p. 284).] We emphasize a particular case.

Theorem 18.5. *If G_α^Γ is a p-group, so is G_α.*

Remark. If, in addition, p is odd then G contains a regular normal subgroup; more generally this is true whenever G_α is nilpotent of odd order, and G primitive (Thompson, 1959).

Primitive groups G with a regular constituent in G_α have been investigated by Rietz (1904) and Weiss (1934). We prove a theorem due to Rietz:

Theorem 18.6. *Let Γ and Δ be paired orbits of G_α. Let the transitive constituents $C = C_\alpha^\Gamma$ and $D = G_\alpha^\Delta$ satisfy the following conditions: C is regular, and D_δ ($\delta \in \Delta$) has more than one fixed point in Δ. Then C is faithful, that is, $|G_\alpha| = |\Gamma|$.*

Proof of 18.6. Choose $\gamma \in \Gamma$. Since C is regular on Γ, we have $C_\gamma = 1$. This means that $G_{\alpha\gamma} = G_{\alpha\Gamma}$. Hence $G_{\alpha\gamma} \trianglelefteq G_\alpha$, that is, $G_\alpha \leq \mathbf{N}G_{\alpha\gamma}$. Since G is primitive, G_α is a maximal subgroup of G. Hence either $\mathbf{N}G_{\alpha\gamma} = G_\alpha$ or $\mathbf{N}G_{\alpha\gamma} = G$.

If $\mathbf{N}G_{\alpha\gamma} = G_\alpha$, choose $s \in G$ such that $\gamma^s = \alpha$ and $\alpha^s = \delta$; this is possible since Γ and Δ are paired orbits of G_α. Transformation by s yields $\mathbf{N}G_{\delta\alpha} = G_\delta$. This implies that the

normalizer of $G_{\delta\alpha}$ in G_α is $G_{\delta\alpha}$. Hence the normalizer of D_δ in D is D_δ, contrary to the assumption of the theorem.

Hence $\mathbf{N}G_{\alpha\gamma} = G$. This implies $G_{\alpha\gamma} = 1$ by 7.1. Consequently, by 3.2, $|G_\alpha| = |\gamma^{G_\alpha}| = |\Gamma|$, as asserted.

Theorem 18.7. *If G_α has an orbit Γ with $|\Gamma| = 2$, then G contains a regular normal subgroup R of index 2. G is a Frobenius group.*

Proof. From $|\Gamma| = 2$ it follows that $|G_\alpha^\Gamma| = 2$, thus G_α^Γ is regular. By 18.5, G_α is a 2-group, hence nilpotent. From 18.6 it now follows that $|G_\alpha| = 2$. Every orbit of G_α therefore has length 1 or 2. However only $\{\alpha\}$ has length 1 (by 8.7). By 5.1, G contains a regular normal subgroup R which has index 2 since $|G_\alpha| = 2$.

Exercise 18.8 (Miller, 1899). *The normal subgroup R mentioned in Theorem* 18.7 *has prime order.*

Remark. It would be interesting to know what can be concluded from the existence of an orbit of G_α of length 3, or of a nilpotent or Frobenius constituent of G_α.

§19. Transitive Extension

The questions dealt with in this chapter so far can be reversed in the following way. Let a permutation group L on Ω be given under which a point α is left fixed. Is there a *transitive* group G on Ω such that $G_\alpha = L$, and how can all such groups be constructed?

Complete results do not seem to exist to date. Sufficient conditions for the existence of a solution G are known, which are especially handy when L is transitive on $\Omega - \alpha$ (W. A. Manning, 1921, p. 41).

The procedure has been used for the construction of multiply transitive groups; for this see, e.g., de Séguier (1912), Zassenhaus (1935b), Witt (1937), Holyoke (1952).

CHAPTER IV

The Method of Schur

In addition to the method of group characters applied with great success to permutation groups, particularly by Frobenius and Burnside, and to which we are indebted for the fundamental theorems 5.1 and 11.7, there is a less known method of Schur (1933) which is able to produce similarly deep results although it is substantially more elementary. The method is designed for the investigation of those permutation groups which contain a regular subgroup of the same degree. Its fundamental idea consists in taking as "points" not, as we have done up to now, arbitrary objects or the numbers from 1 to n, but rather group elements.

§20. Introduction of Group Elements as Points

Differing from Schur, who started with concepts from representation theory which will be discussed in the next chapter, we proceed in the following manner. If a permutation group G on Ω is to be investigated, we choose a regular permutation group H on Ω. It would not have to be contained in G, but this is the most important case, and we will assume $H \leq G$ throughout. We distinguish a point $\alpha \in \Omega$ and associate with every point $\xi \in \Omega$ that uniquely determined permutation $h \in H$ for which $\alpha^h = \xi$. By virtue of this

one-to-one mapping of Ω onto H we can also consider G *as a permutation group on* H; to the permutation $g \in G$ corresponds, on H, the permutation $\binom{h}{h^g}$ in which h^g is uniquely specified by the formulas

$$\alpha^{(h^g)} = \alpha^{hg}, \qquad h^g \in H. \tag{1}$$

(Henceforth the letter h will be reserved for the general element of H.) Where no confusion can occur, we denote the new permutation as well by g and the group on H formed by these permutations (which is therefore different from G only in the designation of points) again by G. The advantage of the new "points" is that for them a multiplication is defined, namely, the group multiplication in H. The regular group H itself assumes a particularly simple form in the new points. From (1) it follows immediately that:

Proposition 20.1. *For* $k \in H$, $h^k = hk$.

[Moreover, this formula shows that every regular group under the replacement of its points by group elements described above goes over into its own right regular representation in the sense of §4. Similarly we can get the left representation: under an appropriate (and in the non-Abelian case different) replacement of points by group elements, the regular group goes over into its left regular representation.] By 20.1 we have in general for two complexes $L, K \subseteq H$: $L^K = LK$. The normalizer of H also assumes a simple form in the new points. (1) implies:

Proposition 20.2. *If* $g^{-1}hg \in H$ *and* $g \in G_\alpha$, *then* $h^g = g^{-1}hg$.

Under the mapping $\Omega \to H$ the distinguished point α of Ω corresponds to the identity element 1 of H. We may therefore write G_1 instead of G_α. The groups conjugate to G_1 are the G_h. In the remainder of Chapter IV we make scarcely any use of Ω. In the next sections we speak only of groups on H, that is, of subgroups of the symmetric group S^H.

§21. Transitivity Modules

We can also apply the permutations g on H considered in the previous section in an obvious way to the formal linear combinations $\eta = \sum_{h\in H} c_h h$, in which the coefficients c_h may be taken from any ring $\mathfrak{R}$ with a unit element. In order to present Schur's method in the most elementary manner we will assume in this chapter that $\mathfrak{R}$ is the ring of rational integers although in the next chapter $\mathfrak{R}$ will be taken as the field of complex numbers. We define

$$\left(\sum c_h h\right)^g = \sum c_h h^g. \tag{1}$$

The set of the $\eta = \sum c_h h$ can in a natural way be interpreted as a module, and under the multiplication defined in H also as an associative ring, the *group ring* $\mathfrak{R}(H)$. We usually denote the elements of a group ring ("quantities") by lower case Greek letters. Those ring elements η, for which the coefficients c_h have only the values 0 and 1 are called *simple* quantities. If K is a complex of elements of H, then we denote by $\underline{K}$ the corresponding simple quantity $\sum_{k\in K} k$.

Any given permutation group G on H produces a decomposition of the point set H into subsets, namely, into the orbits $T_1, \cdots, T_k$ of G. We call the module spanned by the corresponding simple quantities $\tau_i = \underline{T_i}$ $(i = 1, \cdots, k)$ the *transitivity module* $\mathfrak{R}(H, G)$ belonging to G. It consists of all linear combinations $\sum_i c_i\tau_i$ $(c_i \in \mathfrak{R})$. Obviously the following rules hold:

Proposition 21.1. *Let* $\eta \in \mathfrak{R}(H)$. *Then* $\eta \in \mathfrak{R}(H, G)$ *if and only if* $\eta^g = \eta$ *for all* $g \in G$.

Proposition 21.2. *If* $\tilde{G} \leq G \leq S^H$ *and* $s \in S^H$, *then* $\mathfrak{R}(H, \tilde{G}) \supseteq \mathfrak{R}(H, G)$, $\mathfrak{R}(H, s^{-1}Gs) = (\mathfrak{R}(H, G))^s$.

Since for the group $\langle G, \tilde{G}\rangle$ generated by two arbitrary

groups on H the set of fixed blocks is the intersection of the two fixed block sets for G and $\tilde{G}$, we have:

Proposition 21.3. *If* $G \leq S^H$ *and* $\tilde{G} \leq S^H$, *then* $\mathfrak{R}(H, \langle G, \tilde{G} \rangle) = \mathfrak{R}(H, G) \cap \mathfrak{R}(H, \tilde{G})$.

As an example of the determination of transitivity modules, we prove the simple theorem:

Theorem 21.4. *If U is a subgroup of H, then $\mathfrak{R}(H, U)$ is spanned by the left cosets hU.*

Proof. By 21.1, $\eta \in \mathfrak{R}(H, U)$ is equivalent to $\eta^u = \eta$ for all $u \in U$, and this again means the same thing as $\eta u = \eta$ by 20.1.

Which submodules in $\mathfrak{R}(H)$ are transitivity modules? Since the orbits of a permutation group may be prescribed arbitrarily as mutually disjoint sets with union H, the answer obviously is:

Theorem 21.5. *A submodule $\mathfrak{S}$ of $\mathfrak{R}(H)$ is the transitivity module of a group G on H to be chosen appropriately, if and only if $\mathfrak{S}$ has a basis $\alpha_1, \cdots, \alpha_m$, in which each α_i is a simple quantity of $\mathfrak{R}(H)$ and*

$$\sum_{i=1}^{m} \alpha_i = \underline{H}.$$

Definition. We will call such a submodule of $\mathfrak{R}(H)$ an *S-module over H.*

§22. Computation in S-Modules

From the defining property of S-modules, namely, the existence of a basis of simple quantities, four remarks follow immediately, of which the first three are due to Schur (expressed differently; Schur avoided the use of the group ring).

Proposition 22.1. *Let* $\mathfrak{S}$ *be an S-module,* $\sum c_h h \in \mathfrak{S}$, *and* $c \in \mathfrak{R}$. *Then* $\mathfrak{S}$ *also contains the simple quantity* $\sum' h$ *where the summation is over those h for which* $c_h = c$.

Proposition 22.2. *Let* $\mathfrak{S}$ *be an S-module,* $\eta = \sum c_h h \in \mathfrak{S}$ *and K the complex of the elements h actually appearing in* η (*i.e., with* $c_h \neq 0$). *Then the corresponding simple quantity* $\underline{K}$ *is contained in* $\mathfrak{S}$.

Proposition 22.3. *Let* $\mathfrak{S}$ *be an S-module,* $\eta = \sum c_h h \in \mathfrak{S}$, *and* $f(x)$ *an arbitrary* (*single-valued!*) *function with values in* $\mathfrak{R}$, *which is defined for all* $x \in \mathfrak{R}$. *We define* $f[\eta] = \sum f(c_h)\, h$. *Then* $f[\eta] \in \mathfrak{S}$.

Proposition 22.4. *Let* $\mathfrak{S}$ *be an S-module,* $\eta = \sum c_h h$, $\zeta = \sum d_h h$. *We define a "circle multiplication" by* $\eta \circ \zeta = \sum c_h d_h h$. Then $\eta \in \mathfrak{S}$ *and* $\zeta \in \mathfrak{S}$ *imply* $\eta \circ \zeta \in \mathfrak{S}$.

As is easily verified, the following rules hold for the circle multiplication [defined in the whole of $\mathfrak{R}(H)$]:

Proposition 22.5. *The circle multiplication is associative, commutative, and distributive with respect to addition. Moreover,* $(\eta \circ \zeta)^g = \eta^g \circ \zeta^g$ *for all* $g \in G$, *in particular,* $(\eta \circ \zeta)\, h = \eta h \circ \zeta h$ *for all* $h \in H$.

For simple quantities the circle multiplication amounts to the formation of an intersection of the corresponding complexes in H: $\underline{K} \circ \underline{K}' = \underline{K \cap K'}$. An S-module is a ring with respect to addition and circle multiplication.

§23. S-Rings

Definition 23.1. An *S-ring* over H is an S-module over H which is at the same time a subring of the group ring $\mathfrak{R}(H)$ (and therefore contains the product $\eta\zeta$, formed using

the group multiplication in H, whenever it contains η and ζ) and in addition contains the identity element 1 as well as every quantity $\eta^* = \sum c_h h^{-1}$ whenever it contains $\eta = \sum c_h h$.

Note. The identity element can be dispensed with (Wielandt, 1949); however, in the applications to be mentioned in this book it is always present and makes the discussion easier. In the following every S-ring will therefore contain both 1 and the sum $\underline{H}$ of all elements of H. The linear combinations $a \cdot 1 + b \cdot \underline{H}$ form an S-ring which can be characterized as the intersection of all S-rings over H and in the following is called the *trivial* S-ring over H. On the other hand, there is an S-ring over H containing all others, namely, the whole group ring $\mathfrak{R}(H)$.

Definition 23.2. An S-ring $\mathfrak{S}$ over H is called *primitive* if $K = 1$ and $K = H$ are the only subgroups of H for which $\underline{K} \in \mathfrak{S}$ holds.

For example, every trivial S-ring is primitive. There are groups H, over which this is the only primitive S-ring. The significance of such a statement for the theory of permutation groups will be made evident in the next section (Theorem 24.13).

We note the computation rules for $\eta^* = \sum c_h h^{-1}$:

Proposition 23.3. $\eta^{**} = \eta$, $(a\eta + b\zeta)^* = a\eta^* + b\zeta^*$, $(\eta\zeta)^* = \zeta^*\eta^*$, *and* $\eta\eta^* = 0$ *only for* $\eta = 0$.

In the remainder of this section, let $\mathfrak{S}$ be an arbitrary S-ring over H.

Proposition 23.4. *Let* $\underline{K} \in \mathfrak{S}$, $\underline{L} \in \mathfrak{S}$, $c \in \mathfrak{R}$, $M = M_c$ *the set of those* $h \in H$ *for which there are exactly* c *pairs* k, l *with* $kh = l$, $k \in K$, $l \in L$. *Then* $\underline{M} \in \mathfrak{S}$.

Proof. Since $h = k^{-1}l$, $\underline{M}$ is the sum of those elements of H which appear in $\underline{K}^* \underline{L}$ with the coefficient c. By 22.1, $\underline{M} \in \mathfrak{S}$.

Proposition 23.5. *Let $\eta \in \mathfrak{S}$ and M the set of $h \in H$ with $\eta h = \eta$. Then M is a subgroup of H, and $\underline{M} \in \mathfrak{S}$.*

Proof. The group property is clear. If $\underline{K_k}$ is the sum of the elements of H which appear in η with a fixed coefficient k, and $\underline{M_k}$ the sum of the solutions h of $\underline{K_k}h = \underline{K_k}$, then by 23.4 certainly $\underline{M_k} \in \mathfrak{S}$ (choose $K = L = \underline{K_k}$ and $c = |K_k|$). Therefore $\underline{M} = \underline{M_1} \circ \underline{M_{-1}} \circ \underline{M_2} \cdots \in \mathfrak{S}$.

Proposition 23.6. *Let $\eta \in \mathfrak{S}$, $\eta \neq 0$. Let K be the subgroup of H which is generated by the elements h actually appearing in η (i.e., those with $c_h \neq 0$). Then $\underline{K} \in \mathfrak{S}$.*

Proof. First, by 22.2, the sum σ of the elements of H actually appearing in η certainly lies in $\mathfrak{S}$. Because of the ring property the same thing holds for every quantity $\tau = \sigma + \sigma^2 + \cdots + \sigma^m$.

Therefore $\mathfrak{S}$ also contains the sum of the elements actually appearing in τ. For sufficiently large m this coincides with $\underline{K}$. This proves 23.6. It follows that:

Proposition 23.7. *If $\mathfrak{S}$ is primitive, $\eta \in \mathfrak{S}$, $\eta \neq c \cdot 1$, then the elements actually appearing in η generate the whole group H.*

Proposition 23.8. *If $\mathfrak{S}$ is primitive, $\eta \in \mathfrak{S}$, $\eta \neq c\underline{H}$, then $\eta h = \eta$ implies $h = 1$.*

This follows from 23.5. If the underlying group H is Abelian, then the S-rings over H have an important property discovered by Schur:

Theorem 23.9. *Let $\mathfrak{S}$ be an S-ring over the Abelian group H of order n, and let m be an integer. For every $\eta = \sum c_h h \in \mathfrak{S}$ put $\eta^{(m)} = \sum c_h h^m$. Then:*

(a) *If m is prime to n, then $\eta^{(m)} \in \mathfrak{S}$.*

(b) *If $m = p$ is a prime divisor of n and if $\mathfrak{S}$ is in addition primitive, then $\eta^{(p)} \equiv d \cdot 1 \pmod{p}$ for an appropriate integer d. The congruence is to be understood as holding for the coefficients.*

Preliminary Remark. Obviously

$$\text{(I)} \quad (a\eta + b\zeta)^{(m)} = a\eta^{(m)} + b\zeta^{(m)}, \qquad \eta^{(mm')} = (\eta^{(m)})^{(m')},$$
$$\eta^{(-1)} = \eta^*.$$

From the first formula it follows that the proof of Theorem 23.9 has only to be carried out for simple quantities η. The second formula shows that it is sufficient in the proof of part (a) to settle the case that m is a prime number prime to n. Then by (I), (a) applies also to composite exponents $m = \prod_i p_i$, and by the third formula of (I) also to $m = -\prod_i p_i$.

Proof of 23.9. First let p be an arbitrary prime. For a simple quantity η, the well known polynomial congruence $(\sum X_i)^p \equiv \sum X_i^p \pmod{p}$ implies (because of the assumed commutativity of H) the coefficient congruence $\eta^p \equiv \eta^{(p)} \pmod{p}$. If we introduce, for rational integers x,

(II) $f_p(x) =$ smallest non-negative residue of $x \pmod{p}$,

then we have $f_p[\eta^p] = f_p[\eta^{(p)}]$. The first quantity lies in $\mathfrak{S}$ by 22.3 since $\eta^p \in \mathfrak{S}$. Therefore $f_p[\eta^{(p)}]$ lies in $\mathfrak{S}$.

Now let the hypothesis of 23.9(a) be satisfied, hence p not a divisor of n. Then $\eta^{(p)}$ is a simple quantity as is η, consequently $\eta^{(p)} = f_p[\eta^{(p)}] \in \mathfrak{S}$, as asserted.

If on the other hand the hypotheses of 23.9(b) are satisfied, in particular p a divisor of n, then in $f_p[\eta^{(p)}]$ only such elements of H appear which have the form h^p. These generate a *proper* subgroup of H. By 23.7, $f_p[\eta^{(p)}] = d \cdot 1$, thus $\eta^{(p)} \equiv d \cdot 1 \pmod{p}$, as asserted.

We add two supplementary notes to Theorem 23.9.

(A) Since in the group H raising each element to the mth

power in the case $(m, n) = 1$ brings about an automorphism, the induced mapping $\eta \to \eta^{(m)}$ is also an automorphism of $\mathfrak{S}$. If for fixed η, m is allowed to run through all the numbers prime to n, the different quantities $\eta^{(m)}$ are called, after Schur, the *quantities conjugate to* η. If these consist only of η, then η is called *rational*. In particular, for arbitrary η, the sum of all conjugate quantities [the "trace" ("Spur") of η] is always rational (and lies in $\mathfrak{S}$ whenever η does). We do not go further into the rational quantities here, since they will not appear in this book. However, they are important. Applications are found in Schur (1933), Kochendörffer (1937), Wielandt (1949), and Bercov (1962).

(B) If H is not commutative, $\eta^{(m)}$ can still always be formed, but it is not known if—or more precisely to what extent—Theorem 23.9 remains valid. If H does not depart from commutativity too much, 23.9 can be at least partially preserved, as has been shown in the case of the dihedral groups (Wielandt, 1949). For the general case (e.g., the icosahedral group) this question is open.

Remark. An extensive ring-theoretical investigation of an important class of S-rings $\mathfrak{S}$ over H has been undertaken by Tamaschke (1963). The assumption is that $\mathfrak{S}$ lies in the center of the group ring $\mathfrak{R}(H)$.

§24. The Relationship between S-Rings and Permutation Groups

Henceforth let G be a permutation group on H in the sense of §20; *in particular, let H be contained in G*, namely, in the form of its own right regular representation. Then according to 20.1, for $h, k \in H$, we have $h^k = hk$. Such permutation groups G are related to S-rings in a manner which is fundamental for this whole theory:

Theorem 24.1. *The transitivity module of G_1 is an S-ring* (Schur, 1933).

We will deduce this theorem from a more general one.

Theorem 24.2. *The transitivity module of G_1 is a set of left operators for the transitivity module of every subgroup of G. In other words, if $U \leq G$, then $\mathfrak{R}(H, G_1)\,\mathfrak{R}(H, U) \subseteq \mathfrak{R}(H, U)$.*

(Because $1 \in \mathfrak{R}(H, G_1)$ we even have $=$ instead of $\subseteq$.) We carry out the proof in several steps. We begin with a simple remark.

Proposition 24.3. *For all $h \in H$, $g \in G$, h^g is the uniquely determined element of H which satisfies the equation $\underline{G_1}h^g = \underline{G_1}hg$ where $\underline{G_1}$ denotes the sum of all elements of G_1 [in the group ring $\mathfrak{R}(G)$].*

Proof. By §20, Eq. (1), h^g is the uniquely determined element of H for which $\alpha^{h^g} = \alpha^{hg}$ holds. This requirement is equivalent to $G_\alpha h^g = G_\alpha hg$, thus in the new "points" to $G_1h^g = G_1hg$. If this equation is interpreted in the group ring $\mathfrak{R}(G)$, the assertion is obtained.

We generalize 24.3.

Theorem 24.4. *For every $\eta \in \mathfrak{R}(H)$ and $g \in G$, η^g is the uniquely determined element of $\mathfrak{R}(H)$ for which $\underline{G_1}\eta^g = \underline{G_1}\eta g$ holds.*

Proof. (a) If $\eta = \sum c_h h$ then it follows from 24.3 that

$$\underline{G_1}\eta^g = \underline{G_1}\left(\sum c_h h^g\right) = \sum c_h \underline{G_1}h^g = \sum c_h \underline{G_1}hg = \underline{G_1}\eta g.$$

(b) That η^g is characterized within $\mathfrak{R}(H)$ by this property follows from the linear independence of different cosets $\underline{G_1}h$ in the group ring $\mathfrak{R}(G)$.

Handy criteria for the membership of a fixed element of

$\mathfrak{R}(H)$ in $\mathfrak{R}(H, U)$ or $\mathfrak{R}(H, G_1)$ follow from the last theorem. We show:

Theorem 24.5. *Let $\eta \in \mathfrak{R}(H)$. Then $\eta \in \mathfrak{R}(H, U)$ if and only if for every $u \in U$, $\underline{G_1}\eta u = \underline{G_1}\eta$. Equivalently $\underline{G_1}\eta\underline{U} = |\, U \,|\, \underline{G_1}\eta$.*

Proof. The first part follows immediately from 24.4, if the defining property $\eta^u = \eta$ of the quantities of $\mathfrak{R}(H, U)$ is used. The second part follows from the first by adding over all $u \in U$.

Theorem 24.6. *Let $\eta \in \mathfrak{R}(H)$. Then $\eta \in \mathfrak{R}(H, G_1)$ if and only if $\underline{G_1}\eta = \eta\underline{G_1}$ holds.*

Proof. (a) From $\underline{G_1}\eta = \eta\underline{G_1}$ it follows that $\underline{G_1}\eta\underline{G_1} = \underline{G_1^2}\eta = |\, G_1 \,|\, \underline{G_1}\eta$. By 24.5, $\eta \in \mathfrak{R}(H, G_1)$.

(b) We need prove the converse only for simple quantities η since by 21.5 every quantity in $\mathfrak{R}(H, G_1)$ can be built up linearly from simple quantities. Therefore let $\eta = \underline{K}$, $K \subseteq H$. By 24.5 we have $\underline{G_1}\underline{K}\underline{G_1} = |\, G_1 \,|\, \underline{G_1}\underline{K}$, thus by disregarding multiplicity we have $G_1 K = G_1 K G_1$.

This equation shows that the complex $G_1 K$ consists not only of right cosets of G_1 as was clear from the beginning, but also of complete left cosets. [Here a close relationship of $\mathfrak{R}(H, G_1)$ with the double module decomposition of G by (H, H) which was emphasized by W. A. Manning (1939) is evident. On double module decompositions in general see Speiser (1937, §21).] In particular we have $KG_1 \subseteq G_1 K$. Now, however, because of the regularity of H, any two cosets hG_1, $h'G_1$ with $h \neq h'$ are distinct, and therefore KG_1 contains as many elements as $G_1 K$. Consequently, $KG_1 = G_1 K$, hence $\underline{K}\underline{G_1} = \underline{G_1}\underline{K}$ as asserted.

From the last theorem a comprehensive result follows.

Theorem 24.7. *Let* $\eta \in \mathfrak{R}(H)$ *and* $\lambda \in \mathfrak{R}(H, G_1)$. *Then* $(\lambda\eta)^g = \lambda\eta^g$ *for all* $g \in G$.

Proof. $\underline{G_1}\lambda\eta^g = \lambda\underline{G_1}\eta^g = \lambda\underline{G_1}\eta g = \underline{G_1}\lambda\eta g$, and $\lambda\eta^g \in \mathfrak{R}(H)$. By 24.4, $\lambda\eta^g = (\lambda\eta)^g$.

Theorem 24.2, which was formulated in the beginning, follows immediately from 24.7: if $\eta^u = \eta$, then $(\lambda\eta)^u = \lambda\eta^u = \lambda\eta$. Schur's fundamental theorem 24.1 is now easily shown. For by 24.2, $\mathfrak{R}(H, G_1)$ is a ring; we have further $1 \in \mathfrak{R}(H, G_1)$, for G_1 has 1 as an orbit; and finally if $\mathfrak{R}(H, G_1)$ contains η it also contains η^* for from $\underline{G_1}\eta = \eta\underline{G_1}$ and $\underline{G_1} = \underline{G_1}^*$ we have by 23.3 that $\underline{G_1}\eta^* = \eta^*\underline{G_1}$, thus by 24.6 that $\eta^* \in \mathfrak{R}(H, G_1)$.

The fundamental theorem 24.7 specifies certain left multiplications with which the mapping $\eta \to \eta^g$ commutes. There are also right multiplications with this property.

Theorem 24.8. *Let* $\eta \in \mathfrak{R}(H)$, $g \in G$, $K \subseteq H$, *and* $Kg = gK$. *Then* $(\eta\underline{K})^g = \eta^g\underline{K}$.

Proof. $\underline{G_1}\eta^g\underline{K} = \underline{G_1}\eta g\underline{K} = \underline{G_1}\eta\underline{K}g$ and $\eta^g\underline{K} \in \mathfrak{R}(H)$.

The following is proved similarly for an arbitrary subgroup U of G.

Theorem 24.9. *If* $K \subseteq H$ *and* $\underline{U}\underline{K} = \underline{K}\underline{U}$, *then* $\mathfrak{R}(H, U)\,\underline{K} \subseteq \mathfrak{R}(H, U)$.

In particular this implies:

Theorem 24.10. *If* $k \in H \cap \mathbf{N}(U)$, *then* $\mathfrak{R}(H, U)\,k = \mathfrak{R}(H, U)$.

We conclude with several theorems due to Schur which lead to the applications of S-rings to permutation groups.

Theorem 24.11. *G is doubly transitive if and only if the transitivity module of G_1 coincides with the trivial S-module over H, i.e., contains only quantities of the form $a \cdot 1 + b\underline{H}$.*

Proof. By the definition of transitivity module given in §21, the number of basis elements of $\mathfrak{R}(H, G_1)$ coincides with the number of orbits of G_1.

Theorem 24.12. *The group G is primitive if and only if the transitivity module of G_1 is a primitive S-ring in the sense of Definition* 23.2.

Proof. (a) If $\mathfrak{S} = \mathfrak{R}(H, G_1)$ is not primitive, then there is a subgroup K of H such that $1 < K < H$ and $\underline{K} \in \mathfrak{R}(H, G_1)$. By 24.6, $\underline{G_1}\underline{K} = \underline{K}\underline{G_1}$, therefore $G_1K = Z$ is a group. Its order is $|G_1||K|$, hence $G_1 < Z < G$ and therefore G is imprimitive.

(b) If G is imprimitive, there is a group Z with $G_1 < Z < G$. By decomposition of the elements $z \in Z$ in the form $z = gh$ with $g \in G_1$ and $h \in H$, we get that $Z = G_1K$ with $K = H \cap Z$. It follows that $1 < K < H$ and $\underline{G_1}\underline{K} = \underline{Z} = \underline{Z^*} = \underline{K^*}\underline{G_1^*} = \underline{K}\underline{G_1}$, thus $\underline{K} \in \mathfrak{S}$, hence $\mathfrak{S}$ is imprimitive.

For application to a permutation group given in arbitrary form we state the following theorem.

Theorem 24.13. *Let H be regular on Ω. Let the trivial S-ring be the only primitive S-ring over H. Then every group G primitive on Ω and containing H is doubly transitive.*

We will now investigate groups H with this property.

§25. Burnside Groups

Definition 25.1. By a *Burnside-group* (in short: *B-group*) we mean an abstract finite group H with the property that every primitive group containing the regular representation of H as a transitive subgroup is doubly transitive.

We choose this name because Burnside (1911, p. 343) gave the first example of such a group:

Theorem 25.2. *Every cyclic group whose order is of the form p^m (p prime, $m > 1$) is a B-group.*

The proof uses the theory of group characters. In 1921, Burnside tried to prove that every Abelian group which is not elementary Abelian is a B-group. However, this assertion is false. Burnside's error was pointed out by Dorothy Manning (1936). She indicated a class of counterexamples which can be deduced from a paper of W. A. Manning (1906), and which will be generalized below (Theorem 25.7). The first advance beyond Theorem 25.2 was obtained by Schur (1933):

Theorem 25.3. *Every cyclic group of composite order is a B-group.*

We prove this in a stronger form (Wielandt, 1935):

Theorem 25.4. *Every Abelian group of composite order which has at least one cyclic Sylow subgroup is a B-group.*

Proof. Let $|H| = n$. By hypothesis there is a prime p such that p divides n and $p < n$ and such that $x^p = 1$ has exactly p solutions in H. The number of $y \in H$ with $y^p = h$, for given $h \in H$, is therefore 0 or p. There is exactly one subgroup U of order p in H.

Let G be primitive and $\geq H$; in addition, let $\tau = \underline{T}$ be a basis element of $\mathfrak{S} = \mathfrak{R}(H, G_1)$. ($T$ is therefore an orbit of G_1.) By 24.12, $\mathfrak{S}$ is primitive. From 23.9(b) it follows that $\tau^{(p)} \equiv a \cdot 1(p)$; of course, a depends on τ. The number of $y \in H$ with $y^p = h \neq 1$ which actually appear in τ is therefore divisible by p. Hence it is 0 or p. If we put $\alpha = \tau \circ \underline{U}$, then there exists a $\beta \in \mathfrak{R}(H)$ with $\tau = \alpha + \underline{U}\beta$. Hence

$$\tau^2 = \alpha^2 + 2\underline{U}\alpha\beta + \underline{U}^2\beta^2 \equiv \alpha^2 + 2\underline{U}\alpha\beta\ (p),$$

the last statement holding because $\underline{U}^2 = |U| \cdot \underline{U} = p\underline{U}$. Because $\alpha^{(p)} = a \cdot 1$ we have $\underline{U}\alpha = a\underline{U}$, hence

$$\tau^2 - 2a\tau \equiv \alpha^2 - 2a\alpha = \gamma\ (p).$$

The left-hand side of this congruence is in $\mathfrak{S}$. If $f_p(x)$ denotes the smallest non-negative residue mod p, then it follows that $f_p[\tau^2 - 2a\tau] = f_p[\gamma] \in \mathfrak{S}$ by 22.3. From the primitivity of $\mathfrak{S}$ it follows by 23.7 that $f_p[\gamma] = b \cdot 1$ since in γ only elements of U appear.

Let $\gamma = \sum c_h h$ and $\alpha^2 = \sum d_h h$. Then d_h is the number of pairs h_1, h_2 (from the elements $h_1, h_2 \in H$ actually appearing in α) with $h_1 h_2 = h$. In α exactly a elements of H actually appear, thus $0 \leq d_h \leq a$, hence $-2a \leq c_h \leq a$.

We now assume that there is a basis element $\tau \neq 1$ of $\mathfrak{S}$ with $0 < a \leq \frac{1}{2}(p-1)$. Then it follows that $-(p-1) \leq c_h \leq \frac{1}{2}(p-1) < p-1$. From $f_p[\gamma] = b \cdot 1$ it further follows that $c_h \equiv 0(p)$ or $h = 1$, hence because of the last estimate of c_h, $c_h = 0$ or $h = 1$. Thus $\gamma = d \cdot 1$, $\alpha^2 = 2a\alpha + d \cdot 1$. This means that the elements of H appearing in α together with 1 form a subgroup of U. It is $\neq 1$ because $a \neq 0$. However, by 23.7 this is not possible because of the primitivity of $\mathfrak{S}$. Thus for all basis elements $\tau \neq 1$ we have $a = 0$ or $a > \frac{1}{2}(p-1)$.

We now assume that G is not doubly transitive. The number of basis elements of $\mathfrak{S}$ is then >2. If $a > \frac{1}{2}(p-1)$ held for two basis elements τ, τ' of $\mathfrak{S}$ different from 1, then more than $p-1$ elements $\neq 1$ occur in $(\tau + \tau') \circ \underline{U}$ which is impossible because $|U| = p$. Hence there is at least one basis element $\tau \neq 1$ with $a = 0$. For such an element $\tau = \underline{U\beta}$; the set of elements of H appearing in this τ is therefore a set union of residue classes mod U. Let M be the group of all $h \in H$ with $h\tau = \tau$. Then $1 < U \leq M < H$, the latter inequality since 1 does not occur in τ. By 23.5, $\underline{M} \in \mathfrak{S}$, which by 23.7 and 24.12 cannot occur for primitive G. G is therefore doubly transitive, as asserted.

We mention without proof:

Theorem 25.5. *If H is Abelian of type (p^a, p^b) with $a > b$, then H is a B-group.*

This theorem was proved by D. Manning (1936) with the method of Burnside and by Kochendörffer (1937) with the method of Schur. Both proofs are very complicated; the first moreover contains a gap (as D. Manning noticed later) which has not yet been closed. (Lemma II is false.)

Theorem 25.5 has been generalized in the same direction which led from 25.3 to 25.4.

Theorem 25.5'. *Every Abelian group H which has a Sylow group of type (p^a, p^b) with p an odd prime and $a > b$ is a B-group* (Bercov, 1962).

The following non-Abelian groups are known to be B-groups.

Theorem 25.6. (i) *Every dihedral group is a B-group* (Wielandt, 1949).

(ii) *Every generalized dicyclic group (defining relations: $x^{2n} = 1$, $y^2 = x^n$, $y^{-1}xy = x^{-1}$) is a B-group* (Scott, 1957).

(iii) *Let p be a prime number of the form $2 \cdot 3^a + 1$ where $a > 2$. Then the non-Abelian group of order $3p$ is a B-group* (Nagai, 1961).

We now construct the general class of counterexamples to Burnside's assertion, mentioned earlier.

Theorem 25.7. *A group H of the form*

$$H = H_1 \times H_2 \times \cdots \times H_d$$

with $|H_1| = |H_2| = \cdots = |H_d| = a > 2$ and $d > 1$ is never a B-group.

Proof. We choose a set Ω of ad points and decompose it into d subsets Φ_i each of a points: $\Omega = \Phi_1 + \Phi_2 + \cdots + \Phi_d$. We faithfully represent H in the following way as a permutation group on Ω. The elements of H_i $(i = 1, \cdots, d)$ shall permute

the points of Φ_i regularly and leave those of Φ_j fixed for $i \neq j$. For $h = h_1 \times \cdots \times h_d \in H$ ($h_i \in H_i$) we put $\alpha^h = \alpha^{h_i}$ if $\alpha \in \Phi_i$.

Let G be the largest subgroup of S^Ω for which the Φ_i are blocks. Clearly $|G| = d!(a!)^d$. Because $(\Phi_i)^H = \Phi_i$, we have $H \leq G$.

From each Φ_i we choose a point α_i and put $\Delta = \{\alpha_1, \alpha_2, \cdots, \alpha_d\}$. Let G^* be the subgroup of all $g \in G$ with $\Delta^g = \Delta$. Then $|G^*| = d!((a-1)!)^d$, thus $|G : G^*| = a^d = |H|$.

We represent G as a permutation group $\bar{G}$ on the cosets of G^*. This representation is faithful because $\bigcap_{g \in G} g^{-1}G^*g = 1$. Since $H \cap G^* = 1$, H is regular and transitive in this representation.

We show that $\bar{G}$ is primitive but not doubly transitive.

To prove the primitivity of $\bar{G}$ it is sufficient to show that no group lies properly between G^* and G, and for this that $\langle G^*, h\rangle = G$ for $1 \neq h \in H$. We put

$$M_i = G^*_{\Phi_1, \ldots, \Phi_{i-1}, \Phi_{i+1}, \ldots, \Phi_d}.$$

Then $M_i = S^{\Phi_i - \alpha_i}$, hence for every h with $1 \neq h \in H$, there exists some i such that $\langle M_i, h^{-1}M_ih\rangle = S^{\Phi_i}$ because $a > 2$. Since $S^{\Phi_i}, \ldots, S^{\Phi_d}$ are conjugate under G^*, they are all contained in $\langle h, G^*\rangle$. It follows that $\langle h, G^*\rangle \geq \langle S^{\Phi_1}, \cdots, S^{\Phi_d}, G^*\rangle = G$.

We have now to show that $\bar{G}$ is not doubly transitive. For a doubly transitive group P of degree n, we have $|P_\alpha : (P_\alpha \cap P_\beta)| = n - 1$ if $\alpha \neq \beta$ (see §9). Thus if $\bar{G}$ were doubly transitive we would have $|G^* : (G^* \cap h^{-1}G^*h)| = a^d - 1$ for all $h \in H$ with $1 \neq h$.

On the other hand, let $1 \neq h \in H_1$. Then $G^{**} = h^{-1}G^*h \cap G^*$ has the fixed block $\Delta \cup \Delta^h = \{\alpha_1, \alpha_1', \cdots, \alpha_d\}$ where $\alpha_1 \neq \alpha_1' \in \Phi_1$. This results in $|G^{**}| = (a-2)!\,(d-1)!\,((a-1)!)^{d-1}$, hence $|G^* : G^{**}| = d(a-1)$. For $d > 1$ and $a > 2$, however, $d(a-1) < a^d - 1$.

The following problems seem to present themselves next.

(i) Is the direct product of a B-group and a group of relatively prime order always a B-group?

(ii) Which Abelian groups of type $(2, \cdots, 2)$ of order 2^p (p prime) are B-groups? By 25.7 only these elementary Abelian groups need be considered as possible B-groups. Examples of certain groups of semilinear transformations over the finite field $GF(2^p)$ show that, in addition, $2^p - 1$ must also be a prime. It is not known whether this condition is sufficient.

§26. The Extension Group $\mathfrak{G}(H \mid \xi_1, \xi_2, \cdots)$

Again let H be a given fixed regular transitive group and let $\xi_1, \xi_2, \cdots \in \mathfrak{R}(H)$. We consider the set of all groups $G \geq H$ with $\xi_1, \xi_2, \cdots \in \mathfrak{R}(H, G_1)$. The group $\mathfrak{G}(H \mid \xi_1, \xi_2, \cdots)$ generated by all these groups is by 21.3 the largest group $L \geq H$ whose transitivity module $\mathfrak{R}(H, L_1)$ contains $\xi_1, \xi_2, \cdots$.

Definition. $\mathfrak{G}(H \mid \xi_1, \xi_2, \cdots) = \langle G \rangle_{G \geqq H, \xi_1, \xi_2, \ldots \in \mathfrak{R}(H, G_1)}$.

We now wish to determine the structure of $\mathfrak{G}(H \mid \xi_1, \xi_2, \cdots)$ for certain $\xi_1, \xi_2, \cdots$.

Theorem 26.1. *Let $1 < A < H$. Then $\mathfrak{G}(H \mid \underline{A})$ is the maximal imprimitive group with blocks Ah ($h \in H$).*

Proof. Let M denote the maximal imprimitive group with blocks Ah. From $\underline{A} \in \mathfrak{R}(H, G_1)$ it follows by 24.12 that G is imprimitive with blocks Ah. Therefore it follows that $G \leq M$, hence $\mathfrak{G}(H \mid \underline{A}) \leq M$.

Since A is a block of M, it is not moved under application of $M_1 : \underline{A}^{M_1} = \underline{A}$. This means that $\underline{A} \in \mathfrak{R}(H, M_1)$, i.e., $M \leq \mathfrak{G}(H \mid \underline{A})$.

Theorem 26.2. *Let $H = AB$ with $A \cap B = 1$. Then the largest subgroup $D = \mathfrak{G}(H \mid \underline{A}, \underline{B})$ of S^H for which $\underline{A}, \underline{B} \in \mathfrak{R}(H, D_1)$*

holds is a direct product, $D = M \times N$, *with* $M \cong S^B$ *and* $N \cong S^A$. *If in addition* $A \lhd H$ *holds, then* $A \leq N$.

Proof. $\mathfrak{G}(H \mid \underline{A}, \underline{B}) = \mathfrak{G}(H \mid \underline{A}) \cap \mathfrak{G}(H \mid \underline{B})$. We consider the elements of H as elements of a matrix $\mathfrak{M}$ in the following way: we associate the rows of $\mathfrak{M}$ with the right cosets Ah, the columns with the cosets $Bh'(h, h' \in H)$. It is easily verified that $Ah \cap Bh'$ consists of exactly one element of H (there is exactly one pair $a \in A$, $b \in B$ with $h'h^{-1} = b^{-1}a$). We take this element as the element of $\mathfrak{M}$ in the row Ah and the column Bh'. In $\mathfrak{M}$ every element of H appears exactly once. By 26.1 the rows and columns of $\mathfrak{M}$ are blocks of D. Now let M be the subgroup of permutations of D which map every column of $\mathfrak{M}$ onto itself, and N the subgroup of permutations which map every row of $\mathfrak{M}$ onto itself. Clearly $M \cap N = 1$ and $M, N \lhd D$. Moreover $D = MN$, thus $D = M \times N$, since for $d \in D$, if $a \in M$ and $b \in N$ are defined by $(Ah \cap Bh')^a = (Ah)^d \cap (Bh')$ and $(Ah \cap Bh')^b = (Ah) \cap (Bh')^d$, then $d = ab$. By 26.1 the columns and rows of $\mathfrak{M}$ may be arbitrarily permuted by M and N, respectively, thus $M \cong S^B$ and $N \cong S^A$.

We now assume in addition that $A \lhd H$. Let $a \in A$. By 20.1 $(Ah)^a = Aha = Aha\, h^{-1}h = Ah$, thus $a \in N$. Hence 26.2 is completely proved.

We now intend to give an example of an S-ring over H which is not of the form $\mathfrak{R}(H, G_1)$. It is still unknown which additional properties an S-ring $\mathfrak{S}$ over H must have in order that there be a $G \geq H$ such that $\mathfrak{S} = \mathfrak{R}(H, G_1)$.

For the remainder of this section let H be Abelian of type (p, p), for a prime p. We prove a lemma.

Lemma 26.3. *Let* P, P', *and* P'' *be distinct subgroups of* H *of order* p. (*It is possible to find such subgroups because* H *contains* $p + 1 \geq 3$ *subgroups of order* p.) *Let* Q *be a subgroup of* H

of order p. In addition let $\mathfrak{S} = \mathfrak{R}(H, G_1)$ and $\underline{P}, \underline{P}', \underline{P}'' \in \mathfrak{S}$. Then we also have $\underline{Q} \in \mathfrak{S}$.

Proof. $H = P \times P'$, and

$$G \leq \mathfrak{G}(H \mid \underline{P}, \underline{P}', \underline{P}'') \leq \mathfrak{G}(H \mid \underline{P}, \underline{P}') = M \times N$$

with $P \leq M$ and $P' \leq N$ (by 26.2). It now follows that $P \leq G \cap M = M^* \trianglelefteq G$, similarly $P' \leq G \cap N = N^* \trianglelefteq G$. We denote by $\langle g^{-1}Pg \rangle_{g \in G} = \operatorname{Nm} P (\leq M^*)$ the *norm* of P (with respect to G). We obtain $\operatorname{Nm} P \cap \operatorname{Nm} P' \leq M^* \cap N^* = 1$, similarly $\operatorname{Nm} P \cap \operatorname{Nm} P'' = 1$, $\operatorname{Nm} P' \cap \operatorname{Nm} P'' = 1$. M^* and N^* commute elementwise, thus $\operatorname{Nm} P$ and $\operatorname{Nm} P'$ do also. Similarly $\operatorname{Nm} P''$ commutes elementwise with $\operatorname{Nm} P$ and $\operatorname{Nm} P'$, hence also with $\operatorname{Nm} P \times \operatorname{Nm} P' \geq P \times P' = H$. This means that $\operatorname{Nm} P'' \leq \mathbf{Z}(H) = H$. Similarly $\operatorname{Nm} P$, $\operatorname{Nm} P' \leq H$. The norms of P, P', and P'' taken pairwise have only 1 in common. A comparison of their orders shows that P, P', and P'' coincide with their norms. Thus P, P', and P'' are normal subgroups of G.

Let s, s', s'' be generating elements of P, P', P''. Without loss of generality we may assume $s'' = ss'$. Since P, P', P'' are normal subgroups, there exist natural numbers a, b, c with $g^{-1}sg = s^a$, $g^{-1}s'g = s'^b$, $g^{-1}s''g = s''^c$ (a, b, c depend in general on $g \in G$). From $s''^c = s^a s'^b$ it follows that $a = b = c$. Thus for every $g \in G$ there is an a (not depending on the $h \in H$) such that $g^{-1}hg = h^a$. Hence we also have $Q \quad G$. This yields $\underline{G_1 Q} g = \underline{G_1} g^{-1} \underline{Q} g = \underline{G_1 Q}$ for all $g \in G_1$, hence $\underline{Q} \in \mathfrak{S}$ by 24.5.

Now it is easy to give the desired counterexample.

Theorem 26.4. *Let the hypotheses of* 26.3 *hold. In addition, let $p \geq 5$. Then the S-module $\mathfrak{S}$ generated by $1, \underline{P}, \underline{P}', \underline{P}''$, and $\underline{H}$ is an S-ring, but not of the form $\mathfrak{R}(H, G_1)$.*

Proof. The S-module $\mathfrak{S}$ is an S-ring, since because $PP' = H$ the ring property of $\mathfrak{S}$ is satisfied and if $\eta \in \mathfrak{S}$

we always have $\eta^* \in \mathfrak{S}$ since this property holds for the basis elements of $\mathfrak{S}$. $\mathfrak{S}$ has the simple basis quantities

$$\tau_1 = 1, \qquad \tau_2 = \underline{P} - 1, \qquad \tau_3 = \underline{P'} - 1, \qquad \tau_4 = \underline{P''} - 1,$$
$$\tau_5 = \underline{H} - \tau_1 - \tau_2 - \tau_3 - \tau_4 .$$

Now let Q be chosen different from P, P', and P''. If there were a group $G \geq H$ with $\mathfrak{S} = \mathfrak{R}(H, G_1)$, then by 26.3 the quantity $\underline{Q} - 1$ would have to be a linear combination of $\tau_1, \cdots, \tau_5$, and since $\underline{Q} - 1$ contains no sums from $\tau_1, \cdots, \tau_4$, we must have $\underline{Q} - 1 = \tau_5$. However, since $p \geq 5$, a comparison of the number of elements of H appearing on the two sides of the equation shows that this cannot occur.

§27. Supplementary Remarks

What in this chapter was described as the method of Schur does not contain all the ideas of his work of 1933; the connection with representation theory, which was Schur's starting point, will not be discussed until the next chapter. On the other hand, the presentation given here contains in some respects more, in particular the extension in §24 to arbitrary subgroups U of the investigation of the orbits undertaken by Schur only for $U = G_\alpha$, and the introduction of the extension groups in §26. The following remarks will show where these extensions have been used or might be used to advantage.

A. Groups of Degree p. By Burnside's theorem 25.2, a primitive group of degree p^m which contains a cycle of this order is always doubly transitive (p prime, $m > 1$). For $m = 1$ this theorem does not hold, as the regular groups of degree $p > 2$ show. Instead, we have the theorem already mentioned: Every transitive nonsolvable group of prime

degree is doubly transitive. Schur developed the beginning of his methods on this theorem. After Burnside (1901) had proven the theorem with group characters,[1] Schur (1908) published a new proof which was independent of group characters and irrational numbers and which already contained the essential points of the method formulated more generally in 1933; but in addition it made use of entirely different considerations (the representation of permutations over the field of p elements by polynomials). This proof has gone into Carmichael's book (1937) without change. The methods developed in §24 provide a purely group-theoretical proof of the theorem with the following addition.

Theorem 27.1. *Let the transitive group G of prime degree p contain a sharply doubly transitive proper subgroup. Then G is triply transitive.*

We use this opportunity to mention that Itô has investigated groups of degree p by different methods. (Itô, 1960a, 1960b, 1961, 1962b).

B. Groups of Degree p^2. Examples of non-simple Abelian groups which are not B-groups are given by the elementary Abelian groups of order p^2 ($p > 2$, prime). The desire to treat this simplest case, inaccessible by the original methods of Schur, led to the extension groups $\mathfrak{G}(H \mid \xi_1, \xi_2, \cdots)$. For example, the tools developed in §26 produce the following:

Theorem 27.2. *Let G be a primitive but not doubly transitive permutation group of degree p^2. Then $\mid G \mid \equiv 0 (p^3)$. If in addition there are in G two p-Sylow subgroups with intersection $\neq 1$, then G has a normal subgroup of index 2 which is the direct product of two intransitive groups.*

[1] See also Burnside (1906).

C. Groups of Degree p^m. For solvable groups Ritt (1922) proved in an entirely different way a theorem which looks similar to Burnside's theorem 25.2.

Theorem 27.3. *A primitive solvable group of degree p^m (p prime) cannot contain a cycle of degree p^m unless $m = 1$ or $m = p = 2$.*

D. Criteria for Nonsimplicity. An important application of the method of Schur is to demonstrate in certain cases the nonsimplicity of a given permutation group G. It is assumed that G contains a regular subgroup H which in turn has a sufficient number of normal subgroups. As an example we prove the useful theorem:

Theorem 27.4. *Let the permutation group G of degree n contain a transitive Abelian subgroup H of the same degree. Let G be imprimitive and $\psi_1, \cdots, \psi_m$ be a complete system of conjugate blocks ($1 < m < n$). Then those permutations of G which take each block ψ_i into itself form a normal subgroup N of G, which has $\psi_1, \cdots, \psi_m$ as orbits. We have $| N \cap H | = n/m$, hence $1 < N < G$.*

Proof. We have already established in 7.2 that the above-mentioned elements form a normal subgroup N. We now prove that a given block ψ_i is an orbit of N. Let $\alpha \in \psi_i$. Those elements $h \in H$ for which $\alpha^h \in \psi_i$ holds form a subgroup D. This subgroup has order $| \psi_i | = n/m$, because H is regular. Since H induces a transitive Abelian, hence regular, permutation group $\bar{H}$ on the set $\bar{\Omega} = \{\psi_1, \cdots, \psi_m\}$, we have $\bar{D} = \bar{H}_{\psi_i} = 1$, that is, $D \leq N$, hence $D = N \cap H$.

E. Factorization. If a permutation group G satisfies Schur's hypothesis to contain a regular subgroup H, then it can be decomposed into the product $G = HG_\alpha$. Thus H

and G_α are permutable as groups and the intersection of H and G_α is 1. Such "factorizations" $G = AB$ have been investigated generally for abstract groups a number of times in the last few years. The method of Schur can be formulated abstractly as follows. In the group ring of A those quantities which are permutable with $\underline{B}$ are investigated. It would undoubtedly be advantageous to develop the theory symmetrically with respect to both factors, and thus to investigate those quantities in the group ring of B which are permutable with $\underline{A}$, or more generally: those quantities in the group ring of G which are permutable with both $\underline{A}$ and $\underline{B}$. The problem of proving the well-known theorem stating the solvability of groups of order $p^a q^b$ without the use of group characters could serve as a guide for such a development.

F. Dropping of the Regularity of *H*. Let the permutation group G on Ω contain a subgroup H which is transitive but not necessarily regular. Let α be a fixed element chosen from Ω. Then the cosets $G_\alpha h$ may be introduced as new "points." The arguments in §20 and §24 can be applied to this more general case with slight modifications. We ignored this possibility there in order to simplify the presentation, especially since to date no applications exist. Such applications could, for example, occur in the direction of choosing $H = G$ and proving theorems of the kind dealt with in Chapter III. As a preparation, it might be useful to prove the theorems of Chapter III again by the methods of Schur under the additional hypothesis that H contains a regular subgroup.

G. Dropping of the Transitivity of *H*. It might be possible to extend Schur's method to the case of intransitive subgroups H of G. This is suggested by the following criterion for imprimitivity which will be used in §31 in the investigation of groups of degree $2p$.

Theorem 27.5. *Let G be transitive on Ω, $|G|$ not a prime number, $\alpha \in \Omega$, $\beta \in \Omega$, $\alpha \neq \beta$. Let G have a subgroup H intransitive on Ω with the properties $\beta^{G_\alpha} \subseteq \beta^H$ and $|\beta^H| \leq |\alpha^H|$. Then G is imprimitive and $|\beta^H| = |\alpha^H|$.*

Proof. Let V be the complex of all $v \in H$ with $\beta^v \in \beta^{G_\alpha}$ and V^* the complex of the inverse elements, v^{-1}.

(a) We calculate the number $|V| = |V^*|$ in two ways. On the one hand, $H_\beta V \subseteq V$, thus V consists of complete right cosets $H_\beta v$ of H_β. The number of these cosets is $|\beta^V|$. Because of the assumption $\beta^{G_\alpha} \subseteq \beta^H$ we have $\beta^V = \beta^{G_\alpha}$, thus $|V| = |H_\beta|\,|\beta^{G_\alpha}|$. On the other hand, $VH_\alpha \subseteq V$, thus V consists of complete left cosets vH_α of H_α. If the number of these cosets is x, then we have $x = |\alpha^{V^*}|$ and $|V| = x|H_\alpha|$. By combining both results we obtain

$$|H_\beta|\,|\beta^{G_\alpha}| = x|H_\alpha|. \tag{1}$$

Since by assumption $|\beta^H| \leq |\alpha^H|$ holds, we have $|H_\beta| \geq |H_\alpha|$, and it follows that $|\beta^{G_\alpha}| \leq x$.

(b) We now assert that $|\beta^{G_\alpha}| \geq x$ also holds. In order to prove this we first remark that

$$VG_\alpha \subseteq G_\beta V, \tag{2}$$

the right-hand side consisting of all $g \in G$ with

$$\beta^g \in \beta^V = \beta^{G_\alpha}, \qquad \text{and} \qquad \beta^{VG_\alpha} = \beta^{G_\alpha G_\alpha} = \beta^{G_\alpha}.$$

V takes exactly x points of Ω into α; the number of left cosets of G_α in VG_α is therefore x. $G_\beta V$ contains exactly $|\beta^{G_\alpha}|$ right cosets of G_β. Thus we have

$$x|G_\alpha| = |VG_\alpha| \leq |G_\beta V| = |G_\beta|\,|\beta^{G_\alpha}|, \tag{3}$$

hence $x \leq |\beta^{G_\alpha}|$.

(c) Together with $x \geq |\beta^{G_\alpha}|$ this yields $x = |\beta^{G_\alpha}|$. Hence $|H_\alpha| = |H_\beta|$ follows from (1), thus $|\beta^H| = |\alpha^H|$. In addition, it now follows from (3) that $|VG_\alpha| = |G_\beta V|$, hence (2) holds in the stronger form $VG_\alpha = G_\beta V$. This equation may be written in the form (corresponding to 24.6) $gVG_\alpha = G_\alpha gV$, where g is a fixed element of G with $\alpha^g = \beta$.

(d) From this last relation we get $G_\alpha V^* g^{-1} = V^* g^{-1} G_\alpha$, therefore,

$$G_\alpha V^* V = G_\alpha V^* g^{-1} gV = V^* g^{-1} G_\alpha gV = V^* g^{-1} gVG_\alpha = V^* VG_\alpha.$$

Hence G_α commutes with V^*V, hence also with $W = \langle V^*, V\rangle$. WG_α is therefore a group. $WG_\alpha < G$ holds since $W \leq H$ is intransitive. On the other hand, $|\alpha^W| \geq |\alpha^{V^*}| = x = |\beta^{G_\alpha}|$. If $|\beta^{G_\alpha}| = 1$, then $G_\alpha = G_\beta$, hence G is imprimitive by 8.6 and our assumptions. If on the other hand, $|\beta^{G_\alpha}| > 1$ holds, then $|\alpha^W| > 1$, $G_\alpha < G_\alpha W$, hence G is imprimitive by 7.4.

CHAPTER V

Relationship with Representation Theory

In this chapter permutation groups will be considered in the framework of representation theory. First we will indicate how Schur established his method. Then a theorem of Frame on the degrees of the irreducible constituents of permutation groups will be proved (§30). In conclusion it will be shown, in the case of groups of degree $2p$, that the methods of Burnside and Schur are supplementary and can be used together.

§28. The Centralizer Ring

Every permutation g on Ω can be regarded in the following way as a linear substitution in $|\Omega| = n$ variables.

The variables $X_1, \cdots, X_n$ are taken as points. We form column vectors

$$\mathfrak{x} = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}, \qquad \mathfrak{x}^g = \begin{pmatrix} X_{1^g} \\ \vdots \\ X_{n^g} \end{pmatrix} = g^*\mathfrak{x}$$

where $g^* = (\delta_{\alpha^g,\beta})_{\alpha,\beta=1,\ldots,n}$ is the n by n matrix corresponding to the linear transformation $\mathfrak{x} \to \mathfrak{x}^g$. ($\delta_{\alpha\beta} = 1$ for $\alpha = \beta$ and

$=0$ for $\alpha \neq \beta$ is the well-known Kronecker symbol.) We call g^* *the permutation matrix corresponding to* g. Such a matrix contains exactly one 1 in each row and column and zeros everywhere else. In addition, every permutation matrix g^* is *orthogonal*, i.e., the transpose $g^{*'}$ of g^* is identical with its inverse: $g^{*'} = g^{*-1}$. We obtain a faithful representation of S^Ω by $g \to g^*$. Now let $G \leq S^\Omega$. By G^* we denote the group of all matrices g^* with $g \in G$. Obviously G^* is isomorphic to G. We call G^* the *permutation representation* of G.

Definition 28.1. We now assume that G is transitive and consider the orbits of G_1. With each of these orbits Δ (including the trivial $\Delta = \{1\}$) we associate in the following way a matrix $\mathfrak{v}(\Delta) = (v^\Delta{}_{\alpha,\beta})$, $\alpha, \beta = 1, \cdots, n$ with elements:

$$v^\Delta{}_{\alpha\beta} = \begin{cases} 1, & \text{if there exists } g \in G \text{ and } \delta \in \Delta \text{ with} \\ & \quad 1^g = \beta \text{ and } \delta^g = \alpha \\ 0, & \text{otherwise.} \end{cases}$$

Thus, in the first column of $\mathfrak{v}(\Delta)$ we have exactly those $v^\Delta{}_{\alpha 1} = 1$ for which $\alpha \in \Delta$ holds.

If $\Gamma \neq \Delta$, the ones of $\mathfrak{v}(\Gamma)$ and $\mathfrak{v}(\Delta)$ do not occur in the same place. On the other hand, for each place (α, β) there is an orbit Δ of G_1 (namely, the one in which the $\alpha^{g^{-1}}$ with $1^g = \beta$ lies) such that $\mathfrak{v}(\Delta)$ has 1 in this position. We therefore have:

Proposition 28.2. *Let* $\mathfrak{M}$ *be the n by n matrix whose elements are all* 1. *Then* $\sum_\Delta \mathfrak{v}(\Delta) = \mathfrak{M}$. (*Here the summation is over all orbits of* G_1.)

In addition, we may immediately conclude from the transitivity of G and from 28.1 that:

Proposition 28.3. *Every matrix* $\mathfrak{v}(\Delta)$ *is uniquely determined by its elements in any row or column. Every row or column of* $\mathfrak{v}(\Delta)$ *contains exactly* $|\Delta|$ *ones.*

From now on let the elements of all matrices be taken from the field $\mathfrak{R}$ of complex numbers. We prove:

Theorem 28.4. *If a transitive permutation group G is regarded as a matrix group G^*, then the matrices which commute with all the matrices of G^* form a ring $V = V(G)$. We call V "the centralizer ring corresponding to G." V is a vector space over the complex number field which has the matrices $\mathfrak{B}(\Delta)$ corresponding to the orbits Δ of G_1 as a linear basis. In particular, the dimension of V coincides with the number k of orbits of G_1* (Schur, 1933).

Proof. Clearly V is a ring and a vector space. Now let $\mathfrak{B} = (v_{\alpha\beta})$ be an n by n matrix and let $g \in G$. Then

$$g^*\mathfrak{B}g^{*-1} = g^*\mathfrak{B}g^{*'} = (\delta_{\alpha^g,\sigma})\,(v_{\sigma,\tau})\,(\delta_{\tau,\beta^g})$$

$$= \Big(\sum_{\sigma,\tau=1}^{n} \delta_{\alpha^g,\sigma} v_{\sigma,\tau}\delta_{\tau,\beta^g}\Big) = (v_{\alpha^g,\beta^g}).$$

Thus $\mathfrak{B} = (v_{\alpha\beta}) \in V$ if and only if $v_{\alpha\beta} = v_{\alpha^g,\beta^g}$ for all $\alpha, \beta \in \Omega$ and all $g \in G$. From 28.1 it follows immediately that $\mathfrak{B}(\Delta) \in V(G)$ for every orbit Δ of G_1.

On the other hand, let $\mathfrak{B} = (v_{\alpha\beta}) \in V$ and $\mathfrak{B}(\Delta) = (v^{\Delta}_{\alpha\beta})$. If $v^{\Delta}_{\alpha\beta} = v^{\Delta}_{\alpha'\beta'} = 1$ then it follows that $\beta = 1^g$, $\alpha = \delta^g$, $\beta' = 1^{g'}$, $\alpha' = \delta'^{g'}$ with $\delta, \delta' \in \Delta$ and $g, g' \in G$. Hence $\alpha' = \delta'^{g'} = \delta^{sg'} = \alpha^{g^{-1}sg'}$ and $\beta' = \beta^{g^{-1}g'} = \beta^{g^{-1}sg'}$ for an appropriate $s \in G_1$; hence, finally $v_{\alpha\beta} = v_{\alpha'\beta'} = c(\Delta)$. Thus $\mathfrak{B} = \sum_{\Delta} c(\Delta)\,\mathfrak{B}(\Delta)$ as asserted. The last assertion of 28.4 is now evident.

We now aim at Schur's development of his method. Since in Schur's method certain regular subgroups H of G occur, we note an obvious relation between $V(H)$ and $V(G)$:

Proposition 28.5. *From $H \leq G$ it follows that $V(H) \geq V(G)$.*

We now investigate $V(H)$ for a regular permutation group H. Let h_α be the unique permutation of H which takes 1 into α. If we collect the h_α ($\alpha = 1, \cdots, n$) into a column $\mathfrak{H}$,

$$\mathfrak{H} = \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}, \quad \text{we have} \quad \mathfrak{H}h = \begin{pmatrix} h_1 h \\ \vdots \\ h_n h \end{pmatrix} = h^* \mathfrak{H}$$

since

$$h_\alpha h = \begin{pmatrix} 1 & \cdots \\ \alpha & \cdots \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha^h \end{pmatrix} \cdots = \begin{pmatrix} 1 & \cdots \\ \alpha^h & \cdots \end{pmatrix} = h_{\alpha^h}.$$

This, in matrix notation, is the right regular representation of H, introduced in §4, which was there also denoted by H^*. The permutation matrix $^*h = (\delta_{h^{-1}h_\alpha, h_\beta})_{\alpha,\beta=1,\ldots,n}$ assigned to each $h \in H$ by means of the equation $h^{-1}\mathfrak{H} = {}^*h\mathfrak{H}$ leads to a representation $^*H$ of H since

$$\begin{aligned} {}^*(hh')\,\mathfrak{H} &= (hh')^{-1}\mathfrak{H} = h'^{-1}h^{-1}\mathfrak{H} = h'^{-1}({}^*h\mathfrak{H}) = {}^*h({}^*h'^{-1}\mathfrak{H}) \\ &= {}^*h\,{}^*h'\mathfrak{H} (h, h' \in H). \end{aligned}$$

This representation is faithful. It is, in matrix notation, the left regular representation of G. Because $h^{-1}(\mathfrak{H}k) = (h^{-1}\mathfrak{H})k$ it is obvious that:

Proposition 28.6. *The matrix groups H^* and $^*H$ commute elementwise. We have $^*H \subseteq V(H)$.*

Every orbit Δ of H_1 has length 1, i.e., $\Delta = \{h_i\}$. The matrices introduced in 28.1 are in this case permutation matrices. From 28.1 it follows that $\mathfrak{B}(\Delta) = \mathfrak{B}(h_i) = (\delta_{\alpha, i^{h_\beta}})$. In addition, we have $\delta_{\alpha, i^{h_\beta}} = \delta_{h_i^{-1}h_\alpha, h_\beta}$, since $\alpha = i^{h_\beta}$ is equivalent to $h_\alpha = h_{i^{h_\beta}} = h_i h_\beta$, i.e., to $h_i^{-1}h_\alpha = h_\beta$. Thus it follows that:

Proposition 28.7. *For regular H, $*h_i = \mathfrak{B}(h_i)$.*

The connection with Chapter IV is supplied by the following theorem:

Theorem 28.8. *If G contains a regular subgroup H, then $V(G)$ is isomorphic to $\mathfrak{R}(H, G_1)$. The matrices $\mathfrak{B}(\Delta)$ correspond to the simple basis quantities τ_i (introduced in §21) of $\mathfrak{R}(H, G_1)$ (in the left regular representation of H).*

Remark. From this Schur arrived at the simple basis quantities τ_i and obtained the properties of $\mathfrak{R}(H, G_1)$ [without speaking of group rings; he used Frobenius' calculus of complexes, or, where multiplicities were involved, the representation matrices $\mathfrak{B}(\tau_i)$].

Proof of 28.8. By 28.5 and 28.7 every $\mathfrak{B} \in V(G)$ can be put in the form $\mathfrak{B} = \sum c_h *h$. We first show:

$$\mathfrak{B}(\Delta) = \sum_{1^h \in \Delta} *h. \tag{1}$$

Both sides of (1) are matrices of $V(H)$. By 28.3 and 28.4 it is therefore sufficient to show the equality of the first column of both sides of (1). We put $\mathfrak{B}(\Delta) = (v_{\alpha\beta}^{\Delta})$; by 28.1 we have

$$v_{\alpha 1}^{\Delta} = \begin{cases} 1, & \alpha \in \Delta \\ 0, & \alpha \notin \Delta \end{cases}.$$

Let $h_\alpha \in H$ again be defined by $1^{h_\alpha} = \alpha$. From the matrix representation of $*h$ (see the proof of 28.6) it follows that the elements of the first column of the right-hand side of (1) have the form

$$\sum_{1^h \in \Delta} \delta_{h^{-1}h_\alpha, 1} \qquad (\alpha = 1, \ldots, n)$$

(because $h_1 = 1$). This expression is therefore $=1$ if and only if $1^{h_\alpha} = \alpha \in \Delta$, otherwise it is $=0$. Hence (1) is proved.

Under the one-to-one mapping $\sum c_h h \to \sum c_h {}^*h$, $\mathfrak{R}(H, G_1)$ is mapped isomorphically into the n by n matrix ring over $\mathfrak{R}$. Under this isomorphism, the matrix $\mathfrak{B}(\Delta)$ corresponds, because of (1), to that simple basis quantity $\tau = \underline{T} = \sum' h$ (see §21), in which precisely those $h \in H$ appear for which $1^h \in \Delta$ holds. Since V is generated by the $\mathfrak{B}(\Delta)$ and $\mathfrak{R}(H, G_1)$ is generated by the τ, the desired isomorphism is obtained.

With the help of the matrices $\mathfrak{B}(\Delta)$ it is possible to introduce in an entirely different way the paired orbits investigated in Chapter III. We claim:

Theorem 28.9. *The matrices corresponding by* 28.1 *to paired orbits of* G_1 *are transposes:*

$$\mathfrak{B}(\Delta') = (\mathfrak{B}(\Delta))'.$$

Proof. Again let us put $\mathfrak{B}(\Delta) = (v_{\alpha\beta})$. $\delta' \in \Delta'$ means (see §16) there exists $\delta \in \Delta$ and $g \in G$ with $\delta^g = 1$ and $1^g = \delta'$. This yields $v_{\delta^g, 1^g} = v_{1\delta'}$; hence $v_{\delta 1} = 1$ is equivalent to $v_{1\delta'} = 1$. If we put $\mathfrak{B}(\Delta') = (v'_{\alpha\beta})$ we have $v'_{\delta' 1} = 1$ if and only if $\delta' \in \Delta'$. The first columns of $\mathfrak{B}(\Delta')$ and $(\mathfrak{B}(\Delta))'$ therefore coincide; hence, by 28.3 the entire matrices are also the same. $(\mathfrak{B}(\Delta))' \in V$ holds because

$$(\mathfrak{B}(\Delta))' g^* = [g^{*-1}\mathfrak{B}(\Delta)]' = [\mathfrak{B}(\Delta)\, g^{*-1}]' = g^*(\mathfrak{B}(\Delta))'.$$

Remark. With the help of 28.9 the theory of paired orbits may be established in a different way. Theorems 16.1, 16.2, and 16.3 now appear as trivial consequences of 28.9.

In conclusion we prove a theorem which deals with traces [$\mathrm{Tr}\,(v_{\alpha\beta}) = \sum v_{\alpha\alpha}$]:

Theorem 28.10. *Let* Γ *and* Δ *be two orbits of* G_1. *Then*

$$\mathrm{Tr}(\mathfrak{B}(\Gamma)'\mathfrak{B}(\Delta)) = \begin{cases} 0, & \Gamma \neq \Delta, \\ |\,\Gamma\,|\, n, & \Gamma = \Delta. \end{cases}$$

Proof. For $\Gamma \neq \Delta$, since $\Gamma \cap \Delta = \emptyset$ there is never a 1 in the same position of $\mathfrak{B}(\Gamma)$ and $\mathfrak{B}(\Delta)$. Hence $(\mathfrak{B}(\Gamma))' \mathfrak{B}(\Delta)$ for $\Gamma \neq \Delta$ contains only zeros on the diagonal; hence its trace is $=0$. On the diagonal of $(\mathfrak{B}(\Gamma))' \mathfrak{B}(\Gamma)$, we have the number of elements of Γ, which is $|\Gamma|$. Its trace is n times this number, where $n = |\Omega|$.

§29. The Reduction of the Permutation Representation

We now wish to investigate, for any transitive group G, the irreducible constituents of the permutation representation G^* introduced in the previous section. It is convenient to number the orbits of G_1: $\{1\} = \Delta_1, \Delta_2, \cdots, \Delta_k$. Let $n_i = |\Delta_i|$ and let us again put $n = |\Omega|$. Since all our investigations will be carried out over the complex number field, every irreducible representation is also absolutely irreducible.

We take the vector space of all columns C with n complex elements c_i as a right representation module for G^*. Since the action of g on C, defined by $Cg = g^*C$, consists in a permutation of the c_i it is obvious that:

Theorem 29.1. *The representation module associated with G^* contains a one-dimensional invariant subspace corresponding to the identity representation, namely, the one generated by*

$$\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix},$$

and because of the transitivity of G it contains no others. The identical representation therefore appears in G^* with multiplicity exactly 1.

Now let $D_1, \cdots, D_r$ be the different irreducible representations appearing in G^* where D_1 is the identity representation. In the following we always denote by f_i the degree of D_i $(i = 1, \cdots, r)$, and by e_i the multiplicity of D_i in G^*. In particular, we have $e_1 = f_1 = 1$ and $\sum_i e_i f_i = n$. The reduction of G^* gives for an appropriately chosen unitary n by n matrix $\mathfrak{U}$:

$$\mathfrak{U}^{-1}G^*\mathfrak{U} = \begin{bmatrix} D_1 & & & & \\ & \overbrace{D_2 \quad \cdots \quad D_2}^{e_2} & & & \\ & & D_2 & & \\ & & & \ddots & \\ & & & & \overbrace{D_r \quad \cdots \quad D_r}^{e_r} \end{bmatrix}$$

In order to save space, we will in the following write such matrices with "blocks" along the diagonal (and zeros outside) in the form

$$\mathfrak{U}^{-1}G^*\mathfrak{U} = [D_1, \underbrace{D_2, \ldots, D_2}_{e_2}, \ldots, \underbrace{D_r, \ldots, D_r}_{e_r}].$$

Let $\mathfrak{B} \in V$. Then $\mathfrak{W} = \mathfrak{U}^{-1}\mathfrak{B}\mathfrak{U}$ is characterized by the form

$$\mathfrak{W} = [w_1, \mathfrak{W}_{e_2} \times \mathfrak{I}_{f_2}, \cdots, \mathfrak{W}_{e_r} \times \mathfrak{I}_{f_r}].$$

Here $\times$ denotes the Kronecker multiplication. $\mathfrak{W}_{e_i}$ is an arbitrary e_i by e_i matrix, $\mathfrak{I}_{f_i}$ is the f_i by f_i identity matrix. $\mathfrak{W}_{e_i} \times \mathfrak{I}_{f_i}$ is therefore an $e_i f_i$ by $e_i f_i$ matrix. In the upper left-hand corner of $\mathfrak{W}$ there is a single number w_1 because $e_1 = 1$. The module consisting of all the $\mathfrak{W}_{e_i}$ has dimension

e_i^2 over the complex number field; hence it follows for the dimension $\mathrm{Dim}(V)$ of V over $\mathfrak{R}$ (which by 28.4 coincides with the number k of orbits of G_1) that:

Proposition 29.2.

$$\mathrm{Dim}(V) = \sum_{i=1}^{r} e_i^2 = k.$$

From the form of $\mathfrak{W}$ we have that every $\mathfrak{W}$ is a diagonal matrix if and only if all the $e_i = 1$. This is exactly the case in which any two arbitrary matrices of this form commute. We therefore have:

Theorem 29.3. *V is commutative if and only if all the $e_i = 1$.*

Other conditions for the commutativity of V follow.

Theorem 29.4. *$r = k$ if and only if V is commutative. Otherwise we have $r < k$.*

This follows immediately from 29.2 and 29.3.

Theorem 29.5. *If G_1 has no more than four orbits (with the trivial one $\{1\}$), then V is commutative.*

Proof. $e_1 = 1$. By 29.2 every $e_i = 1$ if $\sum_{i=1}^{r} e_i^2 \leq 4$.

Theorem 29.6. *If the n_i are all different, then V is commutative.*

Proof. From 16.3 it follows from our assumption that $\Delta_i' = \Delta_i$ for $i = 1, \cdots, k$. Hence $\mathfrak{B}_i' = \mathfrak{B}_i$ by 28.9. The basis elements of V are Hermitian matrices with Hermitian products, hence they commute, and V is commutative.

In conclusion, we prove another somewhat deeper necessary and sufficient condition (29.8) for the commutativity of V. We first make a preliminary remark.

Let C_i be the ith class of conjugate elements of G $(i = 1, \cdots, h)$. By the ith *class matrix* we mean the matrix $\mathfrak{C}_i = \sum_{g \in C_i} g^*$.

Theorem 29.7. *All the class matrices belong to V. They commute with each other.*

Proof.

$$s^* \mathfrak{C}_i = \sum_{g \in C_i} s^* g^* = \sum_{g \in C_i} s^* g^* s^{*-1} s^* = \mathfrak{C}_i s^*$$

for all $s \in G$. Hence it follows that $\mathfrak{C}_i \mathfrak{C}_j = \mathfrak{C}_j \mathfrak{C}_i$ for $i, j = 1, \cdots, h$.

Theorem 29.8. *V is commutative if and only if the class matrices $\mathfrak{C}_i$ $(i = 1, \cdots, h)$ generate V, i.e., when each $\mathfrak{B} \in V$ has a (not necessarily unique) representation $\mathfrak{B} = \sum_{i=1}^{h} z_i \mathfrak{C}_i$.*

Proof. (a) The $\mathfrak{C}_i$ commute by 29.8. Therefore if V is generated by the $\mathfrak{C}_i$, V is commutative.

(b) Conversely, let V be assumed commutative. Then by 29.3 all the $e_i = 1$ and the matrix $\mathfrak{W} = \mathfrak{U}^{-1} \mathfrak{B} \mathfrak{U} (\mathfrak{B} \in V, \mathfrak{U}$ unitary) has diagonal form: $\mathfrak{W} = [w_1, w_2 \mathfrak{I}_{f_2}, \cdots, w_k \mathfrak{I}_{f_k}]$. We have $k = r$.

Let χ_i be the character of the ith irreducible representation of G and let $\chi_{ij} = \chi_i(g)$ $(g \in C_j)$ be the value of χ_i on the jth class of conjugate elements C_j of G $(i, j = 1, \cdots, h)$. By a theorem from representation theory (Speiser, 1937, p. 172) the determinant of the χ_{ij} is different from 0. In particular, it follows from this that the k characters of the representations $D_1, \cdots, D_k$ are linearly independent.

We can therefore (if necessary with appropriate renumbering) also get the k by k subdeterminant

$$\det (\chi_{ij})_{i,j=1,\ldots,k} \neq 0.$$

From theorems of representation theory (Speiser, 1937, p. 169) we can conclude that

$$\sum_{g \in C_j} D_i(g) = \frac{|\, C_j \,| \, \chi_{ij}}{f_i} \mathfrak{I}_{f_i},$$

whence

$$\mathfrak{U}^{-1} \mathfrak{C}_j \mathfrak{U} = \left[|\, C_j \,| \, \chi_{1j}, \frac{|\, C_j \,| \, \chi_{2j}}{f_2} \mathfrak{I}_{f_2}, \ldots, \frac{|\, C_j \,| \, \chi_{kj}}{f_k} \mathfrak{I}_{f_k} \right].$$

The matrix

$$\left(\frac{|\, C_j \,| \, \chi_{ij}}{f_i} \right)_{i,j=1,\ldots,k} = \left[\frac{1}{f_1}, \ldots, \frac{1}{f_k} \right] (\chi_{ij}) \, [|\, C_1 \,|, \ldots, |\, C_k \,|]$$

is not singular; its columns are therefore linearly independent. Therefore the $\mathfrak{U}^{-1} \mathfrak{C}_j \mathfrak{U}$ and hence also the $\mathfrak{C}_j$ are linearly independent. By 29.2 they form a basis for V, as was to be proved.

We conclude with a condition for the double transitivity of G.

Theorem 29.9. *G is doubly transitive if and only if* $\mathrm{Dim}\, V(G) = 2$. *In this case G^* has exactly two irreducible constituents. In particular, we have $r = k$ and $V(G)$ commutative.*

Proof. If G is doubly transitive, then $k = \mathrm{Dim}\,(V) = 2$ and conversely. By 29.5 V is then commutative, $r = 2$, $e_1 = e_2 = 1$.

Further investigation of the mutual reduction of a permutation group and its centralizer ring can be found in Frame (1941, 1943, 1947, 1948, 1952). For a ring theoretical discussion of the reduction of permutation groups see Tamaschke (1960).

§30. The Degrees of the Irreducible Constituents of a Transitive Permutation Group

Frame has discovered that in a transitive group G of degree n noteworthy relations exist between the degrees n_i of the transitive constituents of G_1 and the degrees f_i of the absolutely irreducible constituents D_i of the permutation representation G^* of G. Frame (1937) conjectured:

Theorem 30.1. (A) *If the irreducible constituents of G^* are all different, i.e., if all the multiplicities $e_i = 1$, then the rational number*

$$q = n^{k-2} \prod_{i=1}^{k} \frac{n_i}{f_i}$$

is an integer.

(B) *If in addition the k numbers n_i are all different, then q is a square.*

(C) *If the irreducible constituents of G^* all have rational characters, then q is a square. The hypothesis is always fulfilled if the degrees f_i are all different.*

It is not known whether (B) is true for $k > 3$. (A) and (C) have been proved by Frame (1941). We give different proofs.

Proof of 30.1(A). It suffices to show that q is an algebraic integer. The notation of the preceding section is continued.

Let $\mathfrak{U}$ again be the unitary transformation matrix introduced in §29. From the hypothesis $e_i = 1$ it follows that every matrix $\mathfrak{W} = \mathfrak{U}^{-1}\mathfrak{V}\mathfrak{U}$ with $\mathfrak{V} \in V$ has diagonal form. Because $\mathfrak{V}_i = \mathfrak{V}(\Delta_i) \in V(G)$ we have in particular

$$\mathfrak{W}_i = \mathfrak{U}^{-1}\mathfrak{V}_i\mathfrak{U} = [w_{1i}, w_{2i}\mathfrak{I}_{f_2}, \cdots, w_{ki}\mathfrak{I}_{f_k}].$$

Let w_i be the diagonal elements of the matrix $\mathfrak{W} = \mathfrak{U}^{-1}\mathfrak{V}\mathfrak{U}$, for arbitrary $\mathfrak{V} \in V$. We put

$$\mathfrak{V} = \sum_i z_i \mathfrak{V}_i , \qquad z = \begin{pmatrix} z_1 \\ \cdot \\ \cdot \\ z_k \end{pmatrix}, \qquad w = \begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ w_k \end{pmatrix},$$

$\mathfrak{N} = [1, n_2, \cdots, n_k]$, $\mathfrak{F} = [1, f_2, \cdots, f_k]$, and $\mathfrak{T} = (w_{ij})$; $i, j = 1, \cdots, k$. From $\mathfrak{W} = \mathfrak{U}^{-1}\mathfrak{V}\mathfrak{U}$ it follows that

$$\overline{\mathfrak{W}}'\mathfrak{W} = \mathfrak{U}^{-1}\overline{\mathfrak{V}}'\mathfrak{V}\mathfrak{U},$$

since $\mathfrak{U}$ was assumed unitary. With the aid of 28.10 we now obtain

$$\bar{z}'\mathfrak{N}nz = \sum_{i=1}^{k} \bar{z}_i z_i n_i n = \sum_{i,j} \bar{z}_i z_j \operatorname{Tr}(\mathfrak{V}_i'\mathfrak{V}_j) = \operatorname{Tr}(\overline{\mathfrak{V}}'\mathfrak{V})$$

$$= \operatorname{Tr}(\overline{\mathfrak{W}}'\mathfrak{W}) = \sum_i \bar{w}_i w_i f_i = \bar{w}'\mathfrak{F}w.$$

Because $w_i = \sum_j z_j w_{ij}$, i.e., $w = \mathfrak{T}z$, we therefore have $\mathfrak{N}n = \overline{\mathfrak{T}}'\mathfrak{F}\mathfrak{T}$. By taking the determinant we get

$$n^k \prod_i n_i = |\mathfrak{N}n| = |\mathfrak{F}|\,|\overline{\mathfrak{T}}'\mathfrak{T}| = \prod_i f_i \,|\overline{\mathfrak{T}}|\,|\mathfrak{T}|.$$

The w_{ij}, as eigenvalues of the matrix $\mathfrak{V}_j$ which has integer coefficients, are algebraic integers, and therefore $|\mathfrak{T}|$ and $|\overline{\mathfrak{T}}|$ are also algebraic integers.

We wish to show that $|\mathfrak{T}|$ is divisible by n. By 28.2 $\sum_j \mathfrak{V}_j = \mathfrak{M}$ where $\mathfrak{M}$ is the n by n matrix consisting of n^2 ones. $\mathfrak{M}$ has the eigenvalue n occurring with multiplicity 1 belonging to the eigenvector

$$\begin{pmatrix} 1 \\ \cdot \\ \cdot \\ 1 \end{pmatrix}.$$

Its remaining eigenvalues are 0. In the diagonal matrix $\sum_j \mathfrak{W}_j$, n therefore appears exactly once, the remaining elements being 0. Therefore $\sum_j w_{ij} = n$ for $i = 1$ and $=0$ for the remaining i. This implies

$$|\mathfrak{T}| = \begin{vmatrix} n & w_{12} & \cdots & w_{1k} \\ 0 & w_{22} & \cdots & w_{2k} \\ \vdots & & & \\ 0 & w_{k2} & \cdots & w_{kk} \end{vmatrix} \equiv 0 \pmod{n}.$$

Hence $q = n^{-2} |\overline{\mathfrak{T}}| |\mathfrak{T}|$ is an algebraic integer, hence also a rational integer.

Proof of 30.1(C). (a) Because of the hypothesis

$$e_1 = \cdots = e_k = 1,$$

the commutativity of V follows by 29.3. Theorem 29.8 yields the existence of k class matrices $\mathfrak{C}_1, \cdots \mathfrak{C}_k$ and of complex numbers x_{ij} such that

$$\mathfrak{B}_i = \sum_{j=1}^{k} x_{ij}\mathfrak{C}_j \qquad (i = 1, ..., k).$$

Conversely by 28.4 there are also x'_{ij} with

$$\mathfrak{C}_i = \sum_{j=1}^{k} x'_{ij}\mathfrak{B}_j .$$

The x_{ij} are, by well-known theorems of linear algebra, uniquely determined and rational, since the matrices $\mathfrak{B}_i$ and $\mathfrak{C}_j$ are rational.

(b) By hypothesis all the irreducible characters appearing in G^* are rational. Thus the matrices $\mathfrak{U}^{-1}\mathfrak{C}_j\mathfrak{U}$ appearing in the proof of 29.8 are also rational. By (a) the matrices

$$\mathfrak{W}_i = \mathfrak{U}^{-1}\mathfrak{B}_i\mathfrak{U} = \sum_i x_{ij}\mathfrak{U}^{-1}\mathfrak{C}_j\mathfrak{U}$$

are then rational. The w_{ij} are therefore rational. Since the w_{ij} were already in the proof of 30.1(A) shown to be algebraic integers, they are rational integers. $|\mathfrak{T}| = |w_{ij}|$ is therefore a rational integer. Since n divides $|\mathfrak{T}|$, $n^{-1}|\mathfrak{T}|$ is also a rational integer, and q is therefore a square as was asserted.

(c) The hypothesis that all the irreducible characters appearing in G^* are rational is fulfilled if the degrees f_i of the irreducible constituents of G^* are all different. For since G^* is rational, with each irreducible representation D_i all representations conjugate to it appear in G^*. Because all of the f_i are different, these coincide with D_i, and χ_i is therefore rational.

We assume in the sequel that V is commutative, i.e., that the irreducible constituents of G^* are all different, and draw some conclusions from 30.1.

Theorem 30.2. *If the nontrivial irreducible representations appearing in G^* all have the same degree f, then the orbits of G_1 different from 1 all have the same length, which also equals f. Hence G is either regular and Abelian ($f = 1$) or (3/2)-fold transitive ($f > 1$).*

Proof. From $f_i = f$ for $i = 2, \cdots, k$ and 30.1(A) it follows that f^{k-1} divides $n^{k-2}\prod_i n_i$. Since f divides $n - 1$, f and n are relatively prime, hence f^{k-1} divides $\prod_i n_i$.

In addition we have

$$(k-1)f = n - 1 = \sum_{i=2}^{k} n_i, \qquad \text{i.e.,} \qquad \frac{1}{k-1}\sum_{i=2}^{k} n_i = f.$$

The geometric mean of the n_i is at most equal to the arithmetic mean, thus $\prod_i n_i \leq f^{k-1}$. With the help of the divisibility property it now follows that $\prod_i n_i = f^{k-1}$. The geometric and arithmetic mean of the n_i therefore coincide. This occurs, however, only if $n_i = f$, as was to be proved.

From 30.2 it follows immediately that:

Theorem 30.3. *If $k = 3$ and $n_2 \neq n_3$, then also $f_2 \neq f_3$. Hence* 30.1(B) *holds for $k = 3$.*

It is not known if in general when the n_i are all different ($i = 2, \cdots, k$) it follows that the f_i are also all different. Should this prove correct, the conjecture 30.1(B) would be true.

In the proof of theorem 30.1 we used the matrix equation $\mathfrak{N}n = \overline{\mathfrak{T}}'\mathfrak{F}\mathfrak{T}$ only to compare the determinants. More precise information can be obtained from the elementary divisors. Since the κ-th elementary divisor of a product of matrices is known to be divisible by the κ-th elementary divisor of each factor, the κ-th elementary divisor of $\mathfrak{N}n$ is divisible by the κ-th elementary divisor of $\mathfrak{F}$. In other words:

Theorem 30.4. *If, under the assumptions of* 30.1(A), *there are l of the numbers f_i divisible by a given prime power p^a then there are at least l of the numbers nn_i divisible by p^a.*

We mention without proof the following generalization (Frame, 1941) of Theorem 30.1 to the case where some multiplicities $e_i > 1$.

Theorem 30.5. *The expression*

$$q = n^{k-2} \prod_{i=1}^{k} n_i \Big/ \prod_{j=1}^{r} f_j^{e_j^2}$$

is a rational integer.

If in addition the irreducible constituents of G^* have rational characters, then q is a square. The hypothesis is always satisfied if the degrees of the different irreducible constituents of G^* are all different.

§31. Primitive Groups of Degree 2p

In this section we wish to prove the following theorem:

Theorem 31.1. *A primitive group of degree $n = 2p$ (p prime) is doubly transitive if n is not of the form $n = a^2 + 1$* (Wielandt, 1956).

Preliminary Remark. The hypothesis $n \neq a^2 + 1$ is not superfluous, for there is a primitive group of degree 10 which is not doubly transitive. It can be obtained in the following way. Let $G = S^{\Omega}$ be the symmetric group on $\Omega = \{1, \cdots, 5\}$. In addition let $\bar{\Omega}$ be the set of the 10 unordered pairs $\{a, b\}$ with $a, b \in \Omega$ and $a \neq b$. To each $g \in G$ we assign in a one-to-one manner a permutation $\bar{g}$ on $\bar{\Omega}$ by $\{a, b\}^{\bar{g}} = \{a^g, b^g\}$. In this way we have represented G faithfully as a permutation group $\bar{G}$ on $\bar{\Omega}$. $\bar{G}$ is not doubly transitive for there is no $\bar{g} \in \bar{G}$ which fixes $\{1, 2\}$ and takes $\{1, 3\}$ into $\{4, 5\}$. On the other hand, $\bar{G}$ is primitive since $\bar{G}_{\{1,2\}}$ is maximal in $\bar{G}$. (It is not known if for $p \neq 5$ there are primitive groups of degree $2p$ which are not doubly transitive.)

Theorem 31.1 is obviously contained in the following theorem:

Theorem 31.2. *Let G be a primitive group of degree $2p$. Then*: (A) *G_1 has at most three orbits (including the trivial one-point orbit).*

(B) *If the number of orbits of G_1 is exactly three, then $2p$ necessarily has the form $2p = (2s + 1)^2 + 1$ for some natural number s. The lengths of the orbits of G_1 are 1, $s(2s + 1)$, $(s + 1)(2s + 1)$. The degrees of the irreducible constituents of G are 1, p, $p - 1$.*

We prepare the proof of this theorem in steps (α)–(λ). In the following let G be assumed to be a primitive but not doubly transitive group of degree $2p$.

(α) *We can assume without loss of generality that $p \neq 2$.*

For if $p = 2$, then G is easily seen to be S^4 or A^4; hence G is doubly transitive.

(β) *Every element different from* 1 *of a Sylow p-subgroup of* G *is a product of two p-cycles. Every Sylow p-subgroup of* G *is semiregular and has order* p.

Proof. Let P be a Sylow p-subgroup of G and $1 \neq x \in P$. Since the order of P is a power of p, x consists of p-cycles and cycles of length 1. By 13.1 (theorem of Jordan) G has no p-cycles and x is therefore a product of two p-cycles. In particular, x moves every point, hence P is semiregular. By 4.2, $|P|$ is a divisor of $2p$, thus $|P| = p$ because $p \neq 2$ by (α).

(γ) *If* $g \in G$ *and* a *is the order of* g, *then either* $a = p$ *or* $(a, p) = 1$.

Proof. We assume that p divides a and $p \neq a$. Then $h = g^{a/p} \neq 1$, thus h has order p. By (β), h is a product of two p-cycles. Therefore in g no cycle can appear whose length is prime to p, since h has only cycles of length p. If g were a $2p$-cycle, G would contain the regular group $\langle g \rangle$, which is cyclic and of composite order $2p$. By 25.3 (theorem of Schur) G would be doubly transitive, which is not the case. g therefore has only p-cycles, hence has order p, which contradicts our assumption.

We again denote by $D_1, \cdots, D_r$ the different irreducible constituents of the permutation representation G^* of G (see §29). In addition let f_i be the degree of D_i ($i = 1, \cdots, r$) and let $\chi_i = \mathrm{Tr}(D_i)$ be the character of D_i. Let the numbering be chosen so that D_1 is the identity representation. We now prove:

(δ) *We can number the irreducible constituents* D_i *of* G^* *such that* $f_2 = p$ *and the representations* $D_3, \cdots, D_r$ *are conjugate. In particular* $f_3 = \cdots = f_r = f$, *and* f *divides* $p - 1$.

Proof. (a) By (β) there is an $x \in G$ which is the product of two p-cycles. Without loss of generality we may put $x = (1\,2 \cdots p)(p + 1 \cdots 2p)$. The characteristic polynomial

of the permutation matrix $\mathfrak{X}$ associated with x is $(z^p - 1)^2$. Hence $\mathfrak{X}$ has the eigenvalues $1, u, \cdots, u^{p-1}$, all with multiplicity 2, where u is a primitive pth root of unity. We wish to investigate how these eigenvalues are distributed among the $D_i(x)$. $D_1(x)$ has the eigenvalue 1 with multiplicity 1 and no others, since D_1 is the identity representation.

(b) We now show that $f_i > 1$ holds for $i \geq 2$. We assume $f_i = 1$. Since G is not Abelian but $D_i(G)$ is Abelian, D_i is not faithful. The normal subgroup N of all $n \in G$ with $D_i(n) = 1$ is therefore different from 1 and hence (by 8.8) is transitive. Thus $D_i(N) = 1$ and also $D_1(N) = 1$, which by 29.1 cannot be the case. (*Note:* This argument is valid for all primitive non-Abelian groups.)

(c) Let the numbering of the irreducible constituents $D_2, \cdots, D_r$ be chosen so that $D_2(x)$ has 1 as an eigenvalue. Because $f_2 > 1$ and since the eigenvalue 1 occurs for $\mathfrak{X}$ only twice, $D_2(x)$ has an eigenvalue different from 1 which without loss of generality may be assumed to be u.

(d) All representations conjugate to a D_i are constituents of G^* since G^* is rational. D_2 is conjugate to itself, for otherwise a $D_i(x)$ with $i \geq 3$ would have the eigenvalue 1, which is impossible since $\mathfrak{X}$ has the eigenvalue 1 altogether only twice. Therefore $D_2(x)$ has the eigenvalues $1, u, \cdots, u^{p-1}$, all with multiplicity 1, for if an eigenvalue, say u, appeared in $D_2(x)$ with multiplicity 2, then because of the rationality of χ_2 so would $u^2, \cdots, u^{p-1}$. Then, however, D_1 and D_2 would be the only irreducible constituents of G^*, and by 29.9 G would be doubly transitive. Hence we obtain $f_2 = p$.

(e) The remaining eigenvalues $u, \cdots, u^{p-1}$ (all with multiplicity 1) of $\mathfrak{X}$ are divided among the remaining representations $D_3, \cdots, D_r$. We now prove that these representations are conjugate to each other and therefore have the same degree f. For $r = 3$ there is nothing more to show. We assume $r \geq 4$. It suffices (without loss of generality) to prove that D_3 is

conjugate to D_4. Let u be an eigenvalue of $D_3(x)$, u^s one of $D_4(x)$ $(1 < s \leq p-1)$. Because $(p, |G|/p) = 1$ [by (β)] there is an m which is a solution of the two congruences $m \equiv s(p)$ and $m \equiv 1(|G|/p)$. This yields $(m, |G|) = 1$, and therefore an irreducible constituent D_i of G^* conjugate to D_3 is defined by $\chi_i(g) = \chi_3(g^m)$ $(g \in G)$. Because of the rationality of D_1 and D_2, we have $i \geq 3$. In addition, $u^m = u^s$ is an eigenvalue of $D_i(x)$. It is also an eigenvalue of $D_4(x)$. Since u^s occurs altogether only once in $D_3, \cdots, D_r$ we have $D_i = D_4$, hence D_4 conjugate to D_3.

(f) In particular we obtain $p - 1 \equiv 0\ (f)$. In addition, (d) and (e) show that all the D_i occur only with multiplicity 1: $e_1 = \cdots = e_r = 1$.

Therefore from 29.3 we have:

(ϵ) *The centralizer ring V of a primitive group G of degree $2p$ is commutative. $r = k$ is the number of orbits of G_1.*

In the following, guided by Burnside's proof of Theorem 11.7 (Burnside, 1911, p. 341), we wish to obtain a contradiction to the assumption $r \geq 4$, thus proving 31.2(A). For this we first need:

(ζ) *If $h \in G$ is not of order p, then $\chi_3(h)$ is rational.*

Proof. (a) Let a be the order of h. By (γ) we have $(a, p) = 1$. As a sum of ath roots of unity, $\chi_3(h)$ lies in the ath cyclotomic field.

(b) Let $\mathfrak{R}$ be a normal field (over the rational numbers) which contains all the elements of the matrices $D_i(g)$. Let K be its Galois group. We may assume that the $D_i(x)$ $(i = 1, \cdots, r)$ are in diagonal form. The primitive pth root of unity u then belongs to $\mathfrak{R}$. In addition let K' be the subgroup of all automorphisms of $\mathfrak{R}$ which leave u fixed. The pth cyclotomic field is the fixed field of K'. For $k \in K'$, $D_3(x)^k$ has the eigenvalue $u^k = u$. Since D_3^k is an irreducible constituent of G^* different from D_1 and D_2, it follows that $D_3^k = D_3$, since

otherwise $D_3(x)^k$ would not have the eigenvalue u [see part (e) of the proof of (δ)]. In particular $\chi_3(h)^k = \chi_3(h)$, and therefore $\chi_3(h)$ also lies in the pth cyclotomic field.

(c) The rationality of $\chi_3(h)$ now follows from (a) and (b).

In the following, again let $x = (1 \cdots p)(p+1 \cdots 2p)$. In addition we put $N(\langle x \rangle) = N$.

(η) $| N | = pf$ (*under the assumption* $r \geq 4$).

Proof. Again let $h \in G$ of order $a \neq p$. By (ζ) $\chi_3(h)$ is rational, thus $\chi_3(h) = \chi_4(h)$. From this and the orthogonality of χ_3 and χ_4 it follows that:

$$\sum_{g \in G} \chi_3(g)\,[-\bar{\chi}_4(g) + \bar{\chi}_3(g)] = \sum_{g \in G} |\, \chi_3(g)\,|^2$$

$$= |\, G\,| = \sum_{Q} \sum_{q \in Q} \chi_3(q)\,[-\bar{\chi}_4(q) + \bar{\chi}_3(q)];$$

here Q runs through all Sylow p-subgroups of G. If s is the number of Sylow p-subgroups, then since every Q is similar to $\langle x \rangle$, we obtain:

$$|\, G\,| = s \sum_{m=1}^{p} \chi_3(x^m)\,[-\bar{\chi}_4(x^m) + \bar{\chi}_3(x^m)] = spf$$

from the orthogonality relations for $\langle x \rangle$. Therefore it follows that $|\, N\,| = s^{-1} |\, G\,| = pf$ as asserted. We put $\{1, \cdots, p\} = \Gamma$ and $\{p+1, \cdots, 2p\} = \Delta$. In addition, let $\bar{N}$ be the set of all $n \in N$ for which $\Gamma^n = \Gamma$ (hence also $\Delta^n = \Delta$) holds. Obviously $\bar{N}$ is a normal subgroup of N and $\bar{N} = N$ holds if and only if N is intransitive on Ω.

(θ) $\bar{N}^\Gamma$ *is a Frobenius group.*

Proof. In any case $\bar{N}^\Gamma \geq \langle x \rangle^\Gamma$ is transitive on Γ. Let

$n \in \bar{N}_{1k}$ with $1 < k \leq p$. Then $n^{-1}xn = x^m$ for some m. Moreover,

$$k = k^n = 1^{x^{k-1}n} = 1^{x^{m(k-1)}} \equiv m(k-1) + 1 \,(p);$$

thus, $m = 1$. By 4.4 we have $n^\Gamma \in \langle x \rangle^\Gamma$, hence $n^\Gamma = 1$, as asserted.

(ι) $\bar{N}_\Gamma = N_\Gamma = 1$.

Proof. Let $n \in N_\Gamma$. Then it follows exactly as in (θ) that $n^{-1}xn = x$, thus $x^\Delta = (p+1, \cdots, 2p) = ((p+1)^n \cdots (2p)^n)$. Hence $n = 1$ or n is a p-cycle on Δ. The latter is, however, not possible because of 13.1. In particular, we have $\bar{N}^\Gamma \cong \bar{N} \cong \bar{N}^\Delta$. Every permutation on $\bar{N}$ is therefore uniquely determined by its effect on the points of Γ. $\bar{N}^\Gamma$ and $\bar{N}^\Delta$ are also isomorphic as permutation groups, i.e., they differ only in the designation of the points which they permute. From (θ) and (ι) it follows that:

(κ) $N_1 = \bar{N}_1$ *has exactly two orbits of length* 1, *namely,* 1 *and a point lying in* Δ (*without loss of generality* $= p+1$). *The remaining orbits of* N_1 *have length* $|N_1|$.

We now assume that N is intransitive. Then $\bar{N} = N$ and $|N_1| = f$. Because $G_1 \geq N_1$ each orbit of G_1 splits up into orbits of N_1. We claim the following:

(λ) *At least one orbit of* N_1 *different from* $\{1\}$ *coincides with an orbit of* G_1.

Proof. That orbit of G_1 which contains $p+1$ has length $\equiv 1(f)$. This length is >1 because of 8.6. The lengths of the remaining orbits of G_1 different from $\{1\}$ are multiples of f. We assume that all these lengths are $\geq 2f$. Since $2(1 + (p-1)f^{-1})$ is, by (κ), the number of orbits of N_1 we obtain for the number k of orbits of G_1:

$$k < 2 + \frac{p-1}{f}.$$

On the other hand, it follows from (δ) and (ϵ) that

$$k = r = 2 + \frac{p-1}{f}.$$

This yields the desired contradiction, hence the proof of (λ).

Proof of 31.2(A) *for intransitive* N: Let ψ be an orbit of N_1 different from $\{1\}$ which is also an orbit of G_1. The existence of such a ψ is guaranteed by (λ). We apply 27.5 with $\alpha = 1$, $\beta \in \psi$, and $H = \langle x \rangle$. We have

$$\beta^{G_1} = \beta^{N_1} = \psi \subseteq \beta^{\langle x \rangle} \qquad \text{and} \qquad |\beta^{\langle x \rangle}| = |1^{\langle x \rangle}| = p.$$

The hypotheses of 27.5 are satisfied, hence G is imprimitive. This is in contradiction to our hypothesis on G. Hence for intransitive N the assumption $r \geq 4$ is refuted, thus 31.2(A) is proved. 31.1 is also proved if we anticipate the proof of 31.2(B).

Proof of 31.2(A) *for transitive* N: If N is transitive, then $\bar{N}$ is a normal subgroup of N of index 2. Because $p \neq 2$, the normalizer $\tilde{N}$ of $\langle x \rangle$ in S^Ω contains an odd permutation, say $(1, p+1) \cdots (p, 2p)$. $n \in \tilde{N}$ is then even if and only if $\Gamma^n = \Gamma$. Hence N, and therefore also G, contains odd permutations. $\bar{G} = G \cap A^\Omega$ is therefore a normal subgroup of G of index 2, and $\bar{N} = N \cap \bar{G}$. The transitivity of $\bar{G}$ follows from the primitivity of G. Theorem 31.1 is already known to be true in the case of intransitive normalizers. Therefore if $\bar{G}$ were primitive, then $\bar{G}$ and hence also G would be doubly transitive. $\bar{G}$ is therefore imprimitive.

(a) Let Φ be the set of all $\alpha \in \Omega$ for which $\alpha^{G_1} = \alpha$ holds. We show that Φ is a block of G. Let $\Phi^g \cap \Phi \neq \emptyset$ be assumed for a $g \in G$, thus $\beta \in \Phi$ and $\alpha = \beta^g \in \Phi$. For all $g_1 \in \bar{G}_1$, $(\beta^g)^{g_1} = \beta^g$ holds. Moreover, $gg_1g^{-1} = \bar{g} \in \bar{G}$ holds, thus $(\beta^{\bar{g}})^g = \beta^g$, $\beta^{\bar{g}} = \beta$. This means that $\bar{g} \in \bar{G}_\beta = \bar{G}_1$ since $\beta \in \Phi$ holds. Hence $g \in \mathbf{N}(\bar{G}_1)$, thus $\Phi^g = \Phi$, as asserted.

Because of the primitivity of G we have either $\Phi = \Omega$ or $\Phi = \{1\}$.

(b) If $\Phi = \Omega$, then $\bar{G}$ is regular on Ω, thus $|\bar{G}| = 2p$. Because $p \neq 2$, $\bar{G}$ by 4.6 contains a normal subgroup P of index 2. As a Sylow subgroup, P is even characteristic in $\bar{G}$, thus we have $P \trianglelefteq G$. On the other hand, because $|P| = p$, P is intransitive, therefore G is imprimitive, in contradiction to the hypothesis.

(c) There remains only the case $\Phi = \{1\}$ to deal with. If Ω were divided into p blocks of length 2 by $\bar{G}$, then a block $\{1, \alpha\}$ of $\bar{G}$ would be fixed by $\bar{G}_1$, therefore we would have $\alpha \in \Phi$, which is not the case. Hence Ω is divided by $\bar{G}$ necessarily into two blocks of length p. We can take these without loss of generality to be Γ and Δ. Let $\overline{\overline{G}}$ be the set of all $g \in \bar{G}$ for which $\Gamma^g = \Gamma$ (hence also $\Delta^g = \Delta$) holds. We have $\overline{\overline{G}} \trianglelefteq \bar{G}$. Let $x \in G$ be an element of order p. Then x is even, $x \in \bar{G}$. If $\Gamma^x = \Delta$, because $p \neq 2$ we would also have $\Gamma = \Gamma^{x^p} = \Delta$. Thus $x \in \overline{\overline{G}}$. Hence the group Q generated by all elements of order p is a subgroup of $\overline{\overline{G}}$, therefore intransitive. On the other hand, we have $Q \trianglelefteq G$, thus G imprimitive. This contradicts our hypothesis. Hence 31.2(A) is completely proved.

Proof of 31.2(B). If the number of orbits of G_1 is exactly three, then $f_1 = 1$, $f_2 = p$, and $f_3 = p - 1$ by (δ). Let the lengths of the orbits $\{1\}$, Δ_2, Δ_3 be $n_1 = 1$, $n_2 = v$, and $n_3 = w$. Then

$$2p = 1 + v + w. \tag{1}$$

By 8.6, we have $v, w > 1$. Moreover, $v + w$ is odd, thus $v \neq w$. Without loss of generality we may assume $1 < v < w$. By 16.3 every orbit is paired with itself.

Let $\mathfrak{I}, \mathfrak{V}, \mathfrak{W}$ be the matrices associated (by 28.1) with the orbits $\{1\}$, Δ_2, Δ_3. By 28.9 these matrices coincide with their transposes, $\mathfrak{V}' = \mathfrak{V}$, $\mathfrak{W}' = \mathfrak{W}$. Their eigenvalues are rational

integers as can be seen from part (b) of the proof of 30.1(C). [The hypotheses of 30.1(C) are satisfied here; the eigenvalues in question were there called w_{ij} .]

In the diagonal of $\mathfrak{B}$ there are only zeros, thus $\mathrm{Tr}\,(\mathfrak{B}) = 0$. Let $\mathfrak{U}$ again be a unitary matrix which transforms $\mathfrak{B}$ into diagonal form [see the proof of 30.1(A)]. From the properties of $\mathfrak{U}$ given in §29 we conclude that for some $c \in \mathfrak{R}$

$$\mathfrak{U}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = c\begin{pmatrix} 1 \\ 1 \\ \cdot \\ 1 \end{pmatrix}.$$

From

$$\mathfrak{B}\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = v\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

it follows that

$$\mathfrak{U}^{-1}\mathfrak{B}\mathfrak{U}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} v \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Therefore, in the upper left-hand corner of the diagonal matrix $\mathfrak{U}^{-1}\mathfrak{B}\mathfrak{U}$ there is a v. Hence, if we denote the j by j identity matrix by $\mathfrak{I}_j$, $\mathfrak{U}^{-1}\mathfrak{B}\mathfrak{U} = [v, s\mathfrak{I}_p, t\mathfrak{I}_{p-1}]$. Therefore we have

$$0 = \mathrm{Tr}\,(\mathfrak{B}) = v + ps + (p-1)\,t \tag{2}$$

with rational integers s, t. Together with 28.10 this yields

$$2pv = \mathrm{Tr}\,(\mathfrak{B}^2) = v^2 + ps^2 + (p-1)\,t^2. \tag{3}$$

From (1) it follows that $v < p$. Were $v = 2$, G_1 would be semiregular by 18.7; hence we would have $v = w$ which contradicts $v < w$. Thus we have $v \geq 3$, i.e., $p \geq 5$. From (2) it follows that $t \equiv v\ (p)$, and (3) yields

$$t^2 \leq \frac{2pv}{p-1} \leq 3v \leq p^2, \qquad \text{thus} \qquad |t| \leq p.$$

Together with $t \equiv v\,(p)$ this yields $t = v$ or $t = v - p$. The assumption $t = v$ leads, however, with (3) to $v = 1$, thus to a contradiction. Therefore $t = v - p$. This inserted in (2) and (3) yields

$$p - v = s + 1, \qquad p = (p - v)^2 + s^2.$$

Now we can express everything in terms of the integer s:

$$\begin{aligned} p &= (s+1)^2 + s^2, & 2p &= (2s+1)^2 + 1, \\ v &= s(2s+1), & w &= (s+1)(2s+1). \end{aligned}$$

Since $s = p - v - 1$ and $v < p$, s is non-negative. And since $v = s(2s + 1)$ is, by definition, a natural number, we have $s \neq 0$. Hence s is a natural number. This completes the proof of 31.2(B) and of 31.1.

Remark. Using modular characters Itô (1962b) has been able to determine all primitive groups G of degree $2p$, $p > 2$, in which the normalizer of a Sylow p-subgroup has the lowest possible order $2p$. On account of a well-known transfer theorem due to Burnside (1911, p. 327) these groups are simple. One of them is only simply transitive ($p = 5, |G| = 60$); the others are doubly transitive and isomorphic to the linear fractional groups $LF(2, q)$ with prime powers $q = 2p - 1$.

Bibliography

Books on group theory in general are designated by (*G*).
Books on permutation groups are designated by (*P*).

BACHMAN, G. (1959). Geometry in certain finite groups. *Math. Z.* **70**, 466–479.

BAYS, S. (1952). Les répartitions imprimitives des n-uples dans le groupe symétrique de degré n. *Comment. Math. Helv.* **26**, 68–77.

BEAUMONT, R. A., and PETERSON, R. P. (1955). Set-transitive permutation groups. *Canad. J. Math.* **7**, 35–42.

BERCOV, R. D. (1962). The double transitivity of a class of permutation groups. Ph. D. Thesis, California Institute of Technology, Pasadena, California.

BOCHERT, A. (1889). Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann. *Math. Ann.* **33**, 584–590.

BRAUER, R. (1943). On permutation groups of prime degree and related classes of groups. *Ann. of Math.* **44**, 57–59.

(*P*) BURCKHARDT, H., and VOGT, H. (1909). Sur les groupes discontinues: Groupes de substitutions. "Encyclopédie des sciences mathématiques pures et appliquées," Édition Française. Algèbre, Tome I, Vol. I (Arithmétique), Chapter I, 8, pp. 532–575.

BURNSIDE, W. (1901). On some properties of groups of odd order. *Proc. London Math. Soc.* **33**, 162–185.

BURNSIDE, W. (1906). On simply transitive groups of prime degree. *Quart. J. Math.* **37**, 215–221.

(*G*) BURNSIDE, W. (1911). "Theory of Groups of Finite Order," 2nd ed. Cambridge Univ. Press, London; reprinted 1958, Chelsea, New York.

BURNSIDE, W. (1921). On certain simply-transitive permutation groups. *Proc. Cambridge Phil. Soc.* **20**, 482–484.

(*G*) CARMICHAEL, R. D. (1937). "Introduction to the Theory of Groups of Finite Order." Ginn, Boston.

(*P*) DE SÉGUIER, J.-A. (1912). "Groupes de substitutions." Gauthier-Villars, Paris.

FEIT, W. (1960). On a class of doubly transitive permutation groups. *Illinois J. Math.* **4**, 170–186.

FRAME, J. S. (1937). The degrees of the irreducible components of simply transitive permutation groups. *Duke Math. J.* **3**, 8–17.

FRAME, J. S. (1941). The double cosets of a finite group. *Bull. Amer. Math. Soc.* **47**, 458–467.

FRAME, J. S. (1943). Double coset matrices and group characters. *Bull. Amer. Math. Soc.* **49**, 81–92.

FRAME, J. S. (1947). On the reduction of the conjugating representation of a finite group. *Bull. Amer. Math. Soc.* **53**, 584–589.

FRAME, J. S. (1948). Group decomposition by double coset matrices. *Bull. Amer. Math. Soc.* **54**, 740–755.

FRAME, J. S. (1952). An irreducible representation extracted from two permutation groups. *Ann. of Math.* **55**, 85–100.

FROBENIUS, G. (1902). Über primitive Gruppen des Grades n und der Klasse $n - 1$. *S. B. Akad. Berlin* **1902**, 455–459.

FROBENIUS, G. (1904). Über die Charaktere der mehrfach transitiven Gruppen. *S. B. Akad. Berlin* **1904**, 558–571.

HALL, M. (1954). On a theorem of Jordan. *Pacific J. Math.* **4**, 219–226.

(*G*) HALL, M. (1959). "The Theory of Groups." Macmillan, New York.

HALL, M. (1962). Automorphisms of Steiner triple systems. *Amer. Math. Soc. Proc. Symp. Pure Math.* **6**, 47–66.

HOLYOKE, T. C. (1952). On the structure of multiply transitive permutation groups. *Amer. J. Math.* **74**, 787–796.

HUPPERT, B. (1955). Primitive, auflösbare Permutationsgruppen. *Arch. Math.* **6**, 303–310.

HUPPERT, B. (1957). Zweifach transitive, auflösbare Permutationsgruppen. *Math. Z.* **68**, 126–150.

HUPPERT, B. (1962). Scharf dreifach transitive Permutationsgruppen. *Arch. Math.* **13**, 61–72.

ITÔ, N. (1955). On primitive permutation groups. *Acta Sci. Math. Szeged* **16**, 207–228.

ITÔ, N. (1958). Normalteiler mehrfach transitiver Permutationsgruppen. *Math. Z.* **70**, 165–173.

ITÔ, N. (1960a). Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten. *Acta Sci. Math. Szeged* **21**, 206–217.

ITÔ, N. (1960b). Zur Theorie der Permutationsgruppen vom Grad p. *Math. Z.* **74**, 299–301.

ITÔ, N. (1961). Zur Theorie der transitiven Gruppen vom Grad p, II. *Math. Z.* **75**, 127–135.

ITÔ, N. (1962a). On a class of doubly transitive permutation groups. *Illinois J. Math.* **6**, 341–352.

ITÔ, N. (1962b). On transitive simple permutation groups of degree $2p$. *Math. Z.* **78**, 453–468.

(*P*) JORDAN, C. (1870). "Traité des substitutions et des équations algébriques." Gauthiers-Villars, Paris.

JORDAN, C. (1871). Théorèmes sur les groupes primitifs. *J. Math. Pures Appl.* **16**, 383–408.

JORDAN, C. (1872). Recherches sur les substitutions. *J. Math. Pures Appl.* **17**, 351–367.

JORDAN, C. (1873). Sur la limite de transitivité des groupes non alternés. *Bull. Soc. Math. France* **1**, 40–71.

JORDAN, C. (1875). Sur la limite du degré des groupes primitifs qui contiennent une substitution donnée. *J. f. reine angew. Math.* **79**, 248–258.

(*P*) JORDAN, C. (1961). "Œuvres". Publiées par J. Dieudonné, Tome I. Gauthier-Villars, Paris.

KOCHENDÖRFFER, R. (1937). Untersuchungen über eine Vermutung von W. Burnside. *Schr. Math. Sem. Inst. angew. Math. Univ. Berlin* **3**, 155–180.

KUHN, H. W. (1904). On imprimitive substitution groups. *Amer. J. Math.* **26**, 45–102.

MANNING, D. (1936). On simply transitive groups with transitive abelian subgroups of the same degree. *Trans. Amer. Math. Soc.* **40**, 324–342.

MANNING, W. A. (1906). On the primitive groups of class ten. *Amer. J. Math.* **28**, 226–236.

MANNING W. A. (1909). On the order of primitive groups. *Trans. Amer. Math. Soc.* **10**, 247–258.

MANNING, W. A. (1910). On the primitive groups of classes six and eight. *Amer. J. Math.* **32**, 235–256.

MANNING, W. A. (1911). On the limit of the degree of primitive groups. *Trans. Amer. Math. Soc.* **12**, 375–386.

MANNING, W. A. (1913). On the primitive groups of class twelve. *Amer. J. Math.* **35**, 229–260.

MANNING, W. A. (1917). On the primitive groups of class fifteen. *Amer. J. Math.* **39**, 281–310.

MANNING, W. A. (1918). The order of primitive groups, III. *Trans. Amer. Math. Soc.* **19**, 127–142.

MANNING, W. A. (1919). On the order of primitive groups, IV. *Trans. Amer. Math. Soc.* **20**, 66–78.

(*P*) MANNING, W. A. (1921). "Primitive Groups," Part I. (Math.

and Astron., Vol. I.) Stanford Univ. Press, Stanford, California.

MANNING, W. A. (1927). Simply transitive primitive groups. *Trans. Amer. Math. Soc.* **29**, 815–825.

MANNING, W. A. (1929). On the primitive groups of class fourteen. *Amer. J. Math.* **51**, 619–652.

MANNING, W. A. (1929). A theorem concerning simply transitive groups. *Bull. Amer. Math. Soc.* **35**, 30–332.

MANNING, W. A. (1933). The degree and class of multiply transitive groups. *Trans. Amer. Math. Soc.* **35**, 585–599.

MANNING, W. A. (1939). On transitive groups that contain certain transitive subgroups. *Bull. Amer. Math. Soc.* **45**, 783–791.

MARGGRAF, B. (1892). Über primitive Gruppen mit transitiven Untergruppen geringeren Grades. Dissertation, Giessen.

MILLER, G. A. (1897). On the primitive substitution groups of degree fifteen. *Proc. London Math. Soc.* **28**, 533–544.

MILLER, G. A. (1915). Limits of the degree of transitivity of substitution groups. *Bull. Amer. Math. Soc.* **22**, 68–71.

NAGAI, O. (1961). On transitive groups that contain non-Abelian regular subgroups. *Osaka Math. J.* **13**, 199–207.

ORE, O. (1951). Some remarks on commutators. *Proc. Amer. Math. Soc.* **2**, 307–314.

PARKER, E. T. (1954). A simple group having no multiply transitive representation. *Proc. Amer. Math. Soc.* **5**, 606–611.

PARKER, E. T. (1959). On quadruply transitive groups. *Pacific J. Math.* **9**, 829–836.

PARKER, E. T., and NIKOLAI, P. J. (1958). A search for analogues of the Mathieu groups. *Math. Tables Aids Comput.* **12**, 38–43.

RIETZ, H. L. (1904). On primitive groups of odd order. *Amer. J. Math.* **26**, 1–30.

RITT, J. F. (1922). On algebraic functions which can be expressed in terms of radicals. *Trans. Amer. Math. Soc.* **24**, 21–30.

RUDIO, F. (1888). Über primitive Gruppen. *J. f. reine angew. Math.* **102**, 1–8.

SCHUR, I. (1908). Neuer Beweis eines Satzes von W. Burnside. *Jahrb. Deutsche Math.-Ver.* **17**, 171–176.

SCHUR, I. (1933). Zur Theorie der einfach transitiven Permutationsgruppen. *S. B. Preuss. Akad. Wiss., Phys.-Math. Kl.* **1933**, 598–623.

SCOTT, W. R. (1957). Solvable factorizable groups. *Illinois J. Math.* **1**, 389–394.

(*G*) SPEISER, A. (1937). "Theorie der Gruppen von endlicher Ordnung," 3. Aufl. Springer, Berlin; 4. Aufl. Birkhäuser, Basel, 1956.

STANTON, R.G. (1951). The Mathieu groups. *Canadian J. Math.* **3**, 164-174.

SUZUKI, M. (1962). On a class of doubly transitive groups. *Ann. of Math.* **75**, 105–145.

TAMASCHKE, O. (1960). Ringtheoretische Behandlung einfach transitiver Permutationsgruppen. *Math. Z.* **73**, 393–408.

TAMASCHKE, O. (1963). Zur Theorie der Permutationsgruppen mit regulärer Untergruppe, I; II. *Math. Z.* **80**, 328–355, 443-465.

THOMPSON, J. G. (1959). Finite groups with fixed-point-free automorphisms of prime order. *Proc. Nat. Acad. Sci. U.S.A.* **45**, 578–581.

THOMPSON, J. G. (1960). Normal p-complements for finite groups. *Math. Z.* **72**, 332–354.

TITS, J. (1952). Généralisations des groupes projectifs basées sur leurs propriétés de transitivité. *Mém. Acad. Roy. Belgique* **27**, Fasc. 2, 115 pp.

TODD, J. A. (1959). On representations of the Mathieu groups as collineation groups. *J. London Math. Soc.* **34**, 406-416.

VINCENT, G. (1947). Les groupes linéaires finis sans points fixes. *Comment. Math. Helv.* **20**, 117–171.

VON NEUMANN, J., and MORGENSTERN, O. (1947). "Theory of Games and Economic Behaviour, "2nd ed. Princeton Univ. Press, Princeton, New Jersey.

WEISS, M. J. (1928). Primitive groups which contain substitutions of prime order p and of degree $6p$ or $7p$. *Trans. Amer. Math. Soc.* **30**, 333–359.

WEISS, M. J. (1934). On simply transitive groups. *Bull. Amer. Math. Soc.* **40**, 401–405.

WIELANDT, H. (1934). Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad. *Schr. Math. Sem. Inst. angew. Math. Univ. Berlin* **2**, 151–174.

WIELANDT, H. (1935). Zur Theorie der einfach transitiven Permutationsgruppen. *Math. Z.* **40**, 582–587.

WIELANDT, H. (1949). Zur Theorie der einfach transitiven Permutationsgruppen, II. *Math. Z.* **52**, 384–393.

WIELANDT, H. (1956). Primitive Permutationsgruppen vom Grad $2p$. *Math. Z.* **63**, 478–485.

WIELANDT, H. (1958). Über die Existenz von Normalteilern in endlichen Gruppen. *Math. Nachr.* **18**, 274–280.

WIELANDT, H. (1960). Über den Transitivitätsgrad von Permutationsgruppen. *Math. Z.* **74**, 297–298.

WIELANDT, H. (1962a). Subnormale Hüllen in Permutationsgruppen. *Math. Z.* **79**, 381–388.

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

WIELANDT, H., and HUPPERT, B. (1958). Normalteiler mehrfach transitiver Permutationsgruppen. *Arch. Math.* **9**, 18–26.

WITT, E. (1937). Die 5-fach transitiven Gruppen von Mathieu. *Abhandl. Math. Sem. Univ. Hamburg* **12**, 256–264.

ZASSENHAUS, H. (1934). Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. *Abhandl. Math. Sem. Univ. Hamburg* **11**, 17–40.

ZASSENHAUS, H. (1935a). Über endliche Fastkörper. *Abhandl. Math. Sem. Univ. Hamburg* **11**, 187–220.

ZASSENHAUS, H. (1935b). Über transitive Erweiterungen gewisser Gruppen aus Automorphismen endlicher mehrdimensionaler Geometrien. *Math. Ann.* **111**, 748–759.

(*G*) ZASSENHAUS, H. (1937). "Lehrbuch der Gruppentheorie, I." Leipzig, Teubner; 2nd English ed. 1958, Chelsea, New York.

Author Index

Notation Used in Text

α^p	1	g^Δ, G^Δ	4
A^Ω	2	$\mid G : H \mid$	3
Δ^K	3	$\mathbf{N}(H)$, $\mathbf{Z}(H)$	3
G_α, G_Δ	5	S^Ω	2

Subject Index