# POLYADIC GROUPS

BY

EMIL L. POST

## TABLE OF CONTENTS

SECTION PAGE

Introduction . . . . . 209

I. GENERAL THEORY OF POLYADIC GROUPS

1. Definition of a polyadic group . . . . . 213
2. Identity, inverse, equivalence . . . . . 214
3. The coset theorem . . . . . 218
4. Subgroups and transforms; expansion in cosets . . . . . 221
5. Reducibility . . . . . 228
6. Arbitrary containing ordinary groups . . . . . 238
7. Determination of all types of semi-abelianisms . . . . . 242
8. On the construction of polyadic groups . . . . . 245

II. FINITE POLYADIC GROUPS

A. $m$-ADIC SUBSTITUTIONS AND SUBSTITUTION GROUPS

9. The symmetric $m$-adic substitution group of degree $n$ . . . . . 248
10. $2^{m-1}$-fold classification of $m$-adic substitutions; the $m$-adic alternating groups . . . 250
11. Associated and containing ordinary groups; commutative $m$-adic substitutions . . 253
12. Further study of the complete $m$-adic $\delta$-group and $m$-adic alternating groups . . . 255
13. Transitive $m$-adic substitution groups . . . . . 261
14. Intransitive $m$-adic substitution groups . . . . . 262
15. Substitutions which are commutative with each of the substitutions of a transitive $m$-adic substitution group . . . . . 263
16. Holomorphs of a regular $m$-adic substitution group . . . . . 267
17. $m$-adic groups of $\mu$-adic substitutions . . . . . 272
18. Primitive and imprimitive $(m, \mu)$ substitution groups . . . . . 273
19. Multiple transitivity; cyclically transitive $m$-adic substitution groups . . . . . 276
20. Class of an $m$-adic substitution group . . . . . 278

B. FINITE ABSTRACT POLYADIC GROUPS

21. Cyclic polyadic groups; ordinary theory . . . . . 282
22. Cyclic polyadic groups; polyadic theory . . . . . 286
23. Abstract polyadic groups of the first three orders . . . . . 293
24. Properties of transforms . . . . . 295
25. Generation of polyadic groups by two groups, one invariant under the elements of the other . . . . . 298
26. $m$-adic groups of order $g$ prime to $m-1$ . . . . . 304
27. Sylow subgroups of order $p^\alpha$ with $g/p^\alpha$ prime to $m-1$ . . . . . 307
28. Representation of an arbitrary $m$-adic group as a regular $m$-adic substitution group . 312
29. Invariant subgroups and quotient groups; the $m$-adic central quotient group . . . 313

Presented to the Society, October 26, 1935; received by the editors January 4, 1940.

30. Commutator, semi-commutator, and quasi-commutator subgroups . . . . . 316
31. The $\phi$-subgroup of an $m$-adic group . . . . . 322
32. Simply isomorphic $m$-adic groups; group of inner isomorphisms . . . . . 324
33. Extension of Frobenius's theorem to $m$-adic groups . . . . . 327
34. Representation of an abstract $m$-adic group as a transitive $(m, \mu)$ substitution group . 328

C. FINITE $m$-ADIC LINEAR GROUPS

35. $m$-adic linear transformations . . . . . 330
36. $m$-adic collineations and collineation-groups . . . . . 334
37. $m$-adic Hermitian invariants . . . . . 337
38. Reduction to canonical form . . . . . 340
39. $m$-adic invariants . . . . . 344
40. Generalization of $m$-adic substitution and transformation groups . . . . . 347

## INTRODUCTION

The group concept is peculiar in the breadth of its application and the narrowness of its formulation. By modifying one or more of its restrictions there have resulted such concepts as that of semi-group, groupoid, mischgruppe, quasi-group, hypergroup, multigroup. In all of these generalizations of the group concept the group operation remains dyadic, that is, it is a function of two independent variables. Our present interest is in that generalization of the group concept which results when, while retaining all other of its special features, the group operation becomes polyadic, that is, a function of any finite number of independent variables.

As far back as 1904, E. Kasner thus considered generalizing the ordinary "group property," and called a set of elements closed under a $k$-adic operation a $k$-adic system(1). But the complete formulation of this generalization seems to have been first effected by Dörnte(2) in 1928 in a paper containing an extensive theory of what he there terms $n$-groups, $n$ being the number of independent variables in the operation. In 1932 Lehmer(3) independently formulated and investigated the special concept he termed triplex, which, in Dörnte's terminology, is an abelian 3-group. Dörnte's $m$-group, to change

(1) While the paper in question, *An extension of the group concept*, has not appeared in print, an abstract thereof will be found in the Bulletin of the American Mathematical Society, vol. 10 (1904), pp. 290–291. Though at one point of the abstract Kasner observes that "the law of combination of the general system is best exhibited by means of its $k$ dimensional multiplication table," his original definition adds the requirement that the combination of no fewer than $k$ elements shall be contained in the system—a requirement that is meaningless unless the $k$-adic operation itself is merely an extended product based on a prior dyadic operation. And the absence of any mention of an associative law, coupled with a reference to the inverse of an element, further suggests that, as in Miller's perfect cosets referred to below, this dyadic operation is understood to be that of some actual group in the ordinary sense containing the given system.

(2) W. Dörnte, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Mathematische Zeitschrift, vol. 29 (1928), pp. 1–19.

(3) D. H. Lehmer, *A ternary analogue of abelian groups*, American Journal of Mathematics, vol. 54 (1932), pp. 329–338.

the symbol, is also our $m$-adic group, or, for unspecified $m$, our polyadic group(4).

As examples of triadic systems, and these also are examples of triadic groups, Kasner mentions "the odd permutations in any number of letters, the $\infty^2$ central symmetries of the plane or the $\infty^3$ of space, the totality of dual or reciprocal transformations, the correlations contained in any projective group, the totality of conformal transformations of the plane which reverse angles." In the introduction of his paper Dörnte mentions, among other examples, residue classes modulo $k$ as $(k+1)$-groups, and in the body of his paper introduces many such arithmetical illustrations as exemplifiers of his abstract development. Apart from examples which are the subject of a major part of our theory, we may add the linear transformations of determinant an $(m-1)$-st root of unity as an $m$-group, and, more significantly, the $m$-group consisting of all the substitutions of a group which, instead of carrying a fixed letter into itself, transform say $a_1 \rightarrow a_2$, $a_2 \rightarrow a_3$, $\cdots$, $a_{m-1} \rightarrow a_1$. In all of these examples the polyadic operation is merely an extended product expressed in terms of a prior dyadic operation. On the other hand, lengths under the operation fourth proportional, now to be written $b:a=c:x$, constitute a 3-group in which, geometrically, the triadic operation is primary(5). Even more so for an abstract $m$-group whose operation is given ab initio by an $m$-dimensional table.

While the abstract formulation of polyadic group must be credited to Dörnte, in its coset theorem the present paper may be said to solve the problem of determining the essential nature of a polyadic group. This basic result is to the effect that any $m$-adic group can have its class of elements so widened, and in that widened class a dyadic operation so introduced, that the enlarged class, under that operation as product, constitutes an ordinary group in which the class of elements of the $m$-adic group is a coset of an invariant subgroup of the ordinary group, and the operation of the $m$-adic group the product of $m$ elements as elements of the ordinary group(6). At first glance this theorem seems to be identical, for finite groups, with a result of Miller's

(4) The present paper arose as a reaction to the importance ascribed to the group concept by C. J. Keyser in his *Mathematical Philosophy*, New York, 1922, Lecture XII. But see the next to the last paragraph of this introduction. We may note that an early attempt on our part to thus generalize the group concept on the basis of its fourfold characterization had failed. But on now turning to the twofold basis as given by Miller (*Finite Groups*, below, p. 52) we found generalization to be immediate.

(5) Analytically, the operation becomes $x=(ac)/b$, and so a variant of $a-b+c$, easily seen to lead to a 3-group. This last is already present in Dörnte's paper, and generalized in his Theorem 7, §1. Note that geometrically even, the binary operation multiplication can nevertheless be defined, even if secondary. The about-to-be-mentioned coset theorem shows the same situation to obtain in general.

(6) Cf. A. Suschkewitsch, *Über die Erweiterung der Semigruppe bis zur ganzen Gruppe*, Communications de la Société Mathématique de Kharkoff, (4), vol. 12 (1935), pp. 81–87.

of 1935([7]). But, apart from other differences in hypothesis, Miller obtains the coset conclusion by essentially *assuming* the given set of elements to be in an ordinary group([8]). However, as a result of the two theorems, finite polyadic group does become identical with Miller's "perfect co-set," some of whose properties he develops, provided the latter is understood to mean set of elements and polyadic operation thereon([9]).

In addition to differences in abstract development, the present paper goes beyond Dörnte's in generalizing the concepts of substitution and linear transformation in such a way that the resulting $m$-adic substitutions and $m$-adic linear transformations naturally lead to $m$-adic groups thereof (see §9 and §35 for their definition). These $m$-adic groups we study as generalizations of ordinary substitution and linear transformation groups. As incentive for this development, we have the theorem that any abstract $m$-adic group (finite) can be represented as a "regular" $m$-adic substitution group, a theorem which, indeed, first gave us our coset theorem. In the final section of the paper these concepts receive a wide extension which remains significant for ordinary groups. But they are then seen to be at least closely related to a type of ordinary group formulated by Specht([10]).

Intermediate between these generalizations of substitution group is one which includes $m$-adic groups of ordinary substitutions. Two of our examples given above are of this type. In this connection we may mention a work of Corral([11]) referred to by Miller. With substitutions on a given finite set of letters in question, Corral calls a set of substitutions a perfect brigade if closed under the operation $ABC$, an imperfect brigade if closed under the operation $AB^{-1}C$. The former is then identical with a 3-group of ordinary substitutions, the latter with a schar of substitutions, schar in Baer's([12]) wider form of a concept due to Prüfer([13]). Prüfer's development had a great influence on

([7]) G. A. Miller, *Sets of group elements involving only products of more than n*, Proceedings of the National Academy of Sciences, vol. 21 (1935), pp. 45–47. All references to Miller other than to *Finite Groups* (below) concern this paper.

([8]) The closing statement in Kasner's abstract, which suggests an anticipation of our coset theorem for triadic groups, is more probably merely related thereto in similar fashion.

([9]) His condition that his set $S$ contain no like subset is in error. Recognizing $S$ as an $(n+1)$-group of order $h$, we see from our §21 that his partial condition "$h$ is a power of $n$" should be "every distinct prime factor of $h$ is a factor of $n$."

([10]) W. Specht, *Eine Verallgemeinerung der Permutationsgruppen*, Mathematische Zeitschrift, vol. 37 (1933), pp. 321–341.

([11]) J. I. Corral, *Brigadas de Substituciones*, Part I, Havana, 1934; Part II, Toledo, 1935.

([12]) R. Baer, *Zur Einführung des Scharbegriffs*, Journal für die reine und angewandte Mathematik, vol. 160 (1929), pp. 199–207. His abstract formulation occurs in the important footnote on page 202. (Condition III therein can be proved in its entirety, and so is unnecessary.) The same footnote proves, in our terminology (see §5), that every schar is reducible to an ordinary group. Had the same situation obtained for polyadic groups, there would have been no need of our coset theorem.

([13]) H. Prüfer, *Theorie der Abelschen Gruppen*, I. *Grundeigenschaften*, Mathematische Zeitschrift, vol. 20 (1924), pp. 165–187.

Dörnte who showed that by rewriting the operation $AB^{-1}C$ formally as $ABC$, Prüfer's schar becomes a special kind of 3-group. This reinterpretation is however no longer possible if the Prüfer hypothesis $AB^{-1}C = CB^{-1}A$ is deleted to give Baer's schar.

While Dörnte's development in large measure consists in extending Prüfer's schar results to $n$-groups, our own work correspondingly attempts to generalize ordinary group theory. Thus, at the very beginning of our developments, where Dörnte's recognizes no identity for an $m$-group with $m>2$, we find that role played by certain sequences of $m-1$ elements of the $m$-group, and are thus led to a development culminating in the coset theorem of §3. The remainder of Part I, which is really a theory of abstract polyadic groups finite or infinite, consists of largely unrelated topics, but each fundamental in the theory. Our program crystallizes in Part II which, in $A$, $B$, $C$, systematically generalizes most of the general topics of three chapters in the Miller, Blichfeldt, Dickson, *Finite Groups*([14]), that is, Miller's Chapters II and III on substitution groups and abstract groups respectively, and Chapter IX, Blichfeldt's introductory chapter on linear groups. The reader will find here certain developments which merely paraphrase the ordinary theory, others which are far richer in their polyadic form, and still others which have no counterpart in ordinary theory. On the whole, the amount that does go over is surprisingly large. The principal failure is the but partial extension of Sylow's theorem. To the student of ordinary groups we may point out, among other connections, that the generalizations quasi-abelianism and quasi-commutator subgroup of §30 remain significant for ordinary groups, that §5 also gives a polyadic superstructure to any ordinary group, and that the coset theorem could be used to translate polyadic group results independently arrived at into ordinary group properties. While much of Dörnte's paper becomes clarified by means of our coset theorem, and several of his developments are carried considerably further in our own work, the present paper by no means can be said to supplant Dörnte's. We are furthermore directly indebted to him for his concepts of semi-invariant subgroup and semi-abelian group.

Useful as the coset theorem is in establishing certain properties of polyadic groups, its very existence greatly minimizes the significance of that generalization. Nevertheless, we cannot agree with Miller who says "the generalization secured by using perfect cosets instead of groups is, however, only apparent." In its autonomous formulation, polyadic group is fundamentally a generalization of ordinary group and, indeed, it is as generalization that

([14]) New York, 1916. Henceforth referred to as *Finite Groups*. Where in Part II the writer refers to the standard proof of an ordinary group result it is the proof in this text that is meant. We may note here that when an ordinary group term is applied without explicit definition to polyadic groups, its polyadic definition is entirely similar.

it lends itself to a corresponding development([15]). However, the final verdict will undoubtedly hang on the question of application([16]). For this end our concept of $m$-adic invariant is no doubt far too special (see §39). Genuine application of polyadic groups will probably therefore have to wait upon the formulation of an adequate concept of polyadic invariant.

We wish here to express our obligation to B. P. Gill to whose efforts we owe the completion of a major phase of our development (see §12). Had we completed the determination of the triadic linear groups in two variables mentioned in our preliminary report, this obligation would have been still greater. We are also indebted to R. Baer who, on two separate occasions, set us on the right path in the maze of ordinary group literature.

## I. General theory of polyadic groups

1. **Definition of a polyadic group.** Given a class of elements $C$, and an operation $c(s_1 s_2 \cdots s_m)$, we shall say that the elements of $C$ constitute an *$m$-adic group* $G$ under $c$ if the following two conditions are satisfied:

1. If any $m$ of the $m+1$ symbols in an equation of the form

$$c(s_1 s_2 \cdots s_m) = s_{m+1}$$

represent elements in $C$, the remaining symbol also represents an element in $C$, and is uniquely determined by this equation.

2. The elements of $C$ satisfy the associative law under $c$, that is, they satisfy

$$c(c(s_1 s_2 \cdots s_m) s_{m+1} s_{m+2} \cdots s_{2m-1}) = c(s_1 c(s_2 \cdots s_m s_{m+1}) s_{m+2} \cdots s_{2m-1})$$
$$= \cdots = c(s_1 s_2 \cdots c(s_m s_{m+1} s_{m+2} \cdots s_{2m-1}))([17]).$$

([16]) It is fundamental to remember, in this connection, that we are dealing not with a mere class of elements, but with a class of elements and an operation thereon; still better, with the properties of a class of elements under a given operation. Thus the genuineness of non-Euclidean geometry is not affected because it can be represented by certain constructions in Euclidean geometry. Had Miller's point of view been adopted, such a development as that of §5, for example, would hardly have been possible.

([16]) E.g., such as the Galois theory in the case of ordinary groups, not applications, such as the examples given above, which are mere illustrations of polyadic groups or of the theory thereof. Much of Corral's development concerns a brigade Galois theory. But this seems to the writer to be merely a restatement of standard Galois theory in terms of brigades rather than a genuine application.

([17]) This formulation, patterned by the author after Miller, is identical with Dörnte's except that Dörnte splits up our 1 into two parts, $P_1$ and $P_3$, according as $S_{m+1}$, or $S_i$, $i \neq m+1$, is to be determined. It is then readily proved by the methods of our next section that in $P_3$ only the existence of the solution $S_i$ need be postulated, its uniqueness being then provable. It can further be shown that this existence of a solution for $S_i$ need only be universally postulated either for a single $i$ with $1 < i < m$, or for both $i = 1$ and $i = m$, the existence of a solution for $S_i$ for all other $i$'s from 1 to $m$ then being provable. If the second form be used in place of $P_3$, and the first can only be used for $m > 2$, the resulting set of postulates would be the exact generalization of the basis for ordinary groups used by Albert in his *Modern Higher Algebra.*

We shall also use Dörnte's phrase "$m$-group" for $G$. Though these conditions are vacuously satisfied when $C$ is a null class, the ordinary group concept tacitly assumes the existence of at least one element, and so we make the same assumption here. An ordinary group is then immediately an $m$-adic group with $m=2$, that is, a dyadic group, or 2-group. Unlike Dörnte, we exclude the case $m=1$.

It is readily proved by induction that the number of elements entering into any combination of elements built up by the operation $c$ is of the form $k(m-1)+1$, where, in fact, $k$ is the number of $c$'s in the assumed symbolic expression of this "extended operation." As the basic operation $c(s_1 s_2 \cdots s_m)$ is on an ordered $m$-ad of elements, an extended operation built up by $c$'s orders the $k(m-1)+1$ elements appearing therein in a linear array $s_1, s_2, \cdots, s_{k(m-1)+1}$. It is then readily proved that as a consequence of the associative law 2 the element given by such an extended operation depends only on the sequence $s_1, s_2, \cdots, s_{k(m-1)+1}$, and is independent of the particular way in which parentheses are introduced in conjunction with the $k$ $c$'s that must enter into such an expression. We are justified, then, in briefly writing any such extended operation $c(s_1 s_2 \cdots s_{k(m-1)+1})$.

2. **Identity, inverse, equivalence.** Let $a_1, a_2, \cdots, a_{m-1}, a_m$ be elements of an $m$-adic group $G$ satisfying the equation

$$c(a_1 a_2 \cdots a_{m-1} a_m) = a_m.$$

Assuming as we do that $m \geqq 2$, we can, in fact, let $a_m$ and $m-2$ of the $m-1$ elements $a_1, a_2, \cdots, a_{m-1}$ be arbitrary elements of $G$, and then determine the remaining element in accordance with 1 of §1 so that this equation will be satisfied. If now $s$ be any element of $G$, we can likewise find $s_2, s_3, \cdots, s_m$ in $G$ so that $c(a_m s_2 s_3 \cdots s_m) = s$. By our assumed equation we will have

$$c(c(a_1 a_2 \cdots a_{m-1} a_m) s_2 s_3 \cdots s_m) = c(a_m s_2 s_3 \cdots s_m).$$

Hence, by the associative law,

$$c(a_1 a_2 \cdots a_{m-1} c(a_m s_2 s_3 \cdots s_m)) = c(a_m s_2 s_3 \cdots s_m),$$

and so

$$c(a_1 a_2 \cdots a_{m-1} s) = s.$$

That is, *if the equation* $c(a_1 a_2 \cdots a_{m-1} s) = s$ *holds for one* $s$ *in* $G$, *it holds for every* $s$ *in* $G$. The sequence, or $(m-1)$-ad, $\{a_1, a_2, \cdots, a_{m-1}\}$ may then be called a left identity of $G$. In the same way we can show that *if* $c(s b_1 b_2 \cdots b_{m-1}) = s$ *holds for one* $s$ *in* $G$, *it holds for every* $s$ *in* $G$, and $\{b_1, b_2, \cdots, b_{m-1}\}$ may be called a right identity of $G$.

We now prove that *every left identity of* $G$ *is a right identity, and conversely*, thus arriving at the unique concept of an $(m-1)$-ad as an *identity* of an $m$-adic group. Let $\{a_1, a_2, \cdots, a_{m-1}\}$ be a left identity. Then $c(a_1 a_2 \cdots a_{m-1} a_1) = a_1$. By the associative law,

$$c(a_0a_1a_2\cdots a_{m-2}c(a_{m-1}a_1a_2\cdots a_{m-1}))=c(a_0c(a_1a_2\cdots a_{m-2}a_{m-1}a_1)a_2\cdots a_{m-1}).$$

Hence

$$c(a_0a_1a_2\cdots a_{m-2}c(a_{m-1}a_1a_2\cdots a_{m-1}))=c(a_0a_1a_2\cdots a_{m-1}).$$

Since the first $m-1$ arguments of the two members of this equation are identical, the last must also be equal by 1, §1. Hence

$$c(a_{m-1}a_1a_2\cdots a_{m-1})=a_{m-1},$$

and $\{a_1, a_2, \cdots, a_{m-1}\}$ is also a right identity. Similarly for the converse.

Our equation $c(a_1a_2\cdots a_{m-1}a_1)=a_1$ shows that if $\{a_1, a_2, \cdots, a_{m-1}\}$ is an identity, so is $\{a_2, \cdots, a_{m-1}, a_1\}$. Hence also $\{a_3, \cdots, a_{m-1}, a_1, a_2\}$, and so on. Of course we have used the preceding result on left identities being the same as right identities. In general, then, *if* $\{a_1, \cdots, a_i, a_{i+1}, \cdots, a_{m-1}\}$ *is an identity, so is* $\{a_{i+1}, \cdots, a_{m-1}, a_1, \cdots, a_i\}$. Otherwise stated, cyclic permutation of the elements of an identity leaves it an identity.

Our initial observation proved the existence of an identity for $m\geqq 2$. Clearly, if $\{a_1, a_2, \cdots, a_{m-1}\}$ is an identity, it is immaterial which $m-2$ of these elements were assumed arbitrarily. Hence all identities of an $m$-adic group can be obtained by arbitrarily assigning values to, say, $a_1, a_2, \cdots, a_{m-2}$, and correspondingly determining $a_{m-1}$. If $G$ be of finite order $g$, there are $g^{m-1}$ $(m-1)$-ads formed from elements of $G$. Hence $G$ has $g^{m-2}$ identities. There will be no ambiguity if we use similar terminology when $g$ is infinite.

While the term identity will thus mean an $(m-1)$-ad of the above kind, a corresponding development in connection with an extended operation on $k(m-1)+1$ arguments leads to what may be termed an extended identity in the form of a $k(m-1)$-ad. Except for their number, extended identities enjoy the same properties as identities. Rather unsymmetrically we may say that $\{a_1, a_2, \cdots, a_{k(m-1)}\}$ is an extended identity if $\{a_1, a_2, \cdots, a_{m-2}, c(a_{m-1}\cdots a_{k(m-1)})\}$ is an identity.

The concept of identity immediately leads to that of inverse. For $m=2$, the inverse of an element $s$ is an element which multiplied into $s$ yields the identity. For $m>2$, to obtain an identity from an element $s$ we must annex $m-2$ other elements. We are thus led to an $(m-2)$-ad as an inverse of $s$. Hence, for $m>2$, an inverse of an element is an element when and only when $m=3$. $\{s_1, s_2, \cdots, s_{m-2}\}$ is then an inverse of $s$ if $\{s, s_1, s_2, \cdots, s_{m-2}\}$ is an identity. As $\{s_1, s_2, \cdots, s_{m-2}, s\}$ is then also an identity, we may therefore say that $s$ is an inverse of the $(m-2)$-ad $\{s_1, s_2, \cdots, s_{m-2}\}$. We are thus led to define inverse for $i$-ads with arbitrary $i$.

First let $i<m-1$. We then define an inverse of an $i$-ad $\{s_1, s_2, \cdots, s_i\}$ to be an $(m-i-1)$-ad $\{s_1', s_2', \cdots, s_{m-i-1}'\}$ such that $\{s_1, s_2, \cdots, s_i, s_1', s_2', \cdots, s_{m-i-1}'\}$ is an identity. As $\{s_1', s_2', \cdots, s_{m-i-1}', s_1, s_2, \cdots, s_i\}$ is then also an identity, $\{s_1, s_2, \cdots, s_i\}$ is an inverse of $\{s_1', s_2', \cdots, s_{m-i-1}'\}$, so that we can talk of a pair of inverse polyads. When $i=m-1$ we must

have recourse to an extended identity, and are thus led to an $(m-1)$-ad as inverse. $\{s_1', s_2', \cdots, s_{m-1}'\}$ is then an inverse of $\{s_1, s_2, \cdots, s_{m-1}\}$ if $\{s_1, s_2, \cdots, s_{m-1}, s_1', s_2', \cdots, s_{m-1}'\}$ is an extended identity. As before, $\{s_1, s_2, \cdots, s_{m-1}\}$ is also an inverse of $\{s_1', s_2', \cdots, s_{m-1}'\}$.

By means of inverses we easily solve an equation of the form

$$c(a_1a_2 \cdots a_isb_1b_2 \cdots b_{m-i-1}) = s_0$$

for $s$[18]. Let $\{a_1', a_2', \cdots, a_{m-i-1}'\}$, $\{b_1', b_2', \cdots, b_i'\}$ be inverses of $\{a_1, a_2, \cdots, a_i\}$, $\{b_1, b_2, \cdots, b_{m-i-1}\}$ respectively. Operating on both sides of the above equation by $c(a_1'a_2' \cdots a_{m-i-1}'|\, b_1'b_2' \cdots b_i')$, the bar indicating the missing argument, applying the associative law, and reducing the left-hand side by the property of identities we obtain

$$s = c(a_1'a_2' \cdots a_{m-i-1}'s_0b_1'b_2' \cdots b_i').$$

When $a$'s or $b$'s are missing, our inverse of an $(m-1)$-ad serves the same purpose. Clearly an equation of the same type arising from an extended operation can always be reduced to the above type by means of the associative law. Our need of inverses of $i$-ads with $i>m-1$ is thus not pressing. However, they can be similarly introduced by means of extended identities. While such an inverse can always be a $j$-ad with $1 \leqq j \leqq m-1$, to preserve the symmetry of the inverse relationship we must allow $j>m-1$ as well, and thus have to introduce extended inverses. Thus if $i=k(m-1)+l$, $0 \leqq l<m-1$, an inverse will be an $(m-l-1)$-ad, while all extended inverses will have $j$ in the form $\kappa(m-1)+(m-l-1)$.

The multiplicity of inverses when the latter are not single elements leads to the concept of equivalent $i$-ads. We can introduce that concept directly, however, as follows. Let $\{a_1, a_2, \cdots, a_i\}$ and $\{b_1, b_2, \cdots, b_i\}$ be such that for some specific $d_1, \cdots, d_j, e_1, \cdots, e_{m-i-j}$

$$c(d_1 \cdots d_ja_1a_2 \cdots a_ie_1 \cdots e_{m-i-j}) = c(d_1 \cdots d_jb_1b_2 \cdots b_ie_1 \cdots e_{m-i-j});$$

that is, replacing the sequence $a_1, a_2, \cdots, a_i$ by $b_1, b_2, \cdots, b_i$ in the specific operation given by the left-hand member of this equation leaves the result unaltered. Let $\{d_1', \cdots, d_{m-j-1}'\}$ and $\{e_1', \cdots, e_{i+j-1}'\}$ be inverses of $\{d_1, \cdots, d_j\}$, $\{e_1, \cdots, e_{m-i-j}\}$ respectively, and let $s_1, \cdots, s_\kappa, s_{\kappa+1}, \cdots, s_{m-i}$

[18] Dörnte solves this equation for $m>2$ by his "querelement" $\bar{a}$, defined as the solution of the equation $c(a \cdots ax)=a$ for $x$. The very economy of this concept, however, helps obscure the concepts of our present section, so necessary for the basic coset theorem. It may be pointed out that actually our method of solution can be so presented as to be independent of the previous theorems on identities, and thus leads to that part of the footnote to §1 concerning the provability of the uniqueness of the solution. Indeed, in this primordial form, the same method is constantly used by Dörnte without specific formulation. The reader may be interested in noting that Dörnte's Theorems 3 and 4, §1, may be considered special cases of our identity results in that the definition of $\bar{a}$ may now be restated: $\{a, \cdots, a, \bar{a}\}$ is a right identity.

be arbitrary elements of $G$. Operating on both sides of the above equation by the extended operation $c(s_1 \cdots s_\kappa d_1' \cdots d_{m'-j-1}' \mid e_1' \cdots e_{i+j-1}' s_{\kappa+1} \cdots s_{m-i})$ we obtain, after simplification,

$$c(s_1 \cdots s_\kappa a_1 a_2 \cdots a_i s_{\kappa+1} \cdots s_{m-i}) = c(s_1 \cdots s_\kappa b_1 b_2 \cdots b_i s_{\kappa+1} \cdots s_{m-i}).$$

A similar argument can be given when $j$, or $m-i-j$, is 0 or $m-1$. Hence, *if the sequence* $b_1 b_2 \cdots b_i$ *can replace* $a_1 a_2 \cdots a_i$ *somewhere in one operation it can do so anywhere in any operation*[19]. Clearly the same result holds good for extended operations as well. The $i$-ads $\{a_1, a_2, \cdots, a_i\}$ and $\{b_1, b_2, \cdots, b_i\}$ will then be said to be *equivalent*. Thus we may define an $m$-group $G$ to be abelian if the dyads $\{s_1, s_2\}$ and $\{s_2, s_1\}$ are equivalent for every pair of elements $s_1$, $s_2$ of $G$. For then the value of $c(s_1 s_2 \cdots s_m)$, $s$'s in $G$, is unaltered by any interchange of adjacent $s$'s, and hence by any permutation of all the $s$'s.

Let $\{a_1, a_2, \cdots, a_i\}$ and $\{b_1, b_2, \cdots, b_i\}$ be equivalent $i$-ads, and let $\{a_1', a_2', \cdots, a_{m'-i-1}'\}$ be an inverse of $\{a_1, a_2, \cdots, a_i\}$. We have then $c(a_1' a_2' \cdots a_{m'-i-1}' a_1 a_2 \cdots a_i s) = s$. Hence also $c(a_1' a_2' \cdots a_{m'-i-1}' b_1 b_2 \cdots b_i s) = s$ so that $\{a_1', a_2', \cdots, a_{m'-i-1}'\}$ is an inverse of $\{b_1, b_2, \cdots, b_i\}$ as well. A similar argument applies when $i = m-1$. That is, *every inverse of one of a pair of equivalent $i$-ads is also an inverse of the other.* Again, let $\{a_1, a_2, \cdots, a_i\}$ and $\{b_1, b_2, \cdots, b_i\}$ both be inverses of $\{a_1', a_2', \cdots, a_{m'-i-1}'\}$. Since we then have $c(a_1' a_2' \cdots a_{m'-i-1}' a_1 a_2 \cdots a_i s) = s = c(a_1' a_2' \cdots a_{m'-i-1}' b_1 b_2 \cdots b_i s)$, it follows that $\{a_1, a_2, \cdots, a_i\}$ and $\{b_1, b_2, \cdots, b_i\}$ are equivalent. That is, *inverses of the same polyad are equivalent.* It follows from these results that if $\{a_1', a_2', \cdots, a_{m'-i-1}'\}$ is an inverse of $\{a_1, a_2, \cdots, a_i\}$, the class of inverses of $\{a_1, a_2, \cdots, a_i\}$ is the class of $(m-i-1)$-ads equivalent to $\{a_1', a_2', \cdots, a_{m'-i-1}'\}$. Conversely, the class of $i$-ads equivalent to $\{a_1, a_2, \cdots, a_i\}$ is the class of inverses of $\{a_1', a_2', \cdots, a_{m'-i-1}'\}$. Finally, the first class is the class of inverses of each member of the second, and conversely. This for $i < m-1$. For $i = m-1$ both classes consist of $(m-1)$-ads.

We shall speak of the class of all $i$-ads equivalent to a given $i$-ad as a *class of equivalent* $i$-ads. As in the case of identities, to obtain all $i$-ads equivalent to a given $i$-ad we may assign arbitrary values to $i-1$ of the elements, the $i$th being then determined. We may therefore say that a class of equivalent $i$-ads has $g^{i-1}$ members. If, on the other hand, we keep $i-1$ elements fixed, and let the remaining element run through $G$, 1 of §1 shows that no two of the resulting $i$-ads can be equivalent, while each class of equivalent $i$-ads thus finds a representative. We may therefore say that for each $i$ there are exactly $g$ classes of equivalent $i$-ads. These classes are, or course, mutually exclusive. For $i = 1$ they are nothing more than the unit classes consisting of single elements of $G$. For $i = m-1$ one class of equivalent $i$-ads is singled out, that is, the class of identities.

(19) This result is proved in part by Dörnte as Theorem 2, §1, but the corresponding concept is not formulated. Clearly this relationship between $i$-ads is an "equivalence relationship."

3. **The coset theorem.** We are now in a position to embed our $m$-adic group $G$ in an ordinary group. Let $C^*$ be the class of all classes of equivalent $i$-ads for $i=1, 2, \cdots, m-1$. Each element of $C^*$ is thus a class of equivalent $i$-ads, and $C^*$ may then be said to have $(m-1)g$ elements, $g$ for each $i$. It is convenient to drop the distinction between a unit class and its sole member, so that we may consider $C$, the class of elements of $G$, a subclass of $C^*$. We proceed now to define a dyadic operation on the elements of $C^*$. But first we must remove the above tacit restriction $i<m$ in our discussion of equivalence. Clearly, by using extended operations, our results go over for $i \geqq m$. Furthermore, we can extend the concept of equivalence to allow an $i$-ad to be equivalent to a $j$-ad. With only the basic operation $c$ involved, we must clearly have $j-i$ a multiple of $m-1$. Without further elaboration, $\{b_1, b_2, \cdots, b_{i+k(m-1)}\}$ will be equivalent to $\{a_1, a_2, \cdots, a_i\}$ if $\{b_1, b_2, \cdots, b_{i-1}, c(b_i \cdots b_{i+k(m-1)})\}$ and $\{a_1, a_2, \cdots, a_i\}$ are equivalent in the original sense([20]).

We first prove the following: if two of the three polyads $\{a_1, a_2, \cdots, a_i\}$, $\{b_1, b_2, \cdots, b_j\}$, $\{a_1, a_2, \cdots, a_i, b_1, b_2, \cdots, b_j\}$ are respectively equivalent to the corresponding two of the three polyads $\{a_1', a_2', \cdots, a_i'\}$, $\{b_1', b_2', \cdots, b_j'\}$, $\{a_1', a_2', \cdots, a_i', b_1', b_2', \cdots, b_j'\}$, the remaining polyads are equivalent. We shall prove this result for $i+j \leqq m$, a corresponding proof with the use of extended operations serving for $i+j>m$. Consider then the operations $c(a_1a_2 \cdots a_ib_1b_2 \cdots b_jd_1 \cdots d_{m-i-j})$ and $c(a_1'a_2' \cdots a_i'b_1'b_2' \cdots b_j'd_1 \cdots d_{m-i-j})$. If the first and second polyads of the first set of three are respectively equivalent to the first and second of the second set of three, we will have $c(a_1a_2 \cdots a_ib_1b_2 \cdots b_jd_1 \cdots d_{m-i-j}) = c(a_1a_2 \cdots a_ib_1'b_2' \cdots b_j'd_1 \cdots d_{m-i-j}) = c(a_1'a_2' \cdots a_i'b_1'b_2' \cdots b_j'd_1 \cdots d_{m-i-j})$, and the third polyads are equivalent. If the hypothesis concerns the first and third polyads, then $c(a_1a_2 \cdots a_ib_1b_2 \cdots b_jd_1 \cdots d_{m-i-j}) = c(a_1'a_2' \cdots a_i'b_1'b_2' \cdots b_j'd_1 \cdots d_{m-i-j}) = c(a_1a_2 \cdots a_ib_1'b_2' \cdots b_j'd_1 \cdots d_{m-i-j})$, whence the corresponding conclusion. Similarly for the second and third polyads.

Let then the dyadic operation $c^*(r_1r_2)$ be defined as follows. If $r_1$ and $r_2$ are members of $C^*$, and if $\{a_1, a_2, \cdots, a_i\}$ is in the class $r_1$ of equivalent $i$-ads, $\{b_1, b_2, \cdots, b_j\}$ in the class $r_2$ of equivalent $j$-ads, then $c^*(r_1r_2)$ is to be the class of $(i+j)$-ads equivalent to $\{a_1, a_2, \cdots, a_i, b_1, b_2, \cdots, b_j\}$ when $i+j \leqq m-1$, the class of $(i+j-(m-1))$-ads equivalent to $\{a_1, a_2, \cdots, a_i,$

([20]) And, of course, our basic theorem on equivalent $i$-ads extends to equivalent polyads. It may then be noted that if we include a null sequence in this framework, an independent proof of the identity of left and right identities results. In fact, the about-to-be-proved coset theorem depends only on the concept of equivalence; and the properties of identity and inverse could therefore be derived with the help of that theorem. Their direct formulation in terms of the operation of the $m$-group, however, will be found indispensable for correct thinking on such topics as those of §5.

$b_1, b_2, \cdots, b_j\}$ when $i+j>m-1$. When $i+j\leqq m-1$, our previous results not only show that $c^*(r_1r_2)$ is independent of the particular $i$-ad and $j$-ad chosen from $r_1$ and $r_2$ respectively, but that if any two symbols in the equation $c^*(r_1r_2) = r_3$ are assigned values in $C^*$, the third is uniquely determined in $C^*$. The same is true when $i+j>m-1$ by the transitive property of equivalence. Hence, condition 1 of §1 for a dyadic group is satisfied by $(C^*, c^*)$; likewise condition 2, that is, the associative law. For let $\{a_1, \cdots, a_i\}$, $\{b_1, \cdots, b_j\}$, $\{c_1, \cdots, c_k\}$ be in $r_1$, $r_2$, $r_3$ respectively. Then, with equivalence extended as above, if $i+j+k=l+\lambda(m-1)$, $1\leqq l\leqq m-1$, both $c^*(c^*(r_1r_2)r_3)$ and $c^*(r_1c^*(r_2r_3))$ represent the class of $l$-ads equivalent to $\{a_1, \cdots, a_i, b_1, \cdots, b_j, c_1, \cdots, c_k\}$, so that, for all members of $C^*$,

$$c^*(c^*(r_1r_2)r_3) = c^*(r_1c^*(r_2r_3)).$$

Hence, *the members of $C^*$ constitute an ordinary group under $c^*$*. With $G$ as the given $m$-adic group, this ordinary group will be symbolized $G^*$.

We have observed that we may consider the members of $G$ to be members of $G^*$, that is, those classes of equivalent $i$-ads for which $i=1$. We now further observe that the operation $c(s_1s_2 \cdots s_m)$ can be identified with the extended operation $c^*(s_1s_2 \cdots s_m)$ when, of course, the $s$'s are in $G$. For $c^*(s_1s_2 \cdots s_m)$ is, indeed, the class of monads equivalent to $\{s_1, s_2, \cdots, s_m\}$, and so consists of but the one monad $c(s_1s_2 \cdots s_m)$([21]). We shall therefore call $G^*$ the *abstract containing ordinary group of $G$*, abstract by contrast with other possibilities to be discussed later. In fact, $G^*$ is clearly determined by the abstract form of $G$. And while $G^*$ as derived is not abstract, it may be made so by replacing the members of $C^*$ by symbols formally obeying the rule of combination $c^*$ as determined above.

To obtain a clearer view of the relationship between $G$ and $G^*$, and thus, indeed, really to solve the problem of the essential nature of a polyadic group, let us consider those members of $G^*$ which are classes of equivalent $(m-1)$-ads. We have already observed that one of these $g$ classes is the class of identities of $G$. Now if in the equation

$$c^*(r_1r_2) = r_3$$

any two of the three symbols represent classes of equivalent $(m-1)$-ads, so does the third. It follows that the $g$ classes of equivalent $(m-1)$-ads constitute an ordinary group under $c^*$, and hence a subgroup of $G^*$. We shall symbolize this ordinary group by $G_0$, and call it *the associated ordinary group of $G$*. It is readily seen that *$G_0$ is an invariant subgroup of $G^*$*([22]). To prove that, it

([21]) If then $G$ has but a finite number of elements, Miller's theorem concerning perfect cosets can be applied immediately to give the coset theorem that follows. However we here make no such restriction on $G$.

([22]) Provided $m>2$. For $m=2$, $G^*=G=G_0$. If then we here allow the term subgroup to include the group itself, the results of the present section are also valid for ordinary groups, though in trivial fashion.

is sufficient to show that in the equation

$$c^*(tr_1) = c^*(r_1r_2)$$

if $t$ is in $G_0$, $r_1$ in $G^*$, then $r_2$ is in $G_0$. But if $r_1$ is a class of equivalent $i$-ads, $t$ being a class of equivalent $(m-1)$-ads, then $c^*(tr_1)$, and hence $c^*(r_1r_2)$, is also a class of equivalent $i$-ads. $r_2$, then, can only be a class of equivalent $(m-1)$-ads, as was to be proved.

Let us now expand $G^*$ in cosets as regards its invariant subgroup $G_0$. As in the invariance proof, if a multiplier $r$ represents a class of equivalent $i$-ads, the corresponding coset consists of classes of equivalent $i$-ads, and indeed, constitutes the class of all $g$ classes of equivalent $i$-ads. While this is immediate when $g$ is finite, in any case if $r_1$ is a class of equivalent $i$-ads, the equation $c^*(r_2r)=r_1$ demands that $r_2$ be in $G_0$, so that $r_1$ is in the coset in question. Hence the expansion of $G^*$ as regards $G_0$ consists of exactly $m-1$ augmented cosets, each being the class of all $g$ classes of equivalent $i$-ads, for some $i=1, 2, \cdots, m-1$. The elements of $G$ itself therefore constitute one of these cosets, that is, that one for which $i=1$. Hence our basic theorem. *Every polyadic group is a coset of an ordinary group with respect to an invariant subgroup*, it being understood that the polyadic operation of the polyadic group is an extension of the dyadic operation of the ordinary group.

With the relationship between $G$, $G_0$ and $G^*$ made thus precise, it becomes desirable to simplify our notation. Hence, when but a single $m$-adic operation $c$ is involved, we shall write the corresponding dyadic operation $c^*(r_1r_2)$ simply as the product $r_1r_2$ of standard group theory. Our identification of $c(s_1s_2 \cdots s_m)$ with $c^*(s_1s_2 \cdots s_m)$ therefore enables us to write $c(s_1s_2 \cdots s_m)$, simply, $s_1s_2 \cdots s_m$. We now finally introduce the completely abstract view of $G^*$ with symbols for elements. Clearly the element of $G^*$ corresponding to the class of identities of $G$ is the identity of $G^*$, and so will be symbolized by 1, as usual. With the elements of $G^*$ as symbols, it will be convenient to call the symbol $r$, representing a class of equivalent $i$-ads, an $i$-ad. Thus $s_1s_2 \cdots s_i$ will be an $i$-ad when the $s$'s are elements of $G$. Conversely, every $i$-ad can be written thus. In particular, $G_0$, itself, consists of all distinct products $s_1s_2 \cdots s_{m-1}$ of $m-1$ elements in $G$. To avoid duplication, of course, we may keep $m-2$ of these elements fixed, and let the remaining one run through $G$.

In particular, if $s$ is an element of $G$, $s^i$ is an $i$-ad, and so may correspondingly be used as multplier in the expansion of $G^*$ in cosets as regards $G_0$. We may therefore write this expansion

$$G^* = G_0s + G_0s^2 + \cdots + G_0s^{m-2} + G_0 = sG_0 + s^2G_0 + \cdots + s^{m-2}G_0 + G_0.$$

Most significantly we may then also write

$$G = G_0s = sG_0.$$

Since $G_0$ consists of products of elements of $G$; we see that $G^*$ itself is generated by the elements of $G$. The expansion of $G^*$ shows the quotient group $G^*/G_0$ to be of order $m-1$, and, indeed, cyclic, with the element corresponding to the given polyadic group $G$ as generator. Our *coset theorem* is thus more precise than its brief formulation, given above, would indicate.

By means of this theorem we shall be able to prove many results concerning polyadic groups by means of known results on ordinary groups. On the other hand, the following almost immediately obvious converse enables polyadic group theory to make contributions to a certain aspect of ordinary group theory. To wit, *if a coset of an ordinary group with respect to an invariant subgroup is of finite order $m-1$ as element of the corresponding quotient group, then the elements of the coset constitute a polyadic group under the product of $m$ elements as operation*([23]). Though easily proved directly, this result may be considered a consequence of the general theorem of §8. It will also be generalized at the end of the next section. Note that such a result cannot be true for a coset corresponding to an element of infinite order of the quotient group.

4. **Subgroups and transforms; expansion in cosets.** Dörnte has treated the subject of expansions of polyadic groups in cosets exhaustively. While not possessing identities and inverses to lead to a concept of transforms, he was enabled adequately to treat invariant subgroups by mere commutativity properties. He further introduced what we shall refer to as semi-invariant subgroups, a concept which the writer completely overlooked in his own development, and was thus led to a more general concept of polyadic quotient groups than is given by invariant subgroups. Nevertheless we shall reexamine these concepts from the point of view of the coset theorem, and a theory of transforms, since not only do they become clearer thereby, but indeed admit of a certain degree of generalization.

A proper subclass of the class of elements of an $m$-adic group $G$ will be said to constitute a subgroup $H$ of $G$ if the elements of that subclass constitute a polyadic group under the polyadic operation of $G$. This is clearly equivalent to the following. If in an equation $c(s_1 s_2 \cdots s_m) = s_{m+1}$ any $m$ elements are in the subclass, the $(m+1)$-st is. For the rest of the definition of $m$-adic group follows from the elements of the subclass being in $G$. Where no confusion can result we shall occasionally allow $G$ to be a subgroup (improper) of itself. We proceed first to investigate the relationship between $H^*$ and $G^*$, $H_0$ and $G_0$.

With $H^*$ and $G^*$ considered as being composed of classes of equivalent $i$-ads, only those members of $H^*$ which are in $H$ will also be members of $G^*$. For if $\{s_1, s_2, \cdots, s_i\}$ is an $i$-ad of $H$, and hence also of $G$, the class of $H$ $i$-ads equivalent to $\{s_1, s_2, \cdots, s_i\}$ is but a proper subclass of the class of $G$ $i$-ads equivalent to $\{s_1, s_2, \cdots, s_i\}$ whenever $i>1$. Nevertheless a 1-1 correspondence is thus set up between the members of $H^*$ and the members of $G^*$

([23]) Already proved by Miller in equivalent form for finite groups.

containing them. For the latter are mutually exclusive. Hence, when $G^*$ is treated abstractly with symbols as elements, we may symbolize the members of $H^*$ correspondingly; and as the operation $c^*(s_1 s_2)$, that is, $s_1 s_2$ as explained above, when set up for $G^*$ now serves also for $H^*$, $H^*$ thereby becomes a subgroup of $G^*$.

The $(m-1)$-ads of $H^*$ are then also $(m-1)$-ads of $G^*$, so that $H_0$ is a subgroup of $G_0$. If $s$ is any element of $H$, we can simultaneously expand $H^*$ and $G^*$ in the form

$$H^* = H_0 s + H_0 s^2 + \cdots + H_0 s^{m-2} + H_0,$$

$$G^* = G_0 s + G_0 s^2 + \cdots + G_0 s^{m-2} + G_0.$$

It follows that the $m-1$ augmented cosets of $H^*$ as regards $H_0$ are respectively contained in the $m-1$ augmented cosets of $G^*$ as regards $G_0$. As an immediate consequence, we have *Lagrange's theorem holds for finite polyadic groups*. For, defining the order of a polyadic group as the number of its elements, the relations $G=G_0 s$, $H=H_0 s$ show that the order $g$ of the polyadic group $G$, and the order $h$ of its subgroup $H$, are respectively the same as the order of the ordinary group $G_0$, and its subgroup $H_0$; and hence, $h$ is a divisor of $g$.

Since $H$ generates $H^*$, and in turn consists of the common elements of $H^*$ and $G$, the correspondence between the subgroups $H$ of $G$, and their abstract containing groups $H^*$, is 1-1. $H_0$ consists of the common elements of $H^*$ and $G_0$, and hence is also determined by $H$. In fact, we shall find useful the result that the products of $m-1$ elements chosen from a subgroup $H$ of $G$ constitute a subgroup of $G_0$, namely $H_0$. On the other hand, different subgroups of $G$ may have the same associated ordinary group $H_0$. Hence, in general, we can only say that the correspondence between the subgroups $H$ of $G$, and their associated ordinary groups $H_0$, is but many-one. Furthermore, not every subgroup $H_0$ of $G_0$ need be the associated ordinary group of a subgroup $H$ of $G$. The coset theorem and its converse, indeed, show that *the necessary and sufficient condition that a subgroup $H_0$ of $G_0$ be the associated ordinary group of some subgroup $H$ of $G$ is that there exist an element $s$ of $G$ such that $H_0$ is invariant under $s$, while $s^{m-1}$ is in $H_0$*. Indeed the subgroups of $G$ are the distinct $H_0 s$'s obtained from all $H_0$'s and $s$'s satisfying this condition.

As has been observed by Dörnte, two subgroups $H$ and $K$ of an $m$-adic group $G$ need have no element in common. Thus, this will always be so if $H$ and $K$ are distinct subgroups of $G$ with the same associated group. If, however, $H$ and $K$ do have an element in common, their common elements clearly constitute a subgroup of each of the subgroups, if they are not identical with one or the other. Moreover, if $s$ be such a common element, by writing $H=H_0 s$, $K=K_0 s$, we see that the associated group of the "crosscut" of $H$ and $K$ is the crosscut of their associated groups.

We consider next the expansion of $G$ in cosets as regards a subgroup $H$ thereof. $H_0$ is clearly a subgroup of $G^*$. We may therefore expand $G^*$ in say right cosets as regards $H_0$. Now it is immediately seen that such a coset of $H_0$ either has no element in $G$, or is completely contained in $G$. For if this coset has an element $s$ in common with $G$, then, since the coset can be written $H_0s$, and $H_0$ is contained in $G_0$, $H_0s$ will be wholly contained in $G=G_0s$. As all the elements of $G$ must appear in the given expansion of $G^*$, we see that the cosets in question containing elements of $G$ constitute a separation of the elements of $G$ into mutually exclusive classes of elements. We may say then that $G$ has thus been *expanded in right cosets as regards* $H$. A similar result holds for *left cosets*.

And now an immediate generalization. In the above discussion $H$ served only to introduce the subgroup $H_0$ of $G_0$. If then $H_0$ be any subgroup of $G_0$, whether it corresponds to a subgroup $H$ of $G$, or not, the above argument holds without change. Hence, *every subgroup of the associated ordinary group of a polyadic group leads to an expansion of the polyadic group in right cosets, and in left cosets, as regards that subgroup.*

Specifically, if in the expansion of $G^*$ in right cosets as regards $H_0$ the corresponding multipliers which are in $G$ are $s_\alpha, s_\beta, \cdots, s_\kappa$, then the expansion of $G$ in right cosets as regards $H_0$ can be written

$$G = H_0s_\alpha + H_0s_\beta + \cdots + H_0s_\kappa.$$

Similarly for left cosets. A not easily proved theorem for ordinary finite groups is that the coset multipliers may be so selected that they are the same on the right as on the left. An immediate corollary of the preceding formulation is that the same is true of finite polyadic groups.

It is sometimes necessary to consider the intersections of cosets in the expansion of $G$ in, say, right cosets as regards subgroups $H_0$, and $K_0$, of $G_0$. We have then immediately that while a coset with respect to $H_0$ and a coset with respect to $K_0$ may have no elements in common, if they do have a common element $s$, then their common elements constitute the set $L_0s$ where $L_0$ is the crosscut of $H_0$ and $K_0$. In particular, if $G$ is finite, all such intersecting pairs of cosets intersect in the same number of elements, namely, a number equal to the order of the crosscut of $H_0$ and $K_0$.

Expansions of $G$ in double cosets likewise admit of simple treatment. With $H_0$ and $K_0$ arbitrary subgroups of $G_0$, we may expand $G^*$ in double cosets $H_0rK_0$. If any element of such a double coset is in $G$, the entire double coset is contained in $G$. Hence, if in the expansion of $G^*$ we select those double cosets with $r$ in $G$, the result will be a separation of the elements of $G^*$ into mutually exclusive sets, that is, the expansion of $G$ in double cosets as regards $H_0$ and $K_0$. In particular, if $G$ has subgroups $H$ and $K$ whose associated ordinary groups are $H_0$ and $K_0$ respectively, the resulting expansion may be

spoken of as the expansion of $G$ in double cosets as regards $H$ and $K$, the case considered by Dörnte(24).

We shall introduce the property of invariance through the more general concept of transform. To insure the fundamental correctness of our concept, we go back to first principles. Given an element $s$, and an $i$-ad $\{s_1, s_2, \cdots, s_i\}$, both considered in the $m$-adic sense, we define the *transform* of $s$ under $\{s_1, s_2, \cdots, s_i\}$ to be the element

$$c(s_1' s_2' \cdots s_{m-i-1}' s s_1 s_2 \cdots s_i)$$

where $\{s_1', s_2', \cdots, s_{m-i-1}'\}$ is an inverse of $\{s_1, s_2, \cdots, s_i\}$. This for $i<m-1$; a similar definition holds for $i=m-1$. Since all inverses of a given polyad are equivalent, this transform is uniquely determined by $s$, and $\{s_1, s_2, \cdots, s_i\}$. Since inverses of equivalent $i$-ads are also equivalent, it follows that equivalent $i$-ads yield identical transforms of a given element.

In saying $s$ and $\{s_1, s_2, \cdots, s_i\}$ are $m$-adic, we tacitly assume that there is some $m$-adic group to which $s$, $s_1$, $s_2$, $\cdots$, $s_i$ belong. Let us then consider the abstract containing ordinary group of this $m$-adic group, and treat it in abstract form, with simplified notation. If, then, $i$-ad $\{s_1, s_2, \cdots, s_i\}$ corresponds to abstract $i$-ad $r$ of the containing group, the $(m-i-1)$-ad $\{s_1', s_2', \cdots, s_{m-i-1}'\}$ will correspond to an abstract $(m-i-1)$-ad $r'$ such that if $s$ be an element of the $m$-adic group, $r'rs=s$. Writing the identity of the containing group as usual, we thus have $r'r=1$, and hence in customary notation, $r'=r^{-1}$. Consequently, if $r$ represents a class of equivalent polyads of a polyadic group, $r^{-1}$ represents the class of inverses of those polyads. The transform of $s$ under $\{s_1, s_2, \cdots, s_i\}$ can now be written $r^{-1}sr$. And so, the transform of an element by an $i$-ad is the ordinary transform of that element by the corresponding abstract $i$-ad in the abstract containing group.

We can now extend our concept of transform to that of the transform of a polyad by a polyad. In general, via the abstract containing group, the transform of $r_1$ by $r_2$ is $r_2^{-1}r_1r_2$. Had we resorted to our primitive concepts in this case, we would have, as with inverses, a class of equivalent transforms. We readily see that in all cases the transform of an $i$-ad, $i \leqq m-1$, is an $i$-ad.

Consider now an $m$-adic group $G$, and an $i$-ad $r$ not necessarily an $i$-ad of $G$. Then, as with ordinary groups, if each element of $G$ is transformed by $r$, there results an $m$-adic group $G'$ which may be said to be simply isomorphic with $G$, and will be termed the transform of $G$ under $r$. In fact, let $s'$ be the transform under $r$ of any element $s$ of $G$. Since $r^{-1}s_1r \cdot r^{-1}s_2r \cdots r^{-1}s_mr = r^{-1}s_1s_2 \cdots s_mr$, we see that the relationship $s_1s_2 \cdots s_m = s_{m+1}$ is equivalent

(24) At first glance it would appear that Dörnte's expansions in cosets and double cosets, while depending on actual subgroups of $G$, are more general than we have stated them to be. However, it is readily seen that Dörnte's expansions with respect to a subgroup, or subgroups, of $G$ are our expansions of $G$ with respect to transforms, in the sense defined below, of the given subgroup or subgroups by polyads of $G$. And since these transforms are again subgroups of $G$, the Dörnte expansions are no more general than we have stated them to be.

to $s_1' s_2' \cdots s_m' = s_{m+1}'$. The defining properties 1 and 2 for an $m$-adic group then follow immediately for the transform of $G$ from the selfsame properties for $G$—hence the $m$-adic group $G'$. In general, two $m$-adic groups $G$ and $G'$ may be said to be *simply isomorphic* if a 1-1 correspondence can be set up between their elements such that if $s'$ of $G'$ is the correspondent of $s$ in $G$, then we will have, for all elements of $G$,

$$[c(s_1 s_2 \cdots s_m)]' = c'(s_1' s_2' \cdots s_m'),$$

$c$ and $c'$ designating the $m$-adic operations of $G$ and $G'$ respectively. For $G'$ the transform of $G$ this is immediate with $c$ and $c'$ the common unexpressed $m$-adic operation.

We reserve a more detailed treatment of transforms for our study of finite polyadic groups, and turn to the question of invariance. An $m$-adic element, polyad, or group will be said to be invariant under an $i$-ad if it is transformed into itself by that $i$-ad. It will then be said to be invariant under an $m$-adic group if it is invariant under every polyad of that group. Since $G^*$ is generated by $G$, it follows that for $K$ to be invariant under $G$, it is sufficient that it be invariant under every element of $G$. If such a $K$ is an element (subgroup) of $G$ it will then be said to be an invariant element (subgroup) of $G$. Clearly, the condition that an $m$-group $G$ be abelian is equivalent to each of its elements being an invariant element of $G$. For, in the notation of the coset theorem, $\{s_1, s_2\}$ and $\{s_2, s_1\}$ being equivalent becomes $s_1 s_2 = s_2 s_1$, or, $s_2^{-1} s_1 s_2 = s_1$; and conversely.

Given an invariant subgroup $H$ of $G$, the expansion of $G$ in cosets as regards $H$ immediately leads to an $m$-adic quotient group $G/H$. In fact, since $H$ is invariant under $G$, it immediately follows that $H_0$, the associated 2-group of $H$, is also invariant under $G$; that is, $H_0$, as subgroup of $G^*$, is invariant under each element of $G$ considered as element of $G^*$. For $H_0$ consists of all products of $m-1$ elements chosen arbitrarily and independently from $H$. Hence the transform of $H_0$ under any element $s$ of $G$ consists of all products of $m-1$ elements chosen arbitrarily and independently from the transform of $H$ under $s$, that is, from $H$ all over again.

Consider then the expansion in cosets $G = H_0 s_\alpha + H_0 s_\beta + \cdots + H_0 s_\kappa$. Then, exactly as in ordinary group theory, the coset in which the element $s_1 s_2 \cdots s_m$ appears depends only on the cosets containing the elements $s_1, s_2, \cdots, s_m$. If then $\sigma_1, \sigma_2, \cdots, \sigma_m$ represent the cosets containing $s_1, s_2, \cdots, s_m$ respectively, we may write the coset containing $s_1 s_2 \cdots s_m$ in the form $\sigma_1 \sigma_2 \cdots \sigma_m$. An $m$-adic operation is thus determined on these cosets as elements; and, again as in classic theory, these cosets constitute an $m$-adic group under this operation. We may therefore call this group the quotient group $G/H$.

As we shall see later, $m$-adic quotient groups arising from invariant subgroups are very special kinds of polyadic groups. However, Dörnte has em-

phasized that $m$-adic quotient groups can arise in more general fashion. In our presentation, his argument reduces to the fact that the only use made of the invariance of subgroup $H$ under $G$ was to prove the invariance of $H_0$ under $G$. We shall call a subgroup $H$ of $G$ whose associated 2-group $H_0$ is invariant under $G$ a *semi-invariant* subgroup of $G$. It follows that every semi-variant subgroup of an $m$-adic group leads to an $m$-adic quotient group.

This result can be made still more general. For we observed earlier that any subgroup $H_0$ of the associated 2-group $G_0$ of $G$ gives rise to expansions in cosets. It therefore follows that *every subgroup of the associated 2-group of an m-adic group which is invariant under the m-adic group leads to an m-adic quotient group.* In the absence of a subgroup $H$ of $G$ we shall write this quotient group $G/H_0$.

It is immediately seen that with $H_0$ thus invariant under $G$, the right cosets of $G$ as regards $H_0$ are identical with the left cosets. For $s^{-1}H_0s=H_0$ yields $H_0s=sH_0$. Conversely, if the right cosets of $G$ as regards $H_0$ are identical with the left cosets, then, for each element $s$ of $G$, $H_0s=sH_0$, so that $H_0$ is invariant under $G$. We thus see that the Dörnte concept of semi-invariance may be said to be the necessary and sufficient condition that a subgroup of a polyadic group give rise to a quotient group. Our extension, however, frees $G$ from the need of possessing a subgroup $H$ corresponding to the $H_0$ invariant under $G$.

In recent literature the concept of homomorphism appears as essentially equivalent to that of quotient group([25]). By means of our coset theorem we readily show the same to be true for $m$-groups([26]). As the analysis is not too immediate, we have refrained from explicitly using this concept except in the last section where it is especially needed.

An $m$-group $G$ with operation $c$ may be said to be *homomorphic* to an $m$-group $\overline{G}$ with operation $\bar{c}$ if there is a many-one correspondence between the elements of $G$ and of $\overline{G}$ such that whenever $s_1, s_2, \cdots, s_m$ of $G$ respectively correspond to $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_m$ of $\overline{G}$, $c(s_1s_2\cdots s_m)$ corresponds to $\bar{c}(\bar{s}_1\bar{s}_2\cdots\bar{s}_m)$. We first show that such a homomorphism between $G$ and $\overline{G}$ determines a homomorphism between their abstract containing groups $G^*$ and $\overline{G}^*$. In fact, let $i$-ad $r$ of $G^*$ be said to correspond to $i$-ad $\bar{r}$ of $\overline{G}^*$ if there exist elements $s_1, s_2, \cdots, s_i$ of $G$, and corresponding elements $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_i$ of $\overline{G}$, such that $r=c^*(s_1s_2\cdots s_i)$, $\bar{r}=\bar{c}^*(\bar{s}_1\bar{s}_2\cdots\bar{s}_i)$. It is readily seen that this sets up a correspondence between all the elements of $G^*$ and all the elements of $\overline{G}^*$. Furthermore, this correspondence is many-one. For suppose $r$ of $G^*$ corresponds to $\bar{r}_1$ and $\bar{r}_2$ of $\overline{G}^*$. Then we must have $r=c^*(s_1s_2\cdots s_i)$, $\bar{r}_1=\bar{c}^*(\bar{s}_1\bar{s}_2\cdots\bar{s}_i)$, and, also, $r=c^*(s_1's_2'\cdots s_i')$, $\bar{r}_2=\bar{c}^*(\bar{s}_1', \bar{s}_2', \cdots, \bar{s}_i')$, with $s_1, s_2, \cdots, s_i, s_1', s_2', \cdots, s_i'$ of $G$ corresponding to $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_i, \bar{s}_1', \bar{s}_2', \cdots, \bar{s}_i'$ respectively of $\overline{G}$. If then $s$ of $G$ corresponds to $\bar{s}$ of $\overline{G}$, the equation

([25]) See, for example, B. L. van der Waerden, *Moderne Algebra*, Berlin, 1930, vol. 1, §9.

([26]) Dörnte's Theorem 8, §6, does the same for his more limited concept of $m$-adic quotient group under the assumption that the homomorph has at least one "first order element."

$c(s_1 s_2 \cdots s_i s \cdots s) = c(s_1' s_2' \cdots s_i' s \cdots s)$, obtained from the two forms of $r$, yields $\bar{c}(\bar{s}_1 \bar{s}_2 \cdots \bar{s}_i \bar{s} \cdots \bar{s}) = \bar{c}(\bar{s}_1' \bar{s}_2' \cdots \bar{s}_i' \bar{s} \cdots \bar{s})$ as a result of the homomorphism between $G$ and $\overline{G}$. Hence $\bar{r}_1 = \bar{r}_2$. Finally, if $r_1$ and $r_2$ of $G^*$ thus correspond to $\bar{r}_1$ and $\bar{r}_2$ of $\overline{G}^*$, $c^*(r_1 r_2)$ corresponds to $\bar{c}^*(\bar{r}_1 \bar{r}_2)$—immediately, if $r_1$ and $r_2$ are an $i$-ad and $j$-ad respectively with $i+j \leqq m-1$, and via the homomorphism between $G$ and $\overline{G}$ if $i+j > m-1$. The many-one correspondence between the elements of $G^*$ and of $\overline{G}^*$ is therefore a homomorphism.

The ordinary theorem on homomorphisms is therefore applicable, and we can state that the elements of $G^*$ corresponding to the identity of $\overline{G}^*$ constitute an invariant subgroup $H_0$ of $G^*$, while the elements of $G^*$ corresponding to any element of $\overline{G}^*$ constitute a coset in the expansion of $G^*$ as regards $H_0$, the quotient group $G^*/H_0$ being then simply isomorphic with $\overline{G}^*$. Since the identity of $\overline{G}^*$ is an $(m-1)$-ad, $H_0$ must consist of $(m-1)$-ads in $G^*$, and is thus a subgroup of $G_0$ invariant under $G$. Those cosets of $G^*$ as regards $H_0$ which involve elements of $G$ therefore constitute an expansion of $G$ as regards $H_0$. Finally, the correspondence between $G^*$ and $\overline{G}^*$ is but the original correspondence for elements of $G$ and $\overline{G}$. We thus have the following theorem. *If m-group G is homomorphic to m-group* $\overline{G}$, *there is an m-adic quotient group* $G/H_0$ *such that the correspondents of each element of* $\overline{G}$ *constitute a coset in* $G/H_0$, *this quotient group then being simply isomorphic with* $\overline{G}$. Actually, as we have seen, $H_0$ consists of the elements of $G_0$ corresponding to the identity of $\overline{G}_0$ in the homomorphism between $G^*$ and $\overline{G}^*$, and hence between $G_0$ and $\overline{G}_0$ determined by the given homomorphism. Since an $m$-group $G$ is clearly homomorphic to any $m$-adic quotient group $G/H_0$, the equivalence of the concepts of homomorphism and quotient group has been shown to hold also for $m$-groups.

A homomorphism between $m$-groups $G$ and $\overline{G}$ is thus always an $(N, 1)$ isomorphism with fixed $N$, $N$ of course finite for finite $m$-groups. A more immediate consequence of the given homomorphism is that it sets up a many-one correspondence between the subgroups of $G$ and the subgroups of $\overline{G}$, an $m$-group being considered now as a subgroup of itself. In fact, given a subgroup of $G$, the corresponding elements of $\overline{G}$ are readily seen to satisfy the conditions for an $m$-group, and thus constitute the uniquely corresponding subgroup of $\overline{G}$. On the other hand, given a subgroup of $\overline{G}$, the set of all corresponding elements of $G$ constitutes a subgroup of $G$ with the given subgroup of $\overline{G}$ as corresponding subgroup, and indeed, contains all such subgroups of $G$. Clearly this many-one correspondence between the subgroups of $G$ and of $\overline{G}$ is preserved under the relation "subgroup of"—subgroup, in the above sense of group or subgroup.

It is also readily verified that if the set $\overline{G}$ is not known to be an $m$-group under operation $\bar{c}$, yet the remainder of the definition of homomorphism between $G$ and $\overline{G}$ is satisfied, then $\overline{G}$ is an $m$-group under $\bar{c}$, and hence the given relation a genuine homomorphism. In fact, the only part of our defi-

nition of $m$-group not immediately given for $\bar{G}$ under $\bar{c}$, as a consequence of its being satisfied by $G$ under $c$, is the uniqueness of the solution of $\bar{c}(\bar{s}_1\bar{s}_2 \cdots \bar{s}_m) = \bar{s}_{m+1}$ for $\bar{s}_i$, $1 \leqq i \leqq m$. Passing by the considerations of the footnote of §1 and a special argument valid only for $\bar{G}$ finite, we can in every case solve corresponding equations $c(s_1s_2 \cdots s_m) = s_{m+1}$ for $s_i$ as in §2, with all $s$'s except $s_i$ and $s_{m+1}$ fixed, and thus find that all such $s$'s must correspond to the same, consequently unique, $\bar{s}_i$([27]).

Our converse of the coset theorem admits of immediate extension to the case of an $m$-adic quotient group. For the statement of this result we need the concept of order, when finite, of an element of an $m$-group as given in the beginning of §21. We may note now, however, that an element $s$ may be said to be of first order if $c(ss \cdots s) = s$, the unit class with sole member $s$ then being a subgroup of the given $m$-group. We see then immediately that *if an element of an m-adic quotient group is of the first order, the corresponding coset constitutes a subgroup of the given m-group.* For the isomorphism between the given $m$-group and the quotient group shows that if in an equation $c(s_1s_2 \cdots s_m) = s_{m+1}$ any $m$ elements are in the coset, the $(m+1)$-st element must also be in that coset. Now consider any element $\sigma$ of finite order $k$ of the quotient group. Anticipating a concept of the next section, we may note now that our given $m$-group will constitute a polyadic group under the extended operation $c(s_1s_2 \cdots s_\mu)$ with $\mu = k(m-1)+1$. Our $m$-adic quotient group likewise extends to a $\mu$-group with the element $\sigma$ now being a first order element of the $\mu$-adic quotient group. The previous result therefore leads to the following. *If an element of an m-adic quotient group is of finite order k, then the elements of the corresponding coset constitute a polyadic group under the operation of the given group extended to $k(m-1)+1$ elements.*

5. **Reducibility.** Given any ordinary group with class of elements $C$ and dyadic operation $s_1s_2$, an $m$-adic group on the same elements will be determined if we set up the $m$-adic operation $c(s_1s_2 \cdots s_m) = s_1s_2 \cdots s_m$. We shall

([27]) If a general isomorphism between $m$-groups $G$ and $\bar{G}$ be defined as a many-many correspondence between their elements in which $m$-adic products of corresponding elements correspond, then, for finite $m$-adic groups, as for finite ordinary groups, the correspondence is that of a simple isomorphism between $m$-adic quotient groups of $G$ and $\bar{G}$. On the other hand, Dickson (these Transactions, vol. 6 (1905), pp. 205–208) has shown by an example that the finite group theorem does not hold for infinite groups, while Loewy (Festschrift Heinrich Weber, 1912, pp. 198–227) calls an isomorphism "vollständig" if inverses of corresponding elements also correspond—the case when the finite group theorem does hold for infinite groups —and derives a number of interesting conditions for a general isomorphism to be "vollständig." In the case of infinite $m$-adic groups, the condition under which the finite $m$-adic group theorem goes over can be written in a variety of ways, but perhaps most symmetrically as follows. If in two equations $c(s_1s_2 \cdots s_m) = s_{m+1}$, $\bar{c}(s_1's_2' \cdots s_m') = s'_{m+1}$, $m$ of the $m+1$ symbols in the first equation, and the $m$ corresponding symbols in the second equation, represent elements of $G$ and $\bar{G}$ respectively that correspond, then the elements represented by the remaining symbols must correspond. The writer is indebted to Reinhold Baer for the above references (as well as for the Neumann reference of §30).

call the $m$-group an extension of the 2-group, and say that it is reducible to that 2-group. Note that while the coset theorem presented an arbitrary polyadic group in a somewhat similar light, the elements of the polyadic group formed but a proper subclass of the class of elements of the 2-group; whereas, when a polyadic group is reducible to a 2-group, the classes of elements are identical.

More generally, given a $\mu$-group with class of elements $C$ and operation $c_\mu(s_1s_2\cdots s_\mu)$, if $m$ is any number in the form $k(\mu-1)+1$ we can form the extended operation $c_\mu(s_1s_2\cdots s_m)=c_\mu(s_1s_2\cdots s_{\mu-1}c_\mu(s_\mu s_{\mu+1}\cdots s_{2\mu-2}(\cdots c_\mu(s_{(k-1)(\mu-1)+1}s_{(k-1)(\mu-1)+2}\cdots s_{k(\mu-1)+1})\cdots)))$. The members of $C$ will then form an $m$-adic group under the operation $c_m(s_1s_2\cdots s_m)=c_\mu(s_1s_2\cdots s_m)$. As before, the $m$-group will be said to be an extension of the $\mu$-group, and reducible to the $\mu$-group.

An $m$-adic operation on a finite number of elements is most naturally exhibited by an $m$-dimensional table. We shall therefore say that an $m$-adic group is of *dimension* $m$. We then see that while a 2-group has an extension for each dimension $m>2$, a $\mu$-group has an extension for those and only those dimensions $m$ for which $m-1$ is a multiple of $\mu-1$.

A given $m$-group will be said to be *reducible to a $\mu$-group* if there exists a $\mu$-group to which it is reducible. The $m$-group will be said to be irreducible if it is not reducible to a $\mu$-group for any $\mu<m$[28]. Dörnte has already given a necessary and sufficient condition that a polyadic group be reducible to a 2-group. We proceed to generalize this result to reducibility to a $\mu$-group.

A $(\mu-1)$-ad $\{a_1, a_2, \cdots, a_{\mu-1}\}$ will be said to be commutative with an element $a$ if the $\mu$-ads $\{a_1, a_2, \cdots, a_{\mu-1}, a\}$ and $\{a, a_1, a_2, \cdots, a_{\mu-1}\}$ are equivalent. We then have the following basic theorem on reducibility. *A necessary and sufficient condition that a given $m$-group be reducible to a $\mu$-group, $m=k(\mu-1)+1$, is that there be a $(\mu-1)$-ad $\{a_1, a_2, \cdots, a_{\mu-1}\}$ formed from elements of the $m$-group such that the $(\mu-1)$-ad is commutative with every element of the $m$-group, and such that the $(m-1)$-ad $\{a_1, a_2, \cdots, a_{\mu-1}, a_1, a_2, \cdots, a_{\mu-1}, \cdots, a_1, a_2, \cdots, a_{\mu-1}\}$ is an identity of the $m$-group.*

The necessity of this condition follows immediately from the existence and properties of identities. For, if the $m$-group is reducible to a $\mu$-group, let $\{a_1, a_2, \cdots, a_{\mu-1}\}$ be an identity of such a $\mu$-group. If $c_\mu$ is the operation of the $\mu$-group, $c_\mu(a_1a_2\cdots a_{\mu-1}s)=s=c_\mu(sa_1a_2\cdots a_{\mu-1})$ for every element $s$ of the $\mu$-group. Hence $\{a_1, a_2, \cdots, a_{\mu-1}\}$ is commutative with every element of the $\mu$-group, and hence, by the hypothesis of reducibility, with every element of the $m$-group. Furthermore, the $(m-1)$-ad $\{a_1, a_2, \cdots, a_{\mu-1}, a_1, a_2, \cdots, a_{\mu-1}, \cdots, a_1, a_2, \cdots, a_{\mu-1}\}$ is an extended identity of the $\mu$-group, and hence an identity of the $m$-group, as was to be proved.

As for the sufficiency of the condition, with $\{a_1, a_2, \cdots, a_{\mu-1}\}$ as in the

(28) "Echt" in Dörnte. Otherwise, "unecht" or "ableitbar."

hypothesis, define the $\mu$-adic operation

$$c_\mu(s_1 s_2 \cdots s_\mu) = c_m(s_1 s_2 \cdots s_\mu a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}).$$

We proceed to prove that the elements of the $m$-group constitute a $\mu$-group under the operation $c_\mu$, and that the given $m$-group is reducible to this $\mu$-group. Of the two conditions defining a polyadic group, condition 1 is satisfied by the proposed $\mu$-group as an immediate consequence of its being satisfied by the given $m$-group. On the other hand, condition 2 for the $\mu$-group becomes

$$\begin{aligned} &c_m(c_m(s_1 s_2 \cdots s_\mu a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) s_{\mu+1} \\ &\qquad \cdots s_{2\mu-1} a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) \\ &= c_m(s_1 c_m(s_2 s_3 \cdots s_{\mu+1} a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) s_{\mu+2} \\ &\qquad \cdots s_{2\mu-1} a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &= c_m(s_1 s_2 \cdots s_{\mu-1} c_m(s_\mu s_{\mu+1} \cdots s_{2\mu-1} a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) a_1 a_2 \\ &\qquad \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}), \end{aligned}$$

which follows from condition 2 for the $m$-group, and the commutativity of $\{a_1, a_2, \cdots, a_{\mu-1}\}$ with each element of the $m$-group. Hence the existence of the $\mu$-group. Finally, using extended operations, and applying the commutativity part of our hypothesis, we will have

$$c_\mu(s_1 s_2 \cdots s_m) = c_m(s_1 s_2 \cdots s_m a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) = c_m(s_1 s_2 \cdots s_m),$$

the second expression involving a sequence consisting of $k(k-1)$ sequences $a_1 a_2 \cdots a_{\mu-1}$, which sequence, therefore, constitutes an extended identity of the $m$-group—since by hypothesis $k$ such sequences constitute an identity. Hence the reducibility of the $m$-group to the $\mu$-group follows.

From the definition of $c_\mu$, we see that the $(\mu-1)$-ad $\{a_1, a_2, \cdots, a_{\mu-1}\}$ is indeed an identity of the resulting $\mu$-group.

The above theorem may be used to prove a polyadic group irreducible, as is shown by the following simple illustration. The class of integers constitutes an infinite $m$-adic group under the operation $s_1+s_2+\cdots+s_m+1$. Since the group is abelian, reducibility to a $\mu$-group with $m=k(\mu-1)+1$ is equivalent to the existence of an integer $a$ such that $ka+s+1=s$, that is, $ka=-1$, which is impossible for any integral $k>1$. Hence the $m$-group is irreducible.

The commutativity condition can be restated to read $\{a_1, a_2, \cdots, a_{\mu-1}\}$ is invariant under the $m$-group. Since the present multiplicity of basic operations makes us refrain from employing the simplifications of the coset theorem, the concept of invariance is preferable only for $\mu-1=1$. Our $(\mu-1)$-ad is now a single element $a$; and the further condition that the $(m-1)$-ad

$\{a, a, \cdots, a\}$ be an identity of the $m$-group may be restated to read: $a$ is of first order. For this condition is equivalent to $c_m(aa \cdots aa) = a$. We may therefore state the special result, a rewording only of Dörnte's, *a necessary and sufficient condition that a given m-group be reducible to an ordinary group is that the m-group possess an invariant element of first order.* Our succeeding development will reveal many general classes of polyadic groups that can be proved reducible to 2-groups. One such class is already at hand, that is, *all m-adic quotient groups arising from invariant subgroups of m-adic groups are reducible to 2-groups.* For the element of the quotient group corresponding to the invariant subgroup is immediately seen to be invariant under the quotient group, and of $m$-adic order one. In this connection we may observe that semi-invariant subgroups also lead to special kinds of polyadic quotient groups, for the element corresponding to that semi-invariant subgroup must again be of first order. On the other hand, any polyadic group can be a quotient group in our most general sense; for, with $H_0$ the identity of $G_0$, $G/H_0$ is identical with $G$.

Given an $m$-adic group $G$, we may ask for the distribution of, and interrelations between, the polyadic groups to which it is reducible. Note immediately that if $G$ is reducible to $G'$, and $G'$ to $G''$, $G$ is reducible to $G''$, so that the class of groups to which $G'$ is reducible is a subclass of the class of groups to which $G$ is reducible whenever $G$ is reducible to $G'$. Our results are of two kinds, both derived from the above theorem.

The first type of result is not much more than a restatement of the condition of the theorem. We recall that, if $G$ is reducible to $G'$, the class of elements of $G$ is identical with the class of elements of $G'$, while the operation of $G$ is an extended operation of $G'$. It follows that a class of equivalent $i$-ads of $G$ is also a class of equivalent $i$-ads of $G'$, and conversely. In particular, the class of identities of $G'$ is a class of equivalent polyads([29]) of $G$, so that the classes of identities of two groups to which $G$ may be reducible are either the same or mutually exclusive.

When the classes of identities are distinct, the two groups in question will be distinct, as their operations cannot then be identical([30]). On the other hand, we easily see that when the classes of identities are the same, the groups are identical. For, if their operations are $c'$ and $c''$, then, with $\{a_1, a_2, \cdots, a_{\mu-1}\}$ an identity of each, we have

$$c'(s_1 s_2 \cdots s_\mu) = c(s_1 s_2 \cdots s_\mu a_1 a_2 \cdots a_{\mu-1} \cdots a_1 a_2 \cdots a_{\mu-1}) = c''(s_1 s_2 \cdots s_\mu),$$

([29]) By a class of equivalent polyads we mean a class of equivalent $i$-ads for some fixed $i$ While the elements of $G^*$ as first written are classes of equivalent $i$-ads with $1 \leqq i \leqq m-1$, in general no such restriction is intended by the above phrase. As suggested in §2, by the use of extended operations the concept of equivalent $i$-ads becomes valid for $i > m-1$. This observation will be of greater importance later in the present section.

([30]) They may however be "abstractly the same" in the sense of being simply isomorphic. See the opening paragraph of §23.

$c$ being an extended operation of each group. Observe finally that in the sufficiency proof of our basic theorem, and in the succeeding observation, if $\{a_1, a_2, \cdots, a_{\mu-1}\}$ satisfies the given condition of that theorem, each $(\mu-1)$-ad equivalent to $\{a_1, a_2, \cdots, a_{\mu-1}\}$ also does. We therefore can state the following result. *There is a* 1-1 *correspondence between the groups to which a given m-adic group is reducible and the classes of equivalent polyads satisfying the condition of the basic theorem, each such class of equivalent polyads being the class of identities of the corresponding group.*

In particular, there are as many 2-groups to which an $m$-adic group is reducible as there are invariant elements of order one in the $m$-group([31]). Thus, consider an ordinary abelian group of finite order $g$. If $d$ is any divisor of $g$, there are at least $d$ elements $a$ in this 2-group with $a^d=1$. If this 2-group be extended to a $(d+1)$-group, each such element $a$ is of order one in the $(d+1)$-group, and invariant therein. The $(d+1)$-group is therefore reducible to at least $d$ distinct 2-groups, each such $a$, in fact, being the identity of the corresponding 2-group.

Our second type of result concerns the possible dimensions of the groups to which a given polyadic group is reducible. The complete result is an immediate consequence of the following theorem. *If an m-group is reducible to a $\mu_1$-group and a $\mu_2$-group, it is reducible to a $\mu$-group where $\mu-1$ is the highest common factor of $\mu_1-1$ and $\mu_2-1$.* To prove this theorem let $\{a_1', a_2', \cdots, a_{\mu_1-1}'\}$ and $\{a_1'', a_2'', \cdots, a_{\mu_2-1}''\}$ be identities of the $\mu_1$-group and $\mu_2$-group respectively. They then satisfy the condition of our basic theorem. Furthermore, all but one of the letters in each can be chosen arbitrarily.

If then $\mu_1>\mu_2$, we may assume $a_1'=a_1'', \cdots, a_{\mu_2-1}'=a_{\mu_2-1}''$. Consider then the sequence $\{a_{\mu_2}', \cdots, a_{\mu_1-1}'\}$ which we shall write $\{a_1''', \cdots, a_{\mu_3-1}'''\}$, with $\mu_3-1=(\mu_1-1)-(\mu_2-1)$. Then all but one of the letters of this sequence are arbitrary. Inductively, we thus obtain the sequence $\{a_1^{(\lambda)}, \cdots, a_{\mu_\lambda-1}^{(\lambda)}\}$, with all but one letter arbitrary, from the sequence $\{a_1^{(\lambda-1)}, \cdots, a_{\mu_{\lambda-1}-1}^{(\lambda-1)}\}$ and the smallest preceding sequence, easily seen to be unique. Clearly the process terminates when and only when $\mu_{\lambda-1}$ is equal to the smallest preceding $\mu$.

Now in terms of the $\mu_\lambda-1$'s, this process is nothing more than the Euclid algorithm for finding the highest common factor of $\mu_1-1$ and $\mu_2-1$, where the process of division is replaced by the more primitive form of repeated subtractions. Hence, the above process terminates, and the last sequence found may be written $\{a_1, \cdots, a_{\mu-1}\}$, where $\mu-1$ is the highest common factor of $\mu_1-1$ and $\mu_2-1$. We now prove that such a $(\mu-1)$-ad satisfies the condition of our basic theorem.

First, the sequence $\{a_1''', \cdots, a_{\mu_3-1}'''\}$ is commutative with every element of the given $m$-group. For we have $\{a_1', \cdots, a_{\mu_1-1}'\}=\{a_1'', \cdots, a_{\mu_2-1}'', a_1''', \cdots, a_{\mu_3-1}'''\}$, so that $c(a_1'' \cdots a_{\mu_2-1}''a_2''' \cdots a_{\mu_3-1}'''s_l s_{l+1} \cdots s_m)=c(s_l a_1'' \cdots$

([31]) In the case of abelian triadic groups this reduces to a theorem of Lehmer's.

$a''_{\mu_2-1}a'''\cdots a'''_{\mu_3-1}s_{l+1}\cdots s_m) = c(a_1''\cdots a''_{\mu_2-1}s_l a_1'''\cdots a'''_{\mu_3-1}s_{l+1}\cdots s_m)$. Hence, by induction, each $\{a_1^{(\lambda)},\cdots, a_{\mu_\lambda-1}^{(\lambda)}\}$ is commutative with every element of the $m$-group, and so $\{a_1,\cdots, a_{\mu-1}\}$ also is thus commutative.

As for the second part of the condition, clearly $m-1=k(\mu-1)$ with integral $k$. As in the commutativity argument, and with the commutativity property, we obtain from the extended identities consisting of $k$ sequences $\{a_1',\cdots, a'_{\mu_1-1}\}$ and $k$ sequences $\{a_1'',\cdots, a''_{\mu_2-1}\}$ an extended identity consisting of $k$ sequences $\{a_1',\cdots, a'''_{\mu_3-1}\}$. By induction, $k$ sequences $\{a_1^{(\lambda)},\cdots, a_{\mu_\lambda-1}^{(\lambda)}\}$ constitute an extended identity for every $\lambda$, and hence the same is true of $k$ sequences $\{a_1,\cdots, a_{\mu-1}\}$. But, since $k(\mu-1)=m-1$, the last is indeed an identity of our given $m$-group. $\{a_1,\cdots, a_{\mu-1}\}$ therefore satisfies completely the condition of our basic theorem, whence the present result.

It follows that if $\mu_0$ is the least dimension of the groups to which a given $m$-group is reducible, all other dimensions $\mu$ of such groups must be such that $\mu-1$ is a multiple of $\mu_0-1$. We shall call $\mu_0$ the *real dimension* of the $m$-group, with, of course, $\mu_0=m$ if the group is irreducible. Since every $\mu-1$ must also be a divisor of $m-1$, we easily obtain the following solution of the problem of the distribution of the dimensions of the groups to which a given polyadic group is reducible. *If a group of dimension $m$ has real dimension $\mu_0$, and we write $m-1=k_0(\mu_0-1)$, then the dimensions of the groups to which the $m$-group is reducible are those and only those numbers $\mu$ for which $\mu-1=k(\mu_0-1)$, $k$ a proper divisor of $k_0$.*

While this result justifies the term real dimension on the basis of a mere enumeration of distinct dimensions, other considerations show that an $m$-group in general, even if reducible, must still be considered an $m$-group. We have already given an example which shows that the same $m$-group may be reducible to different groups of the same dimension, and, indeed, of the real dimension of the $m$-group. We now further observe that an $m$-group may be reducible to an irreducible group of higher dimension than the real dimension of the $m$-group, that is, not every succession of reductions of a group need lead to the real dimension of the group. If we call the dimensions of the irreducible groups to which a polyadic group is reducible the *irreducible dimensions* of the given group, the real dimension of the group is only the smallest of its irreducible dimensions.

In contrast with the class of groups to which an $m$-group is reducible, the class of extensions of an $m$-group is of very simple structure, since it has one and only one group of each dimension $\mu$ with $\mu-1$ a multiple of $m-1$, and no others. Of course, the reason is that extension is the direct process, reduction indirect. We now combine these processes to yield the concept of derived group.

Given an $m$-group $G$, a polyadic group $G'$ will be said to be *derivable from $G$* if it can be obtained from $G$ by a finite succession of extensions and reductions.

The class of all polyadic groups derivable from a given polyadic group will be called a *net* of polyadic groups. From this definition we see that each group of a net yields that net. Furthermore, all groups of a given net have the same class of elements; only the operations differ.

The concept of a net of polyadic groups is considerably simplified by the following result. *Any group of a net can be obtained from any other by a single extension followed by a single reduction.* A single extension or a single reduction can obviously be replaced by an extension followed by a reduction. Since two successive extensions are equivalent to a single extension, two successive reductions to a single reduction, our result will follow if we can show that a reduction followed by an extension is equivalent to an extension followed by a reduction. Let then $G'$ with operation $c'_{m'}$ be reducible to $G''$ with operation $c''_{m''}$, and let $G''$ be extended to $G'''$ with operation $c'''_{m'''}$. With the above subscripts designating dimensionality, we have $m'-1-k'(m''-1)$, $m'''-1=k''(m''-1)$. Now $c'_{m'}$ and $c'''_{m'''}$ are both extensions of operation $c''_{m''}$. If then we extend $c''_{m''}$ to an operation $c^{\text{IV}}_{m^{\text{IV}}}$ with $m^{\text{IV}}-1=k'k''(m''-1)$, $c^{\text{IV}}_{m^{\text{IV}}}$ will be an extension of both $c'_{m'}$ and $c'''_{m'''}$. The corresponding group $G^{\text{IV}}$ is then reducible to both $G'$ and $G''$, whence our result.

Stated otherwise, *given any two groups of a net there is a third group of the net reducible to each of the given groups.* We could therefore redefine a net as the class of groups to which the extensions of a given group are reducible, though the conclusion that a net does not depend on the particular group in it chosen as the given group is then not immediate.

The two types of results referred to in the case of the groups to which a given group is reducible now easily lead to corresponding results for the net of groups derivable from a given group. In this connection, a $(\mu-1)$-ad $\{a_1, a_2, \cdots, a_{\mu-1}\}$ of an $m$-group will be said to be of finite order if some polyad of the form $\{a_1, a_2, \cdots, a_{\mu-1}, a_1, a_2, \cdots, a_{\mu-1}, \cdots, a_1, a_2, \cdots, a_{\mu-1}\}$ is an extended identity of the $m$-group. We then easily prove the following. *There is a* 1-1 *correspondence between the groups of the net of groups derivable from a given group and the classes of equivalent polyads of finite order which are commutative with every element of the given group, each such class of equivalent polyads then being the class of identities of the corresponding group*(32). In fact, the above redefinition of a net immediately yields a many-one correspondence of the above type, which is then seen to be one-one due to any pair of groups of a net being in the class of groups to which a third is reducible.

Actually, it is easily verified that each of the concepts: class of equivalent polyads, commutative with every element, and even polyad of finite order, is independent of the particular group of the net chosen as given group, so that the above result can be restated in terms of the net alone. It is also easily proved that for finite polyadic groups every polyad is of finite order, so that

(32) Here, as elsewhere, "group" unqualified means polyadic group.

in such cases the corresponding condition need not be explicitly stated. In particular, there are as many 2-groups in the net as there are invariant elements of finite order, and hence, for finite polyadic groups, as many as there are invariant elements.

We pause to prove explicitly that the transform of one element of a group of a net by another is independent of the particular group employed. This will be so if true of any pair of groups, one reducible to the other. Since the operation of one of these groups is an extended operation of the other, an identity of the first group is an extended identity of the second; hence an inverse of an element in the first, an extended inverse of that element in the second, whence the identical transforms.

The second type of result is obtained still more easily. We shall call the least dimension of the groups of a net their *outer real dimension*. The outer real dimension of a group is then always less than or equal to its real dimension. Given an $m$-group $G$ of outer real dimension $\mu^0$, some third group $G'$ of the net will be reducible both to the $m$-group, and a group of dimension $\mu^0$. The real dimension of $G'$ will therefore exactly equal $\mu^0$. As $G'$ is reducible to $G$, we see that $m-1$ is a multiple of $\mu^0-1$. That is, if the outer real dimension of an $m$-group is $\mu^0$, then $\mu^0-1$ must be a divisor of $m-1$.

Hence, also, all the groups of the net have dimensions $\mu$ with $\mu-1$ a multiple of $\mu^0-1$. Since, from a group of dimension $\mu^0$, mere extensions yield groups of all such dimensions, we have the following main result. *If the outer real dimension of the groups of a net is* $\mu^0$, *their dimensions are those and only those numbers* $\mu$ *for which* $\mu-1=k(\mu^0-1)$.

The first type of result is easily restated to yield a criterion for determining the outer real dimension of a group. In particular, *the outer real dimension of a group is* 2 *when and only when it contains an invariant element of finite order*. Thus, a finite abelian polyadic group is always of outer real dimension 2, and so is derivable from a 2-group, while a group having no invariant element is always of outer real dimension greater than 2. The existence of the latter type of group is peculiar to polyadic theory. A simple example is furnished by the class of odd substitutions of the symmetric group of degree three. By the converse of the coset theorem they form a triadic group of order three under the product of three substitutions as operation, and yet involve no invariant element. The three elements, incidentally, are all of first order in the triadic group.

As in the case of mere reducibility, we shall call the dimensions of the irreducible groups of a net the *outer irreducible dimensions* of each group in the net. By contrast, a dimension will be said to be a *reducible dimension* of the groups of the net if there is at least one group of the net of that dimension, while all such groups are reducible. While we have no general theorem giving the distribution of these dimensions, the following special results lend a certain insight into the possibilities involved.

First, a group may have its real dimension as its only outer irreducible dimension. This is readily proved to be so for any 2-group which has no invariant element other than the identity. In this case, in fact, the net of groups consists only of the 2-group, and its extensions.

By contrast, a group may have an infinite number of outer irreducible dimensions. Thus it can be shown that for the ordinary cyclic group of order two the outer irreducible dimensions are the infinite set of numbers of the form $2^n+1$, $n=0, 1, 2, \cdots$.

Finally, it can be shown that every finite polyadic group has an infinite number of reducible dimensions. To be specific, if an $m$-group has $g$ elements, there is, of course, at least one group of the net of dimension $(kg+1)(m-1)+1$, for each $k=1, 2, 3, \cdots$, and every group of the net of such a dimension is reducible, reducible to dimension $m$, in fact.

We append a brief discussion of the generalization of the concept of a net of groups that arises from a consideration of the subgroups of a group. Let the *complex* of groups *obtainable* from a given polyadic group be the class of all polyadic groups obtainable from the given group by finite successions of the three operations "extension of," "reduction of," and "subgroup of." It is readily verified by means of the very concepts involved that an extension of a subgroup of a group is also a subgroup of an extension of a group; and that a subgroup of a reduction of a group is also a reduction of a subgroup of the group. It follows that *any group in a complex can be obtained from the given group by an operation of the single form "extension of" followed by "subgroup of" followed by "reduction of" if not merely by "extension of" followed by "reduction of."*

In the case of abelian groups we further have that a reduction of a subgroup of a group is also a subgroup of a reduction of the group, a result obtainable with the help of our criterion of reducibility. It follows that *the complex of groups obtainable from an abelian polyadic group consists of the groups in the corresponding net of groups, and their subgroups.* That this is not true for all complexes can be seen from the case of a group with a first order element, but no invariant element. For the first order element constitutes a subgroup of the given group reducible to a 2-group; while, the outer real dimension of the given group being greater than 2, the dimensions of all the groups in the net, and hence of their subgroups, is greater than 2.

It is readily seen that the groups of a complex whose classes of elements are the same as that of the original group constitute the net of that group, or, as we shall now phrase it, the net of the complex. Clearly the net of a complex also consists of all of its groups from which that complex is obtainable. On the other hand, a group of a complex with class of elements a proper subclass of that of the original group will yield a complex which is a proper subclass of the given complex, and may be called a subcomplex thereof. If we call the nets of the subcomplexes of a complex the subnets of that complex,

then it is clear that the net and subnets of a complex constitute a separation of the groups of the complex into mutually exclusive sets.

The relationship between the subcomplexes of a complex is in part furnished by the following result. *If of two groups in a complex the class of elements of the first group is contained in the class of elements of the second, then the first group is in the complex obtained from the second.* For consider the two groups to be obtained from an initial group according to our first result. Using $(c_m, C)$ to designate a group with $m$-adic operation $c_m$ and class of elements $C$, we may indicate the process as follows:

$$(c_m, C) \to (c'_{m'}, C) \to (c'_{m'}, C') \to (c''_{m''}, C'),$$
$$(c_m, C) \to (c'''_{m'''}, C) \to (c'''_{m'''}, C'') \to (c^{\text{IV}}{}_{\text{IV}}, C'').$$

The two groups in the second column are also reductions of a third group $(c^{\text{V}}_{m\text{V}}, C)$. Since the third column symbolizes groups, it follows that $(c^{\text{V}}_{m\text{V}}, C')$ and $(c^{\text{V}}_{m\text{V}}, C'')$ are groups; and as $C'$ is contained in $C''$ by hypothesis, $(c^{\text{V}}_{m\text{V}}, C')$ is a subgroup of $(c^{\text{V}}_{m\text{V}}, C'')$, if not identical with it. Now $(c^{\text{V}}_{m\text{V}}, C')$, $(c'_{m'}, C')$ and $(c''_{m''}, C')$ are in a single net of groups, as are also $(c^{\text{V}}_{m\text{V}}, C'')$, $(c'''_{m'''}, C'')$ and $(c^{\text{IV}}_{m\text{IV}}, C'')$. Hence $(c''_{m''}, C')$ is in the complex obtainable from $(c^{\text{IV}}_{m\text{IV}}, C'')$, as was to be proved.

A particular application of the above result is the following. *Any two groups of a complex which have the same class of elements are derivable from each other, that is, belong to one and the same net.* It follows that there is a 1-1 correspondence between the subnets, including the net, into which the groups of a complex were separated, and the different classes of elements of the groups in the complex.

Hence also, or directly from our general result, there is a 1-1 correspondence between the subcomplexes, including the complex, of a complex, and the different classes of elements of the groups in the complex, each complex being obtainable from those and only those groups whose classes of elements are identical with the class of elements corresponding to the complex. Moreover, our general result shows that one subcomplex contains a second when and only when the class of elements corresponding to the first contains the class of elements corresponding to the second. We now complete this picture by proving the following. *If two subcomplexes $K'$ and $K''$ of a complex correspond to the classes of elements $C'$ and $C''$, then the logical product of $K'$ and $K''$, null when the logical product of $C'$ and $C''$ is null, is otherwise a complex, namely the complex corresponding to the logical product of $C'$ and $C''$.* For $C'$ and $C''$ must be the classes of elements of two groups $(c''_{m''}, C')$ and $(c^{\text{IV}}_{m\text{IV}}, C'')$ of the complex. In the notation of the previous proof, $(c^{\text{V}}_{m\text{V}}, C')$ and $(c^{\text{V}}_{m\text{V}}, C'')$ are then groups of the complex. If then $C'''$, the logical product of $C'$ and $C''$, is not null, $(c^{\text{V}}_{m\text{V}}, C''')$ is a group of the complex. The case $C'''$ null is immediate. Otherwise, then, there will be a subcomplex $K'''$ corresponding to $C'''$.

Our earlier result then shows immediately that a group $G$ is common to $K'$ and $K''$ when and only when it is in $K'''$.

Further results on the subcomplexes of a complex obtained from a finite polyadic group, and more particularly a finite abelian polyadic group, will be found at the end of §22, our second section on cyclic polyadic groups([33]).

6. **Arbitrary containing ordinary groups.** The coset theorem led to the abstract containing ordinary group $G^*$ of an $m$-group $G$ merely by a consideration of $G$ treated abstractly. Often, however, the elements of $G$ may immediately be given in such a form that the $m$-adic operation is but an extension of a more primitive dyadic operation, as when $G$ is an $m$-adic group of ordinary substitutions. In such a case a containing 2-group arises directly, and may be more useful than the abstract containing group.

A 2-group $G^{*\prime}$ will be called a *containing group* of an $m$-group $G$ if the elements of $G$ are among the elements of $G^{*\prime}$, the operation of $G$ an extension of the operation of $G^{*\prime}$, while $G^{*\prime}$ is generated by the elements of $G$. In what follows we simultaneously investigate the possible structure of $G^{*\prime}$, and its relationship to $G^*$. We must therefore explicitly distinguish between their operations $c^{*\prime}$ and $c^*$ respectively([34]).

Let two polyads $\{s_1, s_2, \cdots, s_i\}$ and $\{s_1', s_2', \cdots, s_{i'}'\}$ of $G$ lead to identical products in $G^*$; that is, let $c^*(s_1s_2 \cdots s_i) = c^*(s_1's_2' \cdots s_{i'}')$. Since $i'-i$ must then be a multiple of $m-1$, we can annex elements $s_1'', \cdots, s_j''$ of $G$, if need be, so that the resulting equation $c^*(s_1s_2 \cdots s_is_1'' \cdots s_j'') = c^*(s_1's_2' \cdots s_{i'}'s_1'' \cdots s_j'')$ can be rewritten $c(s_1s_2 \cdots s_is_1'' \cdots s_j'') = c(s_1's_2' \cdots s_{i'}'s_1'' \cdots s_j'')$ in, perhaps, extended notation. But this equation can now be written $c^{*\prime}(s_1s_2 \cdots s_is_1'' \cdots s_{j'}') = c^{*\prime}(s_1's_2' \cdots s_{i'}'s_1'' \cdots s_j')$, whence we obtain $c^{*\prime}(s_1s_2 \cdots s_i) = c^{*\prime}(s_1's_2' \cdots s_{i'}')$. That is, if two polyads of $G$ lead to identical products in $G^*$ they lead to identical products in $G^{*\prime}$. If then we let every element of the form $c^{*\prime}(s_1s_2 \cdots s_i)$ in $G^{*\prime}$ correspond to element $c^*(s_1s_2 \cdots s_i)$ of $G^*$, a one-many correspondence is set up between those elements of $G^{*\prime}$ and of $G^*$ which are obtainable as products of elements of $G$.

This correspondence is clearly preserved under the respective operations of these groups. For if $r_1$ and $r_2$ of $G^*$ correspond to $r_1'$ and $r_2'$ respectively

---

([33]) The development of the section just ended, lengthy as it is, is probably but one of many possible developments leading to sets of related polyadic groups. Dörnte's Theorem 7, §2, can probably be made the starting point for such a different development. The possibilities are further widened if a theory is contemplated which would include the relationship between a polyadic group and the corresponding "schar."

([34]) It might be thought that now, when the ordinary group demanded by Miller's theorem is immediately given, at least the structure of $G^{*\prime}$ requires no further investigation. But, apart from the fact that Miller's theorem is given for finite groups, his hypothesis that for some integer $n$ the products of any $n$ *but no fewer* elements of $G$ is in $G$ is not immediately given, but is replaced by $G$'s being an $m$-group. As we also need the relationship between $G^*$ and $G^{*\prime}$, we make our development entirely independent of Miller's.

of $G^{*\prime}$, by writing these elements as corresponding products of elements in $G$ we see immediately that $c^*(r_1r_2)$ corresponds to $c^{*\prime}(r_1'r_2')$. Since $G^*$ consists of the products of elements in $G$, it easily follows that the products in $G^{*\prime}$ of elements of $G$ themselves constitute a group which can then be none other than $G^{*\prime}$; for $G^{*\prime}$ is generated by $G$. Furthermore our one-many correspondence, which is therefore a correspondence between all the elements of $G^{*\prime}$ and of $G^*$, is indeed a one-many isomorphism between $G^{*\prime}$ and $G^*$.

For fixed $i$ we shall call the set of elements of $G^{*\prime}$ which are the products of $i$ elements of $G$ the $i$th coset of $G^{*\prime}$. For these elements the above set of equations can be reversed so that our one-many correspondence between $G^{*\prime}$ and $G^*$ becomes a 1-1 correspondence between the elements of the $i$th cosets of $G^{*\prime}$ and of $G^*$ for each $i \geqq 1$. From the corresponding result for $G^*$, it follows that the elements of the $i$th coset of $G^{*\prime}$ will be obtained in 1-1 fashion if in the expression $c^{*\prime}(s_1 \cdots s_{i-1}s)$ we let $s_1, \cdots, s_{i-1}$ be arbitrary fixed elements of $G$, and let $s$ run through $G$.

Let now $k$ designate the least $i$ for which the corresponding coset of $G^{*\prime}$ contains the identity $I'$ of $G^{*\prime}$. It follows, first, that the first $k$ cosets of $G^{*\prime}$ are mutually exclusive. For if we could have $c^{*\prime}(s_1 \cdots s_i) = c^{*\prime}(s_1' \cdots s_j')$ with $1 \leqq i < j \leqq k$, then, by rewriting $c^{*\prime}(s_1' \cdots s_j')$ in the form $c^{*\prime}(s_1 \cdots s_i s_{i+1}' \cdots s_j')$, we would have $c^{*\prime}(s_{i+1}' \cdots s_j') = I'$, in contradiction to our definition of $k$. On the other hand, the $(k+1)$-st coset of $G^{*\prime}$ is identical with the first, that is, with $G$, for we can write its elements in the form $c^{*\prime}(s_1 \cdots s_k s)$ with $c^{*\prime}(s_1 \cdots s_k) = I'$. Hence also the $(k+2)$-nd coset is identical with the 2d, and so on. $G^{*\prime}$ therefore consists of the elements of its first $k$ cosets, while succeeding cosets are cyclic repetitions of these. In particular, the $(m-1)$-st coset must be identical with the $k$th coset. For if $\{s_1, s_2, \cdots, s_{m-1}\}$ is an identity of $G$, $c^{*\prime}(s_1 s_2 \cdots s_{m-1}) = I'$, so that the $(m-1)$-st and $k$th cosets have an element in common. Hence $k$ is a divisor of $m-1$.

Returning to our correspondence between the elements of $G^{*\prime}$ and of $G^*$ we see that it is 1-1 between the elements of $G^{*\prime}$ and the elements of the first $k$ cosets of $G^*$, and of each succeeding set of $k$ cosets of $G^*$. Our one-many correspondence is thus actually $[1, (m-1)/k]$, and we therefore have a $[1, (m-1)/k]$ isomorphism between $G^{*\prime}$ and $G^*$. To complete our analysis we consider the analogue in $G^{*\prime}$ of the associated 2-group $G_0$ of $G$ in $G^*$.

Our $[1, (m-1)/k]$ correspondence is clearly 1-1 between the elements of the $k$th coset of $G^{*\prime}$, and of $G_0$, the $(m-1)$-st coset of $G^*$. Since the product of two elements of the $k$th coset of $G^{*\prime}$ is in the $2k$th coset, and hence also in the $k$th coset, of $G^{*\prime}$, the previous $[1, (m-1)/k]$ isomorphism between $G^{*\prime}$ and $G^*$ is simple between the $k$th coset of $G^{*\prime}$, and $G_0$. It follows that the $k$th coset of $G^{*\prime}$ constitutes a group with operation $c^{*\prime}$ simply isomorphic with $G_0$. We shall call it the associated ordinary group of $G$ in $G^{*\prime}$, and symbolize it $G_0'$. The same argument used in proving $G_0$ invariant under $G^*$ shows $G_0'$ to be invariant under $G^{*\prime}$.

Since the $i$th coset of $G^{*\prime}$ is given by $c^{*\prime}(s_1 \cdots s_{i-1}s)$, with $s_1, \cdots, s_{i-1}$ fixed elements of $G$, $s$ running through $G$, we can let $s_1, \cdots, s_{i-1}$ be the same element $s_0$ of $G$, and write that $i$th coset $s_0^{i-1}G$ in ordinary notation. It can likewise be written $Gs_0^{i-1}$. We thus obtain the expansion $G^{*\prime}=G+Gs_0 +Gs_0^2+ \cdots +Gs_0^{k-1}$. Since $Gs_0^{k-1}=G_0'$, and $Gs_0^k=G$, we therefore have

$$G = G_0' s_0,$$

while the above expansion becomes

$$G^{*\prime} = G_0' s_0 + G_0' s_0^2 + \cdots + G_0' s_0^{k-1} + G_0'.$$

But this is the expansion of $G^{*\prime}$ in augmented cosets as regards the invariant subgroup $G_0'$, assuming $G_0'$ is not itself $G^{*\prime}$. It follows that the quotient group $G^{*\prime}/G_0'$ is of index $k$, while the element in that quotient group corresponding to $G$ generates $G^{*\prime}/G_0'$.

This concludes our discussion of the structure of $G^{*\prime}$. As for its isomorphism with $G^*$, observe first that in that isomorphism elements of $G$ correspond to themselves. We then see that the isomorphism between $G^{*\prime}$ and $G^*$ is determined by this partial correspondence provided $k$, and the element of the $k$th coset of $G^{*\prime}$ which serves as the identity of $G^{*\prime}$, are specified. For the correspondence between elements of $G$ and themselves determines the 1-1 correspondence between the elements of the $i$th cosets of $G^{*\prime}$ and of $G^*$ for every $i$. And given $k$, and $c^{*\prime}(s_1^0 s_2^0 \cdots s_k^0)=I'$, $s$'s in $G$, if $j=\kappa k+l$, $1 \leqq l \leqq k$, the equation $c^{*\prime}(s_1^0 s_2^0 \cdots s_k^0 \cdots s_1^0 s_2^0 \cdots s_k^0 s_1 s_2 \cdots s_l)=c^{*\prime}(s_1 s_2 \cdots s_l)$ serves to identify each symbolized element of the $j$th coset of $G^{*\prime}$ with a unique element of the $l$th coset, and thus completes the correspondence between the elements of $G^{*\prime}$ and $G^*$. In particular, the simple isomorphism between $G_0'$ and $G_0$ is also thus determined. We therefore have the following comprehensive theorem:

*Every containing 2-group $G^{*\prime}$ of an m-group $G$, if not itself a 2-group $G_0'$ to which $G$ is reducible, contains an invariant subgroup $G_0'$ of index $k$, with $k$ a divisor of $m-1$, $G$ a coset of $G^{*\prime}$ as regards $G_0'$, and the quotient group $G^{*\prime}/G_0'$ generated by the element corresponding to $G$. Furthermore, $G^{*\prime}$ admits a $[1, (m-1)/k]$ isomorphism with $G^*$, the abstract containing 2-group of $G$, which reduces to a simple isomorphism between $G_0'$ and $G_0$, the associated 2-group of $G$. This isomorphism makes each element of $G$ correspond to itself, and is, in fact, determined by this correspondence when $k$, which is the smallest $i$ for which an $i$-ad of $G$ yields the identity of $G^{*\prime}$, as well as the class of equivalent $k$-ads of $G$ thus yielding the identity of $G^{*\prime}$, are specified.*

We shall call $k$ the *index* of the containing 2-group. We have then, in particular, that *any two containing groups of index $m-1$ of an m-group are simply isomorphic, the isomorphism in question making each element of the m-group correspond to itself, and being in turn determined by this correspondence.* Hence,

any containing group of index $m-1$ of an $m$-group $G$ may be considered to be the abstract containing group $G^*$ of $G$.

We further have that *any two containing groups of index* 1 *of an m-group are simply isomorphic.* For the $G^{*\prime}$'s are then also the $G_0'$'s which are both simply isomorphic with $G_0$. Observe, however, that the simple isomorphism now no longer makes elements of $G$ correspond to themselves, or the $G^{*\prime}$'s would be identical. In fact, a different element of $G$ serves as identity in each $G^{*\prime}$. Since $G$ is now reducible to $G^{*\prime}$, and conversely, we have as a corollary the following result on the 2-groups to which an $m$-group is reducible, and hence also on the 2-groups in a net. *All 2-groups in a net of groups are simply isomorphic.*

Before considering the same question for two containing groups of index $k$, $1<k<m-1$, we ask when an $m$-group will admit a containing 2-group of index $k$. We then easily obtain the following theorem. *A necessary and sufficient condition that an m-group admit a containing group of index k, $k<m-1$, is that the m-group be reducible to a $(k+1)$-group.* In fact, the observation that in a containing group $G^{*\prime}$ of index $k$ the products of $k+1$ elements of $G$ must be in $G$ is easily extended to show that the elements of $G$ constitute a $(k+1)$-group under the operation $c^{*\prime}(s_1s_2\cdots s_{k+1})$. As $k$ is a divisor of $m-1$, the operation $c(s_1s_2\cdots s_m)=c^{*\prime}(s_1s_2\cdots s_m)$ is an extension of $c^{*\prime}(s_1s_2\cdots s_{k+1})$, and, consequently, $G$ is reducible to the corresponding $(k+1)$-group. Conversely, if $G$ is reducible to a $(k+1)$-group, the abstract containing group of the $(k+1)$-group is of index $k$. But this group is clearly also a containing group of $G$, and of index $k$. In particular, *an irreducible m-group admits containing groups of index $m-1$ only, and conversely.* Hence, the abstract containing group of an irreducible polyadic group may be said to be its only containing group.

This relation to reducibility shows that there are as many essentially different containing groups of index $k<m-1$ of an $m$-group $G$ as there are $(k+1)$-groups to which $G$ is reducible. Hence when $1<k<m-1$, as when $k=1$, two essentially different containing groups of index $k$ will not admit a simple isomorphism which makes each element of $G$ correspond to itself, since the classes of equivalent $k$-ads yielding their identities will be different. Moreover, unlike the case $k=1$, they need not even admit a simple isomorphism which transforms the class of elements of $G$ into itself. For our example of a group having an infinite number of outer irreducible dimensions easily leads to a group $G$ reducible to two groups $G_1$ and $G_2$ of the same dimension, one reducible, the other irreducible. The abstract containing groups of $G_1$ and $G_2$ are containing groups of $G$ of the same index; and did they admit a simple isomorphism of the type in question, $G_1$ and $G_2$ would be simply isomorphic, and hence could not be one reducible, the other irreducible.

Finally, a word about the application of arbitrary containing groups of an $m$-group to the study of the $m$-group. With the containing group $G^{*\prime}$ specified,

we may use ordinary notation for its operation, and write the operation of the $m$-group $G$, $s_1 s_2 \cdots s_m$. If $s$ is an element of $G$, and $\{s', s'', \cdots, s^{(m-2)}\}$ an inverse of $s$, we shall still have $s's'' \cdots s^{(m-2)} = s^{-1}$. It follows that the transform of an element $s_1$ of $G$ by an element $s_2$ will be given by $s_2^{-1} s_1 s_2$ no matter what the containing group. Likewise, if $s's'' \cdots s^{(i)} = r$ in $G^{*\prime}$, the transform of element $s$ of $G$ by the $i$-ad $\{s', s'', \cdots, s^{(i)}\}$ will be given by $r^{-1} s r$. On the other hand, the fact that, for an element $s$ of $G$, $s^{-1}$, in a containing group of index $k < m-1$, can also be written as a product of $k-1$ elements of $G$, or as an element of $G$ when $k=1$, gives but spurious information about the corresponding $(k-1)$-ad, or element, of $G$.

7. **Determination of all types of semi-abelianisms.** In the notation of the abstract containing group of an $m$-group $G$ we may write the condition that $G$ be abelian in the form $s_1 s_2 = s_2 s_1$ for all elements $s_1$, $s_2$ of $G$. Dörnte discovered that an $m$-group, $m > 2$, may satisfy the weaker type of commutativity property $s_1 s_2 \cdots s_{m-1} s_m = s_m s_2 \cdots s_{m-1} s_1$ without necessarily being abelian, and termed such groups semi-abelian. An immediate generalization of the Dörnte type of semi-abelianism is that given by any relation

$$s_1 s_2 \cdots s_{\mu-1} s_\mu = s_\mu s_2 \cdots s_{\mu-1} s_1,$$

where $\mu - 1$ is a divisor of $m-1$, $s$'s arbitrary elements of $G$. We shall then say that $G$ is *$\mu$-semi-abelian*. At least a trivial example of an $m$-group that is $\mu$-semi-abelian, but not abelian, would be given by the extension to an $m$-group of a non-abelian $\mu$-group semi-abelian in Dörnte's sense.

In general we shall say that an $m$-group $G$ is semi-abelian according to the corresponding formal type if for all choices of $s$'s as elements in $G$ a set of relations of the following form are satisfied:

$$\begin{aligned}
s_1 s_2 \cdots s_{l'} &= s_{i'_1} s_{i'_2} \cdots s_{i'_{l'}}, \\
s_1 s_2 \cdots s_{l''} &= s_{i''_1} s_{i''_2} \cdots s_{i''_{l''}}, \\
&\cdots\cdots\cdots\cdots\cdots, \\
s_1 s_2 \cdots s_{l^{(\lambda)}} &= s_{i_1^{(\lambda)}} s_{i_2^{(\lambda)}} \cdots s_{i_{l^{(\lambda)}}^{(\lambda)}},
\end{aligned}$$

each right-hand member being a specific permutation of the left, not all the permutations being the identity. Given $m$, two such formulations will then be said to be equivalent, or to define the *same type of semi-abelianism* if all $m$-groups which are semi-abelian according to one formal type are also semi-abelian according to the other. We proceed to prove that the above extensions of the Dörnte type of semi-abelianism constitute all possible semi-abelianisms. More specifically, by the *displacement* of a letter in a given equation of a set of the above type we shall mean the number of places, right or left, it has to be moved in passing from the left side of the equation to the right. We then prove that *every formal type of semi-abelianism, for given dimension $m$, is equivalent to $\mu$-semi-abelianism with $\mu - 1$ the highest common factor of $m-1$*

*and all the displacements of the letters in the equations defining the semi-abelianism.*

Observe immediately that for $m=2$ there is no semi-abelianism distinct from abelianism. For in some equation a pair of letters $s_i$, $s_j$ will appear in different orders on opposite sides of the equation; and by replacing all other letters by the identity we obtain the condition for abelianism $s_is_j=s_js_i$. This serves to make plausible our general result, and to give a hint of its proof.

In the general case, then, let $G$ be any $m$-group semi-abelian according to a given formal type, and let some letter $s_j$ have a nonzero displacement $k$ in one of the equations defining that semi-abelianism. Since re-symbolization allows either member of the equation to be written first, we may write the equation

$$s_1 \cdots s_{j-1}s_js_{j+1} \cdots s_l = s_{i_1} \cdots s_{i_{j+k-1}}s_js_{i_{j+k+1}} \cdots s_{i_l},$$

so that

$$s_j = [(s_1 \cdots s_{j-1})^{-1}s_{i_1} \cdots s_{i_{j+k-1}}]s_j[s_{i_{j+k+1}} \cdots s_{i_l}(s_{j+1} \cdots s_l)^{-1}].$$

The first bracket is equivalent to some $k$-ad $s's'' \cdots s^{(k)}$. Since at least one letter inside that bracket and outside the parenthesis must be different from all the letters in the parenthesis, that $k$-ad, and hence $s'$, $s''$, $\cdots$, $s^{(k)}$, can be arbitrary. The second bracket is equivalent to some $\kappa$-ad $\bar{s}'\bar{s}'' \cdots \bar{s}^{(\kappa)}$. We can always assume $\kappa>1$, by introducing an identity if need be, and hence at least $\bar{s}^{(\kappa)}$ is arbitrary. That is, for every $s'$, $s''$, $\cdots$, $s^{(k)}$, $\bar{s}^{(\kappa)}$, we can find $\bar{s}'$, $\bar{s}''$, $\cdots$, $\bar{s}^{(\kappa-1)}$ so that

$$s_j = s's'' \cdots s^{(k)}s_j\bar{s}'\bar{s}'' \cdots \bar{s}^{(\kappa-1)}\bar{s}^{(\kappa)}$$

for every $s_j$. Letting $s_j=s'$, we find that $s'' \cdots s^{(k)}s'\bar{s}'\bar{s}'' \cdots \bar{s}^{(\kappa-1)}\bar{s}^{(\kappa)}=1$, whence

$$\bar{s}'\bar{s}'' \cdots \bar{s}^{(\kappa-1)}\bar{s}^{(\kappa)}s'' \cdots s^{(k)}s' = 1.$$

Letting $s_j=\bar{s}^{(\kappa)}$, we find $s's'' \cdots s^{(k)}\bar{s}^{(\kappa)}\bar{s}'\bar{s}'' \cdots \bar{s}^{(\kappa-1)}=1$, whence

$$\bar{s}'\bar{s}'' \cdots \bar{s}^{(\kappa-1)}s's'' \cdots s^{(k)}\bar{s}^{(\kappa)} = 1.$$

It follows that for every $s'$, $s''$, $\cdots$, $s^{(k)}$, $\bar{s}^{(\kappa)}$ in $G$,

$$s's'' \cdots s^{(k)}\bar{s}^{(\kappa)} = \bar{s}^{(\kappa)}s'' \cdots s^{(k)}s'.$$

Dropping momentarily the condition $\mu-1$ a divisor of $m-1$ in our definition of $\mu$-semi-abelianism, we have therefore proved that for each displacement $k>0$, $G$ is $(k+1)$-semi-abelian.

Let now $G$ be $(k_1+1)$-semi-abelian and $(k_2+1)$-semi-abelian. We then prove that $G$ is $(k+1)$-semi-abelian with $k=$H.C.F.$(k_1, k_2)$. This will follow if for every such $k_1$ and $k_2$ with $k_2>k_1$, $G$ is $(k_3+1)$-semi-abelian with $k_3=k_2-k_1$. But under our hypothesis, with all other letters unmoved, we have

$s_1 \cdots s_{k_1+1} \cdots s_{k_2+1} = s_{k_2+1} \cdots s_{k_1+1} \cdots s_1 = s_{k_1+1} \cdots s_{k_2+1} \cdots s_1 = s_1 \cdots s_{k_2+1} \cdots s_{k_1+1}$. Hence $s_{k_1+1} \cdots s_{k_2+1} = s_{k_2+1} \cdots s_{k_1+1}$ as desired.

Finally, we show that if the $m$-group $G$ is $(k+1)$-semi-abelian, it is also $(k'+1)$-semi-abelian with $k' = \text{H.C.F.}(k, m-1)$. Since $G$ is $(k+1)$-semi-abelian, it is also $(\kappa k+1)$-semi-abelian for every positive integral $\kappa$. It is therefore also $(k''+1)$-semi-abelian with $k''$ any positive integer in the form $\kappa k - \lambda(m-1)$. For in the equation defining the $(\kappa k+1)$-semi-abelianism there are at least $\lambda(m-1)$ letters between the first and last letters of each member; and by choosing $\lambda(m-1)$ of these letters consecutively to form an extended identity the desired $(k''+1)$-semi-abelianism is revealed. As positive integers $\kappa$ and $\lambda$ can always be chosen so that $\kappa k - \lambda(m-1) = \text{H.C.F.}(k, m-1)$, our result follows.

From these three special results it follows that every $m$-group possessing a given formal type of semi-abelianism is $\mu$-semi-abelian with $\mu$ as in the statement of our theorem. It remains to be shown that every $m$-group that is $\mu$-semi-abelian also satisfies the given formal semi-abelianism. For each of the given equations separates the letters in the left side of the equation into $\mu-1$ mutually exclusive sets such that each set consists of all letters whose "distance" from a given letter is a multiple of $\mu-1$. Since in passing from the left side to the right side of the equation each letter suffers a displacement itself a multiple of $\mu-1$, the result is to permute the letters of each set among themselves. Now a single application of our hypothesis of $\mu$-semi-abelianism to the left side of the equation in question constitutes a transposition of two letters in the same set. As $\mu$-semi-abelianism implies $[\kappa(\mu-1)+1]$-semi-abelianism, every such transposition can be effected. And, as any substitution is the product of transpositions, successive applications of our hypothesis of semi-abelianism will transform the left side of each equation so that each of its $\mu-1$ sets assumes the form it has on the right. That is, each equation of the given formal semi-abelianism will be satisfied by the elements of any $m$-group that is $\mu$-semi-abelian. The equivalence in question has therefore been demonstrated.

That $\mu$-semi-abelianism is a different type of semi-abelianism for different divisors $\mu-1$ of $m-1$ is readily proved by examples. By the theorem of the next section, an $m$-group $G = G_0 s_0$ will be determined by the following hypothesis: $G_0$ an ordinary cyclic group of order $2^{m-1}-1$ generated by $t$, $s_0^{m-1} = 1$, $s_0^{-1} t s_0 = t^2$. Since $G_0$ is abelian, the first result of the next paragraph shows $G$ to be $m$-semi-abelian. Now a similar argument shows an $m$-group $G$ to be $\mu$-semi-abelian, $\mu-1$ a divisor of $m-1$, when and only when the $(\mu-1)$-ads of $G$ are commutative with the $(m-1)$-ads of $G$. Since $s_0^{m-1}$ is the first ordinary positive power of $s_0$ commutative with $t$, it follows that $G$ is not $\mu$-semi-abelian for any divisor $\mu-1$ of $m-1$ other than $m-1$. Now let $\mu_1-1$, $\mu_2-1$ be any two distinct divisors of $m-1$ with, say, $\mu_1 > \mu_2$. By the preceding method construct a $\mu_1$-group $G'$ which is $\mu_1$-semi-abelian, but not $\mu_3$-semi-

abelian for any divisor $\mu_3-1$ of $\mu_1-1$ other than $\mu_1-1$. The extension of $G'$ to an $m$-group $G''$ then has the same property. It then follows that the $m$-group $G''$ while $\mu_1$-semi-abelian is not $\mu_2$-semi-abelian, since otherwise it would be $\mu_3$-semi-abelian with $\mu_3-1=\text{H.C.F.}(\mu_1-1, \mu_2-1)$, and thus a divisor of $\mu_1-1$ other than $\mu_1-1$. The $m$-group $G''$ thus shows $\mu_1$-semi-abelianism to be not equivalent to $\mu_2$-semi-abelianism whenever $\mu_1 \neq \mu_2$. Coupled with our previous theorem it yields the following result. *There are as many distinct types of semi-abelianism for m-adic groups as there are distinct divisors of* $m-1$.

In what follows we restrict our attention to ordinary, that is, $m$-semi-abelianism, a property implied by any type of semi-abelianism. Since the associated ordinary group $G_0$ of an $m$-group $G$ consists of the products of $m-1$ arbitrary elements of $G$, the condition that $G_0$ is abelian is a condition of semi-abelianism on $G$ of formal type

$$s_1 s_2 \cdots s_{m-1} s_m s_{m+1} \cdots s_{2m-2} = s_m s_{m+1} \cdots s_{2m-2} s_1 s_2 \cdots s_{m-1}.$$

As each letter suffers a displacement $m-1$, by our general result this type of semi-abelianism is equivalent to $m$-semi-abelianism. Hence, *every semi-abelian m-group has an abelian associated group, and conversely.* If an element $s$ of a semi-abelian group $G$ is invariant under $G$, it is also invariant under $G_0$, and hence $G=G_0 s$ is abelian. That is, *if a semi-abelian m-group is non-abelian, it has no invariant element.* If $s_1$ and $s_2$ are any two elements of semi-abelian $G$, $t$ any element of $G_0$, then, since $s_1=t's_2$, with $t'$ in $G_0$, and since $t$ and $t'$ are commutative, we have $s_1^{-1}ts_1=s_2^{-1}ts_2$. Hence, *all the elements of a semi-abelian m-group G transform an arbitrary given element of the associated group* $G_0$ *into the same element.* Now let $H$ be any subgroup of semi-abelian $G$. Its associated subgroup $H_0$ is then invariant under any element $s_0$ of $H$. But every element $s$ of $G$ transforms the elements of $H_0$ as does $s_0$. Hence $H_0$ is invariant under $G$. That is, *every subgroup of a semi-abelian group is semi-invariant*([35]).

8. **On the construction of polyadic groups.** We proceed to prove the following general theorem on the construction of abstract polyadic groups referred to in connection with the converse of the coset theorem. *Given any abstract 2-group* $G_0$ *to serve as associated group, an abstract element* $s_0$ *subject to the condition* $s_0^{m-1}=t_0$, $t_0$ *in* $G_0$, *and any automorphism T of* $G_0$, *which carries* $t_0$ *into itself, and whose* $(m-1)$*-st power is the automorphism of* $G_0$ *under* $t_0$, *to serve as the automorphism of* $G_0$ *under* $s_0$, *then there is one and only one corresponding abstract m-group G; conversely every m-group can be thus determined*([36]).

([35]) See Dörnte's §7 for quite a different set of properties of semi-abelian groups. Dörnte's result that a triadic group consisting of first order elements only must be semi-abelian is equivalent for finite groups to a result of Miller's as a consequence of the above equivalence of the semi-abelianism of $G$, and abelianism of $G_0$. By introducing the polyadic groups $G_i$ of our §34 to take the place of $G_0$ in the discussion of the last paragraph, the results of that paragraph can be specifically generalized to $\mu$-semi-abelianism.

([36]) After this theorem was obtained by the writer, a closely related result was published by Turing as an illustration of a more general theorem in the theory of group extensions. (Not

For the second part of this theorem note that given an $m$-group $G$, and any $s_0$ in $G$, $G_0$, $t_0$, and $T$ are determined, and obviously satisfy the conditions of the theorem. It follows from the first part of the succeeding proof that $G$ is determinable as stated.

We turn then to the first part of the theorem. For purposes of analysis, consider the coset representation of a hypothetical $G$ satisfying the given conditions. We would then have $G=G_0s_0$. If we write the elements of $G_0$ as $t_i$, we may correspondingly symbolize the elements of $G$ by $s_i$, with $s_i=t_is_0$. Of course $s_0$ must then be identified with that $s_i$ for which $t_i$ is the identity of $G_0$, while $t_0$ will appear as some $t_k$. We must then have, for the operation of $G$,

$$\begin{aligned} c(s_{i_1}s_{i_2}\cdots s_{i_m}) &= t_{i_1}s_0t_{i_2}s_0\cdots t_{i_m}s_0 = t_{i_1}(s_0t_{i_2}s_0^{-1})\cdots(s_0^{m-1}t_{i_m}s_0^{-m+1})s_0^m \\ &= (t_{i_1}\cdot T^{-1}t_{i_2}\cdots T^{-(m-1)}t_{i_m}\cdot t_0)s_0, \end{aligned}$$

so that $c(s_{i_1}s_{i_2}\cdots s_{i_m})$, and with it $G$, if it exists, is completely determined by our hypothesis.

We next prove that the elements $s_i=t_is_0$ actually constitute an $m$-group under this operation. As to condition 1 of the definition of an $m$-group, given $c(s_{i_1}s_{i_2}\cdots s_{i_m})=s_{i_{m+1}}$ with all $s$'s but $s_{i_j}$ specified members of $G$, we correspondingly have $t_{i_1}\cdot T^{-1}t_{i_2}\cdots T^{-(m-1)}t_{i_m}\cdot t_0=t_{i_{m+1}}$, with all elements specified members of $G_0$ with the exception of $t_{i_{m+1}}$, when $j=m+1$, $T^{-(j-1)}t_{i_j}$, when $j\neq m+1$. In the first case, a unique $t_{i_{m+1}}$ in $G_0$, and, hence $s_{i_{m+1}}$ in $G$, are immediately determined. In the second case, a unique $T^{-(j-1)}t_{i_j}$ in $G_0$ is determined, hence again $t_{i_j}$ in $G_0$, and $s_{i_j}$ in $G$. As for condition 2, we have

$$\begin{aligned} &c(s_{i_1}\cdots s_{i_{j-1}}c(s_{i_j}\cdots s_{i_{j+m-1}})s_{i_{j+m}}\cdots s_{2m-1}) \\ &\quad= (t_{i_1}\cdots T^{-(j-2)}t_{i_{j-1}}\cdot T^{-(j-1)}(t_{i_j}\cdots T^{-(m-1)}t_{i_{j+m-1}}\cdot t_0) \\ &\qquad\qquad\cdot T^{-j}t_{i_{j+m}}\cdots T^{-(m-1)}t_{i_{2m-1}}\cdot t_0)s_0 \\ &\quad= (t_{i_1}\cdots T^{-(j-2)}t_{i_{j-1}}\cdot T^{-(j-1)}t_{i_j}\cdots T^{-(j+m-2)}t_{i_{j+m-1}} \\ &\qquad\qquad\cdot T^{-(j+m-1)}t_{i_{j+m}}\cdots T^{-(2m-2)}t_{i_{2m-1}}\cdot t_0^2)s_0, \end{aligned}$$

the last since $T^{-(j-1)}t_0=t_0$, and $t_0\cdot t=T^{-(m-1)}t\cdot t_0$, by our hypothesis. The result is thus independent of $j$, whence follows condition 2.

It remains to be shown that the $m$-group $G$ thus obtained actually redetermines, via $s_0$, the $G_0$, $t_0$, $T$ of the given hypothesis([37]). From the operation $c$

---

to be confused with our polyadic concept of §5. See A. M. Turing, *The extensions of a group*, Compositio Mathematica, vol. 5 (1938), pp. 357–367.) From this point of view, the abstract containing groups of $m$-groups with given $G_0$ are the extensions of $G_0$ by the cyclic group of order $m-1$. Our theorem on the determination of $G$ could then have been based on the determination of $G^*$ as cyclic extension of $G_0$. The theorem on cyclic extensions thus envisaged would be not quite Turing's (Theorem 5, loc. cit.), but equivalent thereto by the identification of our $T$ with his $\xi$, $t_0$ with $\mathfrak{z}^{-1}\mathfrak{r}^*$.

([37]) In connection with the preceding footnote it must be mentioned that this part of the proof was overlooked by the writer until the final check-up on the entire paper.

as given, and again with the aid of the relation $T^{-(m-1)}t_{i_m}\cdot t_0 = t_0\cdot t_{i_m}$, we see that equivalent $(m-1)$-ads $\{s_{i_1}, s_{i_2}, \cdots, s_{i_{m-1}}\}$ are those for which the corresponding elements $t_{i_1}\cdot T^{-1}t_{i_2}\cdots T^{-(m-2)}t_{i_{m-1}}\cdot t_0$ of the given 2-group $G_0$ are the same. If then we represent the elements of the associated 2-group of $G$ thus by the elements of the given group $G_0$, and determine the operation of this associated group via $[\{s_{i_1}, s_{i_2}, \cdots, s_{i_{m-1}}\}]\cdot[\{s_{j_1}, s_{j_2}, \cdots, s_{j_{m-1}}\}] = [\{c(s_{i_1}s_{i_2}\cdots s_{i_{m-1}}s_{j_1}), s_{j_2}, \cdots, s_{j_{m-1}}\}]$, bracket meaning class of $(m-1)$-ads equivalent to the specified $(m-1)$-ad, we find this operation, again with the help of the above relation, to be identical with the operation of the given 2-group. That is, abstractly, the given $G_0$ is the associated ordinary group of $G$. Since, for the $s_i = s_0$, $t_i$ is the identity, we immediately have $s_0^{m-1} = [\{s_0, s_0, \cdots, s_0\}] = t_0$ in the above representation. Finally, by introducing identity, hence inverse, and thus transform, in their original polyadic form, it can likewise be shown that if the elements of $G_0$ are transformed by $s_0$ the resulting automorphism of $G_0$ is $T$. Therefore, the proof has been completed.

We have already used the converse of the coset theorem in giving an example of a 3-group of order three having no variant element. This 3-group can now be given abstractly in accordance with the above theorem. For $G_0$, take the cyclic group $(1, t, t^2)$. Let $s_0^2 = 1$, and let the automorphism $T$ of $G_0$ be $T(1, t, t^2) = (1, t^2, t)$. Our hypothesis is verified, thus giving us a 3-group $(s_0, ts_0, t^2s_0)$ of order three. We obtain directly $(ts_0)^{-1}s_0(ts_0) = t^2s_0$, $s_0^{-1}ts_0s_0 = t^2s_0$, $s_0^{-1}t^2s_0s_0 = ts_0$, proving that none of the three elements of the 3-group are invariant under the 3-group.

This theorem may be used to determine all finite abstract polyadic groups of given small order. In this connection we have as an immediate consequence of the preceding theorem the following. *A necessary and sufficient condition that two m-groups $G'$ and $G''$ be simply isomorphic is that a simple isomorphism can be set up between their associated 2-groups $G_0'$ and $G_0''$, and an element $s_0'$ of $G'$ made to correspond to an element $s_0''$ of $G''$, so that $(s_0')^{m-1}$ in $G_0'$ corresponds to $(s_0'')^{m-1}$ in $G_0''$, and $s_0'$ and $s_0''$ transform $G_0'$ and $G_0''$ respectively so that corresponding elements go over into corresponding elements.* We postpone the application of these theorems even to our modest determination of the polyadic groups of the first three orders until our detailed study of cyclic polyadic groups of finite order gives us some basis for comparison of polyadic groups.

However, one result of some theoretical interest emerges immediately. From our general determination theorem, it follows that the number of $m$-adic groups with $g$ given symbols as elements is no greater than the number of 2-groups on $g$ other given symbols as elements times $g$ times the largest number of automorphisms a 2-group of order $g$ can have. We may therefore conclude that *the number of abstract m-adic groups of given finite order g is a bounded function of m.*

## II. FINITE POLYADIC GROUPS

### A. $m$-ADIC SUBSTITUTIONS AND SUBSTITUTION GROUPS

9. **The symmetric $m$-adic substitution group of degree $n$.** An ordinary substitution, finite or infinite, may be considered to be a 1-1 correspondence between the members of a class $\Gamma$ and the members of the same class. Let now $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ be an ordered sequence of $m-1$ equivalent classes. By an *$m$-adic substitution* on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ we shall mean a transformation which in 1-1 fashion carries the members of $\Gamma_1$ into those of $\Gamma_2$, of $\Gamma_2$ into those of $\Gamma_3, \cdots$, of $\Gamma_{m-1}$ into those of $\Gamma_1$[38]. Symbolically we shall write $\Gamma_1 \rightarrow \Gamma_2, \Gamma_2 \rightarrow \Gamma_3, \cdots, \Gamma_{m-1} \rightarrow \Gamma_1$. Intrinsically, therefore, the $\Gamma$'s really enter into an $m$-adic substitution as a cycle, with $\Gamma_1$ following $\Gamma_{m-1}$. If $s_1$ and $s_2$ represent two $m$-adic substitutions on the same sequence of $\Gamma$'s, we may as usual refer to $s_1 s_2$, the product of $s_1$ and $s_2$, that is, the transformation equivalent to performing $s_1$ followed by $s_2$. But in general, for $m > 2$, the product of two $m$-adic substitutions will not be an $m$-adic substitution on the given sequence of $\Gamma$'s, for it will transform $\Gamma_1$ into $\Gamma_3$, instead of $\Gamma_2$. On the other hand, the product of $m$ $m$-adic substitutions on the $m-1$ $\Gamma$'s will again transform $\Gamma_1 \rightarrow \Gamma_2, \Gamma_2 \rightarrow \Gamma_3, \cdots, \Gamma_{m-1} \rightarrow \Gamma_1$, and hence we can expect to have $m$-adic groups of $m$-adic substitutions[39]. We can likewise expect to have $m$-adic groups of $\mu$-adic substitutions provided $\mu - 1$ is a divisor of $m-1$. However, by *$m$-adic substitution group* we shall understand the former, that is, a set of $m$-adic substitutions, all on the same sequence of $\Gamma$'s, and forming an $m$-adic group under the product of $m$ substitutions as operation[40].

When the $\Gamma$'s are mutually exclusive, an $m$-adic substitution can be given by an ordinary substitution where the one class $\Gamma$ is the logical sum of the given $\Gamma$'s. On the other hand, when the $\Gamma$'s have common elements, an $m$-adic substitution cannot in general be thus considered, since one and the same element may be transformed into different elements according to the $\Gamma_i$ of which it is considered to be a member. We shall restrict our attention to the former case[41]. But our results will be foreshadowed not by considering the resulting

[38] Our language is that of transformation; that is, we shall say "$a$ is carried into $b$" where the language of substitution would say "$a$ is replaced by $b$."

[39] On the other hand, the product of $m$ $m$-adic substitutions not all on the same sequence of $\Gamma$'s will "usually" fail to be an $m$-adic substitution for any sequence of $\Gamma$'s. Hence the straight-laced definition following.

[40] The following generalization of ordinary substitution likewise suggests itself in connection with the schar concept. For but two equivalent classes $\Gamma_1, \Gamma_2$, consider transformations which in 1-1 fashion carry the elements of $\Gamma_1$ into those of $\Gamma_2$. If $A, B, C$ are three such transformations, then $AB^{-1}C$ is also such a transformation. Note that here the product of two such transformations does not, in general, even exist.

[41] For simplicity. If each member $a$ of $\Gamma_i$ is replaced by the couple $(i, a)$, $\Gamma$'s not mutually exclusive become mutually exclusive, and it is then readily seen when results obtained for mutually exclusive $\Gamma$'s hold for arbitrary $\Gamma$'s. Actually, our results were first obtained for arbitrary $\Gamma$'s. But that they are so little affected by the overlapping or nonoverlapping of the $\Gamma$'s indicates that we have left wholly unexplored the more interesting part of the complete theory.

$m$-adic substitutions special types of ordinary substitutions, but generalizations of ordinary substitutions, reducing to the latter when $m=2$.

We further restrict our attention to the case where the $\Gamma$'s are finite classes, and hence consist each of the same finite number of members $n$. The analogy with an ordinary substitution will be furthered by saying that the $m$-adic substitution is then of *degree* $n$. Let then the members of $\Gamma_1$ be symbolized $a_{11}, a_{12}, \cdots, a_{1n}$, of $\Gamma_2$, $a_{21}, a_{22}, \cdots, a_{2n}, \cdots$ of $\Gamma_{m-1}$, $a_{(m-1)1}, a_{(m-1)2}, \cdots, a_{(m-1)n}$. Corresponding to the primitive mode of writing ordinary substitutions we have the following form for any $m$-adic substitution on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$:

$$\begin{array}{llll} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{2j_1''} & a_{2j_2''} & \cdots & a_{2j_n''} \\ \cdot & \cdot & \cdots & \\ a_{(m-1)j_1^{(m-1)}} & a_{(m-1)j_2^{(m-1)}} & \cdots & a_{(m-1)j_n^{(m-1)}} \\ a_{1j_1^{(m)}} & a_{1j_2^{(m)}} & \cdots & a_{1j_n^{(m)}} \end{array}$$

where the $i$th row is some permutation of $(a_{i1}a_{i2}\cdots a_{in})$ except for $i=m$, when it is a permutation of the first row, and each letter is carried into the one immediately below it by the substitution. If, as suggested above, we consider our $m$-adic substitution an ordinary substitution on all the letters $a_{ij}$, it can also be written in standard form as a product of cycles on different letters. In that case, each cycle will have a multiple of $m-1$ letters, these letters cyclically running through the $m-1$ $\Gamma$'s.

Since an $m$-adic substitution of degree $n$ is thus determined by $m-1$ independent permutations of $n$ elements each, we thus see that there are $(n!)^{m-1}$ $m$-adic substitutions of degree $n$, the sequence of $\Gamma$'s being understood given. Observe again that if $s_1, s_2, \cdots, s_m$ are $m$-adic substitutions on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, their products $s_1s_2\cdots s_m$ is also an $m$-adic substitution on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$. In detail, $s_1$ will carry $a_{ij}$ into some $a_{(i+1)j'}$, $s_2$ will carry $a_{(i+1)j'}$ into some $a_{(i+2)j''}$, $\cdots$, and $s_m$ a resulting $a_{ij^{(m-1)}}$ into $a_{(i+1)j^{(m)}}$. Hence $s_1s_2\cdots s_m$ carries $a_{ij}$ into $a_{(i+1)j^{(m)}}$ as required. It then easily follows that the $(n!)^{m-1}$ $m$-adic substitutions of degree $n$ constitute an $m$-group under the operation $s_1s_2\cdots s_m$. While the corresponding result holds good apart from our hypothesis of finite mutually exclusive $\Gamma$'s, for the present case it suffices to reinterpret our $m$-adic substitutions as ordinary substitutions. Condition 2 for an $m$-group then follows from the associative law for the multiplication of ordinary substitutions. As for condition 1, the case where all $s$'s but $s_{m+1}$ in $s_1s_2\cdots s_m=s_{m+1}$ are given $m$-adic substitutions has been taken care of. And if all but $s_i$ are given $m$-adic substitutions, $1\leqq i\leqq m$, by letting $s_i$ run through the $(n!)^{m-1}$ possible $m$-adic substitutions, $s_1s_2\cdots s_m$ must do the same, and hence equals $s_{m+1}$ for one and only one $m$-adic substitution $s_i$.

We shall call this $m$-group of order $(n!)^{m-1}$ the *$m$-adic symmetric group of*

*degree n*. It clearly becomes the ordinary symmetric group of degree $n$ when $m=2$. As in the case of ordinary substitution groups, every $m$-adic substitution group on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, or briefly of degree $n$, will be a subgroup of the $m$-adic symmetric group of degree $n$. It readily follows that the necessary and sufficient condition that a finite set of $m$-adic substitutions all on the same sequence of $\Gamma$'s form an $m$-adic substitution group is that the product of any $m$ substitutions in the set be in the set.

Of special interest are those $m$-adic substitutions of degree $n$ in which the last row is an exact repetition of the first row. There are clearly $(n!)^{m-2}$ such substitutions. If $s$ be such a substitution, $s^{m-1}$ clearly carries each letter into itself, and hence $s^m=s$. Conversely, if $s^m=s$, $s$ must be such a substitution. According to a definition already given, $s$ is then of $m$-adic order one. The unit class with $s$ as sole member therefore itself constitutes an $m$-adic substitution group of order one. Hence the $m$-adic symmetric group of degree $n$ has $(n!)^{m-2}$ first order elements, and correspondingly $(n!)^{m-2}$ subgroups of order one. For $m=2$ these become the sole identity of the group.

10. **$2^{m-1}$-fold classification of $m$-adic substitutions; the $m$-adic alternating groups.** The classic theory of positive and negative substitutions involves the use of the determinant

$$\Delta = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix}$$

which is left invariant under every positive substitution on the letters $a_1, a_2, \cdots, a_n$, and is transformed into its negative under every negative substitution on those letters. We generalize this theory by the same means.

We now form the $m-1$ determinants $\Delta_1, \Delta_2, \cdots, \Delta_{m-1}$, where $\Delta_i$ is the determinant $\Delta$ for the $n$ letters $a_{i1}, a_{i2}, \cdots, a_{in}$ of $\Gamma_i$, and transform them accordingly to a given $m$-adic substitution

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{2j_1''} & a_{2j_2''} & \cdots & a_{2j_n''} \\ \cdot & \cdot & \cdots & \cdot \\ a_{(m-1)j_1^{(m-1)}} & a_{(m-1)j_2^{(m-1)}} & \cdots & a_{(m-1)j_n^{(m-1)}} \\ a_{1j_1^{(m)}} & a_{1j_2^{(m)}} & \cdots & a_{1j^{(m)}}. \end{matrix}$$

If in the $i$th row each letter $a_{ij}$ is rewritten $a_{(i+1)j}$[42], then the new $i$th row together with the old $(i+1)$-st row defines an ordinary substitution on the letters of the $(i+1)$-st row. The transform of $\Delta_i$ under the $m$-adic substitu-

[42] $a_{1j}$, when $i=m-1$. Likewise, below, $\Delta_{i+1}$ is $\Delta_1$ when $i=m-1$.

tion is clearly the transform of $\Delta_{i+1}$ under this ordinary substitution, and hence is $\Delta_{i+1}$, or its negative, according as this ordinary substitution is positive or negative. We therefore have under the $m$-adic substitution

$$\Delta_1 \rightarrow \delta_1\Delta_2,\ \Delta_2 \rightarrow \delta_2\Delta_3,\ \cdots,\ \Delta_{m-1} \rightarrow \delta_{m-1}\Delta_1, \qquad \delta_1,\ \delta_2,\ \cdots,\ \delta_{m-1} = \pm 1.$$

With each $m$-adic substitution there is thus associated a sequence of $m-1$ numbers $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$ whose values are $+1$ or $-1$. Clearly, when $n>1$, an $m$-adic substitution of degree $n$ can be written down for every possible assignment of values to the $\delta$'s. The $m$-adic substitutions of degree $n$, $n>1$, thus fall into $2^{m-1}$ mutually exclusive classes corresponding to the $2^{m-1}$ possible *$\delta$-sequences* $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$.

Given $m$ $m$-adic substitutions $s_i$, with the corresponding $\delta$-sequences $[\delta_{i1}, \delta_{i2}, \cdots, \delta_{i(m-1)}]$, the $m$-adic substitution $s_1s_2 \cdots s_m$ has a $\delta$-sequence $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$ which depends only on the $\delta$-sequences of the $s_i$'s. In fact, by following through the effect of the succession of substitutions $s_1, s_2, \cdots, s_m$ on the determinants $\Delta_1, \Delta_2, \cdots, \Delta_{m-1}$, we obtain the following equations for determining $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$:

$$\begin{aligned}
\delta_1 &= \delta_{11}\delta_{22} \cdots \delta_{(m-1)(m-1)}\delta_{m1},\\
\delta_2 &= \delta_{12}\delta_{23} \cdots \delta_{(m-1)1}\delta_{m2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots,\\
\delta_{m-1} &= \delta_{1(m-1)}\delta_{21} \cdots \delta_{(m-1)(m-2)}\delta_{m(m-1)}.
\end{aligned}$$

Now let $K$ be the class of the $2^{m-1}$ possible $\delta$-sequences. If $\sigma_1, \sigma_2, \cdots, \sigma_m$ are any $m$ such $\delta$-sequences, and $\sigma$ is the $\delta$-sequence obtained from $\sigma_1, \sigma_2, \cdots, \sigma_m$ in accordance with the above equations, an $m$-adic operation $k(\sigma_1\sigma_2 \cdots \sigma_m)$ is determined such that $\sigma = k(\sigma_1\sigma_2 \cdots \sigma_m)$. It is then readily shown that $K$ constitutes an $m$-group under $k$. In fact, condition 1 for an $m$-group is immediately verified by referring to the above equations. And condition 2 follows from the associative law for $m$-adic substitutions, and the fact that if $s_1, s_2, \cdots, s_m$ are substitutions corresponding to $\sigma_1, \sigma_2, \cdots, \sigma_m$ respectively, $s_1s_2 \cdots s_m$ corresponds to $k(\sigma_1\sigma_2 \cdots \sigma_m)$. We shall call this $m$-group of order $2^{m-1}$ the *complete $m$-adic $\delta$-group*([43]).

Consider now any $m$-adic substitution group of degree $n$ and form the class $K'$ of $\delta$-sequences corresponding to its members. Since the product of any $m$ substitutions of the group is in the group, the $k$ product of any $m$ $\delta$-sequences in $K'$ will be in $K'$. As $K'$ is a subclass of the class of members of the complete $m$-adic $\delta$-group, and the latter is finite, this suffices to prove

([43]) Actually, then, we have established a homomorphism between the symmetric $m$-adic substitution group of degree $n$, $n>1$, and this complete $m$-adic $\delta$-group. The rest of this section could then largely have been given as a consequence of our general results on homomorphisms between $m$-adic groups, as could indeed the very fact that $K$ is an $m$-group under $k$. In the generalization of this section occurring in the last section of our paper full use will be made of the concept of homomorphism.

the following. *The δ-sequences corresponding to the members of any m-adic substitution group of degree n form the complete m-adic δ-group, or a subgroup thereof.*

By means of the above equations for the $k$ operation we readily prove, as for ordinary substitutions, that *every m-adic substitution group of degree n has the same number of substitutions for each δ-sequence in the corresponding "δ-subgroup"*([44]). In fact, let $s_m$ and $s_{m+1}$ be any two substitutions in the group corresponding to any two given δ-sequences $\sigma_m$ and $\sigma_{m+1}$ of the corresponding δ-subgroup, and choose $s_1, \cdots, s_{m-1}$ so that $s_1 \cdots s_{m-1}s_m = s_{m+1}$. If now we let $s_m$ run through all the substitutions in the group corresponding to $\sigma_m$, $s_{m+1}$ assumes an equal number of values in the group all corresponding to $\sigma_{m+1}$. Hence there are at least as many substitutions in the group corresponding to one δ-sequence as to another, and consequently, by reciprocal reasoning, the same number. Since the order of the complete $m$-adic δ-group is $2^{m-1}$, that of a subgroup thereof must be of the form $2^\mu$([45]). From the above result it follows that the order of an $m$-adic substitution group is a multiple of the order of its δ-subgroup. We therefore have as a corollary of the above result *every m-adic substitution group of odd order has a δ-subgroup of order one*, that is, all of its substitutions correspond to one and the same δ-sequence.

Applied to the symmetric group itself, the above result shows that the $2^{m-1}$ mutually exclusive classes into which the $m$-adic symmetric group of degree $n$ is divided all have the same number of members. Now given any subgroup of the complete $m$-adic δ-group, form the class $C'$ of all the $m$-adic substitutions of degree $n$ corresponding to each δ-sequence in the given δ-subgroup. The product of any $m$ substitutions in $C'$ will therefore be in $C'$. Hence the members of $C'$ form a subgroup of the symmetric group. By analogy with ordinary groups we shall call it an *m-adic alternating group.* Consequently, *there are as many m-adic alternating groups of degree n, $n>1$, as there are subgroups of the complete m-adic δ-group, each alternating group consisting of all the substitutions of the symmetric group with δ-sequences in the corresponding δ-subgroup.* We may now further state that there is a one-many correspondence between the $m$-adic δ-subgroups and $m$-adic substitution groups of degree $n$, $n>1$, that is, between the class consisting of the complete $m$-adic δ-group and its subgroups, and the $m$-adic symmetric group of degree $n$ and its subgroups; and this correspondence is preserved under the relation "group or subgroup of."

For $m=2$ the complete δ-group is the cyclic group of order 2, and its sole subgroup, the identity, corresponds to the sole ordinary alternating group of degree $n$([46]). For $m=3$ the complete δ-group is of order 4. By direct calcula-

([44]) We shall use the phrase δ-subgroup to cover the complete δ-group as well.

([45]) By Lagrange's theorem for polyadic groups—proved in §4.

([46]) van der Waerden has already noted the homomorphism between any substitution group having at least one odd substitution and this cyclic group of order two.

tion we find it to possess exactly four subgroups, that is, with classes of elements $([+1, +1])$, $([-1, -1])$, $([+1, +1], [-1, -1])$, $([+1, -1], [-1, +1])$. Hence, there are exactly four triadic alternating groups of degree $n$, $n>1$.

Thanks to B. P. Gill, we are able to determine the $m$-adic alternating groups of degree $n$ for arbitrary $m$. For this purpose it is essential to obtain a suitable representation of the associated ordinary group of the complete $m$-adic $\delta$-group. The ideas leading up to this are of more general application, and hence at least part of the following digression.

11. **Associated and containing ordinary groups; commutative $m$-adic substitutions.** The substitutions of an $m$-adic substitution group $G$ of degree $n$, considered as ordinary substitutions on $(m-1)n$ letters, generate an ordinary substitution group which satisfies our definition of a containing group of $G$. With $G$ thus an $m$-adic group of $m$-adic substitutions, this containing group will be of index $m-1$, and hence simply isomorphic with the abstract containing group $G^*$ of $G$. We shall therefore use it throughout to represent $G^*$, and for simplicity symbolize it $G^*$. We may likewise refer to the associated group of $G$ with respect to this containing group as $G_0$.

In the terminology of §6, the $i$th coset of $G^*$ consists of the products of $i$ elements of $G$. To avoid duplication, it will be convenient henceforth to assume that $1 \leqq i \leqq m-1$. Since each substitution in $G$ transforms $\Gamma_1 \to \Gamma_2$, $\Gamma_2 \to \Gamma_3$, $\cdots$, $\Gamma_{m-1} \to \Gamma_1$, it follows that the $i$th coset of $G^*$ consists of transformations which in 1-1 fashion carry the members of each $\Gamma_j$ into those of $\Gamma_{j+i}$, $j+i$ reduced modulo $m-1$ if need be. We may therefore call these substitutions of $G^*$ the $i$-ads of $G$. In particular, $G_0$, which consists of the $(m-1)$-ads of $G$ in $G^*$, consists of transformations which transform each $\Gamma_j$ into itself. Each $(m-1)$-ad of $G$ thus appears in $G^*$ as the product of $m-1$ ordinary substitutions, each of these ordinary substitutions being on the letters of a single $\Gamma$. We have incidentally verified that $G^*$ is of index $m-1$.

Considered as ordinary substitution groups on $(m-1)n$ letters we see that for $m>2$, $G^*$ is imprimitive with systems of imprimitivity $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, while $G_0$ is intransitive with the letters in each $\Gamma$ carried into letters of the same $\Gamma$ only, by every substitution of $G$. If then for each $\Gamma$ we separate from each substitution in $G_0$ the substitution involving only the letters of that $\Gamma$, there results an ordinary substitution group on the letters of that $\Gamma$. We shall symbolize these $m-1$ groups on the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ by $G_0', G_0'', \cdots, G_0^{(m-1)}$ respectively, and call them the *associated constituent groups* of the $m$-adic substitution group $G$. It is then significant that *the associated constituent groups of an $m$-adic substitution group are conjugate ordinary groups.* In fact, recall that $G_0$ is an invariant subgroup of $G^*$, and hence is invariant under every $m$-adic substitution $s$ in $G$. Now $s$ carries the letters of each $\Gamma_i$ into those of $\Gamma_{i+1}$. Hence, when the substitutions of $G_0$ are transformed by $s$, the components of these substitutions on the letters of $\Gamma_i$ be-

come the components of the same class of substitutions on the letters of $\Gamma_{i+1}$. We thus have specifically

$$s^{-1}G_0' s = G_0'',\ s^{-1}G_0'' s = G_0''',\ \cdots,\ s^{-1}G_0^{(m-1)} s = G_0',$$

for every $s$ in $G$.

If $s_1$ and $s_2$ are $m$-adic substitutions on the same sequence of $\Gamma$'s, we may consider them as elements of the corresponding $m$-adic symmetric group. The transform of $s_2$ under $s_1$ is then $s_1^{-1}s_2s_1$ in the notation of the containing group of the symmetric group, and hence may be obtained by the ordinary rule for transforming substitutions. Restated for our primitive mode of representing $m$-adic substitutions, this rule becomes the following. Replace each letter in $s_2$ by the letter immediately under it in $s_1$ and rewrite in standard form. Thus, to illustrate, let

$$s_2 = \begin{matrix} a_{11}a_{12}a_{13} \\ a_{22}a_{21}a_{23}, \\ a_{11}a_{13}a_{12} \end{matrix} \qquad s_1 = \begin{matrix} a_{11}a_{12}a_{13} \\ a_{22}a_{23}a_{21}; \\ a_{13}a_{11}a_{12} \end{matrix} \qquad s_1^{-1}s_2s_1 = \begin{matrix} a_{22}a_{23}a_{21} \\ a_{13}a_{12}a_{11} \\ a_{22}a_{21}a_{23} \end{matrix} = \begin{matrix} a_{11}a_{12}a_{13} \\ a_{23}a_{21}a_{22}. \\ a_{12}a_{11}a_{13} \end{matrix}$$

Actually, the result before it is rewritten defines the transform equally well; for, as stated before, it is really the cycle, rather than the sequence, of $\Gamma$'s that is significant.

If $s_2$ is invariant under $s_1$, then $s_1$ and $s_2$ are commutative; and conversely. The problem of determining all $m$-adic substitutions $s$, commutative with a given $m$-adic substitution $s_1$ of degree $n$, and on the same $\Gamma$'s, is best treated by writing the substitutions in ordinary cycle form. We recall that the number of letters in each cycle is then a multiple of $m-1$. If $s_1$ consists of a single cycle, the ordinary substitutions $r$, on the $(m-1)n$ letters of $s_1$, which are commutative with $s_1$, are the $(m-1)n$ ordinary powers of $s_1$. Of these exactly $n$, i.e., those of the form $s_1^{k(m-1)+1}$, are $m$-adic substitutions on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$. We shall later call these the $m$-adic powers of $s_1$, i.e., the elements of the $m$-adic group generated by $s_1$. Hence, the only $m$-adic substitutions on the $\Gamma$'s of $s_1$, commutative with the single cycle $m$-adic substitution $s_1$ of degree $n$, are the $n$ $m$-adic powers of $s_1$. We now have no difficulty in paraphrasing the corresponding argument for ordinary substitutions, and obtain the following results. If $s_1$ consists of $\lambda$ cycles with numbers of letters $(m-1)n_1, (m-1)n_2, \cdots, (m-1)n_\lambda$ no two of which are equal, the $m$-adic substitutions $s$, on the $\Gamma$'s of $s_1$, commutative with $s_1$, are the $n_1n_2 \cdots n_\lambda$ products of the $m$-adic powers of the several cycles. And, if $s_1$ consists of $k$ equal cycles of $(m-1)\nu$ letters each, the $m$-adic substitutions $s$ on the $\Gamma$'s of $s_1$ commutative with $s_1$ are $\nu^k k!$ in number, there being $\nu^k$ such $m$-adic substitutions for each of the $k!$ possible permutations of the $k$ cycles. Clearly in any case, the $m$-adic substitutions $s$, commutative with an $m$-adic substitution $s_1$, and on the $\Gamma$'s of $s_1$, constitute an $m$-adic substitution group.

12. **Further study of the complete $m$-adic $\delta$-group and $m$-adic alternating groups.** The ideas of the preceding section enable us to clear up a certain difficulty in our presentation of the $2^{m-1}$-fold classification of $m$-adic substitutions and in its consequences. Observe that whereas the $\Gamma_i$'s are mere classes, the determinants $\Delta_i$ assume the letters in each $\Gamma_i$ arranged in a sequence. The $\delta$-sequence associated with a given $m$-adic substitution $s$ will therefore in general depend not only on $s$ but also on the original ordering of the letters in the $\Gamma_i$'s. However, we shall see that the same $2^{m-1}$ classes are obtained no matter what ordering is assumed, only their description by $\delta$-sequences being thus affected.

Actually, this ordering is equivalent to a first order $m$-adic substitution $s_0$ which carries each $a_{ij}$ into $a_{(i+1)j}$, $i+1$ being replaced by 1 when $i=m-1$. Let us then write the $m$-adic symmetric group in coset form with arbitrary element $s=ts_0$. $t$ is then in the form $t't''\cdots t^{(m-1)}$ where $t^{(i)}$ is an ordinary substitution on the letters of $\Gamma_i$. If now we associate with $t$ the $\epsilon$-sequence $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1})$, where $\epsilon_i$ is $+1$ or $-1$ according as $t^{(i)}$ is a positive or negative substitution, we see from the effect on the determinants $\Delta_i$ that the $\epsilon$-sequence of $t$ is identical with the $\delta$-sequence of $s$. Let then $s_1=t_1s_0$ and $s_2=t_2s_0$ have the same $\delta$-sequence, and hence $t_1$ and $t_2$ the same $\epsilon$-sequence. Then $s_1s_2^{-1}=t_1t_2^{-1}$ will have an $\epsilon$-sequence $(+1, +1, \cdots, +1)$, i.e., will be the product of positive substitutions only. Conversely, if $s_1s_2^{-1}$ is the product of positive substitutions only, the corresponding $t_1$ and $t_2$ must have the same $\epsilon$-sequence, and $s_1$ and $s_2$ the same $\delta$-sequence. Hence, $s_1$ and $s_2$ belong to the same one of the $2^{m-1}$ classes of $m$-adic substitutions when and only when $s_1s_2^{-1}$ is the product of positive substitutions on the letters of the several $\Gamma$'s. As this criterion is independent of $s_0$, the intrinsic character of our classification has been demonstrated.

The $\epsilon$-sequences may be used to obtain a concrete representation of the associated ordinary group of the complete $m$-adic $\delta$-group. More generally, consider the containing group of the $m$-adic symmetric group of degree $n$, $n>1$. Since each $i$-ad $R$ thereof is the product of $i$ $m$-adic substitutions, $R$ will transform the $\Delta$'s according to some scheme

$$\Delta_1 \to \eta_1\Delta_{i+1}, \Delta_2 \to \eta_2\Delta_{i+2}, \cdots, \Delta_{m-1} \to \eta_{m-1}\Delta_i, \quad \eta_1, \eta_2, \cdots, \eta_{m-1} = \pm 1.$$

With $R$ we may thus associate the $\eta$-sequence (with subscript) $\{\eta_1, \eta_2, \cdots, \eta_{m-1}\}_i$. If $R_1$ thus corresponds to $\{\eta_1', \eta_2', \cdots, \eta_{m-1}'\}_{i_1}$, $R_2$ to $\{\eta_1'', \eta_2'', \cdots, \eta_{m-1}''\}_{i_2}$, $R_1R_2$ will correspond to $\{\eta_1'\eta_{i_1+1}'', \eta_2'\eta_{i_2+2}'', \cdots, \eta_{m-1}'\eta_{i_1}''\}_{i_1+i_2}$, subscripts being reduced modulo $m-1$ if need be. It follows that the containing group of the $m$-adic symmetric group is homomorphic to the resulting complete $\eta$-group (with subscript). Now with $i=1$, the $\eta$-sequence is nothing more than the $\delta$-sequence of the corresponding $m$-adic substitution. From the way in which our operations were obtained it follows that the complete $\eta$-group may be considered a containing group, of index $m-1$,

indeed, of the complete $m$-adic $\delta$-group. The associated group of the complete $m$-adic $\delta$-group will then be composed of the $\eta$-sequences whose subscript is $m-1$. But going back to the $\Delta$'s we see that these $\eta$-sequences are then actually the $\epsilon$-sequences of the corresponding $(m-1)$-ads of $m$-adic substitutions. Under this representation, therefore, the operation of the associated group of the complete $m$-adic $\delta$-group, i.e., of the *complete $\epsilon$-group* as we shall call it, becomes

$$(\epsilon_1', \epsilon_2', \cdots, \epsilon_{m-1}')(\epsilon_1'', \epsilon_2'', \cdots, \epsilon_{m-1}'') = (\epsilon_1'\epsilon_1'', \epsilon_2'\epsilon_2'', \cdots, \epsilon_{m-1}'\epsilon_{m-1}'')(47).$$

We therefore see that the complete $\epsilon$-group is an ordinary abelian group of order $2^{m-1}$. Since each $\epsilon$ is $\pm 1$, its elements other than the identity are all of order two, so that it is indeed of type $(1, 1, \cdots, 1)$.

The complete $m$-adic $\delta$-group is therefore semi-abelian. As it is readily seen to be non-abelian whenever $m>2$, it follows that it then has no invariant element. More specifically, the transform of $[\delta_1, \delta_2, \delta_3, \cdots, \delta_{m-1}]$ by $[\delta_1', \delta_2', \delta_3', \cdots, \delta_{m-1}']$ is easily found, via the complete $\eta$-group, to be

$$[\delta_{m-1}'\delta_{m-1}\delta_1', \delta_1'\delta_1\delta_2', \delta_2'\delta_2\delta_3', \cdots, \delta_{m-2}'\delta_{m-2}\delta_{m-1}'].$$

The condition for invariance is then easily rewritten $\delta_1\delta_1' = \delta_2\delta_2' = \delta_3\delta_3' = \cdots = \delta_{m-1}\delta_{m-1}'$. It follows that there are exactly two $\delta$-sequences leaving any given $\delta$-sequence $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$ invariant, namely, $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$ and $[-\delta_1, -\delta_2, \cdots, -\delta_{m-1}]$.

The present and succeeding paragraph presuppose a partial reading of the later §21 and §22. We have observed that except for the identity the elements of the complete $\epsilon$-group are all of order two. While it follows therefrom that the elements of the complete $m$-adic $\delta$-group are of no other $m$-adic orders than one or two, we find directly that exactly half of them are of order one, half of order two. Thus, if $\sigma$ is the $\delta$-sequence $[\delta_1, \delta_2, \cdots, \delta_{m-1}]$, and $\delta_0 = \delta_1\delta_2 \cdots \delta_{m-1}$, then, with $k$ as in §10, we find $k(\sigma\sigma \cdots \sigma) = [\delta_0\delta_1, \delta_0\delta_2, \cdots, \delta_0\delta_{m-1}]$, $k(\sigma\sigma \cdots k(\sigma\sigma \cdots \sigma)) = [\delta_1, \delta_2, \cdots, \delta_{m-1}]$. Hence, the $m$-adic order of a $\delta$-sequence is one or two according as the product of its $\delta$'s is $+1$ or $-1$.

The cyclic subgroups of the complete $m$-adic $\delta$-group are therefore of orders one or two, there being $2^{m-2}$ first order subgroups, and, for $m>2$, $2^{m-2}$ or $2^{m-3}$ cyclic second order subgroups according as $m$ is even or odd. Our result on the $\delta$-sequences leaving a given $\delta$-sequence invariant, coupled with the easily verified fact that an $m$-group of order two must be abelian, leads to the result that the complete $m$-adic $\delta$-group has exactly $2^{m-2}$ second

(47) Actually, by a slight change in point of view, the transformation of the $\Delta$'s resulting from an $m$-adic substitution can be considered an $m$-adic linear transformation in one variable in the sense of our later §35. The present and several other formulas, derived independently in the present section, would then become special cases of the formulas of §35.

order subgroups for $m>2$. Hence, when $m$ is odd, half of them are non-cyclic([48]).

We turn now to the determination of all the subgroups of the complete $m$-adic $\delta$-group, and consequently, the determination of all $m$-adic alternating groups. Since the complete $m$-adic $\delta$-group is semi-abelian, all of its elements transform a given $\epsilon$-sequence $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1})$ into the same $\epsilon$-sequence. As before, we can employ the operation of the complete $\eta$-group, and thus find the unique transform of $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1})$ under every $\delta$-sequence to be $(\epsilon_{m-1}, \epsilon_1, \epsilon_2, \cdots, \epsilon_{m-2})$. Now if $H$ is a subgroup of the complete $m$-adic $\delta$-group, its associated ordinary group $H_0$ must be a subgroup of the complate $\epsilon$-group invariant under $H$. Hence $H_0$ can only be such a subgroup of the complete $\epsilon$-group that if $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-2}, \epsilon_{m-1})$ is in the subgroup, $(\epsilon_{m-1}, \epsilon_1, \epsilon_2, \cdots, \epsilon_{m-2})$ also is in the subgroup. The determination of these "admissible" subgroups of the complete $\epsilon$-group is the only difficult part of our problem. It was carried through independently by Gill; but he later found that his solution followed essentially the lines of the general theory of the "Verallgemeinerte Abelsche Gruppen," abbreviated V.A.G., as given by Otto Haupt in the second volume of his *Algebra*([49]).

Following Gill we replace the two values $+1$, $-1$ by 0, 1 respectively. If an $\epsilon$-sequence be thus rewritten, the dyadic operation of our complete $\epsilon$-group is best written in additive form, and we have

$$(\epsilon_{11}, \epsilon_{12}, \cdots, \epsilon_{1(m-1)}) + (\epsilon_{21}, \epsilon_{22}, \cdots, \epsilon_{2(m-1)}) = (\epsilon_{11} + \epsilon_{21}, \epsilon_{12} + \epsilon_{22}, \cdots, \epsilon_{1(m-1)} + \epsilon_{2(m-1)}),$$

where addition within the parentheses is modulo 2. Now let $\phi(x)$ be any polynomial in $x$ with coefficients 0 or 1. With $a$ any $\epsilon$-sequence, a unique $\epsilon$-sequence $\phi(x)\cdot a$ is determined as follows. If $a$ is the $\epsilon$-sequence $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-2}, \epsilon_{m-1})$, let $x\cdot a$ be the $\epsilon$-sequence $(\epsilon_{m-1}, \epsilon_1, \epsilon_2, \cdots, \epsilon_{m-2})$. With $1\cdot a=a$, and $x^n\cdot a$ defined inductively through $x^n\cdot a=x\cdot(x^{n-1}\cdot a)$, we can define $\phi(x)\cdot a$ as the sum of the $\epsilon$-sequences obtained by operating on $a$ by the several terms of $\phi(x)$. We now observe two things. First, every $\epsilon$-sequence can be written $\phi(x)\cdot(1, 0, \cdots, 0)$. In fact, to obtain $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1})$, we need merely let $\phi(x)=\epsilon_1+\epsilon_2 x+\cdots+\epsilon_{m-1}x^{m-2}$. Secondly, with $(0, 0, \cdots, 0)$ abbreviated 0, we see that $(1, 0, \cdots, 0)$ satisfies the equation $(x^{m-1}+1)\cdot(1, 0, \cdots, 0)=0$, but fails to satisfy any equation $\phi(x)\cdot(1, 0, \cdots, 0)=0$ with $\phi(x)$ of degree less than $m-1$, and not identically zero. For we have directly that $x^{m-1}\cdot(1, 0, \cdots, 0)=(1, 0, \cdots, 0)$; while with $\phi(x)$ of degree less than $m-1$ our previous expression for $\phi(x)\cdot(1, 0, \cdots, 0)$ applies. Note finally that 0 and 1 constitute a field $K$ under addition modulo 2, and multiplication. The entire theory of V.A.G.'s in general, and Theorem 3 of Haupt

([48]) See §23 for the consequent structure of these second order subgroups.

([49]) Otto Haupt, *Einführung in die Algebra*, Leipzig, 1929, vol. 2, pp. 617–621. The result we need is the Theorem 3 of page 620.

in particular, can then be shown to be applicable, and yield the following result.

*The admissible subgroups of the complete m-adic $\epsilon$-group are in* 1-1 *correspondence with the polynomial divisors, other than unity, of $x^{m-1}+1$ relative to the field of coefficients K. If $\tau(x)$ be such a divisor, and $a=\tau(x)\cdot(1, 0, \cdots, 0)$, then the corresponding subgroup consists of all distinct $\epsilon$-sequences $\phi(x)\cdot a$.*

Actually, if $\mu$ is the degree of $(x^{m-1}+1)/\tau(x)$, then $\phi(x)$ can be restricted to degrees less than $\mu$, different $\phi(x)$'s then also giving different $\epsilon$-sequences. It follows that the order([50]) of the corresponding subgroup is $2^{\mu}$. The subgroup corresponding to $\tau(x)$ can also be described as consisting of all $\epsilon$-sequences $b$ such that $(x^{m-1}+1)/\tau(x)\cdot b=0$. It follows that these subgroups satisfy the same properties with respect to the relation of inclusion as do the subgroups of an ordinary cyclic group, $(x^{m-1}+1)/\tau(x)$ taking the place of the order of the subgroup. Note that the unique factorization theorem applies to polynomials with coefficients in a given field. If then $x^{m-1}+1$ is thus completely factored, the distinct divisors $\tau(x)$ can immediately be written down. Since $x^{m-1}+1=(x+1)(x^{m-2}+\cdots+x+1)$ relative to $K$, $x+1$ is always one of the prime divisors of $x^{m-1}+1$. It can readily be shown that it is the only distinct prime divisor of $x^{m-1}+1$, that is, that $x^{m-1}+1=(x+1)^{m-1}$ relative to $K$, when and only when $m-1$ is itself a power of 2. The different $\tau(x)$'s are then $(x+1)$, $(x+1)^2$, $\cdots$, $(x+1)^{m-1}$, and each corresponding subgroup contains the next.

Having determined the admissible subgroups of the complete $\epsilon$-group in accordance with the above theorem, it is a simple matter to find the subgroups of the complete $\delta$-group. We return here to our original notation. Each $\delta$-subgroup $H$, if written in coset form, will be given by $H=H_0\sigma$, with $H_0$ an admissible $\epsilon$-subgroup, $\sigma$ a $\delta$-sequence. Hence, if $H_0\sigma$ is known to be a $\delta$-subgroup, its elements can immediately be found from $H_0$ and $\sigma$ by the relation

$$(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1})[\delta_1, \delta_2, \cdots, \delta_{m-1}] = [\epsilon_1\delta_1, \epsilon_2\delta_2, \cdots, \epsilon_{m-1}\delta_{m-1}],$$

a mere specialization of the dyadic operation of the complete $\eta$-group.

Since every admissible $\epsilon$-subgroup $H_0$ is invariant under every $\delta$-sequence $\sigma$, it follows from an early theorem of §4 that $H_0\sigma$ will be a $\delta$-subgroup for every first order $\sigma$, and for those second order $\sigma$'s for which $\sigma^{m-1}$ is in $H_0$. The distinct $\delta$-subgroups thus arising will then be all the $\delta$-subgroups for a given $H_0$. Now when $m$ is even, every $\delta$-subgroup must have at least one first order element. Hence in this case, the $\delta$-subgroups corresponding to $H_0$ will be all the distinct $H_0\sigma$'s with $\sigma$ a first order element. Now it is readily proved that if $\tau=(\epsilon_1, \epsilon_2, \cdots, \epsilon_{m-1})$, the order of $\tau\sigma$ is the same as that of $\sigma$, or opposite, according as $\epsilon_0=\epsilon_1\epsilon_2\cdots\epsilon_{m-1}$ is $+1$ or $-1$, and furthermore, that the elements of $H_0$ either all have $\epsilon_0$ equal to $+1$, or exactly half have $\epsilon_0=+1$,

([50]) In the ordinary sense, not that of V.A.G.'s.

half $-1$. Hence, if $H_0$ is of order $2^\mu$, $H_0\sigma$, with $\sigma$ of first order, has $2^\mu$ or $2^{\mu-1}$ first order elements according as the elements of $H_0$ have or have not $\epsilon_0$'s all $+1$. Since the distinct $H_0\sigma$'s with given $H_0$ are mutually exclusive, while each of the $2^{m-2}$ first order elements of the complete $m$-adic $\delta$-group is in some $H_0\sigma$, it follows that when $m$ is even, for each admissible $\epsilon$-subgroup $H_0$ of order $2^\mu$ there are exactly $2^{m-\mu-2}$ or $2^{m-\mu-1}$ corresponding $\delta$-subgroups according as the $\epsilon_0$'s of the elements of $H_0$ are, or are not, all $+1$.

For $m$ odd, and given $H_0$, we also have these subgroups. But now there may be additional subgroups $H_0\sigma$ with all elements of order two. Now if $\sigma$ is of second order, the $\epsilon$-sequence of $\sigma^{m-1}$ is readily seen to be $(-1, -1, \cdots, -1)$. It follows that these additional subgroups can arise only when $H_0$ has the element $(-1, -1, \cdots, -1)$, while the $\epsilon_0$'s of all its elements are $+1$. But then each of the $2^{m-2}$ second order $\delta$-sequences will be in one of these additional subgroups. For such an $H_0$, therefore, in addition to the now $2^{m-\mu-2}$ $\delta$-subgroups consisting wholly of first order elements, there will be $2^{m-\mu-2}$ additional $\delta$-subgroups each, indeed, consisting wholly of second order elements.

Actually, the number of $\delta$-subgroups with given associated ordinary group $H_0$ can be determined without explicitly writing out the elements of $H_0$, but merely by an inspection of the corresponding $\tau(x)$. Thus, we have already seen that the order of $H_0$ is $2^\mu$, where $\mu$ is the degree of $(x^{m-1}+1)/\tau(x)$. By means of the second description given for the subgroup $H_0$, it can further be shown that $(-1, -1, \cdots, -1)$ is in $H_0$ when and only when $(x^{m-1}+1)/\tau(x)$ has $x+1$ for divisor; while from the first description it can be shown that the $\epsilon_0$'s of $H_0$ are all $+1$ when and only when $\tau(x)$ has $x+1$ for divisor. This covers all we need to know about $H_0$.

In particular, for $m>3$, we always have the three distinct divisors of $x^{m-1}+1$ equal to $x^{m-1}+1$, $x^{m-2}+\cdots+x+1$, $x+1$. In the first case $H_0$ is of order one, and consists of but $(+1, +1, \cdots, +1)$, the identity. The corresponding $\delta$-subgroups are the first order $\delta$-subgroups listed above. In the second case $H_0$ is of order two, and consists of $(+1, +1, \cdots, +1)$ and $(-1, -1, \cdots, -1)$. It is obviously the only admissible second order $\epsilon$-subgroup, and hence the corresponding $\delta$-subgroups are all of the second order $\delta$-subgroups as first listed. The third subgroup, of order $2^{m-2}$, is again the only admissible $\epsilon$-subgroup of that order, and consists of all $\epsilon$-sequences with $\epsilon_0$ equal to $+1$. Our general solution then shows that as a result there is but one $\delta$-subgroup of order $2^{m-2}$ for $m$ even, two for $m$ odd.

Actually, the equations of §10 for the $m$-adic operation on $\delta$-sequences directly show that we always have the subgroup of order $2^{m-2}$ consisting of all $\delta$-sequences with $\delta_0=+1$, and for $m$ odd also the subgroup of order $2^{m-2}$ consisting of all $\delta$-sequences with $\delta_0=-1$. Since the complete $m$-adic $\delta$-group is semi-abelian, all of its subgroups are semi-invariant. It is then of interest to note that the above one, or two, subgroups of order $2^{m-2}$ are its only invariant subgroups. In fact, our formula for the transform of one $\delta$-sequence by an-

other shows that $\delta_0$ is always thus left invariant; and it also shows that a $\delta$-sequence can always be found which transforms a given $\delta$-sequence into any other with the same $\delta_0$.

These results are immediately applicable to the corresponding alternating groups, assuming $n>1$. There are thus always $2^{m-2}$ alternating groups with substitutions forming one of the $2^{m-1}$ classes of §10 and, for $m>2$, $2^{m-2}$ alternating groups with substitutions forming two such classes. Passing by the general solution, we note that the conditions $\delta_0=+1$, and $\delta_0=-1$, correspond to an $m$-adic substitution considered as an ordinary substitution being positive, or negative. Hence, the only alternating groups invariant under the symmetric group are the alternating group of all positive substitutions, and, for $m$ odd, also the alternating group of all negative substitutions. On the other hand, every alternating group is a semi-invariant subgroup of the symmetric group.

The last observation restricts the possible simplicity of $m$-adic alternating groups. Regarding the nonexistence of a quotient group of lower order than itself as the distinguishing mark of an ordinary simple group, we are led to define a *simple* $m$-group as one whose associated group has no subgroup other than the identity invariant under the $m$-group. It follows that for $n>2$ only alternating groups corresponding to first order $\delta$-subgroups can be simple. For in any other case, $(+1, +1, \cdots, +1)$, the identity of the associated $\epsilon$-subgroup, is a subgroup thereof invariant under the $\delta$-subgroup. Hence the elements of the associated group of the alternating group with $\epsilon$-sequence $(+1, +1, \cdots, +1)$ then constitute a subgroup of the associated group invariant under the alternating group. We now proceed to show, on the strength of the corresponding result for ordinary groups, that when $n>4$ every alternating group $H$ corresponding to a first order $\delta$-subgroup is a simple. Since the associated $\epsilon$-subgroup has but the sole $\epsilon$-sequence $(+1, +1, \cdots, +1)$, the associated ordinary group $H_0$ of the alternating group $H$ consists of all elements $t=t't''\cdots t^{(m-1)}$ where $t^{(i)}$ is any positive substitution on the letters of $\Gamma_i$, and is thus the direct product of the ordinary alternating groups $A_1, A_2, \cdots, A_{m-1}$ on the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ respectively. Let then $K_0$ be any subgroup of $H_0$ invariant under $H$. If there could be more than one $t$ in $K_0$ with the same components $t', t'', \cdots, t^{(m-2)}$, then there would be more than one $t$ in $K_0$ with each component $t', t'', \cdots, t^{(m-2)}$ the identity. Now these $t$'s must constitute a subgroup of $K_0$, and this subgroup will be invariant under $H_0$ as a consequence of the invariance of $K_0$ under $H_0$. The corresponding $t^{(m-1)}$'s must then constitute an invariant subgroup of $A_{m-1}$, if not $A_{m-1}$ itself. Under the present supposition the last would be true; for with $n>4$, the alternating group $A_{m-1}$ is simple. But then $K_0$ would coincide with $H_0$, instead of being a subgroup of $H_0$. For, $K_0$ being invariant under any $s$ in $H$, if we transform the above elements of $K_0$ by $s, s^2, \cdots, s^{(m-2)}$, we would have in $K_0$ every element of $H_0$ any $m-2$ of whose components are the identity; and the

products of these elements constitute $H_0$. We have therefore proved that an element $t=t't''\cdots t^{(m-1)}$ of $K_0$ is uniquely determined by its first $m-2$ components. If then we transform $t$ by any element of $H_0$ the first $m-2$ of whose components are the identity, the first $m-2$ components of $t$, and hence $t$ itself, will be unchanged. $t^{(m-1)}$ is then always an invariant element of $A_{m-1}$, and, again with $n>4$, can only be the identity. The same argument would show each component of an element of $K_0$ to be the identity, so that $K_0$ is the identity.

We have therefore proved that *for $n>4$ the $2^{m-2}$ $m$-adic alternating groups of degree $n$ corresponding to first order $\delta$-subgroups are simple, the others not.* For $n=4$ no $m$-adic alternating group is simple, since we can let $K_0$ be the direct product of the axial groups on the letters of the several $\Gamma$'s. Again, for $n=3$, no $m$-adic alternating group is simple for any $m>2$. The preceding argument breaks down at the one point where the invariance of $t^{(m-1)}$ under $A_{m-1}$ is used to prove $t^{(m-1)}$ the identity. $K_0$ may now be the third order group obtained from the simple isomorphism between $A_1, A_2, \cdots, A_{m-1}$ that results when $A_i$ is transformed into $A_{i+1}$ by a fixed element $s$ of $H$. Finally, when $n=2$, the very first step of our argument breaks down. The $m$-adic alternating groups can now be identified with the $\delta$-subgroups themselves. The simple $\delta$-subgroups are those whose associated $\epsilon$-subgroups have no admissible $\epsilon$-subgroup for subgroup other than the identity. Hence, in terms of the above general determination of admissible $\epsilon$-subgroups, the simple $\delta$-subgroups are those whose associated $\epsilon$-subgroups have $(x^{m-1}+1)/\tau(x)$ prime.

13. **Transitive $m$-adic substitution groups.** Since an $m$-adic substitution group $G$ can carry the letters of $\Gamma_i$ only into those of $\Gamma_{i+1}$, we are led to define a *transitive* $m$-adic group $G$ as one whose substitutions will carry each letter of each $\Gamma$ into every letter of the succeeding $\Gamma$. Clearly, the $m$-adic symmetric group of arbitrary degree $n$, and the $m$-adic alternating groups of degree $n>2$ are then transitive. Our analysis in the next section shows that $G$ will be transitive if the above condition is true for any one $\Gamma$, and indeed for any one letter of a $\Gamma$, i.e., if the substitutions of $G$ carry one letter of one $\Gamma$ into every letter of the succeeding $\Gamma$, the same is true of every letter of every $\Gamma$, and G is transitive.

It is readily proved that the containing 2-group $G^*$ of a transitive $m$-group $G$ is transitive. In fact, let $a_{ij}$ and $a_{(i+k)j'}$ be any two letters of the $\Gamma$'s. Considering $i+k$ reduced modulo $m-1$, we may assume $1\leqq k\leqq m-1$. We need not consider $k=1$. For $k>1$ let $r$ be any $(k-1)$-ad. It will carry $a_{ij}$ into some $a_{(i+k-1)j''}$. Some $s$ will carry $a_{(i+k-1)j''}$ into $a_{(i+k)j'}$. Hence the $k$-ad $rs$, which is a substitution in $G^*$, carries $a_{ij}$ into $a_{(i+k)j'}$ as required. Conversely, if $G^*$ is transitive, a substitution in $G^*$ carrying $a_{ij}$ into $a_{(i+1)j'}$ belongs to $G$, and hence $G$ is transitive.

In terms of $G_0$, the associated 2-group of $G$, we likewise see that $G$ is transitive when and only when the substitutions of $G_0$ carry each letter of each $\Gamma$

into every letter of the same $\Gamma$. Recalling our definition of the associated constituent groups $G_0'$, $G_0''$, $\cdots$, $G_0^{(m-1)}$ of $G$, we thus have that $G$ is transitive when and only when its associated constituent groups are transitive. As the latter are conjugate, it follows that $G$ is transitive if any one of its associated constituent groups is known to be transitive.

Let $(G_0)_{ij}$ be the subgroup of $G_0$ which consists of all substitutions in $G_0$ that carry $a_{ij}$ into itself. If we expand $G$ in right cosets as regards $(G_0)_{ij}$, the members of each single coset carry $a_{ij}$ into one and the same letter of $\Gamma_{i+1}$. Also, if $s_1$ and $s_2$ of $G$ carry $a_{ij}$ into the same letter, $s_1 s_2^{-1}$ will be in $(G_0)_{ij}$, so that $s_1$ and $s_2$ are in the same coset. Each coset therefore consists of all the substitutions of $G$ carrying $a_{ij}$ into the corresponding letter. If then $G$ is transitive of degree $n$, there will be exactly $n$ such cosets, one for each letter of $\Gamma_{i+1}$. Hence, the order of $(G_0)_{ij}$ is equal to $g/n$ if $G$ is a transitive group of order $g$, and degree $n$. *The order of a transitive $m$-adic substitution group is therefore a multiple of its degree.* Furthermore, *the number of substitutions of a transitive $m$-adic substitution group that carry any letter $a_{ij}$ into any letter $a_{(i+1)k}$ is, for all such pairs of letters, equal to the order of the group divided by its degree.*

Since for $m>2$ an $m$-adic substitution group cannot carry a letter into itself, we have to turn to the associated group of a transitive $m$-adic substitution group for an average number of letters theorem. For this purpose we write the substitutions of the associated group in standard cycle form. Observe first that each associated constituent group $G_0^{(i)}$ being transitive, and of degree $n$, the average number of its letters appearing in its substitutions is $n-1$. Fixing our attention on $G_0^{(i)}$, we consider the subgroup $H_0^{(i)}$ of $G_0$ consisting of all the substitutions of $G_0$ whose component in $G_0^{(i)}$ is the identity of $G_0^{(i)}$. If we expand $G_0$ in cosets as regards $H_0^{(i)}$, each coset is easily seen to consist of all the substitutions of $G_0$ which have a fixed component in $G_0^{(i)}$. Each substitution of $G_0^{(i)}$ therefore occurs the same number of times in $G_0$. It follows that *the average number of letters of each $\Gamma_i$ occurring in the substitutions of the associated group of a transitive group of degree $n$ is $n-1$.* This is our strongest result. From it, or from our discussion of $(G_0)_{ij}$, we also have that *the average number of all letters appearing in the substitutions of the associated group of a transitive $m$-adic substitution group of degree $n$ is $(m-1)(n-1)$.* This may also be seen as follows. Since the containing group $G^*$ of the transitive $m$-adic group $G$ is transitive, and of degree $(m-1)n$, the average number of letters in its substitutions is $(m-1)n-1$. The total number of letters in its substitutions is then $(m-1)g[(m-1)n-1]$, $g$ being the order of $G$. Of the $(m-1)g$ substitutions in $G^*$, the $(m-2)g$ substitutions not in $G_0$ each has its full complement of $(m-1)n$ letters. The total number of letters in the substitutions of $G_0$ is thus the remaining $(m-1)(n-1)g$ letters, whence the result.

14. **Intransitive $m$-adic substitution groups.** Let $G$ be any $m$-adic substitution group on the letters of $\Gamma_1$, $\Gamma_2$, $\cdots$, $\Gamma_{m-1}$, and let $\Gamma_1'$, $\Gamma_2'$, $\cdots$, $\Gamma_{m-1}'$ be the subclasses of the letters of $\Gamma_1$, $\Gamma_2$, $\cdots$, $\Gamma_{m-1}$ respectively into which $a_{(m-1)1}$

is carried by the elements, dyads, $\cdots$, $(m-1)$-ads of $G$. If $s$ is any substitution in $G$, then as $r$ ranges through the $i$-ads of $G$, $rs$ ranges through the $(i+1)$-ads of $G$. Hence $s$ transforms the letters of $\Gamma_i'$ in 1-1 fashion into the letters of $\Gamma_{i+1}'$ for each $i$, and thus determines an $m$-adic substitution on $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$. Furthermore, if $a_{ij}$ and $a_{(i+1)k}$ are any two letters of $\Gamma_i'$ and $\Gamma_{i+1}'$ respectively, some $s$ of $G$ will carry $a_{ij}$ into $a_{(i+1)k}$. For some $i$-ad $r_1$ of $G$ carries $a_{(m-1)1}$ into $a_{ij}$, and some $(i+1)$-ad $r_2$ of $G$ carries $a_{(m-1)1}$ into $a_{(i+1)k}$. Hence element $r_1^{-1}r_2$ of $G$ carries $a_{ij}$ into $a_{(i+1)k}$. The $m$-adic substitutions on $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$ obtained from all the substitutions of $G$ therefore constitute a transitive $m$-adic substitution group on $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$. If $G$ is transitive, this group is identical with $G$. If $G$ is not transitive, we may call this group a *transitive constituent group* of the *intransitive group* $G$. In that case, by accounting for all the letters of $\Gamma_{m-1}$, we obtain a number of transitive constituent groups of $G$ such that every substitution in $G$ is the product of a selection of substitutions from the transitive constituent groups of $G$.

This result can also be obtained by analysing the containing group $G^*$ of $G$, whence it also appears that the transitive constituent groups of $G^*$ are the containing groups of the transitive constituent groups of $G$.

The direct product and simple isomorphism methods for obtaining intransitive ordinary groups admit of immediate extension to $m$-adic groups. In the latter case, let $G_1$ and $G_2$ be the same $m$-adic substitution group written on different letters. If the letters of $G_1$ form the sets $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$, of $G_2$, $\Gamma_1'', \Gamma_2'', \cdots, \Gamma_{m-1}''$, the products of corresponding substitutions in $G_1$ and $G_2$ will be $m$-adic substitutions on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, where $\Gamma_i$ consists of all the letters of $\Gamma_i'$ and $\Gamma_i''$. Clearly, an $m$-adic substitution group is thus formed simply isomorphic with $G_1$ and $G_2$, but of twice their degree. Similarly for any number of groups obtained by writing a given $m$-adic substitution group on different letters.

As for the direct product method, let $H_1$ and $H_2$ be $m$-adic substitution groups on $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$ and $\Gamma_1'', \Gamma_2'', \cdots, \Gamma_{m-1}''$ with all letters distinct. As before, form $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$. Then, if $s_i'$ and $s_j''$ be any two substitutions in $H_1$ and $H_2$ respectively, $s_i's_j''$ will be an $m$-adic substitution on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$. The set of all such products clearly constitutes an $m$-adic substitution group $G$ of order equal to the product of the orders of $H_1$ and $H_2$, and degree equal to the sum of their degrees. When $m=2$, the existence of an identical element, coupled with the ambiguity of the cycle notation, allows us to consider $H_1$ and $H_2$ subgroups of $G$ which can then be said to be generated by $H_1$ and $H_2$. When $m>2$ this is no longer possible. We shall therefore refrain from calling $G$ the direct product of $H_1$ and $H_2$, reserving that phrase for a more special concept found useful in the sequel([51]).

15. **Substitutions which are commutative with each of the substitutions**

([51]) In fact, while $G$ is an $m$-adic substitution group, the $m$-group "generated" by $H_1$ and $H_2$ is, for $m>2$, a hybrid sort of an affair of order $m-1$ times the order of $G$. On the other hand,

**of a transitive $m$-adic substitution group.** Recalling that the order of a transitive $m$-adic substitution group is a multiple of its degree, we may most briefly define a *regular* $m$-adic substitution group as a transitive $m$-adic substitution group whose order is equal to its degree. In view of the corresponding general result for transitive groups, this is equivalent to defining a regular $m$-adic substitution group as an $m$-adic substitution group, which, for any pair of letters in consecutive $\Gamma$'s, has one and only one substitution carrying the first letter into the second. Other transitive group results, coupled with the order criterion of regularity, show that an $m$-adic substitution group is regular if and only if its containing group is regular; also, if and only if its associated constituent groups are regular. The orders of the associated group, and the associated constituent groups, then being the same, it also follows that a regular $m$-adic substitution group is a transitive group whose associated group has no substitutions other than the identity omitting a letter. Regular $m$-adic substitution groups play the same role in polyadic as in ordinary group theory, since we later show that every finite abstract $m$-adic group can be represented as a regular $m$-adic substitution group.

According to a theorem of Jordan, the substitutions on the letters of a regular group commutative with each of its substitutions constitute a group conjugate to the regular group and known as its conjoint. We extend this theorem to a regular $m$-adic substitution group $G$ by directly applying it to the containing group $G^*$, which is known to be regular. In fact, since $G^*$ is generated by $G$, the ordinary substitutions on the letters of $G$ commutative with each of its substitutions are the same as those commutative with each of the substitutions of $G^*$. Hence, to find the $m$-adic substitutions on the letters of $G$ commutative which each of its substitutions we need merely pick out those substitutions in the conjoint of $G^*$ which are $m$-adic substitutions.

To do this we must re-examine the standard proof of Jordan's theorem. In this proof the letters on which the given regular group is written are replaced by the symbols $s_i$ used for the substitutions in the group. Then, in the simple isomorphism established between the group and its conjoint, the $j$th substitution of the given group in its new form replaces each symbol $s_i$ by the symbol for the substitution $s_i s_j$, while the corresponding substitution in the conjoint replaces each $s_i$ by $s_j s_i$. Finally, it is shown that the given group is transformed into its simply isomorphic conjoint by the substitution which carries the second letter of each substitution of the given group into the second letter of the corresponding substitution of the conjoint when all the substitutions([52]) are written in cycle form with the same first letter.

---

if either $H_1$ or $H_2$ has a first order element, $G$ will contain a subgroup $H_2'$ or $H_1'$ simply isomorphic to $H_2$ or $H_1$ respectively; and if both $H_1$ and $H_2$ possess an invariant first order element, the corresponding $H_2'$ and $H_1'$ will generate $G$, and $G$ will then be the direct product of $H_1'$ and $H_2'$ in the sense later defined (§25).

([52]) All except the identity, that is. Likewise later in the proof.

For our purpose it suffices to determine the nature of this substitution in the case of the regular group $G^*$. With $G$ a regular $m$-adic substitution group on the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, the substitutions of $G^*$ can be grouped into corresponding classes $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$ according as they are elements, dyads, $\cdots$, $(m-1)$-ads of $G$. When $G^*$ is rewritten in accordance with the proof of Jordan's theorem, $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$ take the place of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$. In fact, if $s_i$ is a $k$-ad in $G^*$, $s_j$ an $l$-ad, $s_i s_j$ is a $(k+l)$-ad. Hence, in the above description applied to $G^*$, if $s_j$ is an $l$-ad, the $j$th substitution of $G^*$ transforms each $\Gamma_k'$ into $\Gamma_{k+l}'$, and hence is an $l$-ad on $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$. But the same reasoning shows the corresponding substitution in the conjoint of $G^*$ also to be an $l$-ad on $\Gamma_1', \Gamma_2', \cdots, \Gamma_{m-1}'$. Or, returning to $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, we have that in the simple isomorphism between $G^*$ and its conjoint the correspondant of an $i$-ad in $G^*$ is an $i$-ad. If then we write the substitutions of $G^*$ and its conjoint with the same first letter, say $a_{11}$, if the corresponding substitutions in $G^*$ and its conjoint are both $i$-ads, their second letters will both be in $\Gamma_{i+1}$. Hence, the substitution which transforms $G^*$ into its conjoint transforms each $\Gamma$ into itself, and consequently is an $(m-1)$-ad on the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$.

Our result now immediately follows. The $(m-1)$-ad will transform only the $m$-adic substitutions of $G^*$ into $m$-adic substitutions. Hence the $m$-adic substitutions in the conjoint of $G^*$ are the transforms of the $m$-adic substitutions in $G^*$ by the $(m-1)$-ad, i.e., the transforms of the substitutions in $G$. Since the transform of an $m$-adic group is a simply isomorphic $m$-adic group, we thus have the following extension of Jordan's theorem. *The $m$-adic substitutions on the sequence of $\Gamma$'s of a regular $m$-adic substitution group commutative with all the substitutions of the group constitute a regular $m$-adic substitution group of the same order, and this group is the transform of the given group by an $(m-1)$-ad of $m$-adic substitutions.* Clearly, the relationship between the two groups is a reciprocal one, and we may call each the *conjoint* of the other. Either directly, or as a consequence of a later general result on transforms, it may be verified that each group can be transformed into the other by an $m$-adic substitution, and hence, according to any $m$-adic definition, are conjugate.

We further have, as a result of the above discussion, that every ordinary substitution on the letters of a regular $m$-adic substitution group of degree $n$ commutative with all the substitutions of the group are polyads of $m$-adic substitutions, there being $n$ such $i$-ads for every $i$. Together they of course constitute the conjoint of the containing group of the given group; and this conjoint is now seen to be the containing group of the conjoint of the given group.

In passing from regular $m$-adic substitution groups to arbitrary transitive $m$-adic substitution groups for the purpose of extending Kuhn's theorem to $m$-adic groups, we shall adopt the viewpoint of the last paragraph, and seek

all substitutions on the letters of the transitive $m$-adic group commutative with each of its substitutions; for now $m$-adic substitutions of this kind will exist only if the given group satisfies a special condition. If $G$ is a transitive $m$-adic substitution group, $G^*$ is transitive. Again, the substitutions on the letters of $G$ commutative with every substitution in $G$ are the substitutions on the letters of $G^*$ commutative with each of its substitutions, and hence can be found by applying Kuhn's theorem to $G^*$. As before, we assume all substitutions written in cycle form.

According to Kuhn's generalization of Jordan's theorem the number of substitutions on the letters of $G^*$ commutative with each of its substitutions is the same as the number of letters omitted in all substitutions of $G^*$ which omit a given letter. Actually, such substitutions will be in $G_0$, the associated group of $G$. Let $\{a_{ij}\}$ designate the set of letters omitted by all substitutions of $G^*$ that omit $a_{ij}$. Since $G^*$ is transitive, it follows that if $a_{i_1j_1}$ is in $\{a_{ij}\}$, then $\{a_{i_1j_1}\} = \{a_{ij}\}$, and a substitution $r$ of $G^*$, carrying $a_{ij}$ into $a_{i_1j_1}$, carries the set of letters $\{a_{ij}\}$ into itself. But $r$ carries all the letters of $\Gamma_i$ into all those of $\Gamma_{i_1}$, and hence all the letters of $\{a_{ij}\}$ that are in $\Gamma_i$ into all the letters of $\{a_{ij}\}$ that are in $\Gamma_{i_1}$. Hence, if there are $\alpha$ letters of $\{a_{ij}\}$ in one $\Gamma$, there are $\alpha$ letters of $\{a_{ij}\}$ in every $\Gamma$ that has at least one of them. Now with the $\Gamma$'s arranged in a cycle, let $\delta$ be the least difference between the subscripts of consecutive $\Gamma$'s that have letters of $\{a_{ij}\}$. Then some $\delta$-ad $r$ in $G^*$ will transform the set $\{a_{ij}\}$ into itself. As $r$ will then carry the letters of $\{a_{ij}\}$ which are in any $\Gamma_i$ into letters of $\{a_{ij}\}$ which are in $\Gamma_{i+\delta}$, it follows that the $\Gamma$'s having letters in $\{a_{ij}\}$ have subscripts which are in arithmetic progression, with the common difference, indeed, a divisor of $m-1$. Finally, the known properties of transitive groups show the different sets $\{a_{ij}\}$ to be mutually exclusive, and transformable into each other by the substitutions of $G^*$. It follows that the numbers $\alpha$ and $\delta$ are the same for all such sets; and since together they exhaust the letters of $G^*$, that $\alpha$ is a divisor of $n$. Hence the following result. *If $G$ is a transitive $m$-adic substitution group of degree $n$, then the number of letters omitted by all substitutions of the containing group $G^*$ that omit a given letter is of the form $\kappa\alpha$, where $\kappa$ is a divisor of $m-1$, $\alpha$ a divisor of $n$; furthermore, there are $\alpha$ of these letters in every $\Gamma$ that has at least one, the subscripts of these $\Gamma$'s forming an arithmetic progression.*

According to the proof of Kuhn's theorem the resulting $\kappa\alpha$ substitutions on the letters of $G^*$ commutative with each of its substitutions are obtained as follows. Let $H_{11}$ be the subgroup of $G^*$ composed of the substitutions of $G^*$ which leave the set of letters $\{a_{11}\}$ unchanged, and let $C_{11}$ be the conjoint of the regular group $K_{11}$, on the letters $\{a_{11}\}$, formed by the components on those letters of the substitutions in $H_{11}$. For each substitution in $C_{11}$, form the product of all the distinct transforms of that substitution under $G^*$. These products are the $\kappa\alpha$ substitutions on the letters of $G^*$ commutative with each of its substitutions. According to our distribution result

for the set of letters $\{a_{11}\}$, there are $\alpha$ of these letters in each of the $\kappa$ $\Gamma$'s, $\Gamma_1, \Gamma_{1+\delta}, \cdots, \Gamma_{1+(\kappa-1)\delta}$, where $\kappa\delta = m-1$. Clearly, the substitutions of $H_{11}$ can only be $i$-ads with $i = \delta, 2\delta, \cdots, \kappa\delta$. Since $K_{11}$ is regular on the letters $\{a_{11}\}$, it will have, for each of the above $i$'s, $\alpha$ substitutions which are components of $i$-ads in $H_{11}$. Our proof of the extended Jordan theorem applies sufficiently to the relationship between $K_{11}$ and its conjoint $C_{11}$ to show that $C_{11}$ also consists of $\alpha$ "components of $i$-ads" for each $i = \delta, 2\delta, \cdots, \kappa\delta$. Now when a substitution of $C_{11}$ is transformed by the substitutions of $G^*$, the set of letters $\{a_{11}\}$ will go over into all the mutually exclusive distinct sets $\{a_{ij}\}$, there being one and only one distinct transform of the substitution of $C_{11}$ for each set $\{a_{ij}\}$. If the substitution in question is a component of an $i$-ad, each transform will also be a component of an $i$-ad. As the sets $\{a_{ij}\}$ are mutually exclusive, and exhaust the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, the product of these transforms will exactly constitute an $i$-ad. We thus have the following extension of Kuhn's theorem. *The only substitutions on the letters of the $\Gamma$'s of a transitive $m$-adic substitution group commutative with each of its substitutions are polyads of $m$-adic substitutions on the same sequence of $\Gamma$'s; in the notation of the distribution theorem, if $\delta = (m-1)/\kappa$, these polyads can only be $i$-ads with $i = \delta, 2\delta, \cdots, \kappa\delta$, there being exactly $\alpha$ such $i$-ads for each admissible $i$.*

In particular, if we restrict our attention to $m$-adic substitutions, we have the following result. *The necessary and sufficient condition that there be at least one $m$-adic substitution on the sequence of $\Gamma$'s of a transitive $m$-adic substitution group commutative with each of its substitutions is that the subgroup of the associated group consisting of all its substitutions omitting a given letter in one $\Gamma$ omits a fixed letter in the following $\Gamma$; if then that subgroup omits exactly $\alpha$ letters from one $\Gamma$, it will omit $\alpha$ letters from every $\Gamma$, and there will be exactly $\alpha$ such $m$-adic substitutions.*

16. **Holomorphs of a regular $m$-adic substitution group.** The concept of holomorph of a regular group admits both of an immediate extension to regular $m$-adic substitution groups, as well as of a further generalization peculiar to polyadic theory. For the immediate extension, let $G$ be a regular $m$-adic substitution group of order $n$ on the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$. Then all the $m$-adic substitutions on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ which transform $G$ into itself constitute an $m$-adic substitution group of degree $n$ which we shall call the *principal holomorph* of $G$. Clearly, the principal holomorph of $G$ not only contains $G$, but also the conjoint of $G$. Since the transforms of commutative substitutions are commutative, it follows that the principal holomorph of $G$ is in fact also the principal holomorph of its conjoint.

If $K$ is the principal holomorph of $G$, then $(K_0)_{11}$, the subgroup of the associated group $K_0$ of $K$ consisting of all the substitutions of $K_0$ omitting $a_{11}$, may be identified as the *group of isomorphisms* of $G$. That is, $(K_0)_{11}$ transforms $G$ into all of its possible automorphisms, each automorphism being given by but one substitution of $(K_0)_{11}$. In fact, the argument used in extending

Jordan's theorem shows that the substitutions of one of two simply isomorphic regular $m$-adic substitution groups on the same sequence of $\Gamma$'s can be transformed into the corresponding substitutions of the other by an $(m-1)$-ad which omits, say, $a_{11}$. Hence, every automorphism of $G$ can be obtained by transforming $G$ by the substitutions in $(K_0)_{11}$. Furthermore, if two distinct substitutions of $(K_0)_{11}$ yielded the same automorphism of $G$, a substitution of $(K_0)_{11}$ other than the identity would transform each member of $G$ into itself. But this substitution would have to be in the associated group of the conjoint of $G$, and, as this conjoint is regular, the substitution in question, which omits $a_{11}$, could only be the identity.

We can now prove, as in the ordinary case, that *the order of the principal holomorph of a regular m-adic substitution group is equal to the product of the order of the group and the order of its group of isomorphisms.* In fact, if $\overline{G}$ is the conjoint of the regular group $G$, $K$ its holomorph, by expanding $K$ in cosets as regards its invariant subgroup $\overline{G}$, we see that the substitutions of $K$ transform $G$ in $k/n$ different ways, $k$ being the order of $K$. But $K$ as well as $(K_0)_{11}$ must transform $G$ into all of its possible automorphisms. For if $s$ is in $K$, $t$ in $(K_0)_{11}$, as $t$ runs through $(K_0)_{11}$ giving all the automorphisms of $G$, $ts$ in $K$ yields an equal number of automorphisms of $G$. Hence the order of $(K_0)_{11}$ is $k/n$, whence the above result.

To illustrate this result, consider the cyclic triadic group of degree and order two generated by the triadic substitution $s_1=(a_{11}a_{21}a_{12}a_{22})$ given in cycle form. The letters of $\Gamma_1$ are $a_{11}$, $a_{12}$, of $\Gamma_2$, $a_{21}$, $a_{22}$. The sole other triadic substitution on $\Gamma_1$, $\Gamma_2$ generated by $s_1$ is $s_2=(a_{11}a_{22}a_{12}a_{21})$, so that the group is seen to be regular. $s_2$ also is a generator of the group, whence it follows that the group admits exactly two automorphisms. Hence the order of its principal holomorph is four. We find directly that $s_3=(a_{11}a_{21})(a_{12}a_{22})$ and $s_4=(a_{11}a_{22})(a_{12}a_{21})$ interchange $s_1$ and $s_2$, so that the principal holomorph consists of $s_1$, $s_2$, $s_3$, $s_4$. It is actually the entire triadic symmetric group of degree two. This example serves to answer the question whether some subgroup of the principal holomorph itself, instead of its associated ordinary group, can be identified with the group of isomorphisms of the given group. The answer in the present instance is no. For such a subgroup would have to possess as element $s_1$ or $s_2$ to yield the identical automorphism, but would then have for elements both $s_1$ and $s_2$, each yielding that one automorphism.

The immediate extension of the concept of complete group to $m$-adic groups turns out to be rather trivial. Defining an $m$-adic group $G$ to be *complete in the narrow sense* if its own elements transform it in 1-1 fashion into all of its possible automorphisms, we obtain the following result. *An m-group is complete in the narrow sense when and only when it is reducible to a complete ordinary group.* In fact, its sole element yielding the identical automorphism must be of first order, and invariant under the group—hence the reducibility.

The rest of the theorem follows from the easily demonstrated facts that if $G$ is reducible to $G'$, every automorphism of one group is also an automorphism of the other, while the automorphisms induced by any element of either is the same for both. Since $G$ can have but one invariant element, it also follows that *the net of derived groups of an m-adic group complete in the narrow sense consists of a single complete 2-group, and its extensions, which are then also complete in the narrow sense.* If $G$ is regular, and complete in the narrow sense, we may use its elements as multipliers in the expansion of $K$ in cosets as regards $\overline{G}$. We shall express this fact by saying that *the principal holomorph of an m-group complete in the narrow sense is the direct product of the group and its conjoint.* A precise abstract definition of this rather narrow concept of direct product will be given in §25.

We do not obtain a less restrictive concept of completeness by asking that the elements of $G_0$ transform $G$ into all of its possible automorphisms in 1-1 fashion; for the coset theorem shows that $G$ and $G_0$ transform $G$ according to the same number of distinct automorphisms. We therefore define $G$ to be *complete in the wide sense* if the elements of its abstract containing group $G^*$ transform it in 1-1 fashion according to all of its possible automorphisms. Since only the identity of $G^*$ is now invariant under $G$, it follows that an $m$-group complete in the wide sense is irreducible. If this $m$-group $G$ is of order $g$, and is expressed as a regular $m$-adic substitution group, the order of its principal holomorph $K$ will be $(m-1)g^2$. We now turn to the containing groups for a direct product theorem, and easily find that *the containing group of the principal holomorph of an m-group complete in the wide sense is the direct product of the containing groups of the group and its conjoint.*

Actually, a type of completeness can be defined for each divisor $k$ of $m-1$, an $m$-group $G$ being said to be complete in the $k$-sense if it admits some containing group of index $k$ whose elements yield in 1-1 fashion all the automorphisms of $G$. We then have that an $m$-group is complete in the $k$-sense when and only when it is reducible to a $(k+1)$-group complete in the wide sense. Furthermore, the net of derived groups of an $m$-group complete in the $k$-sense consists of a single $(k+1)$-group complete in the wide sense, and its extensions. With $G$ written as a regular $m$-adic substitution group, its principal holomorph will of course be of order $kg^2$. But there does not then seem to be a direct product theorem in terms of groups.

We turn now to the purely $m$-adic generalization of holomorph. In ordinary group theory, due to the presence of the identity, if all of the elements of a group $H$ transform a group $G$ into one and the same group, that group must be $G$ itself. Hence if $G$ is a regular substitution group, $H$ a substitution group on the letters of $G$, $H$ will be the holomorph of $G$, or a subgroup thereof. This need not be so for $m$-adic groups with $m>2$. Let then $G$ be a regular $m$-adic substitution group with $m>2$, $H$ an $m$-adic substitution group on the

sequence of $\Gamma$'s of $G$ such that all of the substitutions of $H$ transform $G$ into one and the same group $G''$([53]). It follows that all of the substitutions of $H$ transform $G''$ into one and the same group $G'''$, and so on. Since the $m$-ads of $H$ must transform $G$ as do its elements, it follows that there will be a cycle of $\mu-1$ distinct, though not necessarily mutually exclusive, $m$-adic groups $(G', G'', \cdots, G^{(\mu-1)})$, such that $G'=G$, $\mu-1$ is a divisor of $m-1$, and all the elements of $H$ transform each $G$ into the cyclically following $G$. Now all the $m$-adic substitutions on the sequence of $\Gamma$'s of $G$ which transform $G'\to G''\to \cdots \to G^{(\mu-1)}\to G$ constitute an $m$-adic substitution group $K$ containing $H$. We shall then call $K$ *a holomorph* of $G$, and *the holomorph* of the cycle $(G', G'', \cdots, G^{(\mu-1)})$. When $\mu-1=1$, $K$ becomes the principal holomorph of $G$.

Given the regular $G$, an $m$-adic substitution $s$ on the sequence of $\Gamma$'s of $G$ will be said to be *holomorphic* if it belongs to some holomorph of $G$. We then readily see that *the necessary and sufficient condition that $s$ be holomorphic is that $s^{m-1}$ is in the associated group of the principal holomorph of $G$.* For that associated group consists of all the $(m-1)$-ads on the sequence of $\Gamma$'s of $G$ which transform $G$ into itself. The necessity of the condition then follows from the fact that $s^m$ must transform $G$ into the same group that $s$ does, the sufficiency from the fact that all the elements of the cyclic $m$-group generated by $s$ will then transform $G$ into one and the same group. In particular, the $(n!)^{m-2}$ first order substitutions of degree $n$ are all holomorphic for the regular $G$ of degree $n$. Hence, when the order of the principal holomorph of $G$ is less than $(n!)^{m-2}$, as must be so, for example, in the case of cyclic $m$-groups of order greater than three, we are assured of the existence of a holomorph other than the principal holomorph. Clearly, any element $s$ of a holomorph of $G$ determines the corresponding cycle $(G', G'', \cdots, G^{(\mu-1)})$, and hence the holomorph. It follows that all the holomorphs of a given $G$ are mutually exclusive.

Our next result shows that the order of any holomorph of $G$ is no greater than that of the principal holomorph of $G$. In fact, let $K', K'', \cdots, K^{(\mu-1)}$ be the principal holomorphs of $G', G'', \cdots, G^{(\mu-1)}$, $K$ the holomorph of the cycle $(G', G'', \cdots, G^{(\mu-1)})$. By writing an element $t$ of $K_0$ as the product of $m-1$ elements of $K$, we see that $t$ must leave each $G^{(i)}$ invariant, and hence be in each $K_0^{(i)}$. Conversely, if $t$ is in each $K_0^{(i)}$, it will transform each $G^{(i)}$ into itself. If then $s$ is in $K$, $ts$ will also be in $K$, so that $t$ must be in $K_0$. That is, *the associated group of the holomorph of $(G', G'', \cdots, G^{(\mu-1)})$ is the logical product of the associated groups of the principal holomorphs of $G', G'', \cdots, G^{(\mu-1)}$.* It is readily verified that an $s$ in $K$ actually transforms $K'\to K''\to \cdots \to K^{(\mu-1)}\to K'$, and hence also $K_0'\to K_0''\to \cdots \to K_0^{(\mu-1)}\to K_0'$. Hence, a subgroup of $K_0'$ invariant under $s$ must be contained in $K_0$. We thus have, in terms of $G$ alone, *the associated group of the holomorph of $G$ correspond-*

([53]) The reader will note the marked analogy with Corral's concept of a function pertaining to a brigade, that is, one carried into the same function by all the substitutions of the brigade.

*ing to a holomorphic s is the largest group or subgroup of the associated group of the principal holomorph of G invariant under s.*

On turning to an order theorem for these $m$-adic holomorphs, we observe first that *the holomorph of a cycle* $(G', G'', \cdots, G^{(\mu-1)})$ *is also the holomorph of the "conjoint cycle"* $(\overline{G}', \overline{G}'', \cdots, \overline{G}^{(\mu-1)})$. For, inasmuch as transforms of commutative substitutions are commutative, transforms of conjoint regular groups are conjoint. Hence, if $s$ transforms $G'\to G''\to \cdots \to G^{(\mu-1)}\to G'$, it must transform $\overline{G}'\to\overline{G}''\to \cdots \to\overline{G}^{(\mu-1)}\to\overline{G}'$, and conversely. Now let $K$ be the holomorph of the cycle $(G', G'', \cdots, G^{(\mu-1)})$. Each $s$ in $K$ transforms in 1-1 fashion the elements of $G'\to G''\to \cdots \to G^{(\mu-1)}\to G'$, and hence determines a $\mu$-adic substitution on the $\mu-1$ classes of elements $G', G'', \cdots, G^{(\mu-1)}$ which may be termed a $\mu$-adic automorphism of the cycle $(G', G'', \cdots, G^{(\mu-1)})$. The class of all such $\mu$-adic substitutions on $G', G'', \cdots, G^{(\mu-1)}$ obtained through substitutions in $K$ clearly constitutes an $m$-adic group which we shall term the *restricted m-adic group of isomorphisms* of the cycle $(G', G'', \cdots, G^{(\mu-1)})$, restricted, both by the possible narrowness of $K$, and by the fact that while an $m$-adic substitution will transform any one $G^{(i)}$ into $G^{(i+1)}$ according to any simple isomorphism, it need not be able to do this arbitrarily and simultaneously for each $i$. Now $s_1$ and $s_2$ of $K$ will yield the same $\mu$-adic automorphism of the cycle $(G', G'', \cdots, G^{(\mu-1)})$ when and only when the $(m-1)$-ad $s_2s_1^{-1}$ transforms each element of each $G^{(i)}$ into itself, and hence, when and only when $s_2s_1^{-1}$ is in $\overline{\overline{G}}_0=\overline{G}_0'\overline{G}_0''\cdots\overline{G}_0^{(\mu-1)}$(54). Note that $K_0$ consists of all $(m-1)$-ads which transform each $G^{(i)}$ into itself, and hence has $\overline{\overline{G}}_0$ for subgroup, one, indeed, invariant under $K$. By expanding $K$ in cosets as regards $\overline{\overline{G}}_0$, we then obtain the following result. *The order of the holomorph of* $(G', G'', \cdots, G^{(\mu-1)})$ *is the product of the order of the crosscut of the associated groups of the conjoints of* $G', G'', \cdots, G^{(\mu-1)}$ *and the order of the restricted m-adic group of isomorphisms of* $(G', G'', \cdots, G^{(\mu-1)})$.

This result is weaker than the result for the principal holomorph of $G$ in two ways. On the one hand, the order of $\overline{\overline{G}}_0$ replaces the order of $G$ itself. More significantly, in the case of the principal holomorph, we identified $(K_0)_{11}$ with the group of isomorphisms of $G$. Note that there both $K$ and $K_0$ yielded every possible automorphism of $G$. In the present case $K_0$ transforms each $G^{(i)}$ into itself, the distinct transformations being $(\mu-1)$-ads of $\mu$-adic substitutions on $G', G'', \cdots, G^{(\mu-1)}$, and constituting the associated group of the restricted $m$-adic group of isomorphisms of the cycle $(G', G'', \cdots, G^{(\mu-1)})$. If then we ask whether $(K_0)_{11}$ can be identified with this associated restricted group of isomorphisms, we find that while no two members of $(K_0)_{11}$ can transform the $G^{(i)}$'s in the same way, for $(K_0)_{11}$ to transform the $G$'s in every way that $K_0$ does, it is necessary and sufficient that $K_0$ carry $a_{11}$ into no other letters than does its subgroups $\overline{\overline{G}}_0$. We have not succeeded in answering the

(54) Product here is logical product.

question thus posed; and hence, whether $(K_0)_{11}$, or any other subgroup of $K_0$, can be identified as the associated restricted group of isomorphisms of the cycle $(G', G'', \cdots, G^{(\mu-1)})$ remains one of our unsolved problems[55].

17. **$m$-adic groups of $\mu$-adic substitutions.** The present extension of the concept of $m$-adic substitution group is indispensable for a self-contained theory of primitivity, our next topic. This extension has the advantage of including $m$-adic groups of ordinary substitutions in its scope. However, the fact that any abstract $m$-adic group can be represented as a regular $m$-adic substitution group is perhaps sufficient reason for our restricting the explicit study of this wider class of substitution groups to the next section.

Given a cycle of $\mu-1$ equivalent classes $\Gamma_1, \Gamma_2, \cdots, \Gamma_{\mu-1}$, not only will the product of $\mu$ $\mu$-adic substitutions on these $\Gamma$'s be a substitution of the same kind, but also the product of any $m$ such substitutions, provided $m$ is in the form $k(\mu-1)+1$. We are thus led to the concept of an $m$-adic group of $\mu$-adic substitutions, or $(m, \mu)$ *substitution group*, with $m$ and $\mu$ subject to the sole condition that $\mu-1$ *be a divisor of* $m-1$. We have already met this concept in the last section where the corresponding $\Gamma$'s, $G', G'', \cdots, G^{(\mu-1)}$, while distinct, were probably not necessarily mutually exclusive[56]. In what follows, for simplicity, as in our previous development, we shall assume the $\Gamma$'s to be mutually exclusive.

It is not difficult to review our previous work to see how much goes over to $(m, \mu)$ substitution groups. The chief failure turns out to be the extension of Jordan's theorem on regular groups. Particular mention must be made of the structure of the containing group of an $(m, \mu)$ group $G$. Letting, for simplicity, $G^*$ symbolize the containing ordinary group of $G$ generated by the elements of $G$, $G^*$ will now be of some index $k$ which is a divisor of $m-1$ and a multiple of $\mu-1$. We must now distinguish between $i$-ads of $G$ and $i$-ads in $G^*$, the former being the products of any $i$ substitutions in $G$, the latter all products in $G^*$ of $i$ $\mu$-adic substitutions. In particular, there will be $k/(\mu-1)$ cosets in $G^*$ consisting of $(\mu-1)$-ads, one and only one of these cosets being $G_0$.

In connection with the next section, the extension of the concept of transitivity to $(m, \mu)$ substitution groups is of most importance. Actually, our definition of transitivity as applied to $m$-adic substitution groups can be restated

---

[55] The above theory of $m$-adic holomorphs can be paraphrased for ordinary groups. Thus, if $s$ is a substitution on the letters of an ordinary regular group $G'$, but not in the holomorph of $G'$, and if $s^{m-1}$ is the first positive power of $s$ in the holomorph of $G'$, then a cycle of regular groups $G', G'', \cdots, G^{(m-1)}$ is determined such that, under $s$, $G' \to G'' \to \cdots \to G^{(m-1)} \to G'$. The set of all substitutions on the letters of $G'$ thus transforming this now given cycle of $G$'s will then constitute an $m$-adic group of ordinary substitutions, which may then be called an $m$-adic holomorph of $G$. The above theory, in somewhat simpler form, will then go over.

[56] On the other hand, the most general possibility is still not there illustrated; for a given element is carried into a single element independently of the $G^{(i)}$ of which it is an element. Note that our last footnote further introduced an $(m, 2)$ substitution group as $m$-adic holomorph of an ordinary regular group.

verbatim for $(m, \mu)$ substitution groups. It is then readily verified that all of the results of §13 go over, with the possible replacement of $m$ by $\mu$, with one exception. And that is that the transitivity of $G^*$ no longer assures the transitivity of $G$([57]).

18. **Primitive and imprimitive $(m, \mu)$ substitution groups.** The distinct sets $\{a_{ij}\}$ of §15 are transformed as units under all the substitutions of the containing group $G^*$ of the transitive $m$-adic substitution group $G$, and hence under the substitutions of $G$. We recall that each set $\{a_{ij}\}$ had $\alpha$ letters in each of $\kappa$ $\Gamma$'s whose subscripts formed an arithmetic progression, $\alpha$ being a divisor of $n$, the degree of $G$, $\kappa$ of $m-1$. Let $\nu=n/\alpha$, $m'-1=(m-1)/\kappa$. Each set $\{a_{ij}\}$ then has letters in one and only one of the first $(m'-1)$ $\Gamma$'s, there being $\nu$ sets for each such $\Gamma$. The $(m'-1)\nu$ distinct sets $\{a_{ij}\}$ thus fall into $m'-1$ mutually exclusive classes $\Gamma_1'$, $\Gamma_2'$, $\cdots$, $\Gamma_{m'-1}'$ of $\nu$ members each. As any $m$-adic substitution $s$ in $G$ transforms each $\Gamma_i$ into $\Gamma_{i+1}$, it will in 1-1 fashion transform the members of $\Gamma_1' \rightarrow \Gamma_2'$, $\Gamma_2' \rightarrow \Gamma_3'$, $\cdots$, $\Gamma_{m'-1}' \rightarrow \Gamma_1'$, and so define an $m'$-adic substitution on $\Gamma_1'$, $\Gamma_2'$, $\cdots$, $\Gamma_{m'-1}'$. The totality of these $m'$-adic substitutions will then constitute an $(m, m')$ substitution group $G'$ of degree $\nu$. As $G$ is transitive, it follows that $G'$ is transitive, there being, as in the ordinary case, a $(1, N)$ isomorphism between $G'$ and $G$. With a restriction to be noted later, $G$ will be said to be imprimitive with systems of imprimitivity $\{a_{ij}\}$ whenever $1<(m'-1)\nu<(m-1)n$, this however, as in the ordinary case, being but an example of the general concept of imprimitivity.

We thus see that even if we start with transitive $m$-adic substitution groups, i.e., $(m, m)$ groups, we are led to $(m, \mu)$ groups. This extension is however sufficient for our purpose. For if we start with a transitive $(m, \mu)$ substitution group $G$, and define the sets $\{a_{ij}\}$ as before, we obtain, by the same argument, an analogous distribution theorem, and then, as above, a transitive $(m, \mu')$ substitution group $G'$ with $\mu'-1$ a divisor of $\mu-1$.

In general, then, let $G$ be a transitive $(m, \mu)$ substitution group of degree $n$ on $\Gamma_1$, $\Gamma_2$, $\cdots$, $\Gamma_{\mu-1}$, with, of course, $\mu-1$ a divisor of $m-1$, and let there be some separation of the $(\mu-1)n$ letters of the $\Gamma$'s into mutually exclusive classes such that these classes are transformed as units under all the substitutions of $G$, and hence of $G^*$. An entirely analogous argument to the one used in determining the distribution of the letters in the sets $\{a_{ij}\}$ leads to a corresponding conclusion here. That is, each class consists of the same number $\kappa\alpha$ of letters, with $\alpha$ a divisor of $n$, $\kappa$ of $\mu-1$, there being $\alpha$ letters in each of $\kappa$ $\Gamma$'s whose subscripts are in arithmetic progression. As with the $\{a_{ij}\}$'s, each such

([57]) On the other hand, if $G^*$ is transitive, we may form a sequence of mutually exclusive $\Gamma$'s, $\Gamma_1'$, $\Gamma_2'$, $\cdots$, $\Gamma_{\mu'-1}'$, such that $G$ is a transitive $(m, \mu')$ group on the $\Gamma'$'s. Here $\mu'-1$ is a multiple of $\mu-1$, and a divisor of $m-1$; while the $\Gamma'$'s are successively subclasses of the $\Gamma$'s run through cyclically $(\mu'-1)/(\mu-1)$ times, and together exhausting the $\Gamma$'s. If we call such an $(m, \mu)$-group $G$ semi-transitive, then the main result of §14 goes over for an arbitrary $(m, \mu)$-group if we replace the transitive constituent groups by semi-transitive constituent groups.

separation of the letters of the Γ's leads to a transitive $(m, \mu')$ substitution group $G'$ of degree $\nu$, where $\nu = n/\alpha$, $\mu' - 1 = (\mu - 1)/\kappa$. The numbers $\alpha$ and $\kappa$, of course, depend on the separation in question.

In accordance with the standard definition we would then define $G$ to be imprimitive if some such separation into mutually exclusive classes is possible with $1 < (\mu' - 1)\nu < (\mu - 1)n$, the classes then being the corresponding systems of imprimitivity of $G$. This restriction is equivalent to $\kappa$ and $\alpha$ not being both one, or simultaneously equal to $\mu - 1$ and $n$ respectively. But then $G$ would always be imprimitive for $\mu > 2$, since its substitutions transform the Γ's themselves as units. We therefore exclude the case $\alpha = n$, and thus have the following definition. *$G$ will be said to be imprimitive if it admits systems of imprimitivity for which $\alpha < n$, $\kappa$ and $\alpha$ not both unity*; otherwise $G$ will be said to be primitive.

The rather artificial restriction $\alpha < n$ is entirely natural in the case $\mu = 2$, and, indeed, we have here the only complete generalizations of the primitivity theorems of ordinary groups. $G$ is now an $m$-adic group of ordinary substitutions on letters which may then be written $a_1, a_2, \cdots, a_n$. It is easily seen that if $G$ is transitive, so are $G^*$ and $G_0$, the converse however holding only for $G_0$. On the other hand, with $G$ transitive, if $G$ is imprimitive, so are $G^*$ and $G_0$, the converse holding only for $G^*$. Thus, with $m = n + 1$, $G$ can be the intransitive group consisting of the single substitution $(a_1 a_2 \cdots a_n)$, while $G^*$ is transitive. And the following is an example of a transitive primitive $G$ for which $G_0$ is imprimitive. Let $G_0$ be the transitive imprimitive group of order four: 1, $(a_1a_2)(a_3a_4)$, $(a_1a_3)(a_2a_4)$, $(a_1a_4)(a_2a_3)$. Then $s = (a_1a_2a_3)$ transforms $G_0$ into itself, while $s^3 = 1$ is in $G_0$. Hence $G = G_0 s$ is a transitive tetradic group of ordinary substitutions, and is easily seen to be primitive.

Turning to the ordinary theorems on primitivity, with $G$ thus a transitive $(m, 2)$ group, there will be at least one substitution in $G$ carrying $a_1$ into itself, and the totality of these substitutions will constitute a subgroup $G_1$ of $G$. We then have the complete analogue of the corresponding theorem for ordinary substitution groups, i.e., *a necessary and sufficient condition that a transitive $m$-adic group $G$ of ordinary substitutions is imprimitive is that $G_1$ is contained in a larger subgroup of $G$.* While this can be proved by applying the ordinary theorem to $G^*$, the ordinary proof([58]) can here be directly carried over. Thus, if $G$ is imprimitive, the substitutions of $G$ transforming the system of imprimitivity of which $a_1$ is a member into itself constitute a subgroup $K$ of $G$ containing $G_1$, and larger than $G_1$. Conversely, if $K$ is a subgroup of the transitive $G$ containing $G_1$, and larger than $G_1$, expand $G$ in right cosets as regards $K$. Each coset will consist of the same number $\alpha > 1$ of right cosets of $G$ as regards $G_1$, and hence will carry $a_1$ into $\alpha$ letters, distinct for each coset, and will

([58]) Rather what the proof of the more general theorem of *Finite Groups*, page 39, would become if given directly for the more special result. We have interchanged the order of the two results.

consist of all the substitutions of $G$ carrying $a_1$ into one of those letters. Finally, any substitution $s$ of $G$ will transform these mutually exclusive sets of letters as units. For if $K_0 s_1$ is the coset carrying $a_1$ into one of these sets, that set will be transformed by $s$ as $a_1$ is by $K_0 s_1 s$. But $K_0 s_1 s$ is the same as $s_0 K_0 s_2$, with $s_0$ in $G_1$, $s_2$ some element in $G$, and hence transforms $a_1$ into that one of the above sets into which the coset $K_0 s_2$ carries $a_1$.

We shall prove in §24 that if an element or subgroup of an $m$-group $G$ is transformed by the elements of $G$, the resulting set of distinct transforms constitutes a "complete set of conjugates" under $G$, and is transformed by the elements of $G$ according to a transitive $m$-adic group of ordinary substitutions having a $(1, N)$ isomorphism with $G$. We again then are concerned with the case $\mu = 2$; and either by applying the preceding result in conjunction with that isomorphism, or by directly extending the ordinary proof as was done above, we again obtain the complete analogue of the corresponding ordinary group theorem([59]). *A necessary and sufficient condition that a complete set of conjugate elements or subgroups under an m-group G of an element or subgroup of G is transformed under G according to an imprimitive m-adic group of ordinary substitutions is that the largest subgroup of G which transforms into itself one of these elements or subgroups is contained in a larger subgroup of G.*

When $G$ is a transitive $(m, \mu)$ group with $\mu > 2$ we no longer have an analogue of $G_1$ for $G$ itself. We must therefore go outside of $G$ for theorems on imprimitivity. $G^*$ will still be transitive; and apart from the restriction $\alpha < n$, a set of systems of imprimitivity of either $G$ or $G^*$ will also be one of the other. Our description of the possible systems of imprimitivity of $G$ therefore applies equally well to $G^*$, and we conclude that *$G$ will be imprimitive when and only when $G^*$ admits a set of systems of imprimitivity for which $\alpha < n$.* As $G^*$ is an ordinary transitive substitution group, we easily supplement the standard result concerning its imprimitivity to obtain the following. *A transitive $(m, \mu)$ group $G$ is imprimitive when and only when $G^*$ has a subgroup containing $G_{11}^*$, larger than $G_{11}^*$, but not containing $G_0$.* $G_{11}^*$ is of course the subgroup of $G^*$ consisting of all of its substitutions omitting $a_{11}$. In proving this result we observe that as a consequence of the transitivity of $G$ the substitutions of $G_0$ will carry any letter into every letter in its $\Gamma$. If then $G$, and hence $G^*$, is imprimitive, the subgroup $K$ of $G^*$, composed of all the substitutions of $G^*$ which transform the system of imprimitivity of which $a_{11}$ is a member into itself, satisfies the conditions of the theorem. For $K$ is known to be a subgroup of $G^*$ containing $G_{11}^*$, and larger than $G_{11}^*$. And as it can carry $a_{11}$ into only $\alpha < n$ letters of $\Gamma_1$, it cannot contain $G_0$. Conversely, if $K$ is a subgroup of $G^*$ satisfying the conditions of the theorem, the letters into which the substitutions of $K$ carry $a_{11}$ are known to form one of a set of systems of imprimitivity of $G^*$. As $K$ will then contain all the substitutions of $G^*$ which carry $a_{11}$ into any letter that

([59]) At least as stated on page 39, *Finite Groups*.

one substitution of $K$ carries $a_{11}$ into, could it carry $a_{11}$ into all the letters of $\Gamma_1$ it would contain $G_0$, contrary to hypothesis. Hence, the $\alpha$ of the resulting systems of imprimitivity of $G$ is less than $n$, whence $G$ too is imprimitive.

A criterion for the imprimitivity of $G$ in terms of $G_0$ would be preferable to one in terms of $G^*$. Our example of a primitive $(m, 2)$ group whose associated group was imprimitive precludes such a criterion for an arbitrary $(m, \mu)$ group. However when $\mu=m$ we do have the following partial criterion in terms of, better than $G_0$, the associated constituent groups of $G$. *A transitive $m$-adic substitution group $G$ admits systems of imprimitivity with $\alpha>1$ when and only when the associated constituent group $G_0'$ is imprimitive.* In fact, systems of imprimitivity of $G$ must be permuted as units under $G_0$. Hence the portions of these systems in $\Gamma_1$ are permuted as units under $G_0'$. As $\alpha>1$ by hypothesis, and $\alpha<n$ by definition, we thus have a set of systems of imprimitivity of $G_0'$. Conversely, given a set of systems of imprimitivity of $G_0'$, any $s$ of $G$ will transform $G_0' \rightarrow G_0'' \rightarrow \cdots \rightarrow G_0^{(m-1)} \rightarrow G_0'$, and hence will successively transform the systems of imprimitivity of $G_0'$ into systems of imprimitivity of $G_0'', \cdots, G_0^{(m-1)}$. The result of transforming these systems of imprimitivity of $G_0^{(m-1)}$ by $s$ is the same as that of transforming the given systems of imprimitivity of $G_0'$ by $s^{m-1}$. As $s^{m-1}$ is in $G_0$, it transforms the systems of imprimitivity of $G_0'$ as units. Hence $s$ transforms the totality of systems of imprimitivity of $G_0', G_0'', \cdots, G_0^{(m-1)}$ as units. As $G_0$ does the same, so will $G=G_0 s$ which is therefore imprimitive with $1<\alpha\ (<n)$.

For the exceptional case $\alpha=1$ we have to return to $G^*$. The same considerations that gave us our general criterion for the imprimitivity of a transitive $(m, \mu)$ group yield the following result. *A transitive $(m, \mu)$ group $G$ admits systems of imprimitivity with $\alpha=1$ when and only when $G^*$ has a subgroup containing $G_{11}^*$, larger than $G_{11}^*$, but having no other substitutions than those of $G_{11}^*$ that carry each $\Gamma$ into itself.* The last condition is equivalent to the crosscut of the subgroup in question and $G_0$ being identical with $(G_0)_{11}$, the crosscut of $G_{11}^*$ and $G_0$, and hence, for an $m$-adic substitution group $G$, with $G_{11}^*$.

Though all of the development of the next section, and, with certain restrictions, of the one following, can be given for $(m, \mu)$ substitution groups, we restrict ourselves, for the sake of simplicity, to $m$-adic substitution groups, i.e., $(m, m)$ groups.

19. **Multiple transitivity; cyclically transitive $m$-adic substitution groups.** Various extensions of the concept of multiple transitivity suggest themselves. According to the simplest, an $m$-adic substitution group $G$ would be said to be $r$-fold transitive if any $r$ letters belonging to any one $\Gamma$ can be transformed into any $r$ letters of the succeeding $\Gamma$ by the substitutions of the group. It is readily proved that a necessary and sufficient condition that $G$ be thus $r$-fold transitive is that the associated constituent groups $G_0', G_0'', \cdots, G_0^{(m-1)}$ (or any one of them) be $r$-fold transitive in the ordinary sense. Since the order of $G_0'$ is a divisor of the order of $G_0$, and hence of $G$, it follows from the corre-

sponding ordinary group result that the order of an $r$-fold transitive $m$-adic substitution group of degree $n$ is a multiple of $n(n-1)\cdots(n-r+1)$.

Of special interest in polyadic theory is the type of multiple transitivity we term cyclic transitivity. An $m$-adic substitution group $G$ will be said to be *cyclically transitive* if, given any two selections from the classes of letters $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$, some substitution of $G$ will carry the letters of one selection into the letters of the other. Actually then, if one selection is $a_{1j_1}, a_{2j_2}, \cdots, a_{(m-1)j_{m-1}}$, the other $a_{1k_1}, a_{2k_2}, \cdots, a_{(m-1)k_{m-1}}$, the substitution will carry $a_{1j_1}\rightarrow a_{2k_2}, a_{2j_2}\rightarrow a_{3k_3}, \cdots, a_{(m-1)j_{m-1}}\rightarrow a_{1k_1}$. Every cyclically transitive $m$-adic substitution group is then transitive, and, indeed, for $m=2$ cyclic transitivity reduces to transitivity. The symmetric and alternating $m$-adic groups of degree $n$, previously observed to be transitive—in the latter cases at least for $n>2$—are now seen to be cyclically transitive.

The $m-1$ $\Gamma$'s, of $n$ letters each, give rise to $n^{m-1}$ selections which we shall call *cycles*. Any $m$-adic substitution $s$ on the $\Gamma$'s will merely permute these cycles, and hence will determine an ordinary substitution on these $n^{m-1}$ cycles as new "permutants." Since this relationship is preserved under multiplication, the members of an $m$-adic substitution group $G$ of degree $n$ will thus give rise to substitutions on the cycles forming an $m$-adic group $G'$ of ordinary substitutions, of degree $n^{m-1}$, isomorphic with $G$. Clearly, different $m$-adic substitutions yield different substitutions of the cycles. Hence $G'$ is indeed simply isomorphic with $G$. In particular, then, $G'$ and $G$ are of the same order. Finally, if $G$ is cyclically transitive, $G'$ will be transitive, and, indeed, conversely. Since the order of an $m$-adic transitive group of ordinary substitutions is a multiple of its degree, we have, as our first result, *the order of a cyclically transitive $m$-adic substitution group of degree $n$ is a multiple of $n^{m-1}$.*

We have seen that transitive $m$-adic groups of ordinary substitutions have the complete analogue of the $G_1$ of ordinary transitive groups. Actually, all of the corresponding theory goes over. In our simple isomorphism between $G$ and $G'$, the subgroup of $G'$ consisting of all of its substitutions "omitting" a given cycle $C$ will correspond to the subgroup $G_C$ of $G$ consisting of all of its substitutions which carry $C$ into itself. We shall call $G_C$ *the cycle subgroup of $G$*, corresponding to $C$. Actually, if $C$ is the selection $a_{1j_1}, a_{2j_2}, \cdots, a_{(m-1)j_{m-1}}$, it will be transformed into itself according to the cyclic substitution $(a_{1j_1}a_{2j_2}\cdots a_{(m-1)j_{m-1}})$ by all the substitutions of $G_C$. Hence, if the $m$-adic substitutions of $G$ be written as ordinary substitutions on $(m-1)n$ letters in cycle form, $G_C$ will consist of those substitutions of $G$ which have this cyclic substitution as component. It will be convenient to speak of these substitutions as having the cycle $C$. Clearly, then, *an $m$-adic substitution of degree $n$ cannot have more than $n$ cycles.*

Each of the $n^{m-1}$ cycles yields thus a corresponding cycle subgroup of the cyclically transitive $G$. The simple isomorphism between $G$ and $G'$ then immediately transforms the corresponding properties of $G'$ to yield, among

others, the following results on $G$. The order of each cycle subgroup of $G$ is equal to the order of $G$ divided by $n^{m-1}$. The cycle subgroups of $G$ are conjugate, forming a complete set of conjugates under the substitutions of $G$. If all the substitutions of a given cycle subgroup have exactly $\alpha$ cycles in common, and they have one cycle in common by definition, then the $n^{m-1}$ cycles can be separated into mutually exclusive sets of $\alpha$ cycles each such that different cycles yield the same cycle subgroup when and only when they belong to the same set.

There are thus $n^{m-1}/\alpha$ distinct cycle subgroups of $G$. The only information that $G'$ yields concerning $\alpha$ is that it is a divisor of $n^{m-1}$. However, our observation that an $m$-adic substitution of degree $n$ cannot have more than $n$ cycles shows that $\alpha \leqq n$. Hence, *a cyclically transitive $m$-adic substitution group of degree $n$ has a number $N$ of cycle subgroups with $N \geqq n^{m-2}$ and a divisor of $n^{m-1}$*. Whether $N$ is actually a multiple of $n^{m-2}$, i.e., $\alpha$ a divisor of $n$, is another of our unsolved problems.

20. **Class of an $m$-adic substitution group.** The class of an ordinary substitution group is the smallest number of letters appearing in any of its substitutions, other than the identity, when those substitutions are written in cycle form. Since the substitutions of an $m$-adic substitution group $G$ never carry a letter into itself when $m>2$, we are led to define the class of $G$ as the class of its associated group $G_0$. This also is the class of its containing group $G^*$([60]).

With this definition most of the elementary theory of class goes over to $m$-adic substitution groups. We have almost immediately that the $m$-adic symmetric group of degree $n$, $n>1$, is a primitive group of class 2, while the $m$-adic alternating groups of degree $n$, $n>2$, are primitive groups of class 3. That these $m$-adic groups are primitive follows from the fact that their constituent associated groups are either the symmetric, or alternating, ordinary groups of degree $n$, and hence primitive, so that the $m$-adic groups do not admit systems of imprimitivity with $\alpha>1$; and, being cyclically transitive, they cannot admit systems of imprimitivity with $\alpha=1$. As for their class, they are clearly at most of the class indicated. And could an alternating group actually be of class 2, the $\epsilon$-subgroup of its corresponding $\delta$-subgroup would have an $\epsilon$-sequence with one $-1$; but then the $\delta$-subgroup would be the complete $\delta$-group, and hence the given group not an alternating group, but the symmetric group.

We now prove that, as in the standard theory, the converses of these results also hold. First then let $G$ be a primitive $m$-adic substitution group of degree $n$ and of class 2. On the one hand, its associated constituent group $G_0'$ will be primitive; on the other hand, its associated group $G_0$ will have some substitution whose component in each $G_0^{(i)}$ but one is the identity, and in

([60]) Not necessarily so, however, for $(m, \mu)$-groups with $\mu<m$.

that one a transposition. By the invariance of $G_0$ under $G$, we see that $G_0$ has a substitution $t_0$ of the form $t_0' \cdot 1 \cdots 1$, with $t_0'$ in $G_0'$ and a transposition. Now let $\overline{G}_0'$ be that subgroup([61]) of $G_0'$ composed of all the substitutions $t'$ of $G_0'$ for which $t' \cdot 1 \cdots 1$ is in $G_0$. The subgroup $\overline{G}_0'$ is clearly an invariant subgroup of $G_0$, and hence of $G_0'$, and it has the transposition $t_0'$. Now the standard proof of the fact that a primitive (ordinary) group of class 2 is the corresponding symmetric group also yields the following more general statement. An invariant subgroup([62]) of class 2 of a primitive group is the corresponding symmetric group. Hence $\overline{G}_0'$ is the symmetric group of degree $n$. $G_0$ therefore has among its elements every substitution of the form $t' \cdot 1 \cdots 1$. Since $G_0$ is invariant under $G$, it also has every substitution of the form $1 \cdots t^{(i)} \cdots 1$, for each $i$, and hence every substitution of the form $t't'' \cdots t^{(m-1)}$. $G_0$ is therefore the associated group of the $m$-adic symmetric group of degree $n$, and hence $G$ the symmetric group itself. Hence, *every primitive m-adic substitution group of class 2 and degree n is the corresponding symmetric group, and conversely for* $n>1$.

If $G$ is a primitive $m$-adic substitution group of degree $n$ and class 3, we have as before that $G_0'$ is primitive, while $G_0$ has a substitution of the form $t_0' \cdot 1 \cdots 1$ with $t_0'$ of the form $abc$, the last since the substitution of class 3 in $G_0$ must consist of a single cycle of three letters which, in turn, must then belong to a single $\Gamma$. Defining $\overline{G}_0'$ as before, we see that $\overline{G}_0'$ is of class 3, and hence, by the corresponding extension of the standard result, is the alternating group of degree $n$. We therefore conclude that $G_0$ has, perhaps among others, every substitution of the form $t't'' \cdots t^{(m-1)}$ with the $t^{(i)}$'s positive substitutions. $G_0$ therefore has every possible substitution corresponding to the $\epsilon$-sequence $(+1, +1, \cdots, +1)$, and hence every possible substitution for each of the $\epsilon$-sequences of its substitutions. It is therefore the associated group of an alternating group, i.e., $G$ is an alternating group. Hence, *every primitive m-adic substitution group of degree n and of class 3 is an alternating group of degree n, and conversely for* $n>2$.

Actually two cases arise as far as $G_0'$ is concerned. When the above found substitutions of $G_0$ are its only substitutions, $(+1, +1, \cdots, +1)$ is its only $\epsilon$-sequence, $G$ is an alternating group whose $\delta$-subgroup is of the first order, while $G_0'$ is identical with $\overline{G}_0'$, and hence is itself the alternating group. Otherwise, $G_0'$ will be larger than $\overline{G}_0'$, while containing it, and hence will be the symmetric group, while $G$ will be an alternating group whose $\delta$-subgroup is of order greater than one. Note also that in both of the above results the hypothesis of the primitivity of $G$ was used only in deducing the primitivity of $G_0'$. We therefore conclude that there does not exist an $m$-adic substitution group $G$ of class 2 or 3 for which $G$ is imprimitive, $G_0'$ primitive.

---

([61]) If not $G_0'$ itself.

([62]) Actually improper, therefore.

Let now $G$ be a primitive $m$-adic group of degree $n$ and of class $p$, $p$ a prime greater than 3. As before, the substitution of class $p$ in $G_0$ must consist of a single cycle of letters which therefore belong to a single $\Gamma$. Hence $n \geqq p$. Furthermore, $\overline{G}_0'$ will have a substitution of class $p$ for element, and hence be of class $p$. Finally $G_0'$ is primitive, with $\overline{G}_0'$ as invariant subgroup. With the corresponding ordinary proof generalized as in the preceding cases, we then find that $\overline{G}_0'$ is $(n-p+1)$-fold transitive. The remainder of the standard proof is then directly applicable to $\overline{G}_0'$ and shows that $n$ cannot be greater than $p+2$. Hence, *if a primitive m-adic substitution group is of class p, p being a prime number greater than 3, its degree can only be p, p+1 or p+2.* Note that actually $\overline{G}_0'$ is then itself primitive—immediately so for $n=p$, and as a consequence of its being more than simply transitive for $n=p+1$ or $p+2$. Hence, in each of these cases, $\overline{G}_0'$ is the unique primitive ordinary group of class $p$ and degree $n$.

We consider in detail only the case $n=p$. $\overline{G}_0'$ is then the group of order $p$, as is also each $\overline{G}_0^{(i)}$, defined in analogous fashion. Each $\overline{G}_0^{(i)}$ is therefore a cyclic group, and is, in fact, generated by a single cycle of the $p$ letters of $\Gamma_i$. By relettering the members of the $\Gamma$'s we may therefore assume that $\overline{G}_0^{(i)}$ is generated by the substitution $t_0^{(i)} = (a_{i1}a_{i2} \cdots a_{ip})$. Now any substitution $t$ of $G_0$ will transform each $\overline{G}_0^{(i)}$ into itself, and hence will transform $t_0^{(i)}$, the generator of $\overline{G}_0^{(i)}$, into some power $\nu^{(i)}$ of itself, with $\nu^{(i)} = 1, 2, \cdots, p-1$. Hence, with each $t$ in $G_0$ we can thus associate a $\nu$-sequence $(\nu', \nu'', \cdots, \nu^{(m-1)})$. Likewise, if $s$ is any substitution in $G$, $s$ will transform each $\overline{G}_0^{(i)}$ into $\overline{G}_0^{(i+1)}$. It will therefore transform each $t_0^{(i)}$ into some power $\mu^{(i)}$ of $t_0^{(i+1)}$, $\mu^{(i)} = 1, 2, \cdots, p-1$. Hence, with each $s$ in $G$ we can thus associate a $\mu$-sequence $[\mu', \mu'', \cdots, \mu^{(m-1)}]$. Since $G_0$ has the substitution $1 \cdots t^{(i)} \cdots 1$ whenever $\overline{G}_0^{(i)}$ has the substitution $t^{(i)}$, we see that $G_0$ has the invariant subgroup

$$\overline{G}_0 = \overline{G}_0' \, \overline{G}_0'' \cdots \overline{G}_0^{(m-1)},$$

the direct product of the $\overline{G}_0^{(i)}$'s, when it is not $\overline{G}_0$ itself. Now $\overline{G}_0^{(i)}$ consists of all the substitutions on the letters of $\Gamma_i$ that transform $t_0^{(i)}$ into itself. It follows that $\overline{G}_0$ consists of all the $(m-1)$-ads, consequently $p^{m-1}$ in number, which transform each $t_0^{(i)}$ into itself. $G_0$, therefore, has among its elements each of the $p^{m-1}$ $(m-1)$-ads with which we can associate the $\nu$-sequence $(1, 1, \cdots, 1)$. By expanding $G_0$ in cosets as regards $\overline{G}_0$, we then easily verify that $G_0$ likewise has each of the $(m-1)$-ads with which we can associate the $\nu$-sequence of any one of its members, there being exactly $p^{m-1}$ $(m-1)$-ads for each $\nu$-sequence. Likewise, by expanding $G$ in cosets as regards $\overline{G}_0$, which is invariant under $G$, we find that $G$ has every $m$-adic substitution on the $\Gamma$'s with which we can associate the $\mu$-sequence of any one of its members, there being exactly $p^{m-1}$ such substitutions for each $\mu$-sequence.

$G$ is therefore determined by the set of $\mu$-sequences of its members. Actually, if $s_i$ in $G$ has the $\mu$-sequence $[\mu_i', \mu_i'', \cdots, \mu_i^{(m-1)}]$, then $s = s_1 s_2 \cdots s_m$,

also in $G$, will have the $\mu$-sequence $[\mu', \mu'', \cdots, \mu^{(m-1)}]$ given by the equations

$$\begin{aligned}
\mu' &= \mu_1' \mu_2'' \cdots \mu_m', \\
\mu'' &= \mu_1'' \mu_2''' \cdots \mu_m'', \\
&\cdots\cdots\cdots\cdots\cdots, \\
\mu^{(m-1)} &= \mu_1^{(m-1)} \mu_2^{(m-1)} \cdots \mu_m^{(m-1)},
\end{aligned}$$

the products being reduced modulo $p$ to one of the numbers $1, 2, \cdots, p-1$. It follows that the $\mu$-sequences of the members of $G$ constitute an $m$-adic group under this $m$-adic operation isomorphic with $G$, and, indeed, simply isomorphic with the quotient group $G/\overline{G}_0$. $G$ is therefore determined by its corresponding "$\mu$-subgroup."

This suggests a development analogous to that of the symmetric and alternating groups, and their relationship to the complete $\delta$-group. Let $P$, the "symmetric power group of degree $p$," be the $m$-adic substitution group of degree $p$ consisting of all $m$-adic substitutions on the $\Gamma$'s that transform each $t_0^{(i)} = (a_{i1}a_{i2} \cdots a_{ip})$ into a power of $t_0^{(i+1)}$. Its associated group $P_0$ will then consist of all $(m-1)$-ads on the $\Gamma$'s transforming each $t_0^{(i)}$ into a power of itself. Note that actually $\overline{P}_0^{(i)}$ is identical with the preceding $\overline{G}^{(i)}$, $\overline{P}_0$ with $\overline{G}_0$, a fact that merely emphasizes the fact that for the class of groups under consideration these groups are independent of $G$. With each $t$ in $P_0$ we can associate a $\nu$-sequence, with each $s$ in $P$, a $\mu$-sequence. Clearly, for each of the $(p-1)^{m-1}$ possible $\nu$-sequences there is at least one $t$ in $P_0$ having that $\nu$-sequence, and hence, as for $G_0$, $p^{m-1}$ such $t$'s. $P_0$ is therefore of order $[p(p-1)]^{m-1}$. Hence the symmetric power group $P$ is also of order $[p(p-1)]^{m-1}$, having $p^{m-1}$ substitutions for each of the $(p-1)^{m-1}$ possible $\mu$-sequences. Actually, if $s_0$ is the $m$-adic substitution carrying each $a_{ij}$ into $a_{(i+1)j}$, it will be in $P$ with the $\mu$-sequence $[1, 1, \cdots, 1]$, so that we can write $P = P_0 s_0$; and if in $s = ts_0$ we let $t$ run through all substitutions in $P_0$ with a given $\nu$-sequence, $s$ will run through all substitutions in $P$ having that $\nu$-sequence for $\mu$-sequence.

Under the above $m$-adic operation the $(p-1)^{m-1}$ possible $\mu$-sequences constitute an $m$-adic group which we may call the complete $\mu$-group. As in the case of the complete $\delta$-group, the associated group of the complete $\mu$-group may be considered to have the $(p-1)^{m-1}$ $\nu$-sequences as elements under the dyadic operation $(\nu_1', \nu_1'', \cdots, \nu_1^{(m-1)})(\nu_2', \nu_2'', \cdots, \nu_2^{(m-1)}) = (\nu_1'\nu_2', \nu_1''\nu_2'', \cdots, \nu_1^{(m-1)}\nu_2^{(m-1)})$, the $\nu$-sequence corresponding to an $(m-1)$-ad of $\mu$-sequences being given by the above operation on $\mu$-sequences with the $\mu_m^{(i)}$'s omitted. The complete $\mu$-group is therefore semi-abelian; and by the use of the $\mu$-sequence $[1, 1, \cdots, 1]$ the unique $\nu$-sequence into which $(\nu', \nu'', \cdots, \nu^{(m-1)})$ is transformed by every $\mu$-sequence is again found to be $(\nu^{(m-1)}, \nu', \cdots, \nu^{(m-2)})$.

Corresponding to each subgroup of the complete $\mu$-group there will be an

"alternating power group," the $m$-adic substitution group of degree $p$ consisting of all the $m$-adic substitutions on the $\Gamma$'s with $\mu$-sequences in the $\mu$-subgroup under consideration. Each of our $G$'s is therefore an alternating power group(63). To complete our investigation within its present scope we need merely find which of the alternating power groups are primitive groups of class $p$. Actually they are all primitive. For their $\overline{G}_0'$ is the primitive $\overline{P}_0'$, so that their $G_0'$ is primitive. And their $\overline{G}_0$ is always $\overline{P}_0$, which can carry any selection of letters chosen from the $\Gamma$'s into any other selection, so that in fact, they are cyclically transitive. As for their class, it is immediately seen to be at most $p$. Now actually a substitution on the letters of $\Gamma_i$ carrying $t_0^{(i)} = (a_{i1}a_{i2} \cdots a_{ip})$ into a power of itself other than the first must be of class $p-1$. It follows that an alternating power group of degree $p$ is of class less than $p$, in fact $p-1$, when and only when the associated group of its $\mu$-subgroup has a $\nu$-sequence with one and only one number not unity. This is easily transformed into a condition on the $\mu$-subgroup itself to yield the following result. *The primitive groups of class $p$ and degree $p$, $p$ being a prime greater than 3, are the alternating power groups of degree $p$ whose $\mu$-subgroups do not have a pair of $\mu$-sequences differing in one and only one component*(64).

## B. Finite abstract polyadic groups

21. **Cyclic polyadic groups; ordinary theory**(65). Given the $m$-adic operation $c$, we define the $m$-adic powers of an element $s$ under $c$ inductively as follows. $s$ itself will be rewritten $s^{[0]}$; and having $s^{[n]}$, we define $s^{[n+1]}$ as $c(s \cdots s s^{[n]})$. If then $s^{[n]}$ be written out in full, $n$ is the number of $c$'s occurring in the resulting extended operation, the number of $s$'s being $n(m-1)+1$. By the associative law it follows that any extended operation involving $n$ $c$'s and but the single element $s$ repeated can be rewritten in the form $s^{[n]}$. We thus easily obtain the following $m$-adic power laws:

$$c(s^{[n_1]}s^{[n_2]} \cdots s^{[n_m]}) = s^{[n_1+n_2+\cdots+n_m+1]}, \qquad (s^{[n_1]})^{[n_2]} = s^{[(m-1)n_1n_2+n_1+n_2]}.$$

Note that for $m=2$ our $n$th power is the ordinary $(n+1)$-st power(66).

(63) Unless it were $P$ itself. But $P$ is readily seen to be of class $p-1$.

(64) The actual problem of determining the subgroups of the complete $\mu$-group remains unsolved. Gill has pointed out to the writer that while the problem of determining the associated groups of these $\mu$-subgroups can superficially be expressed as a problem in V.A.G.'s, actually the theory is now inapplicable, since the coefficients of the polynomials no longer form a field.

(65) For the special case $m=3$, the results of the present section reduce to those given by Lehmer. Likewise those of the next section involving mere reducibility, now of necessity to a 2-group.

(66) By contrast, Dörnte writes $a^z$ in usual notation with, however, $z$ subject to the restriction $z \equiv 1 \pmod{m-1}$. While our laws of powers are, as a result, more complicated than Dörnte's, we find great comfort in the fact that our $s^{[n]}$ is an "$m$-adic element" for every positive integral, or zero, $n$. Our lack of negative $m$-adic powers could easily be supplied.

If $s$ is an element of an $m$-adic group $K$, each of its $m$-adic powers will represent elements of $K$. With $K$ a finite group we therefore must have for some $n_0$ and $n_0+n$, $n>0$, $s^{[n_0]}=s^{[n_0+n]}$. Since $s^{[n_0+n]}$ can be rewritten $c(s^{[n_0]}s\cdots ss^{[n-1]})$, it follows that $\{s, \cdots, s, s^{[n-1]}\}$ is an identity, whence we have

$$s^{[n]} = s.$$

The smallest postive integral value of $n$ for which this equation holds will be called the ($m$-adic) *order* of $s$. If then $s$ is of order $g$, the sequence of its $m$-adic powers $s^{[0]}, s^{[1]}, s^{[2]}, \cdots$ starts with $g$ distinct elements which are then repeated in order. It follows on the one hand that $s^{[n]}=s$ when and only when $n$ is a multiple of $g$; and, more generally, that $s^{[n_1]}=s^{[n_2]}$ when and only when $n_1-n_2$ is a multiple of $g$. On the other hand, since but a finite number of elements are involved, our first law of $m$-adic powers shows that the $g$ distinct elements constitute an abelian $m$-adic group $G$ of order $g$ which may then be called the *cyclic $m$-adic group generated by $s$*. The order of $s$ is therefore equal to the order of the cyclic group it generates. Again by the first law of $m$-adic powers it is immediately seen that two cyclic $m$-groups of the same order are simply isomorphic. Furthermore, the same law shows that apart from an assumed $m$-group $K$, $g$ distinct elements $s_0, s_1, \cdots, s_{g-1}$, subject to the $m$-adic operation obtained by writing $s_n=s^{[n]}$, with $s^{[g]}=s$, constitute an $m$-group which is then the cyclic $m$-group of order $g$ generated by $s=s_0$. Hence, as in ordinary group theory, we may say there is one and only one cyclic $m$-group whose order is an arbitrary natural number(67).

Let then $G$ be the cyclic $m$-group of order $g$, $s$ a generator of $G$. We first ask for the order of any power $s^{[n]}$ of $s$. This will be the least value of $N$ for which $(s^{[n]})^{[N]}=s^{[n]}$, hence the least value of $N$ for which $(m-1)nN+N+n-n=[(m-1)n+1]N$ is a multiple of $g$. It follows that *the order of $s^{[n]}$ is equal to the order of $s$ divided by the highest common factor of $(m-1)n+1$ and the order of $s$*. In particular, the order of $s^{[n]}$ will be the same as the order of $s$ when and only when $(m-1)n+1$ is prime to the order of $s$. Hence *an element $s$ is generated by those and only those of its $m$-adic powers $s^{[n]}$ for which $(m-1)n+1$ is prime to the order of $s$.*

We can now determine what orders the elements of $G$ can have. $\gamma$ will be the order of an element of $G$ if $\gamma=g/d$, $d=$H.C.F. $[(m-1)n+1, g]$ for some $n$. It is necessary then that $d$ be a divisor of $g$, and prime to $m-1$. We now show that this is also sufficient. We have to find, then, an $n$ and $k$ such that $(m-1)n+1=kd$, $g=\gamma d$ with $k$ relatively prime to $\gamma$. Since $m-1$ is prime to $d$ by hypothesis, for some $n=n_0$, $k=k_0$, we will have $(m-1)n_0+1=k_0d$.

(67) The following discussion tacitly assumes that a symbol representing the order of an element or group is restricted to positive integral values, one representing an $m$-adic power to non-negative integral values. On the other hand, symbols entering into a diophantine equation may at first be allowed to assume arbitrary integral values which are then restricted in the above manner as the need arises.

The general solution of $(m-1)n+1=kd$ is then given by $n=n_0+\lambda d$, $k=k_0+\lambda(m-1)$ with arbitrary $\lambda$. Now the particular solution shows $k_0$ to be prime to $m-1$. Hence the arithmetic progression $k_0+\lambda(m-1)$ has, indeed, an infinite number of primes, and hence certainly a number prime to $\gamma$ as was to be proved. We thus have the following result. *A cyclic m-group of order g has at least one element of every order $\gamma$ such that $\gamma$ is a divisor of g, and $g/\gamma$ is prime to $m-1$, and no element of any other orders.* In particular, *a cyclic m-group of order g has a first order element when and only when g is prime to $m-1$.*

We can now generalize the ordinary cyclic group argument to prove the following. *A cyclic m-group of order g has one and only one subgroup whose order is any given divisor $\gamma$ of g such that $g/\gamma$ is prime to $m-1$, and no others.* The one subgroup is immediately yielded by the cyclic subgroup generated by an element of order $\gamma$, whose existence is insured by the preceding result. For the converse, consider any subgroup of the given cyclic group, and let its order be $\gamma$. By Lagrange's theorem extended, $\gamma$ is a divisor of $g$. By the same theorem, each element $s$ of the subgroup has an order which is a divisor of $\gamma$, and hence must satisfy the equation $s^{[\gamma]}=s$. Now consider all the elements of the given cyclic group, generated, say, by $s_0$, that satisfy this equation. If $s=s_0^{[n]}$, we have, as in a preceding argument, that $\gamma[(m-1)n+1]=kg$ for some $k$, and hence, with $g/\gamma=d$, that $(m-1)n+1=kd$—and conversely. We first see that $d$ is prime to $m-1$, and hence that $\gamma$ is the order of a cyclic subgroup of the given group. Furthermore, since $\gamma d=g$, our general solution $n=n_0+\lambda d$, $k=k_0+\lambda(m-1)$, of the equation $(m-1)n+1=kd$ shows that exactly $\gamma$ such $n$'s are to be found with values in the set $0, 1, 2, \cdots, g-1$. Hence the elements $s$ satisfying the equation $s^{[\gamma]}=s$ are exactly $\gamma$ in number, and consequently must be the $\gamma$ elements of the above cyclic subgroup of order $\gamma$. Our assumed subgroup of order $\gamma$ must therefore be that cyclic subgroup, whence our result.

From this proof flow a number of corollaries. We have immediately that *every subgroup of a cyclic polyadic group is cyclic.* Furthermore, our proof shows that an element of given order of a cyclic group is contained in those and only those subgroups of the cyclic group whose orders are multiples of the order of the element. It follows, on the one hand, that the necessary and sufficient condition that one element of a cyclic group generate a second is that the order of the first be a multiple of the order of the second. On the other hand, we see that two subgroups of a cyclic polyadic group intersect in the subgroup whose order is the highest common factor of the orders of the given subgroups, and generate the subgroup whose order is the least common multiple of those orders.

Apart from the possible orders of elements and subgroups of a cyclic polyadic group the above results are the same as for ordinary cyclic groups. Our condition on those possible orders $\gamma$ can be transformed into the following more usable form. *Let $g_0$ be the largest divisor of g prime to $m-1$, and let*

$\gamma_0 = g/g_0$. *Then the cyclic m-group of order g has at least one element, and exactly one subgroup, of those and only those orders* $\gamma$ *for which* $\gamma = \delta\gamma_0$, $\delta$ *a divisor of* $g_0$. In fact, if $\gamma$ is a divisor of $g$ with $g/\gamma$ prime to $m-1$ as per our original condition, $g/\gamma$, being a divisor of $g$ prime to $m-1$, must be a divisor of $g_0$. Hence $g_0 = \delta(g/\gamma)$ with $\delta$ a divisor of $g_0$, whence $\gamma = \delta\gamma_0$. Conversely, if $\gamma = \delta\gamma_0$ with $\delta$ a divisor of $g_0$, $g/\gamma = g_0/\delta$, so that $\gamma$ is a divisor of $g$ with $g/\gamma$ prime to $m-1$.

We thus see that $\gamma_0$ is the least order of a subgroup of our cyclic group, with all of the subgroups of the cyclic group containing the unique subgroup of order $\gamma_0$. At one extreme, when $\gamma_0 = 1$, which is equivalent to $g$ prime to $m-1$, the cyclic group has a subgroup of first order. This corresponds to the element of first order previously noted, which is now seen to be unique. Every subgroup then contains this first order element, and their orders are the same as the orders of the subgroups of an ordinary cyclic group of order $g$. At the other extreme $\gamma_0 = g$, which is equivalent to every distinct prime factor of $g$ being a factor of $m-1$. The cyclic group then has no (proper) subgroup, each of its elements being of order $g$, and thus generating the entire cyclic group([68]). In particular, if $g$ is a prime $p$, the corresponding cyclic group is always of one of these two special types. Note that unlike an ordinary group, a polyadic group whose order is a prime $p$ need not be cyclic. By the extended Lagrange theorem its elements must be of order 1 or $p$. If it has an element of order $p$, it must be the cyclic group of order $p$. However all of its elements may be of order one, in which case it is noncyclic.

In the general case the orders of the subgroups are multiples of $\gamma_0$, the multipliers being the orders of the subgroups of an ordinary cyclic group of order $g_0$. Hence, if $g = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\rho^{\alpha_\rho}q_1^{\beta_1}q_2^{\beta_2}\cdots q_\sigma^{\beta_\sigma}$, with $p_1, p_2, \cdots, p_\rho$ distinct primes not factors of $m-1$, $q_1, q_2, \cdots, q_\sigma$ factors of $m-1$, then the number of subgroups of the cyclic $m$-group of order $g$ is $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_\rho+1)-1$.

We can now also find an expression for the number of elements of given order in a cyclic $m$-group. With that order one for which there is at least one element, the total number of elements of that order will be the same as the number of generators of a cyclic $m$-group of that order. We proceed therefore to find the number of generators of a cyclic $m$-group of order $g$ generated, say, by $s_0$. We first show that if $m-1$ is prime to $g$ the number of generators is $\phi(g)$ as for ordinary cyclic groups. In fact, if we recall our formula for the order of $s_0^{[n]}$ we see that the number of generators in question is the number of numbers $(m-1)n+1$, $n = 0, 1, \cdots, g-1$, prime to $g$. But with $m-1$ prime to $g$ this is the same as the number of numbers $0, 1, \cdots, g-1$ prime to $g$, that is, $\phi(g)$. Now, in the general case, expand the given cyclic $m$-group of order $g$ in cosets as regards its subgroup of order $\gamma_0$. The resulting quotient group is then an $m$-group of order $g_0$ prime to $m-1$. Now let $s$ be any element of the given group, $\sigma$ the corresponding element of the quotient group. Then $s$

([68]) Whence our correction of a statement of Miller.

is a generator of the given group when and only when $\sigma$ is a generator of the quotient group. That $\sigma$ generates the quotient group if $s$ generates the given group is immediate. As for the converse, $s$ will then generate a group having a complete set of multipliers for our coset expansion. But it must also generate all the elements of the subgroup of order $\gamma_0$, and hence all the elements of the group. It follows, on the one hand, that the quotient group is itself cyclic, and hence has $\phi(g_0)$ generators, and hence, finally, that *the number of generators of a cyclic m-group of order g is* $\gamma_0\phi(g_0)$.

Among the few extensions of topics of the ordinary theory of cyclic groups omitted in the above development is that of the $k$th powers of elements of a cyclic group. We state the result for $m$-groups without further proof. *The distinct kth powers of a cyclic m-group of order g constitute a subgroup of order* $g/h$ *where h is the highest common factor of g and* $(m-1)k+1$; *furthermore, each element of this subgroup is the kth power of exactly h elements of the given group.*

22. **Cyclic polyadic groups; polyadic theory.** We have observed that a cyclic $m$-group of order $g$ has a first order element when and only when $m-1$ is prime to $g$. As this element, when it exists, is invariant under the group, it follows that *a cyclic m-group of order g is reducible to a 2-group when and only when g is prime to* $m-1$. We turn now to the general discussion of reducibility for cyclic polyadic groups. Our first result is immediate. *Every group to which a cyclic group is reducible is cyclic.* For if $s$ is a generator of the given cyclic group, $c$ its operation, $c'$ the operation of the reduced group, every element of the given group is given by an extended $c$ operation involving $s$'s only, hence also by an extended $c'$ operation involving $s$'s only. $s$ is therefore a generator of the reduced group, which is thus cyclic.

In applying our general criterion of reducibility to cyclic groups, questions of commutativity are automatically disposed of, since every cyclic group is abelian. A cyclic $m$-group will then be reducible to a $\mu$-group, $m=k(\mu-1)+1$, if for some $(\mu-1)$-ad, which may be written $\{s^{[n_1]}, s^{[n_2]}, \cdots, s^{[n_{\mu-1}]}\}$, $s$ being a generator of the cyclic group, the $(m-1)$-ad $\{s^{[n_1]}, s^{[n_2]}, \cdots, s^{[n_{\mu-1}]}, \cdots, s^{[n_1]}, s^{[n_2]}, \cdots, s^{[n_{\mu-1}]}\}$ is an identity of the cyclic group. Hence also if $s^{[k(n_1+n_2+\cdots+n_{\mu-1})+1]}=s$, i.e., if $kn+1$ is a multiple of $g$, where $g$ is the order of the group, $n=n_1+n_2+\cdots+n_{\mu-1}$. It follows first that the cyclic $m$-group is reducible to a $\mu$-group when and only when $k=(m-1)/(\mu-1)$ is prime to $g$. Furthermore, with $k$ prime to $g$, if $kn'+1$ and $kn''+1$ are both multiples of $g$, then $k(n'-n'')$, and hence $n'-n''$, must be a multiple of $g$. It follows from our first law of $m$-adic powers that the $(\mu-1)$-ads corresponding to $n'$ and $n''$ are equivalent. Recalling our general theory of reducibility, we thus see that a cyclic $m$-group is reducible to but one $\mu$-group for each admissible $\mu$.

The least value of $\mu$ for which $(m-1)/(\mu-1)$ is prime to $g$ corresponds to a $k$ which is the largest divisor of $m-1$ prime to $g$. We thus obtain the following result. *The real dimension of a cyclic m-group of order g is equal to* $(m-1)/k_0+1$ *where* $k_0$ *is the largest divisor of* $m-1$ *prime to g.* In particular

*a cyclic m-group of order g is irreducible when and only when each prime factor of $m-1$ is also a prime factor of g.* Our previous uniqueness result easily enables us to complete the picture as far as mere reducibility is concerned. We thus see that *the real dimension of a cyclic m-group of order g is its only irreducible dimension; and the groups to which the cyclic m-group is reducible, all cyclic, consist of a single group of dimension equal to the real dimension of the given group, and those of its extensions whose dimensions are of the form $k(\mu_0-1)+1$, where $\mu_0$ is the real dimension in question, k any proper divisor of $k_0=(m-1)/(\mu_0-1)$.*

Since the subgroups of a cyclic group are themselves cyclic, we can find their real dimensions by applying the above formula. $\gamma$ will be the order of a subgroup of a cyclic $m$-group of order $g$ if it is a divisor of $g$ with $g/\gamma$ prime to $m-1$. Writing $g=d\gamma$, with $d$ prime to $m-1$, we see that the largest divisor of $m-1$ prime to $\gamma$ is also the largest divisor of $m-1$ prime to $g$. Hence, *all the subgroups of a cyclic polyadic group have the same real dimension, namely the real dimension of the group itself.* It follows that a subgroup of a cyclic $m$-group is reducible to a $\mu$-group when and only when the given group is reducible to a $\mu$-group. In particular, *all the subgroups of an irreducible cyclic group are irreducible.* We now readily verify that the following simple situation holds. *If a cyclic m-group be reduced to a $\mu$-group, the subgroups of the m-group are thereby reduced to the subgroups of the $\mu$-group*(69). In fact, half of this situation obtains for arbitrary polyadic groups. For from the very definition of reducibility, if a polyadic group $G$ is reduced to a polyadic group $G'$, the subgroups of $G'$ are also subgroups of $G$, or more exactly, reductions of subgroups of $G$. Moreover, if $G$ is abelian, every reduction of a subgroup of $G$ can be effected by thus reducing $G$ to some $G'$. For the satisfaction of our general criterion of reducibility by the subgroup then holds equally well for $G$, and the same operation that serves to reduce the subgroup is shown by the proof of that criterion to reduce $G$ as well. If now $G$ is cyclic and reducible to a $\mu$-group, every subgroup of $G$ is reducible to a $\mu$-group; and since $G$ can be reduced to but a single $\mu$-group $G'$, that reduction must reduce all the subgroups of $G$ to subgroups of $G'$, and hence by the first part of the proof to the subgroups of $G'$. Our proof incidentally shows that by varying $\mu$ every possible reduction of a subgroup of $G$ will thus be obtainable. We furthermore have the following corollary which, indeed, can easily be proved directly, and itself used to give a different turn to our proofs. *The polyadic orders of the elements of a cyclic polyadic group remain unchanged under every reduction of the group.*

While cyclic groups form a closed set with respect to the two operations "subgroup of" and "reduction of," they do not form a closed set under the operation of extension, of which reduction is the inverse, and hence under the more general operation of derivation. We proceed to prove that *a cyclic*

(69) We prove this result independently of the discussion of complexes which concluded §5, since that discussion was extremely sketchy.

*m-group of order g remains cyclic when extended to a $\mu$-group, $\mu = k(m-1)+1$, when and only when k is prime to g.* Let the polyadic $n$th powers of an element $s$ in the two groups be written more explicitly $s^{[n]_m}$ and $s^{[n]_\mu}$. By counting $c$'s we then have immediately

$$s^{[n]_\mu} = s^{[kn]_m}.$$

Let $s$ be a generator of the extended group, assuming that group to be cyclic. The elements of that group, and hence of the given group, will then be given by the $\mu$-adic powers of $s$, and hence by those $m$-adic powers of $s$ of the form $s^{[kn]_m}$. For each $N$, therefore, there must be an $n$ such that $s^{[N]_m} = s^{[kn]_m}$, and hence an $n$ and $\nu$ such that $N = kn + g\nu$. This will be so when and only when $k$ is prime to $g$.

A group may therefore be reducible to a cyclic group without itself being cyclic. It will be convenient to have the phrase "reducible to a cyclic group" cover even the irreducible cyclic groups. The class of groups reducible to cyclic groups is therefore a wider class than the class of cyclic groups. While it is obviously closed under the operation "extension of," the situation has become obscured so far as the operations "reduction of" and "subgroup of" are concerned. It turns out that the following discussion of the corresponding associated groups clears up the entire situation.

We first reinterpret $m$-adic power and $m$-adic order in terms of the coset theorem. More generally, let $s$ be an element of an arbitrary $m$-group $K$, $K^{*\prime}$ an arbitrary containing group of $K$. Then, in the notation of $K^{*\prime}$, the $m$-adic $n$th power $s^{[n]}$ of $s$ is the ordinary power of $s$, $s^{(m-1)n+1}$. The $m$-adic order of $s$ is therefore the least positive integral value of $n$ for which $s^{(m-1)n+1} = s$, i.e., for which $s^{(m-1)n} = 1$. It follows that the $m$-adic order $g$ of $s$ is identical with the ordinary order of $s^{m-1}$. As for the ordinary order of $s$ as element of $K^{*\prime}$, we can offhand merely say that it is a divisor of $(m-1)g$. If, however, $K^{*\prime}$ is of index $m-1$, in particular if it be the abstract containing group $K^*$ of $K$, then $s^N = 1$ is possible only if $N$ is a multiple of $m-1$, and hence the ordinary order of $s$ will be exactly $(m-1)g$.

These observations are immediately applicable to our discussion of cyclic polyadic groups, and are in turn illuminated thereby. We first observe that *every containing group $G^{*\prime}$ of a cyclic m-group G is cyclic.* For if $s$ is a generator of $G$, the elements of $G$ being the $m$-adic powers of $s$ are also ordinary powers of $s$ in $G^{*\prime}$. Hence the elements of $G^{*\prime}$, being products of elements of $G$, are also ordinary powers of $s$, and $G^{*\prime}$ is an ordinary cyclic group generated by $s$. Note that if $G^{*\prime}$ is of index $m-1$, as is always the case when $s$ is an element of $K$ with $K^{*\prime}$ of index $m-1$, then the order of $G^{*\prime}$ is $m-1$ times the order of $G$ and thus again the ordinary order of $s$, $m-1$ times its $m$-adic order.

Since the abstract containing group $G^*$ of a cyclic $m$-group $G$ is cyclic, it follows that its subgroup $G_0$, the associated ordinary group of $G$, is cyclic. Indeed, our earlier result to the effect that the $m$-adic order of $s$ is equal to the

ordinary order of $s^{m-1}$ shows that an element $s$ of an $m$-group $G$ generates $G$ when and only when $s^{m-1}$, then an element of $G_0$, generates $G_0$.

This result can be immediately generalized to the following. *The associated ordinary group of a group reducible to a cyclic polyadic group is cyclic.* For the abstract containing group of the cyclic polyadic group is a containing group of the given group. The abstract associated group of the cyclic polyadic group, cyclic by the preceding result, is therefore the associated group of the given group corresponding to the above containing group. But we have shown in §6 that all containing groups of a given polyadic group yield simply isomorphic associated groups.

We have seen that every containing group of a cyclic polyadic group is cyclic. While the last argument shows that some containing group of a group reducible to a cyclic polyadic group is cyclic, it is not true that every containing group of such a group is cyclic. In fact it is readily proved that if the abstract containing group of a polyadic group is cyclic, the polyadic group itself must be cyclic. Hence, while cyclic polyadic groups are characterized by the fact that their abstract containing groups are cyclic, we must seek elsewhere for a similarly definite characterization of groups reducible to cyclic polyadic groups.

This characterization cannot consist merely of the associated ordinary group of a polyadic group being cyclic; for the abelianism of cyclic polyadic groups makes every group reducible to a cyclic polyadic group abelian, while non-abelian polyadic groups exist whose associated ordinary groups are cyclic. The added hypothesis of abelianism is however sufficient. We proceed to prove the following result which will enable us to close the entire polyadic development of cyclic groups. *Every abelian polyadic group with cyclic associated ordinary group is reducible to a cyclic polyadic group.* Since the commutativity of two elements can be tested by any extended operation, it follows that an abelian group can be reducible only to an abelian group. Coupled with the previous observations on containing and associated groups, it follows that if an abelian group with cyclic associated group is reducible to a second group, the latter is also an abelian group with cyclic associated group. Our result will therefore have been proved if we show that every irreducible polyadic group of this type is in fact cyclic.

Let then $G$ be an irreducible abelian $m$-adic group of order $g$ with cyclic associated group $G_0$. With $s_0$ a fixed element of $G$, $t$ a generator of $G_0$, the $g$ elements of $G$ may be written $s_0t^n$, $n=0, 1, 2, \cdots, g-1$, in accordance with the coset theorem. The $(m-1)$-ad $s_0^{m-1}$ will itself be in $G_0$. Let then $s_0^{m-1}=t^\kappa$. Since $G$ is abelian, its reducibility to a $\mu$-group, with $m-1=k(\mu-1)$, would be equivalent to the existence of a $(\mu-1)$-ad $\{s_0t^{i_1}, s_0t^{i_2}, \cdots, s_0t^{i_{\mu-1}}\}$ such that $(s_0t^{i_1}s_0t^{i_2}\cdots s_0t^{i_{\mu-1}})^k=1$, i.e., such that

$$k(i_1 + i_2 + \cdots + i_{\mu-1})+\kappa\equiv 0 \pmod g\ (70),$$

(70) $G$ being abelian, $s_0$ and $t$ are commutative.

and hence to the H.C.F.$(k, g)$'s being a divisor of $\kappa$. It follows that the irreducibility of $G$ is equivalent to the combined condition, each prime divisor of $m-1$ is a divisor of $g$, $\kappa$ is prime to $m-1$. On the other hand, we have seen that an element $s$ of $G$ generates $G$ when and only when $s^{m-1}$ generates $G_0$. With $s=s_0t^\nu$, $s^{m-1}=t^{\kappa+(m-1)\nu}$. Since, for our irreducible $G$, $\kappa$ is prime to $m-1$, the arithmetic progression

$$\kappa + (m-1)\nu, \qquad \nu = 0, 1, 2, \cdots,$$

will certainly include a value which is prime to $g$. With $\nu$ thus chosen, $t^{\kappa+(m-1)\nu}$, i.e., $s^{m-1}$, is a generator of the cyclic $G_0$, and hence $s$ of the consequently cyclic $G$.

We thus see that the class of polyadic groups reducible to cyclic polyadic groups is identical with the class of abelian polyadic groups with cyclic associated groups. The first formulation immediately showed this class of groups to be closed under the operation "extension of." The second formulation was already used to prove it closed under the operation "reduction of." It also easily shows the class to be closed under the operation "subgroup of." For such a subgroup must be abelian; while its associated group, being a subgroup of the associated group of the parent group, must be cyclic. Hence the class of polyadic groups reducible to cyclic polyadic groups is closed under the three operations "reduction of," "extension of," and "subgroup of."

In particular, the net of groups derivable from a cyclic polyadic group, or for that matter from a group reducible to a cyclic polyadic group, consists wholly of groups reducible to cyclic polyadic groups. The irreducible groups of the net are therefore all cyclic. Since we are dealing with abelian groups of finite order, the outer real dimension of these groups is 2. Hence the net of groups is in fact also derivable from an ordinary cyclic group. We proceed then to study the net of groups derivable from a cyclic 2-group of order $g$. Our general theory shows that for each $m \geqq 2$ there will be $g$ $m$-groups in the net, one for each class of equivalent $(m-1)$-ads of the 2-group, said class serving as the class of identities of the $m$-group. In terms of the given 2-group, equivalent polyads are equivalent to a unique element of the group. Hence the groups of the net are determined in 1-1 fashion by letting $m$ run through the values 2, 3, 4, $\cdots$, and $s$, the element of the 2-group equivalent to their identities, run through the $g$ elements of that 2-group. By utilizing the expression for the operation of a polyadic group in terms of the operation of a group it is reducible to, and the fact that for any two groups of a net there is a third reducible to each, we find the following expression, in terms of the operation of the 2-group, for the operation $c$ of an $m$-group of the net with identities equivalent to $s$:

$$c(s_1s_2 \cdots s_m) = s_1s_2 \cdots s_ms^{-1}.$$

By means of this formula we easily find which groups of the net are cyclic,

and hence also which are the irreducible groups of the net. While it also enables us to study in detail the relation of reducibility for the groups of the net, the resulting picture is quite complicated, and will not be entered into here.

Let $s_0$ be a generator of the cyclic 2-group, and let $s=s_0^{\lambda}$. If then $s_0^{\nu}$ be any element of the $m$-group of the net with identities equivalent to $s$, the above operation yields the following expression for the corresponding $m$-adic $n$th power of $s_0^{\nu}$:

$$(s_0^{\nu})^{[n]} = s_0^{n(m-1)\nu+\nu-n\lambda}.$$

We then easily find the condition under which, for some $\nu$, $s_0^{\nu}$ is a generator of the $m$-group, and thus obtain the following result. *If $s_0$ is a generator of an ordinary cyclic group of order $g$, the cyclic groups of the net of groups derivable from the given group are those $m$-groups whose identities are equivalent to an $s_0^{\lambda}$ for which* H.C.F.$(m-1, \lambda, g)=1$. If $\gamma$ is the order of $s_0^{\lambda}$ in the 2-group, this condition is equivalent to $g/\gamma$ prime to $m-1$. Thus all of the $g$ $m$-groups of the net for given $m$ are cyclic when and only when $m-1$ is prime to $g$. Since the irreducible groups of the net are the irreducible cyclic groups of the net, we see that *the irreducible groups of the net are those for which the prime divisors of $m-1$ are all divisors of $g$ while $\lambda$ is prime to $m-1$.* Hence, *for $g \geqq 2$, a cyclic polyadic group of order $g$ has an infinite number of outer irreducible dimensions.*

The full force of our closedness results for groups reducible to cyclic polyadic groups is brought out by the complexes obtained from such groups. We have then that the complex of groups obtainable from a cyclic polyadic group, or, in general, from a group reducible to a cyclic polyadic group, consists wholly of groups reducible to cyclic polyadic groups. We recall that the groups of any complex separate into mutually exclusive nets, there being a 1-1 correspondence between these nets and the different classes of elements the groups of the complex can have. In the present instance each net is of the type discussed above, being derivable from a group reducible to a cyclic polyadic group. Furthermore, these "group-bearing" classes now admit of very simple description. As most of the resulting picture holds good for arbitrary finite abelian polyadic groups we so present our development.

Observe first that our simplification of the operations yielding an arbitrary complex shows that its group-bearing classes, apart from that of the initial group, can all be obtained from the subgroups of the extensions of the initial group. Since a finite abelian polyadic group is always derivable from a 2-group, we may then assume that initial group to be a 2-group. That 2-group is then its own associated and containing group, and can be identified with the associated and containing group of each of its extensions. The relationship between the subgroups of a polyadic group and of its associated group, actually valid for an arbitrary containing group, then yields the following result. *The group-bearing classes of a complex obtained from a finite*

*abelian polyadic group are, apart from the class of elements of the given group, the classes of elements of the subgroups of any 2-group derivable from the given group and the cosets of those subgroups.*

We recall that the problem of the intersection of two subcomplexes of a complex was reduced to that of the intersection of their corresponding group-bearing classes. The above result then shows that, for finite abelian groups, either two group-bearing classes have no elements in common, or their common elements constitute an augmented coset of the crosscut of the subgroups of the 2-group of which they are augmented cosets. Note actually that the 2-groups derivable from the given finite abelian group are in 1-1 correspondence with the elements of the group, the element corresponding to a 2-group being the identity of the 2-group. If then $s$ be any element of the given group, the group-bearing classes containing $s$ constitute the subgroups of the 2-group having $s$ as identity. It follows that *if two group-bearing classes of the complex obtained from a finite abelian group have a common element, they are the classes of elements of two subgroups of one and the same 2-group derivable from the given group, and intersect accordingly.*

In particular, then, for a cyclic polyadic group of order $g$ the group-bearing classes of its complex are $g/\gamma$ in number, of $\gamma$ elements each, for every divisor $\gamma$ of $g$. And two group-bearing classes, with $\gamma_1$ and $\gamma_2$ elements respectively, either have no elements in common, or exactly H.C.F.$(\gamma_1, \gamma_2)$ elements in common.

The above development can be given a somewhat different turn. For any finite polyadic group a finite number of extensions of the group, and subgroups of those extensions, suffice to yield all group-bearing classes, as these are now finite in number. From the corresponding situation for a pair of groups of a net it follows that for any finite number of groups of a net there is a group of the net itself reducible to each of the given groups. Hence the above extensions can themselves be extended to one and the same group. In this process the subgroups of these groups are extended to subgroups of the resulting group. Hence, *the group-bearing classes of the complex obtained from a finite polyadic group are the classes of elements of a single suitable extension of the group, and of the subgroups of that extension.* For any finite polyadic group, therefore, the intersection of two group-bearing classes can be pictured as the intersection of two subgroups of one and the same extension of that group. And now for the earlier picture. Clearly any element of finite order in a polyadic group is of first order in some extension of that group, and hence is the sole member of a group-bearing class of the complex obtained from that group. It follows that the elements of the above "suitable extension" of a finite polyadic group are all of first order. Hence that extension will itself be reducible to each of the 2-groups derivable from the given group. If, furthermore, the given group is abelian, each of its elements $s$ will be the identity of a 2-group to which that extension is reducible, and the subgroups of that ex-

tension containing $s$ will thereby be reduced to the subgroups of the 2-group—hence that first picture.

In conclusion, then, while the theory of cyclic groups requires for its completion the introduction of groups reducible to cyclic polyadic groups, the theory of these groups is entirely self-contained. While it would therefore be desirable to complete this theory by developing the properties of these groups, and we have at hand the instruments that would yield this development, we have perhaps already spent too much time on such very special developments, and so pass on to the more general topics of the theory.

23. **Abstract polyadic groups of the first three orders.** The concepts of the last two sections give a certain basis for distinguishing between polyadic groups. As in ordinary theory, in counting abstract polyadic groups no distinction will be made between groups that are simply isomorphic. By contrast, in the theory of reducibility such a distinction is imperative, for two groups on the same class of elements, but with different multiplication tables, must there be considered different even if simply isomorphic. Our present interest lies not only in the results to be obtained but in the illustrations of method thus afforded.

For each $m \geqq 2$ there is of course the single abstract $m$-group of order one. Its sole element is of the first order, and hence the group is cyclic, and reducible to the cyclic 2-group whose sole element is the identity.

The abstract $m$-groups of order two can be determined directly from their possible multiplication tables([71]). If they are written on the abstract elements $\alpha$ and $\beta$, and $c$ represents the $m$-adic operation, the value of $c(\alpha\alpha \cdots \alpha)$, that is, of $\alpha^{[1]}$, determines the table; for each change in the value of an argument must change the value of the result. Hence there are at most two abstract $m$-groups of order two. It further follows that $\alpha^{[1]}$ is, or is not, equal to $\beta^{[1]}$ according as $m$ is even or odd. If $m$ is even, then if $\alpha^{[1]}=\alpha$, $\beta^{[1]}=\alpha$, while if $\alpha^{[1]}=\beta$, $\beta^{[1]}=\beta$, and the two possible groups are changed into each other on interchanging $\alpha$ and $\beta$. On the other hand, if $m$ is odd, if $\alpha^{[1]}=\alpha$, $\beta^{[1]}=\beta$, and if $\alpha^{[1]}=\beta$, $\beta^{[1]}=\alpha$, and the two groups cannot be simply isomorphic. These groups are then readily identified to yield the following result. When $m$ is even, there is but one abstract $m$-group of order two, namely, the cyclic $m$-group of order two. It then consists of one first order element and one second order element, and is reducible to the ordinary cyclic group of order two, if it be not that group. When $m$ is odd there are exactly two abstract $m$-groups of order two; one group consisting of two first order elements, and being the non-cyclic second order $m$-group reducible to the ordinary cyclic group of order two, the other group being the cyclic $m$-group of order two, consisting of two second order elements, and hence not reducible to a 2-group.

([71]) Dörnte used this method to determine the number of $m$-groups on two symbols as elements, but did not consider the question of those $m$-groups being abstractly the same.

To obtain the abstract $m$-groups $G$ of order three, we employ the general coset theorem method of §8. The associated ordinary group $G_0$ must be cyclic, and hence its elements may be written 1, $t$, $t^2$. If $s_0$ be a fixed element of $G$ with $s_0^{m-1}=t_0$, $t_0$ in $G_0$, we may assume that either (1) $t_0=1$, (2) $t_0=t$; for were $t_0=t^2$, groups simply isomorphic with those of case (2) would result. $G_0$, furthermore, admits of but two automorphisms, i.e., (a) the identical automorphism, (b) the automorphism interchanging $t$ and $t^2$ while, of course, leaving 1 invariant. With either of these automorphisms as the automorphism of $G_0$ under $s_0$, and either of the two choices of $t_0$, an $m$-group will be correspondingly determined provided (A) the automorphism carries $t_0$ into itself, (B) the $(m-1)$-st power of the automorphism is the automorphism of $G_0$ under $t_0$. Of the four cases thus to be considered (1) (a) and (2) (a) satisfy both (A) and (B) for all $m$'s, and hence always determine a corresponding $m$-group. (1) (b) satisfies (A) for all $m$'s, but (B) only for $m$ odd; for if $m$ be even, the $(m-1)$-st power of the automorphism interchanges $t$ and $t^2$ whereas $t_0=1$ leaves them unchanged. Hence (1) (b) determines an $m$-group when and only when $m$ is odd. Finally, there is no polyadic group of order three corresponding to (2) (b), as (A) is then never satisfied.

We now identify and distinguish between the groups thus determined. The group (1) (a) is abelian since $s$ and $t$ are then commutative. Since $G_0$ is cyclic, $G$ is therefore cyclic, or reducible to a cyclic group. Direct calculation then shows that if $m-1$ is a multiple of 3, each element is of first order, and hence the group is noncyclic, but reducible to the ordinary cyclic group of order three. On the other hand, when $m-1$ is not a multiple of 3 we find that while $s_0$ is of first order, $ts_0$, and in fact $t^2s_0$, are not, and hence must be of the third order. The group is therefore cyclic, but reducible to the ordinary cyclic group.

In the case of the group (2) (a), $s_0$, not being of the first order, must be of the third order. The group is therefore cyclic. When $m-1$ is not a multiple of 3 it is therefore simply isomorphic with the group (1) (a). On the other hand, when $m-1$ is a multiple of 3, and hence not prime to $g=3$, the group contains no first order element. It is therefore not reducible to an ordinary group, and consists of three third order elements.

Finally group (1) (b), $m$ odd, is non-abelian, since $s_0$ does not leave $t$ invariant. Being therefore noncyclic, each of its elements is of the first order. We have already given this group with $m=3$ as an example of one with no invariant element. This property holds for each admissible $m$. In fact, since any two of the three elements must generate the whole non-abelian group, each element is invariant under no other element than itself. It follows that each element transforms a second element into the third, a property which by itself can be shown to determine the multiplication table of that third order $m$-group for odd $m$. It is needless to add that this group is not reducible to an ordinary group.

The third order abstract polyadic groups may then be tabulated as follows, the numbers in the parentheses being the orders of the elements.

$\mu=0, 1, 2, \cdots$

| $m-1=$ | $6\mu+1$ | $6\mu+2$ | $6\mu+3$ | $6\mu+4$ | $6\mu+5$ | $6\mu+6$ |
|---|---|---|---|---|---|---|
| cyclic (3, 3, 1) | 1 | 1 | | 1 | 1 | |
| cyclic (3, 3, 3) | | | 1 | | | 1 |
| abelian (1, 1, 1) | | | 1 | | | 1 |
| non-abelian (1, 1, 1) | | 1 | | 1 | | 1 |
| total | 1 | 2 | 2 | 2 | 1 | 3 |

In particular, the one ordinary third order group comes under the case $m-1=6\mu+1$ with $\mu=0$. We further see that the smallest value of $m$ for which there are three abstract third order groups is $7$([72]).

24. **Properties of transforms.** The coset theorem enabled us to write the transform of an element $s$ by a polyad $r$ in the ordinary form $r^{-1}sr$. A fundamental $m$-group is of course tacitly presupposed. Since the $m$-adic $n$th power of an element can likewise be written as an ordinary $(m-1)n+1$ power, it follows that

$$(r^{-1}sr)^{[n]} = r^{-1}s^{[n]}r.$$

Hence, also, the $m$-adic order of an element is unchanged under transformation.

Suppose now that $r^{-1}sr=s^{[\alpha]}$. By raising both sides of this equation to the $m$-adic $\beta$th power we then have

$$r^{-1}s^{[\beta]}r = (s^{[\beta]})^{[\alpha]};$$

for our $m$-adic formula for the power of a power shows that $(s^{[\alpha]})^{[\beta]}=(s^{[\beta]})^{[\alpha]}$. Hence we have the following generalization of the corresponding ordinary theorem. *If a polyad transforms a generator of a cyclic m-group into its $\alpha$th power, it transforms every element of this cyclic group into its $\alpha$th power.*

Commutativity is related to transform through invariance. Given two noncommutative elements $s_0$ and $s$, we consider what $m$-adic powers, if any, of $s$ are commutative with $s_0$. If $s$ is of $m$-adic order $k$, its ordinary order in the fundamental abstract containing group is $(m-1)k$. Let $\gamma_0$ be the least positive value of $\gamma$ for which the ordinary power $s^\gamma$ is commutative with $s_0$. $\gamma_0$ is then a divisor of $(m-1)k$ and the distinct ordinary powers of $s$ commutative with $s_0$ are $s^{n\gamma_0}$, $n=1, 2, \cdots, (m-1)k/\gamma_0$. The $m$-adic powers $s^{[\beta]}$ commuta-

([72]) The two third order $m$-groups falling under the case $m-1=6\mu+2$ have been given by Miller for $\mu=0$

tive with $s_0$ are those for which $(m-1)\beta+1$ is a multiple of $\gamma_0$. It follows first that there will be an $m$-adic power of $s$ commutative with $s_0$ when and only when $\gamma_0$ is prime to $m-1$. $\gamma_0$ is then a divisor of $k$; and if $\beta_0$ is the least value of $\beta$ for which $s^{[\beta]}$ is commutative with $s_0$, the $m$-adic powers of $s$ commutative with $s_0$ are $s^{[\beta_0+n\gamma_0]}$, $n=0, 1, \cdots, (k/\gamma_0-1)$. Actually these $k/\gamma_0$ $m$-adic powers of $s$ commutative with $s_0$ must constitute a subgroup, necessarily cyclic, of the cyclic $m$-group generated by $s$. They are therefore the $m$-adic powers of some one of their number, not, however, necessarily of $s^{[\beta_0]}$ [73].

If we form the successive transforms

$$s^{-1}s_0s = s_1,\ s^{-1}s_1s = s_2,\ \cdots,\ s^{-1}s_{n-1}s = s_n,\ \cdots,$$

the resulting elements are the transforms of $s_0$ under the various ordinary powers of $s$. In general, therefore, they will not all be gotten by transforming $s_0$ by the elements of the cyclic $m$-group generated by $s$, but by the elements of the abstract containing group of that cyclic $m$-group, or, what is the same thing, by the various polyads of the cyclic $m$-group.

This suggests that given any $m$-group $G$ and element $s_0$ we consider the transforms of $s_0$ under the various polyads of $G$. These will then constitute a complete set of conjugates of $s_0$ under the abstract containing group $G^*$ of $G$. The following discussion applies equally well to an $m$-group $K$ taking the place of the element $s_0$.

With $s$ an element in $G$, $G_0$ the associated ordinary group of $G$, we have the expansion $G^*=G_0s+G_0s^2+\cdots+G_0s^{m-2}+G_0$, with $G_0s=G$. Since $G_0$ is an ordinary group, the number of transforms of $s$ under the elements of $G_0$ is some divisor $\nu$ of $g$, the common order of $G$ and $G_0$. Each coset $G_0s^i$ therefore transforms $s_0$ into $\nu$ distinct elements. If two cosets yield a common transform of $s_0$, by writing those cosets in the form $r_1G_0$, $r_2G_0$, $r_1$ and $r_2$ being elements of the cosets yielding that common transform, we see that the set of transforms yielded by one coset is identical with the set yielded by the other. The transforms of $s_0$ under $G^*$ thus fall into a certain number $\kappa$ of mutually exclusive classes of $\nu$ elements each. By a method entirely analogous to that used in the analysis of an arbitrary containing group, we easily find that $\kappa$ is a divisor of $m-1$, and that the first $\kappa$ cosets all yield distinct sets of $\nu$ transforms each, these being repeated in order by each succeeding set of $\kappa$ cosets. We thus have the following theorem. *The number of transforms of an element under the polyads of an m-group of order g is of the form* $\kappa\nu$, *where* $\nu$ *is a divisor of g,* $\kappa$ *a divisor of* $m-1$. *For each i the i-ads of the group yield* $\nu$ *distinct transforms. The* $\kappa\nu$ *transforms can be obtained from the i-ads with* $i=1, 2, \cdots, \kappa$; *and these* $\kappa$ *mutually exclusive sets of* $\nu$ *transforms each are cyclically repeated for i-ads with* $i>\kappa$.

We can now connect the theory of transforms with that of groups of sub-

[73] As may be shown by an example.

stitutions. For convenience set $\kappa=\mu-1$, and let $\Gamma_1, \Gamma_2, \cdots, \Gamma_{\mu-1}$ be the mutually exclusive sets of $\nu$ transforms each corresponding to $i=1, 2, \cdots, \mu-1$ respectively. If $s_j$ is any element of $G$, and $s'$ is the transform of $s_0$ by an $i$-ad of $G$, $s_j^{-1}s's_j$ will be the transform of $s_0$ by an $(i+1)$-ad of $G$. It follows that $s_j$ transforms the members of each $\Gamma_i$ in 1-1 fashion into the members of $\Gamma_{i+1}$. Thus each element of $G$ determines a $\mu$-adic substitution on $\Gamma_1, \Gamma_2, \cdots, \Gamma_{\mu-1}$. Clearly, the product of $m$ elements of $G$ yields a $\mu$-adic substitution which is the product of the $\mu$-adic substitutions yielded by those elements. Certainly then, for our finite $G$ the class of all $\mu$-adic substitutions corresponding to elements of $G$ constitutes an $m$-adic group of $\mu$-adic substitutions isomorphic with $G$. It is readily seen that if $N$ elements of $G$ correspond to one $\mu$-adic substitution, exactly $N$ elements of $G$ correspond to each $\mu$-adic substitution, and the isomorphism is $(1, N)$. Finally, this $(m, \mu)$ substitution group is transitive. For if element $s'$ of $\Gamma_i$ is the transform of $s_0$ by the $i$-ad $\{s_{j_1}, s_{j_2}, \cdots, s_{j_i}\}$ of $G$, the transforms of $s'$ by the elements $s_j$ of $G$ are the transforms of $s_0$ by the $(i+1)$-ads $\{s_{j_1}, s_{j_2}, \cdots, s_{j_i}, s_j\}$ of $G$, hence by all $(i+1)$-ads of $G$, and so constitute the whole class $\Gamma_{i+1}$.

When $\kappa=1$, the $(m, \mu)$ substitution group becomes a transitive $m$-group of ordinary substitutions. The transforms of $s_0$ under the elements of $G$, now identical with the transforms of $s_0$ under the polyads of $G$, then include $s_0$, and are such that each is transformed into the entire set by the elements of $G$. On the other hand, when $\kappa>1$, the transforms of $s_0$ under the elements of $G$ are transformed by the elements of $G$ into an entirely different set. Nor can they then include $s_0$; for $s_0$, being transformed into itself by that $(m-1)$-ad of $G$ which is the identity of $G_0$, appears for the first time in the set of transforms for which $i=\kappa$. We thus see that the transforms of $s_0$ under the elements of $G$ must be said to constitute a complete set of conjugates of $s_0$ under $G$ when and only when $\kappa=1$. And the fact that then and only then is $s_0$ included in that set of transforms needs only restatement to become the following useful criterion. *The necessary and sufficient condition that the transforms of an element $s_0$ by the elements of an $m$-group $G$ constitute a complete set of conjugates under $G$ is that $s_0$ is commutative with some element of $G$.* As in the case of ordinary groups, the elements of $G$ thus leaving $s_0$ invariant constitute a subgroup $H$ of $G$. If $G$ is expanded in right cosets as regards $H$, each coset consists of all the elements of $G$ transforming $s_0$ into some one element. Hence, here too the number of conjugates of $s_0$ under $G$ is the order of $G$ divided by the order of the largest subgroup of $G$ leaving $s_0$ invariant.

If $s_0$ is actually an element of $G$, the above condition is automatically satisfied with $s_0$ itself as element commutative with $s_0$. We thus have the significant fact that the transforms of an element of a polyadic group under the elements of the group always constitute a complete set of conjugates under the group([74]). Hence, as for ordinary groups, *all the elements of an $m$-group $G$*

([74]) Essentially a result of Miller's when stated for "perfect cosets."

*can be separated into distinct complete sets of conjugates as regards G, and this separation can be performed in only one manner.*

In the case of an $i$-ad of $G$ with $i>1$ the transforms of the $i$-ad by the elements of $G$ need no longer constitute a complete set of conjugates. Thus in the non-abelian 3-group of order three a dyad not the identity has but one transform under the elements of the group, two under the polyads of the group. However, our general theorem holds in this case; and since the $i$-ad is invariant under itself, it readily follows that $\kappa$ is a divisor of H.C.F.$(i, m-1)$.

25. **Generation of polyadic groups by two groups, one invariant under the elements of the other.** We shall consider two distinct cases. In the first, a 2-group $H_0$ is invariant under each element of an $m$-group $K$, in the second, an $m$-group $H$ is invariant under each element of an $m$-group $K$. The discussion of the $m$-group $G$ generated by the two given abstract groups can also be carried through from two different points of view, the first, that of the investigation of properties of groups assumed given, the second, that of the construction of groups hitherto unknown.

We have already illustrated the constructional point of view in §8. Our present interests being largely theoretical, we shall not further pursue the complexities introduced by that point of view in the field of abstract group theory, but merely obtain the results given by the first point of view([75]).

([76]) This is the point of view really followed by Miller in §25, *Finite Groups*, despite the section heading "Construction of Groups with Invariant Subgroups." He thus obtains the theorem: "If all the elements of a group $H$ transform $G$ into itself, then $H$ and $G$ generate a group whose order is the order of $G$ multiplied by the index under $H$ of the crosscut of $G$ and $H$." The constructional point of view, while using his treatment for purposes of analysis, would necessitate the following complications. $H$ and $G$ would be given by group-satisfying multiplication tables on specified symbols as elements. These tables must then satisfy the consistency condition that $H$ and $G$ have at least one element in common, and that the product of two elements common to $H$ and $G$ is the same in $H$ as in $G$. With each element of $H$ there would be given a corresponding automorphism of $G$ which is to be the automorphism of $G$ induced by transforming it by that element of $H$. These automorphisms must then satisfy the consistency conditions that the product of the automorphisms corresponding to two elements of $H$ is the automorphism corresponding to the product of those elements, while the automorphism corresponding to any element of $H$ common to $H$ and $G$ is the automorphism of $G$ induced by that element as element of $G$. That posited, our guess is that $H$ and $G$, assumed finite, will generate a unique group in the sense that there exists a group $K$ which, with respect to itself as fundamental group, is the group generated by $H$ and $G$, while all such groups are simply isomorphic; a simple isomorphism being in fact determined by letting each element of $H$ and $G$ correspond to itself.

The above criticism assumes that we are dealing with abstract groups, the title of the chapter in which the above section appears. If the generating groups be given as substitution groups, for example, the divergence between the two points of view disappears, as there is always the symmetric group on all the letters involved to act as fundamental group. A similar situation obtains for $m$-adic groups of ordinary substitutions as is shown in the last footnote of our present section.

It should be pointed out that what we have termed the constructional point of view is followed in the related theory of group extensions. (See the first footnote to §8.) That it is but

This point of view assumes a given $m$-group $F$. In the first of our two cases, $H_0$ is a subgroup of the associated ordinary group $F_0$ of $F$ which is invariant under each element of a subgroup $K$ of $F$. It is convenient here to consider $F$ a subgroup of itself. The crosscut of all subgroups of $F$ which are such that $H_0$ is a subgroup of their associated groups, $K$ of themselves, is itself one of these subgroups, and will be said to be the $m$-group $G$ generated by $H_0$ and $K$. We may then also say that the $m$-group $G$ generated by $H_0$ and $K$ is the smallest subgroup $G$ of $F$ such that $H_0$ is a subgroup of $G_0$, $K$ of $G$. Similarly, if $H$ and $K$ are two subgroups of $F$ with $H$ invariant under each element of $K$, the $m$-group $G$ generated by $H$ and $K$ is the smallest subgroup $G$ of $F$ such that $H$ and $K$ are subgroups of $G$. The existence and uniqueness of $G$ is thus assured, but is entirely relative to the given $m$-group $F$.

We shall first consider the subcase of the general $H_0$, $K$ case where $K$ is the cyclic $m$-group generated by an element $s$ of $F$. The $m$-group generated by $H_0$ and $K$ may then also be said to be generated by $H_0$ and $s$. The invariance condition now reduces to $H_0$ being transformed into itself by $s$. Consider the cosets $H_0s$, $H_0s^{[1]}$, $H_0s^{[2]}$, $\cdots$. If $\gamma$ is the $m$-adic order of $s$, $H_0s = H_0s^{[\gamma]}$. Let then $\kappa$ be the smallest positive integer for which $H_0s = H_0s^{[\kappa]}$. It then easily follows that the cosets $H_0s$, $H_0s^{[1]}$, $\cdots$, $H_0s^{[\kappa-1]}$ are mutually exclusive, while succeeding cosets are cyclic reproductions of these. Hence, also, $\kappa$ is a divisor of $\gamma$.

We now readily show that the $m$-group $G$ generated by $H_0$ and $s$ is given by

$$G = H_0s + H_0s^{[1]} + \cdots + H_0s^{[\kappa-1]}.$$

Since $H_0$ is a subgroup of $F_0$, $s$ an element of $F$, the set $G$ thus defined is contained in $F$. Furthermore, the invariance of $H_0$ under $s$ coupled with the above coset analysis shows that the product of $m$ elements of $G$ is in $G$. Hence $G$ is, indeed, a subgroup of $F$. $G$ has $s$ for element, in fact, as a member of $H_0s$. Hence $G_0 = Gs^{-1}$ has $H_0$ as subgroup. Finally, as with $F$, every subgroup of $F$ whose associated group has $H_0$ as subgroup, while it has $s$ as element, contains $G$. Hence $G$ is the $m$-group generated by $H_0$ and $s$. We thus have the theorem: *If $s$ is an element of an $m$-group, $H_0$ a subgroup of the associated group of that $m$-group invariant under $s$, then if $s^{[\kappa]}$ is the smallest positive $m$-adic power of $s$ which is in the coset $H_0s$, $H_0$ and $s$ generate an $m$-group whose order is $\kappa$ times the order of $H_0$.*

In the general $H_0$, $K$ case let $L_0$ be the crosscut of $H_0$ and $K_0$. Since $H_0$ and $K_0$ are invariant under each element of $K$, the same is true of $L_0$. Expand $K$ in cosets as regards $L_0$, and let $s_1, s_2, \cdots, s_\kappa$ be a corresponding set of multi-

---

a related theory may be seen from the definition of an extension $K$ of $G$ by $H$ as a group having $G$ as invariant subgroup, with the quotient group $K/G$ simply isomorphic to $H$. The above complication arising from the common elements of $H$ and $G$ goes not then arise.

pliers. We then show that the $m$-group $G$ generated by $H_0$ and $K$ has the expansion

$$G = H_0 s_1 + H_0 s_2 + \cdots + H_0 s_\kappa$$

with all indicated elements distinct. As a consequence of the invariance of $H_0$ under each $s_i$ we can reduce the product of $m$ elements of the set $G$ thus defined to the form $ts$, with $t$ in $H_0$, $s$ in $K$. As $s$ can further be written $t's_i$ with $t'$ in $L_0$, and hence in $H_0$, $s_i$ one of the above $\kappa$ multipliers, we see that the product in question is in $G$. It then follows as in the special case that $G$ is the $m$-group generated by $H_0$ and $K$. Moreover, suppose that with $t_1$ and $t_2$ in $H_0$ we have $t_1 s_{i_1} = t_2 s_{i_2}$. Then $t_2^{-1} t_1 = s_{i_2} s_{i_1}^{-1}$. Since the left side of this equation represents an element of $H_0$, the right of $K_0$, this one element $\tau$ is in $L_0$. But then $s_{i_2} = \tau s_{i_1}$, contradicting the assumption that $s_1, s_2, \cdots, s_\kappa$ were the set of multipliers in question. The indicated elements of $G$ are thus distinct, and we have the theorem: *If $K$ is a subgroup of an $m$-group, $H_0$ a subgroup of the associated group of the $m$-group invariant under each element of $K$, then $H_0$ and $K$ generated an $m$-group whose order is the order of $H_0$ multiplied by the index under $K$ of the crosscut of $H_0$ and the associated ordinary group $K_0$ of $K$.*

We turn now to the more interesting case of the $m$-group $G$ generated by two $m$-groups $H$ and $K$, with $H$ invariant under each element of $K$. Note that $H_0$, the associated ordinary group of $H$, is then also invariant under $K$. It is readily seen that while the $m$-group generated by $H_0$ and $K$ is contained in the $m$-group generated by $H$ and $K$, it will be identical with that $m$-group when and only when it contains an element of $H$. This means that for some $t$ in $H_0$, $s$ in $K$, $s'$ in $H$, $ts = s'$. But this is equivalent to $s = t^{-1}s'$, i.e., to $s$'s also being in $H$. Hence *the $m$-group generated by $H$ and $K$ is identical with the $m$-group generated by $H_0$ and $K$ when and only when $H$ and $K$ have a common element.*

In particular, if $H$ and $K$ have but one common element, while each element of $H$ is commutative with each element of $K$, we shall say that the $m$-group $G$ generated by $H$ and $K$ is their *direct product*. $G$, then, is also the $m$-group generated by $H_0$ and $K$, and by $K_0$ and $H$, and correspondingly has expansions which may be briefly written $G = H_0 \times K = K_0 \times H$. For $L_0$ now reduces to the identity, so that in the first case, for example, the multipliers $s_i$ are all the elements of $K$. More symmetrically then, $G = (H_0 \times K_0)s$, with $s$, say, the unique common element of $H$ and $K$. It follows that $G_0 = H_0 \times K_0$ is the ordinary direct product of $H_0$ and $K_0$. Clearly $s$ must be of first order, since all of its $m$-adic powers must be common elements of $H$ and $K$; and being invariant under $H$ and $K$, it must also be invariant under $G$. All three groups are therefore reducible to ordinary groups, and simultaneously so. These considerations immediately extend to the "direct product" of any number of $m$-groups provided the unique common element is also the only element common to each group and the group generated by the remaining groups.

Special as this concept of direct product thus turns out to be, it is very useful in the theory of abstract polyadic groups. By contrast, the direct product method as applied to $m$-adic substitution groups, while involving no restriction on the groups per se, did not yield the $m$-group generated by the given $m$-groups, and hence is restricted in its usefulness to the construction of desired $m$-groups.

In the most general $H$, $K$ case consider the abstract containing groups of the $m$-groups involved. Since $H$, $K$, and $G$ are subgroups of the fundamental $m$-group $F$, their abstract containing groups $H^*$, $K^*$, and $G^*$ may be considered subgroups of the abstract containing group $F^*$ of $F$. As the elements of an $m$-group generate the corresponding containing group, it easily follows that $G^*$ is the ordinary group generated by $H^*$ and $K^*$. Since $H^*$ will be invariant under each element of $K^*$, the standard theorem tells us that the order of $G^*$ is equal to the order of $H^*$ multiplied by the index under $K^*$ of the crosscut of $H^*$ and $K^*$. But the order of the abstract containing group of an $m$-group is $m-1$ times the order of the $m$-group. Hence the order of $G$ is equal to the order of $H$ multiplied by that index.

It is easy indeed to write the actual expansion of $G$. According to the standard theory, if we expand $K^*$ in cosets as regards the crosscut of $H^*$ and $K^*$, and let $r_1, r_2, \cdots, r_n$ be the corresponding set of multipliers, then $G^*=H^*r_1+H^*r_2+\cdots+H^*r_n$ with all indicated elements distinct. If then $r_j$ is an $i_j$-ad of $K$, the elements of $H^*r_j$ in $G$ will be the $(m-i_j)$-ads of $H$ multiplied by $r_j$. We may therefore write, in notation thus suggested,

$$G = (H)_{m-i_1}r_1 + (H)_{m-i_2}r_2 + \cdots + (H)_{m-i_n}r_n.$$

Returning to the order of $G$, we seek a useful expression for the index in question. The crosscut $\overline{L}$ of $H^*$ and $K^*$ will consist of the common $i$-ads of $H$ and $K$ for $i=1, 2, \cdots, m-1$. For $i=m-1$, these common $i$-ads constitute the crosscut $L_0$ of $H_0$ and $K_0$. Let $l$ be the order of $L_0$, $\kappa$ the smallest value of $i$ for which $H$ and $K$ have a common $i$-ad. Then, by methods already made familiar, we find that $\kappa$ is a divisor of $m-1$, while $\overline{L}$ consists of $l$ $i$-ads for each of the $(m-1)/\kappa$ $i$'s, $i=\kappa, 2\kappa, \cdots, m-1$. The order of $\overline{L}$ is thus $l(m-1)/\kappa$. If now $k$ is the order of $K_0$, the order of $K^*$ is $(m-1)k$. Hence the index under $K^*$ of $\overline{L}$ is $\kappa k/l$. But $k/l$ is the index under $K_0$ of $L_0$. Hence the index of $\overline{L}$ under $K^*$ is $\kappa$ times the index of $L_0$ under $K_0$. We therefore have the following theorem. *If $H$ and $K$ are two subgroups of an $m$-group such that all the elements of $K$ transform $H$ into itself, then $H$ and $K$ generate an $m$-group whose order is the order of $H$ multiplied by the index under $K_0$ of the crosscut of $H_0$ and $K_0$ multiplied by a divisor $\kappa$ of $m-1$, where $\kappa$ is the smallest value of $i$ for which $H$ and $K$ have a common $i$-ad.*

Of special interest is the case where $K$ is the cyclic $m$-group generated by an element $s$ which transforms $H$ into itself. $K^*$ is then an ordinary cyclic group also generated by $s$. Hence if $s^\lambda$ is the smallest positive ordinary power

of $s$ in $H^*$, $\lambda$ will be the index under $K^*$ of the crosscut of $H^*$ and $K^*$. We thus have as our first result: *If an element $s$ of an $m$-group transforms a subgroup $H$ of that $m$-group into itself, and if $s^\lambda$ is the smallest positive ordinary power of $s$ in the containing group $H^*$ of $H$, then $s$ and $H$ generate an $m$-group $G$ whose order is $\lambda$ times the order of $H$.* Indeed, the expansion of $G$ is now readily seen to be

$$G = (H)_{m-1}s + (H)_{m-2}s^2 + \cdots + (H)_{m-\lambda}s^\lambda.$$

Note that if $k$ is the $m$-adic order of $s$, and hence $k(m-1)$ its ordinary order, $\lambda$ is a divisor of $k(m-1)$. Since the order of $G$ must exceed the order of $H$ whenever $s$ is not in $H$, we obtain the following useful corollary further generalized below. *If $s$ is of $m$-adic order one, and not in $H$, then the order of $G$ is equal to the order of $H$ multiplied by a divisor, not unity, of $m-1$.*

More refined results are yielded by our earlier analysis of the above mentioned index. The associated group $K_0$ of the cyclic $m$-group $K$ generated by $s$ will be the cyclic ordinary group generated by $s^{m-1}$. Hence, if $s^{\nu(m-1)}$ is the smallest positive power of $s^{m-1}$ in $H_0$, $\nu$ will be the index under $K_0$ of the crosscut of $H_0$ and $K_0$. Consequently, *the order of $G$ is also equal to the order of $H$ times $\nu$ times $\kappa$, where $s^{\nu(m-1)}$ is the smallest positive power of $s^{m-1}$ in $H_0$, $\kappa$ the smallest value of $i$ for which $H$ and the cyclic $m$-group generated by $s$ have a common $i$-ad.*

We may note certain relationships between the constants thus involved. The connecting link between our two expressions for the order of $G$ is the equation $\lambda = \nu\kappa$. $\lambda$ is thus determined by $\nu$ and $\kappa$. Conversely $\nu$ and $\kappa$ are determined by $\lambda$ and $m$. For the common elements of $H^*$ and $K^*$ are $s^\lambda, s^{2\lambda}, \cdots, s^{k(m-1)}$. It therefore easily follows that $\kappa = \text{H.C.F.}(m-1, \lambda)$, and hence $\nu = \lambda/\text{H.C.F.}(m-1, \lambda)$. By means of $m$-adic groups of ordinary substitutions it is readily shown that $\lambda$ and $m$ may assume arbitrary values. In the case of $\kappa$, $\nu$, and $m$, we have already observed that $\kappa$ is a divisor of $m-1$. Our expressions for $\kappa$ and $\nu$ in terms of $\lambda$ and $m$ further show that $(m-1)/\kappa$ is prime to $\nu$. Now it is readily verified that if $\kappa$, $\nu$, and $m$ are arbitrarily chosen subject to these two conditions, then $\lambda = \nu\kappa$ redetermines the same $\kappa$ and $\nu$ by means of the above formulas. It follows that $\kappa$, $\nu$, and $m$ may assume any values subject to these conditions. If we now further introduce the $m$-adic orders $h$ and $k$ of $H$ and $s$, we obtain the further conditions $\nu$ a divisor of $k$, $h\nu$ a multiple of $k$; the first from the index interpretation of $\nu$, the second from the order requirement imposed by $s^{\nu(m-1)}$'s being in $H_0$. We have not carried the investigation far enough, however, to see whether the resulting four necessary conditions on $h$, $k$, $\kappa$, $\nu$ and $m$ suffice to insure a corresponding $H$ and $s$([76]).

([76]) When $h=k$, the fourth condition is automatically satisfied. In this case the writer has verified by an example that $h=k$, $\kappa$, $\nu$, and $m$ may have arbitrary values subject to the first three conditions.

In constructing such examples by means of $m$-adic groups of ordinary substitutions, we

$H$ is clearly an invariant subgroup of the generated group $G$. If then $\sigma$ is the element of the $m$-adic quotient group $G/H$ corresponding to $s$, $\nu$ is seen to be the $m$-adic order of $\sigma$. For the least positive $\nu$ with $s^{\nu(m-1)}$ in $H_0$ is the least positive $\nu$ with $s^{[\nu]}$ in $H_0 s$, and hence the least positive $\nu$ with $\sigma^{[\nu]}=\sigma$. By a simple result of our later §29 the $m$-adic order of $\sigma$ is a divisor of the $m$-adic order of $s$. Our previous corollary thus generalizes to the following. *The order of $G$ is equal to the order of $H$ multiplied by a multiple of a divisor other than unity of the $m$-adic order of $s$ whenever the $m$-adic order of the element of $G/H$ corresponding to $s$ is not unity; when the latter order is unity, and yet $s$*

---

are naturally led to the ordinary groups they generate as containing groups. On the other hand, our theory concerns their abstract containing groups only. In the $\lambda$, $m$ example referred to above, it was possible to avoid this difficulty by so choosing $H$, $K$, and the fundamental $F$ that their concrete containing groups were all of index $m-1$, and so simply isomorphic with their abstract containing groups. On the other hand, especially in the case of $F$, it is desirable to dispense with this requirement. For we could then fully make use of the fact that as for ordinary substitution groups, so for $m$-adic substitution groups, a fundamental $F$ is always at hand, namely, the extension to an $m$-group of the ordinary symmetric group on all the letters involved; and clearly all fundamental $F$'s which are $m$-adic groups of ordinary substitutions yield the same $G$.

Actually, we can easily obtain the desired information concerning the abstract containing groups, and so the order of $G$, from any containing groups. We shall consider our general $H$, $K$ case. Let $F$ be a corresponding fundamental $m$-group, $F^{*\prime}$ any containing group of $F$. The subgroups of $F^{*\prime}$ generated by the elements of $H$ and $K$ respectively will then be containing groups $H^{*\prime}$ and $K^{*\prime}$ of $H$ and $K$. In the above case of $m$-adic groups of ordinary substitutions, $F^{*\prime}$ may be the ordinary substitution group generated by the substitutions of $F$, in which case $H^{*\prime}$ and $K^{*\prime}$ will be the ordinary substitution groups generated by the substitutions of $H$ and $K$, and so obtainable without the explicit use of $F^{*\prime}$. Let $H^{*\prime}$, $K^{*\prime}$, $F^{*\prime}$ be of indices $\rho_1$, $\rho_2$, $\rho$. All three indices will then be divisors of $m-1$. Furthermore, it is readily seen that $\rho_1$ and $\rho_2$ will be multiples of $\rho$. Now if the cosets into which these containing groups are broken up are cyclically repeated until there are $m-1$ of each, the $i$th cosets of $H^{*\prime}$ and $K^{*\prime}$ will be contained in the $i$th coset of $F^{*\prime}$ for $i=1, 2, \cdots, m-1$. In particular, the $(m-1)$-st cosets will be the associated ordinary groups $H_0'$, $K_0'$, $F_0'$. And in the simple isomorphism between $F_0'$ and $F_0$, the abstract associated ordinary group of $F$, the subgroups $H_0'$ and $K_0'$ will correspond to $H_0$ and $K_0$. Hence, *the index under $K_0$ of the crosscut of $H_0$ and $K_0$ is also the index under $K_0'$ of the crosscut of $H_0'$ and $K_0'$*, where the latter may now be considered the $\rho_1$th and $\rho_2$th cosets in $H^{*\prime}$ and $K^{*\prime}$. As for $\kappa$, note that two products of $i$ elements each taken from an $m$-group will be identical in a containing group of an $m$-group when and only when those two $i$-ads of elements are equivalent. Hence, the smallest value of $i$ for which $H^*$ and $K^*$ have a common $i$-ad is also the smallest value of $i$ for which $H^{*\prime}$ and $K^{*\prime}$, repeated as above, have a common $i$-ad. Actually, the pairs of $i$th cosets of $H^{*\prime}$ and $K^{*\prime}$ start repeating after $i=$L.C.M. $(\rho_1, \rho_2)$. Hence, $\kappa$ *may be found from $H^{*\prime}$ and $K^{*\prime}$ if their cosets be cyclically repeated to a total number equal to* L.C.M. $(\rho_1, \rho_2)$ *each.* Clearly $\kappa$ is a divisor of L.C.M. $(\rho_1, \rho_2)$. If desired, it is not difficult to give a number theoretic expression for $\kappa$ in terms of the distribution of $(i, j)$'s for which an $i$-ad of $H^{*\prime}$ and a $j$-ad of $K^{*\prime}$ in their unrepeated form are identical.

The order of $G$ is thus determinable from $H^{*\prime}$ and $K^{*\prime}$. Explicitly $F^{*\prime}$ does not enter. Hence, in the case of $H$ and $K$ $m$-adic groups of ordinary substitutions, no further reference need be made to $F$. In particular, then, if $H^{*\prime}$ and $K^{*\prime}$ are each of index $m-1$, the order of $G$ is found exactly as if they were the abstract containing groups of $H$ and $K$.

*is not in H, then the order of G is equal to the order of H multiplied by a divisor, not unity, of* $m-1$.

26. $m$-**adic groups of order** $g$ **prime to** $m-1$. Let $G$ be any $m$-group whose order $g$ is prime to $m-1$. The order of any element $s$ of $G$, being a divisor of $g$, will then also be prime to $m-1$. The cyclic $m$-group generated by $s$ therefore has one and only one first order element $s_0$, i.e., $s$ generates one and only one first order element $s_0$. $G$ therefore has at least one first order element; and if it has exactly $\lambda$ first order elements, all of its elements can be separated into $\lambda$ corresponding mutually exclusive classes of elements, each class consisting of all the elements of $G$ which separately generate the corresponding first order element. Now no first order element of $G$ can transform another first order element of $G$ into itself. For otherwise, by the first of the two corollaries of the last section, the two would generate a subgroup of $G$ whose order would be a divisor, not unity, of $m-1$. But, as in the case of an element of $G$, the order of any subgroup of $G$ must be prime to $m-1$. It follows that if element $s$ of $G$ generates the first order element $s_0$, and hence transforms $s_0$ into itself, it can transform no other first order element of $G$ into itself; for otherwise $s_0$, a power of $s$, would transform that other first order element into itself. The class of elements of $G$ each generating $s_0$ therefore consists of all the elements of $G$ which transform $s_0$ into itself, and hence constitute a subgroup of $G$. As this subgroup has $s_0$ for invariant first order element, it is reducible to an ordinary group. We have thus proved that *if G is an m-group whose order is prime to* $m-1$, *the elements of G can be separated into a number* $\lambda$ *of mutually exclusive subgroups of G, all reducible to ordinary groups, where* $\lambda$ *is the number of first order elements of G, and each subgroup contains one and only one first order element of G, and, indeed, consists of all the elements of G that transform that first order element into itself.*

Other immediate consequences of the above proof are the following. *G is reducible to a 2-group when and only when it has but a single first order element. If G has more than one first order element, it has no invariant element, and hence is not derivable from a 2-group.* In particular, *every abelian m-group whose order is prime to* $m-1$ *has one and only one first order element, and hence is reducible to a 2-group*([77]).

We may note in passing the marked simplicity, from the standpoint of polyadic theory, of those $m$-groups of order prime to $m-1$ which are reducible to 2-groups. As seen below, the one first order element of such an $m$-group is also the one and only first order element of each of its subgroups. These subgroups are therefore also reducible to 2-groups. Furthermore, both the group and its subgroups are reducible to 2-groups in one and only one way. It easily follows by a slight modification of our cyclic $m$-group argument that when the above $m$-group is reduced to the 2-group, its subgroups are reduced to the subgroups of that 2-group.

([77]) This generalizes a theorem of Lehmer on abelian 3-groups.

Returning to our arbitrary $m$-group $G$ of order $g$ prime to $m-1$, we proceed to show that *the* $\lambda$ *first order elements of* $G$, *as well as the corresponding* $\lambda$ *subgroups into which* $G$ *was decomposed, constitute a complete set of conjugates under* $G$. It will then follow that *these* $\lambda$ *subgroups are all of the same order*, and hence that *the number of first order elements of* $G$ *is a divisor of the order of* $G$[78]. Let $s_0', s_0'', \cdots, s_0^{(\lambda)}$ be the first order elements of $G$, $k_1, k_2, \cdots, k_\lambda$ the orders of the corresponding $\lambda$ subgroups of $G$. Since exactly $k_i$ elements of $G$ transform $s_0^{(i)}$ into itself, $s_0^{(i)}$ is transformed into $g/k_i$ different elements by all the elements of $G$. As the transform of a first order element is also of the first order, $g/k_i \leqq \lambda$, i.e., $k_i \geqq g/\lambda$. Since $g = k_1 + k_2 + \cdots + k_\lambda$, it follows that the equality sign must hold for each $i$. Each $s_0^{(i)}$ therefore has the $\lambda$ first order elements of $G$ for its different transforms under the elements of $G$, whence the first half of our theorem. Now if $s_1$ generates the first order element $s_0^{(i)}$, say $s_1^{[n]} = s_0^{(i)}$, then $(s^{-1}s_1 s)^{[n]} = s^{-1}s_1^{[n]}s = s^{-1}s_0^{(i)}s$; that is, the transform of $s_1$ under $s$ generates that first order element which is the transform of $s_0^{(i)}$ under $s$. Hence, if element $s$ of $G$ transforms $s_0^{(i)}$ into $s_0^{(j)}$, it transforms the subgroup corresponding to $s_0^{(i)}$ into the subgroup corresponding to $s_0^{(j)}$, whence the rest of our result.

It follows from the above that the $\lambda$ first order elements of $G$ also constistitute a complete set of conjugates under the $m$-group they generate. For that $m$-group will have an order prime to $m-1$, while its first order elements will be the $\lambda$ first order elements of $G$. Since the $m$-group generated by a given set of elements chosen from a finite $m$-group will actually consist of all extended products of elements chosen from the set, it follows that *the* $\lambda$ *first order elements of* $G$ *constitute a "generalized" complete set of conjugates under themselves*, that is, each can be obtained from any other by a succession of transforms by first order elements only. Actually, this statement is weaker than the one immediately preceding, since it amounts to saying that the $\lambda$ first order elements of $G$ constitute a complete set of conjugates under any containing group of the $m$-group they generate. In any case, the question whether they constitute a complete set of conjugates under themselves, in the sense that any one can be transformed into any other by a third, is left open[79].

We have already observed that $\lambda$ is a divisor of $g$. While it is therefore prime to $m-1$, we now find an additional restriction imposed upon it by $m-1$. The first order element $s_0'$ is of course invariant under itself. On the

(78) For, if $k$ is the common order of these $\lambda$ subgroups, $g = k\lambda$. That the number of first order elements of an arbitrary $m$-group need not be a divisor of its order is illustrated by the ordinary symmetric group of degree three extended to a 3-group. This 3-group of order six has four first order elements.

(79) Note that the statement of Miller, page 30 of *Finite Groups*, to the effect that the Sylow subgroups of order $p^\beta$ of a group constitute a complete set of conjugates under themselves must also be interpreted in the above sense of a generalized complete set of conjugates. At least, that is all the proof there given allows us to infer.

other hand, since any other first order element $s_0^{(i)}$ is not invariant under $s_0'$, it will be transformed by the polyads $\{s_0'\}$, $\{s_0', s_0'\}$, $\{s_0', s_0', s_0'\}$, $\cdots$ into a number, not unity, of first order elements which either directly, or by our general theorem on transforms, is seen to be a divisor of $m-1$. Since the sets of transforms of different $s_0^{(i)}$'s by the above polyads are mutually exclusive when not identical, a separation of the $\lambda$ first order elements into mutually exclusive classes is thus effected, one class consisting of but one element, every other class of a number of elements which is a divisor, not unity, of $m-1$. Hence, *if* $p_1, p_2, \cdots, p_\nu$ *are the distinct prime divisors of* $m-1$, $\lambda$ *is of the form* $\lambda = 1+k_1p_1+k_2p_2+\cdots+k_\nu p_\nu$, $k_i \geqq 0$. In particular, if $m-1$ is a power of a single prime $p$, the number of first order elements of $G$ is of the form $\lambda = 1+kp$. While for $\nu > 1$ the expression for $\lambda$ gives information concerning small $\lambda$'s only, every sufficiently large number being so representable, when $m-1$ is a power of a single prime $p$ the condition includes the condition $\lambda$ prime to $m-1$, and for $p > 2$, is stronger than that condition.

A peculiar property of the sets of transforms arising in the preceding proof is that each set, clearly invariant under $s_0'$, in turn generates $s_0'$. More generally, *any set of first order elements of* $G$ *which is transformed into itself by a first order element* $s_0$ *of* $G$ *in turn generates* $s_0$. This result is itself an immediate consequence of the following. *A first order element of* $G$ *which transforms a subgroup of* $G$ *into itself must be contained in that subgroup.* The proof of the last result consists in noting that, otherwise, that first order element and the subgroup would generate a subgroup of $G$ whose order was the order of the given subgroup multiplied by a divisor, not unity, of $m-1$. As for the result preceding, the subgroup of $G$ generated by the given set, being consequently invariant under $s_0$, must contain $s_0$.

Since the order of a subgroup of $G$ must also be prime to $m-1$, there will be associated with every subgroup of $G$ an existent subset of the $\lambda$ first order elements of $G$, namely, the set of first order elements of the subgroup. These "group-bearing" subsets of the $\lambda$ first order elements of $G$ can be independently characterized as those existent subsets of the $\lambda$ first order elements which generate no other first order elements. By the reasoning of the preceding paragraph, a first order element which transforms a group-bearing subset of first order elements into itself must be contained in that subset. As the converse must also be true, it follows that a first order element, and hence indeed any element, of $G$ either leaves both a subgroup of $G$ and the set of first order elements of that subgroup invariant, or else transforms neither into itself. Clearly, two subgroups of $G$ have a common element when and only when their sets of first order elements have a common element. We finally note the following. *If* $s_0^{(t_1)}, s_0^{(t_2)}, \cdots, s_0^{(t_{\lambda'})}$ *are the first order elements of some subgroup of* $G$, *then of all subgroups of* $G$ *with exactly those first order elements there is one contained in, and one containing each.* The smallest subgroup is of course the crosscut of all the subgroups in question, and will indeed be

the subgroup $H$ generated by those first order elements([80]). Now let $K$ be the subgroup of $G$ consisting of all the elements of $G$ which transform $H$ into itself. $K$ will then contain all of the above subgroups. And since each of the first order elements of $K$ transforms $H$ into itself, they will all be in $H$, and hence will be the given first order elements. $K$ is therefore that largest subgroup of our theorem.

The above theory is significant only if there exist $m$-groups of order prime to $m-1$ with more than one first order element, and, preferably, not consisting wholly of first order elements. For odd $m-1 \neq 1$ such an $m$-group is furnished by the complete $m$-adic $\delta$-group which is of order $2^{m-1}$ and has $2^{m-2}$ first order elements. The $2^{m-2}$ second order subgroups are then the corresponding mutually exclusive subgroups into which the elements of the group are separated. For $m-1$ even, and $\lambda$ prime to $m-1$, the $\lambda$ second order elements of the ordinary dihedral group of order $2\lambda$ constitute such an $m$-group under the product of $m$ elements as operation. In this $m$-group all $\lambda$ elements are of $m$-adic order one. However, by the direct product method, we can obtain from this $m$-group, and a cyclic $m$-group of order $g/\lambda$, an $m$-group of arbitrary order $g$ prime to the even $m-1$, and with an arbitrary divisor $\lambda$ of $g$ as the number of its first order elements. Most of the theory can be illustrated by means of these examples.

27. **Sylow subgroups of order $p^\alpha$ with $g/p^\alpha$ prime to $m-1$.** That Sylow's theorem is not universally valid for polyadic groups is shown by cyclic polyadic groups. We recall that a cyclic $m$-group of order $g$ has a subgroup of order $\gamma$, $\gamma$ a divisor of $g$, when and only when $g/\gamma$ is prime to $m-1$. Hence, if $p$ is a prime divisor of $g$, and $p^\alpha$ is the largest power of $p$ which divides $g$, a cyclic $m$-group of order $g$ will have a "Sylow subgroup" of order $p^\alpha$ when and only when $g/p^\alpha$ is prime to $m-1$. This example shows that our extension of Sylow's theorem to polyadic groups as given below is the most general that can be given in terms of a condition involving only the order and dimension of the group([81]). Note also that our cyclic group will have a Sylow subgroup for each of two distinct prime divisors of $g$ when and only when $g$ itself is prime to $m-1$, in which case it will have a Sylow subgroup for every distinct

([80]) In this connection a theorem of Dörnte's is of interest. To wit, if an $m$-group is semi-abelian, and has at least one first order element, then its first order elements themselves constitute a subgroup of the $m$-group.

([81]) Other theorems however are possible. Thus, if $G$ is an $m$-group of order $g$ whose associated ordinary group $G_0$ has but one Sylow subgroup corresponding to a prime divisor $p$ of $g$, in particular if $G$ is semi-abelian, then the necessary and sufficient condition that $G$ have a Sylow subgroup corresponding to $p$ is that $G$ have at least one element whose order is a power, possibly the zeroth, of $p$. Necessary, immediately; and sufficient. For if $H_0$ is that sole Sylow subgroup of $G_0$ of order a power of $p$, $s$ the element of $G$, then $s$ can transform $H_0$ only into itself, while $s^{m-1}$, being of ordinary order a power of $p$, must be in $H_0$. Hence $H=H_0s$ is an $m$-group, and thus a subgroup of $G$ of the requisite order. However, the Sylow subgroups of $G$ corresponding to the prime $p$ need not then constitute a complete set of conjugates under $G$. Thus, if $G'$ is

prime divisor of $g$. The same situation holds for the *applicability* of our extension of Sylow's theorem to polyadic groups.

We proceed then to prove the following. *If the order $g$ of an $m$-group $G$ is divisible by $p^\alpha$ but not by $p^{\alpha+1}$, $p$ a prime divisor of $g$, then if $g/p^\alpha$ is prime to $m-1$, $G$ will have at least one subgroup of order $p^\alpha$.* Our proof consists in expressing $G$ in accordance with our basic coset theorem, and applying the Sylow theorem for ordinary groups to the associated ordinary group $G_0$ of $G$. By that coset theorem, and in the notation of the abstract containing group $G^*$ of $G$, we may write $G=s'G_0$, where $s'$ is any element of $G$. Since $G_0$ is also of order $g$, it will have at least one Sylow subgroup $H_0$ of order $p^\alpha$. As $G_0$ is invariant under $s'$, $H_0$ will be transformed by $s'$ into a Sylow subgroup $H_0'$ of $G_0$ of order $p^\alpha$. But the Sylow subgroups of $G_0$ of order $p^\alpha$ constitute a complete set of conjugates under $G_0$. Hence some element $t$ of $G_0$ will transform $H_0'$ into $H_0$. It follows that the element $s''=s't$ of $G$ transforms $H_0$ into itself.

Now $s''$ as element of $G$ will be of some $m$-adic order $\gamma$ which is a divisor of $g$. If then $p^\beta$ is the largest power of $p$ which divides $\gamma$, $\gamma/p^\beta$ will be prime to $m-1$. It follows from our theory of cyclic groups that $s''$ will generate an element $s$, also in $G$, of $m$-adic order $p^\beta$. That is, $s$ as element of $G^*$ will be of ordinary order $p^\beta(m-1)$, and hence $s^{m-1}$ of ordinary order $p^\beta$. But $H_0$, being invariant under $s''$, must also be invariant under $s$, and hence under $s^{m-1}$. Since $s^{m-1}$ of order $p^\beta$ is in $G_0$, and transforms Sylow subgroup $H_0$ of $G_0$ of order $p^\alpha$ into itself, $s^{m-1}$ must be in $H_0$. It follows from the converse of the coset theorem that $H=H_0s$ is an $m$-group, hence a subgroup of $G$, and of order $p^\alpha$.

Our proof actually shows then that for each Sylow subgroup of order $p^\alpha$ of $G_0$ there is at least one "Sylow subgroup" of order $p^\alpha$ of $G$ whose associated ordinary group is that Sylow subgroup of $G_0$. Conversely, the associated ordinary group of any subgroup of order $p^\alpha$ of $G$ will be a subgroup of order $p^\alpha$ of $G_0$, and hence a Sylow subgroup of order $p^\alpha$ of $G_0$. Since one and only one subgroup of $G_0$ can be the associated ordinary group of a given subgroup of $G$, we thus see that there is a one-many correspondence thus set up between the Sylow subgroups of order $p^\alpha$ of $G_0$, and those of $G$.

Of the three results which together constitute Sylow's theorem for ordi-

---

an ordinary abelian group, some extension of it $G$, also abelian, will consist wholly of first order elements. There will then be $g/p^\alpha$ Sylow subgroups of $G$ of order $p^\alpha$, yet each is invariant under $G$.

Again, in attempting to generalize the standard substitution group proof of the existence of Sylow subgroups by means of $m$-adic substitution groups, the writer succeeded in constructing a Sylow subgroup corresponding to the prime $p$ for any symmetric $m$-adic substitution group of degree a power of $p$. It may be of interest to note that the rest of that standard proof goes over except for the last step. This one point of failure, and failure there must be for an arbitrary $m$-group, lay in our being able to establish that the number of elements in a double coset $H_1sH_2$ was the order of a subgroup of $H_1$ only for the case when $H_2$ and the transform of $H_1$ under $s$ have a common element.

nary groups we have therefore proved that the first, pertaining to the existence of Sylow subgroups, go over for polyadic groups under the given order condition. We now show that under the same condition the third result also goes over. That is, *under the condition of the preceding theorem the Sylow subgroups of order $p^\alpha$ of the m-group G constitute a complete set of conjugates under G.* We have to show then that each subgroup of order $p^\alpha$ of $G$ can be transformed into any other by an element of $G$. Let $H'$ and $H$ be any two such Sylow subgroups of $G$, $H_0'$ and $H_0$ the corresponding Sylow subgroups of $G_0$. Some element $t$ of $G_0$ will transform $H_0'$ into $H_0$. That same $t$ will then transform $H'$ into a Sylow subgroup $H''$ of $G$ also corresponding to $H_0$, i.e., having $H_0$ for associated ordinary group. If then we can show that some element $s'$ of $G$ will transform $H''$ into $H$, it will follow that element $s=ts'$ of $G$ must transform $H'$ into $H$ as required by our theorem.

Our problem therefore reduces to showing that of all Sylow subgroups $H^{(i)}$ of $G$ corresponding to one and the same Sylow subgroup $H_0$ of $G$, each can be transformed into any other by an element of $G$. Since $H_0$ is the associated ordinary group of each $H^{(i)}$, it will be transformed into itself by the elements of each $H^{(i)}$. If then $\overline{G}$ is the subgroup of $G$ consisting of all the elements of $G$ which transform $H_0$ into itself, each $H^{(i)}$ will be a subgroup of $\overline{G}$. On the one hand, therefore, Lagrange's theorem for polyadic groups shows that if $\bar{g}$ is the order of $\overline{G}$, then $\bar{g}$ will be divisible by $p^\alpha$, but not by $p^{\alpha+1}$, while $\bar{g}/p^\alpha$ will be prime to $m-1$. On the other hand, since $H_0$ is invariant under each element of $\overline{G}$, it will be an invariant subgroup of $\overline{G}_0$, the associated ordinary group of $\overline{G}$. First then, $H_0$, whose order proclaims it to be a Sylow subgroup of $\overline{G}_0$, is the only Sylow subgroup of $\overline{G}_0$ of order $p^\alpha$. And since $\overline{G}$ satisfies the order condition of our first theorem, it follows from the proof of that theorem that the subgroups $H^{(i)}$, which constitute all the Sylow subgroups of order $p^\alpha$ of $G$, and hence of $\overline{G}$, corresponding to $H_0$, actually are the only subgroups of order $p^\alpha$ of $\overline{G}$.

If we expand $\overline{G}$ in cosets as regards $H_0$, each subgroup $H^{(i)}$, having $H_0$ for associated group, will appear as one of these cosets. Since $H_0$ is invariant under each element of $\overline{G}$, these cosets are the elements of the $m$-adic quotient group $\Gamma=G/H_0$. $H_0$ then appears as the identity of $\Gamma_0$, the associated ordinary group of $\Gamma$, each $H^{(i)}$ as an element $\sigma^{(i)}$ of $\Gamma$. If $s$ is an element of $H^{(i)}$, $s^{m-1}$ is in $H_0$. Hence for each $\sigma^{(i)}$, $[\sigma^{(i)}]^{m-1}=1$. That is, each $\sigma^{(i)}$ is a first order element of the $m$-group $\Gamma$. Conversely, if $\sigma$ be any first order element of $\Gamma$, the corresponding coset of $\overline{G}$ constitutes a subgroup of $\overline{G}$ with $H_0$ for associated group, and hence is an $H^{(i)}$. The elements $\sigma^{(i)}$ are therefore the only first order elements of $\Gamma$. But the order of $\Gamma$ is $\bar{g}/p^\alpha$ which is prime to $m-1$. The preceding section therefore tells us that the elements $\sigma^{(i)}$ constitute a complete set of conjugates under the elements of $\Gamma$. It follows that each of the subgroups $H^{(i)}$ of $\overline{G}$ can be transformed into any other by an element of $\overline{G}$, and hence of $G$. Our proof is thus completed.

Clearly, the Sylow subgroups of order $p^\alpha$ of $G$ are also the Sylow subgroups of order $p^\alpha$ of the subgroup of $G$ generated by those Sylow subgroups. As that generated subgroup must satisfy the order condition of our theorem, it follows that the Sylow subgroups of order $p^\alpha$ also constitute a complete set of conjugates under the elements of the $m$-group they generate. As in the case of the preceding section, a weaker form of this result is that the Sylow subgroups of order $p^\alpha$ of $G$ constitute a generalized complete set of conjugates under their own elements, that is, each can be obtained from another by a succession of transforms by their own elements.

Under the condition $g/p^\alpha$ prime to $m-1$, two of the three parts of Sylow's theorem have thus been shown to hold verbatim for polyadic groups. Not so for the remaining part concerning the number of Sylow subgroups of order $p^\alpha$. Let us return to the one-many correspondence between the Sylow subgroups of order $p^\alpha$ of $G_0$ and of $G$. As stated in different guise in the preceding proof, an element $t$ of $G_0$ which transforms one Sylow subgroup of $G_0$ into a second will transform the Sylow subgroups of $G$ corresponding to that first Sylow subgroup of $G_0$ into those corresponding to the second. Each Sylow subgroup of order $p^\alpha$ of $G_0$ therefore has the same number $\lambda$ of corresponding Sylow subgroups of $G$. As seen above, $\lambda$ is actually the number of first order elements of an $m$-group of order $\bar{g}/p^\alpha$ prime to $m-1$. Hence our result of the preceding section, coupled with the corresponding part of the Sylow theorem for ordinary groups, yields the following as the remaining part of our Sylow theorem for polyadic groups. *Under the condition of the preceding theorems the number of Sylow subgroups of order $p^\alpha$ of the $m$-group $G$ of order $g$ is of the form $(1+kp)\lambda$ where $\lambda$ is a divisor of $g/p^\alpha$ and hence prime to $m-1$ and $p$.*

In contrast with the above, we are able to extend the ordinary result that every element and subgroup of order a power of $p$ is contained in a Sylow subgroup of order $p^\alpha$, only for several still narrower classes of polyadic groups. It will be convenient to refer to this as the *inclusion property*. We do have immediately that *under the conditions of the preceding theorems if element $s$ of order $p^\beta$ of $G$, $\beta \geqq 0$, transforms a Sylow subgroup $H$ of order $p^\alpha$ of $G$ into itself, then $s$ is in $H$.* For otherwise, by our generalized corollary of §25, $s$ and $H$ would generate a subgroup of $G$ whose order would be either $p^\alpha$ times a multiple of $p$, or $p^\alpha$ times a divisor, not unity, of $m-1$, neither of which possibility is consistent with the given conditions. Hence also, if each element of a subgroup $K$ of order $p^\beta$ of $G$ transforms $H$ into itself, then $K$ is contained in $H$. It follows that if $G$ has but one Sylow subgroup of order $p^\alpha$, in particular then if $G$ is abelian, the inclusion property holds. Again, as in the proof of the first part of our extension of Sylow's theorem, we see that if element $s$ of order $p^\beta$ of $G$ transforms a Sylow subgroup $H_0$ of order $p^\alpha$ of the associated ordinary group $G_0$ into itself, then $s$ must be in a Sylow subgroup of order $p^\alpha$ of $G$, namely, $H_0 s$; likewise then for a subgroup $K$ of order $p^\beta$ of $G$ that transforms $H_0$ into itself. For $K_0$ will then be contained in $H_0$; and with $s$ in $K$, Sylow

subgroup $H_0s$ of $G$ will contain $K=K_0s$. Hence, if $G_0$ has but one Sylow subgroup, in particular if $G_0$ is abelian, i.e., $G$ semi-abelian, the inclusion property is satisfied.

If we attempt to generalize the standard proof of the inclusion property for ordinary groups, we see that while the number of Sylow subgroups of order $p^\alpha$ of the $m$-group $G$ is shown by our formula to be again prime to $p$, our work on transforms merely shows the number of transforms of a Sylow subgroup under the polyads formed from $s$ or $K$ to be a divisor of $p^\beta(m-1)$. We are thus led to the inclusion property only when $m-1$ itself is a power of the prime $p$. More generally, however, let $G$ be reducible to a $\mu$-group $G'$, with $\mu-1$ a power of $p$, say $p^\gamma$. The abstract containing group $G'^*$ of $G'$, of order $p^\gamma g$, will then be a containing group of $G$. The corresponding containing group of the cyclic $m$-group generated by $s$, or of $K$, will be a subgroup of $G'^*$. It follows that the above number of transforms will also be a divisor of $p^\gamma g$, and hence actually be a power of $p$. The standard proof therefore again generalizes. Hence, *under the condition of the preceding theorems the inclusion property holds whenever $G$ is reducible to a $\mu$-group with $\mu-1$ a power of $p$*; in particular, then, whenever $G$ is reducible to an ordinary group.

An interesting consequence of this result is that the inclusion property for $G$ holds under the condition of this section *whenever $G$ has an invariant element*. For let $s$ be an invariant element of $G$. Since its $m$-adic order is a divisor of $g$, the condition $g/p^\alpha$ prime to $m-1$, coupled with our formula for the real dimension of a cyclic $m$-group, shows that the cyclic $m$-group generated by $s$ is reducible to a $\mu$-group with $\mu-1$ a power of $p$. If then we apply our general criterion of reducibility to a $\mu$-group to this cyclic $\mu$-group, we obtain a condition which, with the invariance of $s$ under $G$, becomes the condition that $G$ be reducible to a $\mu$-group. Note that in this case, which is that of a $G$ derivable from a 2-group, for each Sylow subgroup of order $p^\alpha$ of $G_0$ there is but one corresponding Sylow subgroup of $G$. For the invariant element $s$ will generate some invariant element of order a power of $p$, which, consequently, must be in every Sylow subgroup of order $p^\alpha$ of $G$. On the other hand two Sylow subgroups of $G$ corresponding to the same Sylow subgroup of $G_0$ can have no common element.

All of the above concerned the Sylow subgroups of $G$ corresponding to the single prime $p$. As stated early in this section, if the condition $g/p^\alpha$ prime to $m-1$ is to be satisfied for two distinct prime factors of $g$, then $g$ itself must be prime to $m-1$, in which case the condition is satisfied for every prime factor of $g$. Hence, when $g$ is prime to $m-1$, our extension of Sylow's theorem is universally valid. In particular, if $G$ is abelian with $g$ prime to $m-1$, then $G$ has one and only one Sylow subgroup for each distinct prime divisor of $g$. By the preceding section, $G$ then has one and only one first order element, which must then be in each of the Sylow subgroups of $G$, and, indeed, be the only element common to one such subgroup and the subgroup generated by

the others. $G$, therefore, is then the direct product of its Sylow subgroups; and when it is reduced to a 2-group, in the one manner allowed by its unique first order element, its Sylow subgroups are reduced to the Sylow subgroups of that 2-group.

Actually, this last result is but a special instance of a general result. We have earlier observed that when an $m$-group $G$ is reduced to a $\mu$-group $G'$, each subgroup of $G'$ is the reduction of a subgroup of $G$, but a subgroup of $G$ may not reduce to a subgroup of $G'$. On the other hand, let $G$ satisfy our general condition $g/p^\alpha$ prime to $m-1$. Then $G'$ satisfies the corresponding condition $g/p^\alpha$ prime to $\mu-1$. Our extension of Sylow's theorem is therefore applicable to both groups. Since transforms of elements by elements are the same in $G$ and in $G'$, our complete set of conjugates result, applied to a Sylow subgroup of order $p^\alpha$ of $G'$ and that of $G$ reducing to it, shows that *when $G$ is reduced to $G'$ the Sylow subgroups of order $p^\alpha$ of $G$ are reduced to the Sylow subgroups of order $p^\alpha$ of $G'$*. Finally, if $m-1$ is prime to $g$, the Sylow subgroups of $G$, without qualification, are reduced to the Sylow subgroups of $G'$.

28. **Representation of an arbitrary $m$-adic group as a regular $m$-adic substitution group.** We shall prove our result without the use of the coset theorem. The proof will then, indeed, immediately lead to another proof of the coset theorem, actually, the writer's original proof([82]).

Let $G$ be an arbitrary $m$-group of order $g$. The classes $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ are then to have for members the $g$ classes of equivalent $i$-ads for $i=1, 2, \cdots, m-1$. It will be convenient to symbolize the $g$ members of $\Gamma_i$ by $a_{ij}, j=1, 2, \cdots, g$. Let $s$ be any element of $G$. Then, as proved in more general form in §3, if the $i$-ads $\{s_1', s_2', \cdots, s_i'\}$ and $\{s_1'', s_2'', \cdots, s_i''\}$ of $G$ are equivalent, the $(i+1)$-ads $\{s_1', s_2', \cdots, s_i', s\}$ and $\{s_1'', s_2'', \cdots, s_i'', s\}$ of $G$ are equivalent, and conversely. $s$ thus becomes an operator which carries the $g$ classes of equivalent $i$-ads in 1-1 fashion into the $g$ classes of equivalent $(i+1)$-ads. Furthermore, if $c$ represents the $m$-adic operation of $G$, then if the $(m-1)$-ads $\{s_1', s_2', \cdots, s_{m-1}'\}$ and $\{s_1'', s_2'', \cdots, s_{m-1}''\}$ are equivalent, the elements $c(s_1' s_2' \cdots s_{m-1}' s)$ and $c(s_1'' s_2'' \cdots s_{m-1}'' s)$ are identical, and conversely. It follows that $s$ thus carries in 1-1 fashion the letters of $\Gamma_1 \to \Gamma_2$, $\Gamma_2 \to \Gamma_3, \cdots, \Gamma_{m-1} \to \Gamma_1$, that is, determines an $m$-adic substitution on the $\Gamma$'s.

Now given any $i$-ad $\{s_1, s_2, \cdots, s_i\}$, and any $(i+1)$-ad $\{s_1', s_2', \cdots, s_i', s_{i+1}'\}$, there is one and only one element $s$ of $G$ for which the $(i+1)$-ads $\{s_1, s_2, \cdots, s_i, s\}$ and $\{s_1', s_2', \cdots, s_i', s_{i+1}'\}$ are equivalent. It follows on the one hand that no two distinct elements of $G$ can yield the same $m$-adic substitution on the $\Gamma$'s. The correspondence between the elements of $G$ and the $m$-adic substitutions they determine is therefore 1-1. And since the $m$-adic substitution determined by $c(s_1 s_2 \cdots s_m)$ is clearly the product of the $m$-adic substitutions determined by $s_1, s_2, \cdots, s_m$, it follows that the $m$-adic substitu-

([82]) While the proof as given is for finite $m$-groups, it holds with little change for all $m$-groups. Hence the full generality of the consequent proof of the coset theorem.

tions determined by the elements of $G$ constitute an $m$-adic substitution group simply isomorphic with $G$. Furthermore, the initial observation of this paragraph shows that given any two letters in successive $\Gamma$'s there is one and only one element $s$ of $G$, and hence one and only one $m$-adic substitution of the simply isomorphic substitution group, that carries the letter in the first $\Gamma$ into that of the second. This $m$-adic substitution group is therefore regular. We have consequently proved the following generalization of Cayley's theorem. *Every m-adic group can be represented as a regular m-adic substitution group.* In this connection, as seen in §16, the argument of §14 shows that *two regular m-adic substitution groups on the same letters which are simply isomorphic are conjugate.*

If we now wish to obtain the coset theorem from this result, we need merely observe that the ordinary group generated by the $m$-adic substitutions of the representation of $G$, as in the case of all $m$-adic substitution groups, is a containing group of the representation of $G$ of index $m-1$, and hence by resymbolization of its elements can be made a containing group of $G$ leading to the desired result. Since we have developed our theory of abstract polyadic groups abstractly, comparatively few applications of this generalization of Cayley's theorem are to be found in the present paper. Perhaps the most important of these is that it allows the concept of holomorph to apply to an arbitrary abstract polyadic group.

29. **Invariant subgroups and quotient groups; the $m$-adic central quotient group.** The present section may be considered a continuation of §4, our attention now being restricted to finite polyadic groups. We recall that if $G$ is an $m$-group with ordinary associated group $G_0$, then every subgroup $H_0$ of $G_0$ that is invariant under $G$ leads to an $m$-adic quotient group $Q=G/H_0$ isomorphic with $G$. Clearly, if $H_0$ is of order $h$, the isomorphism between $G$ and $Q$ is $(h, 1)$. $H_0$ and $Q$ may be called complementary groups as regards $G$. Since the elements of $Q$ are the cosets of $G$ as regards $H_0$, the order of $G$ is the product of the orders of $H_0$ and $Q$. Similarly for an actual subgroup $H$ of $G$ corresponding to $H_0$.

Let $\sigma$ be any element of $Q$, $s$ any one of the elements of the corresponding coset. Then the $m$-adic order $n$ of $s$ must be divisible by the $m$-adic order $\nu$ of $\sigma$. For, since $s^{[n]}=s$, $\sigma^{[n]}=\sigma$, and hence $n$ is a multiple of $\nu$. That is, *the order of any element of an m-adic quotient group divides the orders of all the elements of the corresponding coset.* We recall that each coset corresponding to a first order element of $Q$ constitutes a subgroup of $G$. These subgroups in fact are all the subgroups of $G$ having $H_0$ for associated ordinary group, and hence also are semi-invariant subgroups of $G$. In particular, if $H_0$ is of order prime to $m-1$, each coset thus corresponding to a first order element of $Q$ has at least one first order element.

Unlike the corresponding situation for ordinary groups, an element $\sigma$ of $Q$ may be of order a power of a prime $p$ without any element of the correspond-

ing coset being of order a power of that prime. Thus, let $G$ be a cyclic $m$-group of order $p^\alpha k$ where $k$, prime to $p$, is not prime to $m-1$. Then no element of $G$ can have an order a power of $p$. But with $H_0$ the subgroup of $G_0$ of order $k$, $Q=G/H_0$ is cyclic, and of order $p^\alpha$. Some element $\sigma$ of $Q$ will then indeed be of order $p^\alpha$, while the corresponding coset has no element of order a power of $p$.

However, let $\sigma$ be of order $p^\beta$, $H_0$ of order $p^\alpha k$, $k$ prime to $p$, and suppose that $k$ is prime to $m-1$. The elements of the cosets corresponding to the $m$-adic powers of $\sigma$ will then together constitute a subgroup $G'$ of $G$ of order $p^{\alpha+\beta}k$. Since $k$ is prime to $m-1$, $G'$ will have a Sylow subgroup $K$ of order $p^{\alpha+\beta}$([83]). As the crosscut of $K_0$ and $H_0$ must be of order a power of $p$, it follows that $K$ must have exactly $p^\alpha$ elements in each of the $p^\beta$ cosets of $G'$ as regards $H_0$. The coset corresponding to $\sigma$ therefore has at least one element of order $p^\gamma$ with, of course, $\gamma \geqq \beta$. That is, *if the order of an element of an m-adic quotient group is a power of a prime number p, while the largest divisor prime to p of the order of the complementary group is prime to $m-1$, then the corresponding coset involves an element whose order is a power of p.*

We recall the ordinary group result that every invariant subgroup of index 2 under any group includes all the elements of odd order contained in this group. In the case of an $m$-adic quotient group of order two, we recall our results of §23, and note that for $m$ odd no such result can be expected. In fact, when the quotient group consists of two first order elements, each of the corresponding cosets, both then invariant subgroups of the given group as a consequence of the abelianism of the quotient group, may have an element of odd order; while when the quotient group consists of two second order elements both cosets consist of even order elements only. On the other hand, for $m$ even the quotient group must consist of one first and one second order element. The coset corresponding to the first order element of the quotient group will then be an invariant subgroup of the given group, and any elements of odd order in the given group must be included in that invariant subgroup.

If $H_0$ is a subgroup of $G_0$, the index of $H_0$ under $G$ may be defined as the order of $G$ divided by the order of $H_0$, and, of course, gives the number of cosets in the expansion of $G$ in either right or left cosets as regards $H_0$—likewise for an $H$ actually a subgroup of $G$. In the case of ordinary groups, we know that the index of the crosscut of two subgroups of a group under one of those subgroups is less than or equal to the index of the other subgroup under the group; while if the two subgroups are conjugate under the group, the inequality always prevails. If now $H$ is a subgroup of an $m$-group $G$, $K_0$ a subgroup of $G_0$, let $L_0$ be the crosscut of the associated ordinary group $H_0$ of $H$, and $K_0$. Then, by writing $G$ in the form $G_0 s$, with $s$ in $H$, we see that the expansion of $H_0$ in right cosets as regards $L_0$, and the expansion of $G_0$ in right

([83]) Unless $\alpha=\beta=0$. But that case has already been treated. Actually, the first order elements of $G$ may then conveniently be considered its Sylow subgroups of order $p^0$.

cosets as regards $K_0$, become the expansions of $H$ and $G$ in right cosets as regards $L_0$ and $K_0$ respectively. It then follows immediately that the index of $L_0$ under $H$ is less than or equal to the index of $K_0$ under $G$. Now let $K_0$ be the associated ordinary group of a subgroup $K$ of $G$ conjugate to $H$ under $G$. Since $H$ and $K$ are subgroups of $G$, we see from the discussion in §24 that $H$ can also be transformed into $K$ by some element $t$ of $G_0$. Since $t$ then transforms $H_0$ into $K_0$, the 2-group result for conjugate subgroups is applicable and thus yields the following. *If $H$ and $K$ are conjugate subgroups of an $m$-group $G$, the index of the crosscut of $H_0$ and $K_0$ under one of the subgroups is always less than the index of these subgroups under $G$.*

In this formulation we use "subgroup" in the strict sense, and thereby avoid the need of specifying that $H_0$ and $K_0$, or $H$ and $K$, are distinct. Now, as in the corresponding 2-group illustration, let $H$ be of index 2 under $G$. With $K$ conjugate to $H$, the above result shows $H_0$ and $K_0$ to be identical. $H$ is then at least a semi-invariant subgroup of $G$. But since the resulting quotient group $G/H$, being of order two, is abelian, it follows that $H$ is actually invariant under $G$. Hence, as for ordinary groups, *a subgroup of index 2 under any polyadic group is invariant.*

If an $m$-group $G$ has at least one invariant element, these invariant elements clearly constitute an invariant subgroup of $G$ which may be called the *central* of $G$. Note that a necessary and sufficient condition that our finite $m$-group $G$ have a central is that it be derivable from an ordinary group. The central $C$ of $G$, when it exists, is of course abelian, and coincides with $G$ when and only when $G$ is abelian. The quotient group $G/C$ may be called the central quotient group of $G$, and, as with ordinary groups, is easily proved noncyclic whenever $G$ is non-abelian.

It is readily seen that, when the central $C$ of $G$ exists, the associated ordinary group $C_0$ of $C$ consists of all the elements of $G_0$ which are invariant under $G$. In general then, let us define the *associated central* $C_0$ of $G$ as the subgroup of $G_0$ consisting of all the elements of $G_0$ invariant under $G$. $C_0$ then always exists, and being a subgroup of $G_0$ invariant under $G$, always leads to a quotient group $G/C_0$. Since $G/C=G/C_0$ whenever $C$ exists, we may call $G/C_0$ the *central quotient group* of $G$ irrespective of the existence of $C$. Since each element of $C_0$ is also invariant under $G_0$, $C_0$ is a subgroup of the central of $G_0$ when it does not coincide with the central of $G_0$. It is readily seen, in fact, that the central of $G_0$ is invariant under $G$, each element of $G$ yielding the same automorphism of that central. It follows that $C_0$ consists of those elements of the central of $G_0$ which are left invariant under any one element of $G$. In particular, when $C$ exists, $C_0$ will coincide with the central of $G_0$. In any case, $C_0$ is abelian, and coincides with $G_0$ when and only when $G$ is abelian. It is then again easily proved that *the central quotient group of an $m$-group $G$ is noncyclic whenever $G$ is non-abelian.*

Any subgroup of $G$ having $C_0$ for associated group leads to the central

quotient group $G/C_0$ and may be called a *relative central* of $G$. The relative centrals of $G$ are then those cosets, if any, of the expansion of $G$ as regards $C_0$ which correspond to first order elements of the central quotient group. They are of course semi-invariant subgroups of $G$, and are easily seen to be abelian. They can be independently characterized as the maximal subgroups of $G$ having the property that, on being transformed by an element of $G$, each element of the subgroup is multiplied by one and the same element $t$ of $G_0$. Together, the elements of the relative centrals of $G$ constitute all elements $s$ of $G$ with $s^{m-1}$ in $C_0$. The relative centrals corresponding to invariant first order elements of the central quotient group are characterized by the above multiplier $t$'s always being in $C_0$, in which case, indeed, $t^{m-1}=1$. The unique central $C$, when it exists, is then the only one for which $t$ is always 1.

30. **Commutator, semi-commutator, and quasi-commutator subgroups.** A direct extension to polyadic groups of the concepts of commutator, and commutator subgroup, is immediately obtainable. Given an $m$-group $G$, and in the notation of the abstract containing group of $G$, if $s_1$ and $s_2$ are any two elements of $G$, we may, as in ordinary theory, define the commutator of $s_1$ and $s_2$ to be $t=s_1^{-1}s_2^{-1}s_1s_2$. We shall also refer to $s_1$ and $s_2$ as the elements of the commutator. The commutator of $s_1$ and $s_2$ is then not an element of $G$, but of $G_0$, the associated ordinary group of $G$, and is indeed that element of $G_0$ by which $s_1$ has to be multiplied on the right to yield the transform of $s_1$ under $s_2$. The different commutators thus formed from elements of $G$ therefore generate a subgroup of $G_0$, if not $G_0$ itself, which may then be called the *commutator subgroup for G.*

As in ordinary group theory, the theory of commutator subgroups for polyadic groups is intimately bound up with the property of abelianism. But now our general formulation of semi-abelianism given in §7 suggests the need of a corresponding formulation of semi-commutator subgroup. The relative complexity of the resulting formulation then suggests a still further generalization of both concepts to what we term quasi-abelianism, and quasi-commutator subgroup. This wider generalization is also significant for ordinary groups. But while thus intimately related to certain recent work, in particular of Hall and Neumann([84]), its direction seems to be new.

The immediate connection between abelianism and commutator subgroup is more clearly in evidence if we rewrite the usual $s_1s_2=s_2s_1$ for the former in the equivalent form $s_1^{-1}s_2^{-1}s_1s_2=1$. Now the expression $s_1^{-1}s_2^{-1}s_1s_2$ that thus enters into both concepts is but a special instance of a word in the sense of Hall, or a rational expression in the sense of Baer. In general, a word $W$ will be any expression of the form $s_{i_1}^{\nu_1}s_{i_2}^{\nu_2}\cdots s_{i_N}^{\nu_N}$, where the exponents are arbitrarily $+1$ or $-1$, the subscripts arbitrarily equal or unequal. If such an expression is to assume the value 1 for any choice of $s$'s in an $m$-group $G$, the notation

([84]) B. H. Neumann, *Identical relations in groups* I, Mathematische Annalen, vol. 114 (1937), pp. 506–525. References will here be found to the work of Hall.

being that of the abstract containing group of $G$, the exponents must satisfy the condition $\nu_1+\nu_2+\cdots+\nu_N\equiv 0 \pmod{m-1}$. Given $m$, consider then any specific class of words $W_j$ whose exponents satisfy this condition. An $m$-group $G$ will then be said to be *quasi-abelian* of corresponding formal type if the equations $W_j=1$ are satisfied for every assignment of elements in $G$ as values of the $s$'s, i.e., form a set of identical relations for $G$ in the sense of Neumann. Now given an arbitrary $m$-group $G$, as a result of the exponent condition on the given class of words $W_j$ each word assumes an element of $G_0$ as value when its letters are assigned elements of $G$ as values. We shall call these words formal quasi-commutators, their values quasi-commutators, of the given formal type. The subgroup of $G_0$ generated by all of the quasi-commutators thus obtainable from elements of $G$ will then be called the *quasi-commutator subgroup for* $G$ of corresponding formal type.

In particular, any formulation of semi-abelianism as given in §7 can be rewritten in the above form. We correspondingly have formal semi-commutators, semi-commutators, and *semi-commutator subgroup* for an $m$-group $G$. While a certain degree of arbitrariness enters into the manner in which the equations of §7 are thus rewritten, it will be seen that this is irrelevant in the formation of the corresponding semi-commutator subgroup for $G$. In fact, our central theorem will be to the effect that the correspondence between type of quasi-abelianism and type of quasi-commutator subgroup, at present purely formal, is in fact intrinsic([85]).

Our initial development, paralleling that of ordinary theory up to its main conclusion, will be given for quasi-commutator subgroups, the results then also holding for the successive specialization to semi-commutator and commutator subgroups. Consider then any one formulation of quasi-commutator subgroup for $m$-groups. From its very definition we then have that *the quasi-commutator subgroup for an $m$-group $G$ reduces to the identity when and only when $G$ is quasi-abelian of corresponding formal type.* Clearly the transform $W_j$ by $s$ is the same expression with each letter in $W_j$ replaced by its transform

([85]) Note that while we are interested in all, in the present instance finite, $m$-groups satisfying a given set of identical relations, Neumann considered instead the class of all identical relations satisfied by a given, of course ordinary, group. But it is the former concept that generalizes abelianism. Again, Hall, in the first paper cited by Neumann, builds up higher commutator forms merely out of ordinary commutators. His later concept of word-subgroup is identical, for ordinary groups, with our quasi-commutator subgroup. But again the emphasis is on all word-subgroups of a given group, rather than word-subgroup of given type for all groups—say of cardinal number less than, or less than or equal to, a given cardinal. And so our particular contribution of the relation between type of word-subgroup and type of identical relations is again unnoticed. We hasten to add that the researches of these authors in the directions they do pursue are profound. We also note that on reading Neumann's paper we changed our original formulation involving a finite number of identical relations to an arbitrary set of identical relations. In the case of our formulation of semi-abelianism, the finite can stand; for our theorem of §7 shows that an infinite set would always be equivalent to a finite subset thereof.

under $s$. That is, the transform of each quasi-commutator by an element of $G$ is also a quasi-commutator. Hence, the *quasi-commutator subgroup for $G$ of the given formal type is a subgroup of $G_0$ invariant under $G$, when not $G_0$ itself.* We may therefore form the $m$-adic quotient group of $G$ relative to this quasi-commutator subgroup, i.e., the corresponding *quasi-commutator quotient group* of $G$. We then readily see that as in the ordinary theory, *the quasi-commutator quotient group of $G$ of given formal type is quasi-abelian of the corresponding formal type.* For the isomorphism between $G$ and the quotient group shows that a quasi-commutator formed from any elements of the quotient group corresponds to the quasi-commutator formed in the same way from corresponding elements of $G$, and hence is always the identity. Conversely, consider any quotient group of $G$ which is quasi-abelian according to the given formulation. Again quasi-commutators of $G$ correspond to quasi-commutators of this quotient group. Since the latter quasi-commutators can only be the identity, the former must be in the subgroup of $G_0$ complementary to this quotient group. That is, *every subgroup of $G_0$ which is invariant under $G$, and whose complementary quotient group is quasi-abelian of given formal type, contains the quasi-commutator subgroup for $G$ of corresponding formal type.*

We are now able to prove the following fundamental theorem. *If two formulations of quasi-abelianism for $m$-adic groups are such that every $m$-group satisfying either satisfies the other, then the corresponding quasi-commutator subgroups for an $m$-group are always identical.* For let $A'$ and $A''$ symbolize the two formulations of quasi-abelianism. If then, for a given $m$-group $G$, $C_0'$ and $C_0''$ are the quasi-commutator subgroups corresponding to $A'$ and $A''$ respectively, the quasi-commutator quotient group $G/C_0'$ satisfies $A'$, $G/C_0''$ satisfies $A''$. By our hypothesis, therefore, the $m$-group $G/C_0'$ also satisfies $A''$, $G/C_0''$ also satisfies $A'$. Hence, by our last theorem, $C_0'$ contains $C_0''$ and $C_0''$ contains $C_0'$, that is, $C_0'$ and $C_0''$ are identical.

The converse of this theorem is immediate; for if two formulations of quasi-commutator subgroup lead to identical subgroups for each $m$-group, then, if either of these subgroups is the identity, the other also is the identity. If then we say that two formulations of quasi-abelianism for $m$-adic groups define the same *type of quasi-abelianism* if every $m$-group satisfying either satisfies the other, while two formulations of quasi-commutator subgroup for $m$-adic groups define the same *type of quasi-commutator subgroup* if they yield identical subgroups for each $m$-group, we can conclude that *there is a* 1-1 *correspondence between types of quasi-abelianism for $m$-adic groups and types of quasi-commutator subgroup.* The correspondence between quasi-abelianism and quasi-commutator subgroup, originally depending on a particular formulation, has thus been shown to be intrinsic.

A useful partial consequence of our earlier proof is the following. *If two formulations of quasi-abelianism for $m$-adic groups are such that every $m$-group satisfying the first satisfies the second, then the quasi-commutator subgroup for an*

*m-group corresponding to the first formulation always contains the one corresponding to the second.* In this connection note that quasi-commutator subgroups of different types may be identical for a particular $m$-group. We therefore pause to prove the following. Given any finite set of distinct types of quasi-abelianism, there exists an $m$-group for which the corresponding quasi-commutator subgroups are all distinct. In fact, for each pair of these types there must exist an $m$-group quasi-abelian according to one type, but not according to the other. Represent these $m$-groups say as $m$-adic substitution groups on different letters, and form the $m$-group $G$ therefrom by the direct product method. $G$ then has the desired property. For it is readily proved from commutativity considerations that each quasi-commutator of $G$ is the product of quasi-commutators of the same form, one for each of the above constituent groups of $G$, and conversely. Hence the quasi-commutator subgroups for $G$ corresponding to any two of the given types of quasi-abelianism have, on the letters of the corresponding constituent group of $G$, a constituent group which is the identity in one case, not the identity in the other, and hence are themselves distinct.

Our basic "equivalence theorem" immediately translates our determination of the distinct types of semi-abelianism effected in §7 into a determination of the distinct types of semi-commutator subgroup. Since the proof of distinctness for the former was carried through by means of finite groups, we can therefore state that *there are as many distinct types of semi-commutator subgroups for m-adic groups as there are distinct divisors of* $m-1$. For a divisor $\rho$ of $m-1$, the semi-commutator subgroup corresponding to $\rho$-semi-abelianism may be called the $\rho$-semi-commutator subgroup. From the above more general result it follows that *there exists an m-group for which the semi-commutator subgroups of all the distinct types are distinct.* In this case a simpler example of such a group is obtained merely by taking the direct product of groups, one for each divisor $\rho-1$ of $m-1$, which, as in §7, are $m$-groups $\rho$-semi-abelian, but not $\rho'$-semi-abelian for any divisor $\rho'-1$ of $\rho-1$ other than $\rho-1$. Whether the semi-commutator subgroups of a given $m$-group are distinct or not, we may note the following relations between them. Since $\rho_1$-semi-abelianism implies $\rho_2$-semi-abelianism whenever $\rho_1-1$ is a divisor of $\rho_2-1$, it follows that in this case the $\rho_1$-semi-commutator subgroup contains the $\rho_2$-semi-commutator subgroup. More generally then, the crosscut of the $\rho_1$ and $\rho_2$-semi-commutator subgroups contains the $\rho_3$-semi-commutator subgroup, where $\rho_3-1=\text{L.C.M.}(\rho_1-1, \rho_2-1)$, while the subgroup generated by the $\rho_1$ and $\rho_2$-semi-commutator subgroups is contained in the $\rho$-semi-commutator subgroup, where $\rho-1=\text{H.C.F.}(\rho_1-1, \rho_2-1)$. In the second case, however, we can prove that *the subgroup generated by the* $\rho_1$ *and* $\rho_2$*-semi-commutator subgroups is the* $\rho$*-semi-commutator subgroup with* $\rho-1=\text{H.C.F.}(\rho_1-1, \rho_2-1)$. For by the general theorem of §7, the semi-abelianism defined by the combination of $\rho_1$-semi-abelianism and $\rho_2$-semi-abelianism is equivalent to $\rho$-semi-

abelianism with the above $\rho$. The $\rho$-semi-commutator subgroup is therefore also the subgroup generated by all semi-commutators of the $\rho_1$ and $\rho_2$ formal types, and hence by the $\rho_1$ and $\rho_2$-semi-commutator subgroups themselves.

In our march to the equivalence theorem we neglected certain developments related only to semi-commutators, or merely commutators, which might well have come first. In the limited generality of the first specialization we note that *each semi-commutator subgroup for an m-group G contains the commutator subgroup of the ordinary associated group $G_0$ of G.* In fact, if $H_0$ be such a semi-commutator subgroup, the quotient group $G_0/H_0$ can be identified as the associated ordinary group of the semi-commutator quotient group $G/H_0$. Since $G/H_0$ is semi-abelian, $G_0/H_0$, by a result of §7, is abelian, whence the above.

Clearly, two elements of a polyadic group are commutative when and only when their commutator is the identity. As in the corresponding situation for ordinary groups, it is readily proved that if the elements of a commutator respectively belong to two invariant subgroups of a polyadic group, the commutator is contained in the crosscut of the associated ordinary groups of those subgroups. It follows that *if two invariant subgroups of a polyadic group are such that their associated ordinary groups have only the identity in common, then every element of one of these subgroups is commutative with every element of the other.* Since two subgroups having at least one element in common have as many elements in common as have their associated ordinary groups, the above result is in this case equivalent to the following. *If two invariant subgroups of a polyadic group have one and only one element in common, then every element of one of these subgroups is commutative with every element of the other.* Actually, this special case is almost an immediate consequence of the corresponding ordinary theorem; for the one common element is then an invariant first order element of each of the subgroups, and hence of the polyadic group they generate([86]), so that all three of these groups are reducible, and simultaneously so, to ordinary groups.

We have observed that the commutator of elements $s_1$ and $s_2$ of $G$ is the element of $G_0$ which must be multiplied into $s_1$ to obtain the transform of $s_1$ under $s_2$. Hence the complete set of conjugates of $s_1$ under $G$ can be obtained by multiplying $s_1$ by commutators formed from elements of $G$. Since the commutator subgroup for $G$ is invariant under $G$, it readily follows from this that all the transforms of an $i$-ad of $G$ by polyads of $G$ can be obtained by multiplying the $i$-ad by elements of the commutator subgroup for $G$. More specifically, it can be proved by way of the equivalence theorem that the transforms of an $i$-ad of an $m$-group $G$ by the elements of $G$ can be obtained by multiplying one such transform by elements of the $\rho$-semi-commutator subgroup for $G$, where $\rho-1=\text{H.C.F.}(i, m-1)$; whence likewise for the transforms of the $i$-ad by the $j$-ads of $G$ with fixed $j$. It follows from this result that if $G$ is $\rho$-semi-

([86]) Their direct product, therefore, as defined in §25.

abelian, all elements of $G$ transform the $i$-ad into the same $i$-ad, as also do all $j$-ads with fixed $j$, a fact also easily shown directly.

We have defined an $m$-group $G$ to be simple if $G_0$ has no subgroup other than the identity invariant under $G$. It follows then immediately that if a simple $m$-group $G$ is not quasi-abelian of specified type, the corresponding quasi-commutator subgroup for $G$ is identical with $G_0$. If then, rather narrowly, we define $G$ to be perfect if the commutator subgroup for $G$ is identical with $G_0$, it follows that every simple polyadic group of composite order is perfect. For otherwise $G$ would be abelian, while $G_0$ would possess a subgroup other than the identity, yet invariant under $G$.

As in the case of ordinary groups, a subgroup of an $m$-group $G$ may be called a characteristic subgroup of $G$ if it corresponds to itself under every automorphism of $G$. Every automorphism of $G$ determines an automorphism of $G_0$. We may then define a subgroup of $G_0$ to be an associated characteristic subgroup of $G$ if it corresponds to itself under every automorphism of $G$. In the case of invariance, a subgroup of $G_0$ invariant under $G$ is always invariant under $G_0$, but not conversely. Here the reverse situation holds. For clearly a characteristic subgroup of $G_0$ is also an associated characteristic subgroup of $G$, but not always conversely, as shown by the following example. The complete $m$-adic $\delta$-group for $m=3$ is a triadic group of order four which has exactly two second order subgroups, one cyclic, the other non-cyclic. Each of the subgroups is therefore a characteristic subgroup of the group. Evidently the associated ordinary group of any characteristic subgroup of a polyadic group is an associated characteristic subgroup of the group. On the other hand, the associated ordinary group of this triadic $\delta$-group is the ordinary axial group, and hence itself has no characteristic subgroup of order two.

It is readily proved that if $G$ is non-abelian, then the central of $G$, if existent, is a characteristic subgroup of $G$, while the associated central of $G$ is an associated characteristic subgroup of $G$. We now observe that every quasi-commutator subgroup for $G$, when not identical with $G_0$, is an associated characteristic subgroup of $G$. In fact it is readily seen that under any automorphism of $G$ a quasi-commutator involving certain elements of $G$ will correspond to a quasi-commutator of the same form involving the corresponding elements of $G$. As the first set of elements take on all values in $G$, so do the second, so that actually the set of quasi-commutators of $G$ of given formal type corresponds to itself under the automorphism.

Granting that the concept of quasi-abelianism and quasi-commutator subgroup has a certain degree of generality, ever further generalizations suggest themselves([87]). Perhaps a guiding principle in such generalizations might

([87]) Thus, if the above concepts be termed categorical, the following generalization, which we give only for ordinary groups, can be effected. With each of a given class of words $W_i$ is associated a class of words $W_{ik}$ involving only the letters of $W_i$. A group $G$ will then be conditionally quasi-abelian of corresponding formal type if each $W_i=1$ is satisfied for every assign-

be the existence of an equivalence theorem. It may then be of interest to present our equivalence theorem in the following light. Each type of quasi-commutator subgroup for $m$-groups may be thought of as a function which assumes for each $m$-group $G$ a subgroup of $G_0$, if not $G_0$, as value. Our equivalence theorem then asserts that this function is completely determined when it is known for what values of its argument it assumes the value 1.

31. **The $\phi$-subgroup of an $m$-adic group.** The concept of a set of elements of a group being a set of independent generators of the group is equally applicable to a polyadic group. Whereas an ordinary group always has at least one element, namely the identity, which can never be one of a set of independent generators of the group([88]), this need not be so in the case of a polyadic group. Thus a cyclic $m$-group of order $g$ such that each prime divisor of $g$ divides $m-1$ can be generated by any one of its elements, and hence fails to possess an element of the type in question. If, however, an $m$-group $G$ has at least one element which cannot be one of a set of independent generators of the group, then the set of all such elements constitutes a characteristic subgroup of $G$ which may be called the *$\phi$-subgroup* of $G$. It is a mark of the generality of the concept of the $\phi$-subgroup that the self-same proofs which yield the corresponding results for ordinary groups apply verbatim to polyadic groups to give the following. *The $\phi$-subgroup of an $m$-group $G$ is the crosscut of all the maximal subgroups of $G$. If the $\phi$-subgroup of an $m$-group $G$ involves a non-invariant element or subgroup, the number of conjugates under $G$ of this element or subgroup is greater than the number of the corresponding conjugates under the $\phi$-subgroup.* As an application of the first of these results we may note that if a cyclic $m$-group $G$ is of order $g=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\rho^{\alpha_\rho}\gamma_0$, the $p$'s being the distinct prime divisors of $g$ not divisors of $m-1$, then the $\phi$-subgroup of $G$ exists if there be at least one such prime $p$, and is then the subgroup of order $p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_\rho^{\alpha_\rho-1}\gamma_0$. Hence also, if we continue forming $\phi$-subgroups starting with the cyclic $m$-group $G$, we finally arrive at the subgroup of order $\gamma_0$ which has no $\phi$-subgroup. Since the $\phi$-subgroup is always a "proper" subgroup, if we start with any finite $m$-group and successively form $\phi$-subgroups,

---

ment of elements in $G$ as values of its letters for which each $W_{ik}=1$ is satisfied. Correspondingly, the conditional quasi-commutator subgroup of $G$ is to be the smallest subgroup of $G$ having the property that each $W_i$ is in that subgroup for every assignment of elements in $G$ as values of its letters for which each $W_{ik}$ is in that subgroup. Our development up to, and including, the equivalence theorem then goes over. But now symbolic logic suggests that our conditions might involve more explicitly its apparent variables and other apparatus, and our horizon keeps receding. Thus, also, Neumann suggests the possibility of allowing constant elements of a group to enter into his identical relations, while Hall, in his higher commutator forms, from the start allows arbitrary subgroups of $G$ individually to replace $G$ as domain of a corresponding variable. It may be that a postulational procedure, perhaps centering around our actual development, or around the point of view about to be suggested, would bring order out of the chaos that thus threatens.

([88]) Unless the group is the identity.

we arrive at a subgroup whose $\phi$-subgroup is nonexistent. This weak statement, supported by the above example for $m>2$, contrasts with the case $m=2$ when the last existent $\phi$-subgroup is always the identity.

In applying the second of the above two general results to the Sylow subgroups of the $\phi$-subgroup of an arbitrary $m$-group $G$, we are hampered by the order condition of our extension of Sylow's theorem. Within the scope of that condition, we note first that if the $\phi$-subgroup of $G$ is of order $g'$, and if, with $p^{\alpha'}$ the largest power of the prime $p$ dividing $g'$, $g'/p^{\alpha'}$ is prime to $m-1$, then the $\phi$-subgroup has a Sylow subgroup of order $p^{\alpha'}$ which then, as in the ordinary case, is unique. If then $g'$ itself is prime to $m-1$, the $\phi$-subgroup will have one and only one Sylow subgroup for each distinct prime divisor of $g'$. Since, with $g'$ prime to $m-1$, the first order elements of the $\phi$-subgroup constitute a complete set of conjugates under the $\phi$-subgroup, it follows as for the Sylow subgroups that the $\phi$-subgroup then has one and only one first order element. That is, when the order of the $\phi$-subgroup of an $m$-group is prime to $m-1$, the $\phi$-subgroup is reducible to a 2-group. When so reduced its Sylow subgroups are reduced to the Sylow subgroups of the 2-group. As in the ordinary case, the $\phi$-subgroup is then the direct product of its Sylow subgroups.

This result has an interesting consequence when the order of the given $m$-group is itself prime to $m-1$. The $\phi$-subgroup, if it exists, then has but one first order element. The invariance of the $\phi$-subgroup therefore entails the invariance of this first order element under the given $m$-group. But this can only be the case if the $m$-group has no other first order element. Hence, *if an $m$-group of order prime to $m-1$ has more than one first order element, its $\phi$-subgroup is nonexistent*; that is, if an $m$-group of order prime to $m-1$ is not reducible to a 2-group, each of its elements can be one of a set of independent generators of the group. On the other hand, if the $m$-group is reducible to a 2-group, its sole first order element can be generated by any other element, and hence is in the consequently existent $\phi$-subgroup of the group.

We restrict our discussion of the $\phi$-subgroups of primitive groups to primitive m-adic groups of ordinary substitutions. By the corresponding theorem of §18, the subgroups consisting of all substitutions omitting a given letter are maximal subgroups. Since these maximal subgroups can only have the identity in common, it follows that *the $\phi$-subgroup of a primitive $m$-adic group of ordinary substitutions is either the identity, or else is nonexistent.* Certainly then when the primitive group in question does not possess the identity, and hence a fortiori when it is not reducible to a 2-group, its $\phi$-subgroup is nonexistent. Strangely enough, the same may be true even when the identity is in the primitive group, then consequently reducible to a 2-group. Thus, the ordinary cyclic substitution group of order and degree a prime $p$ remains primitive when extended to a $(p+1)$-group. Yet, while the identity and any other element together generate the $(p+1)$-group, each alone generates only itself.

32. **Simply isomorphic $m$-adic groups; group of inner isomorphisms.** We have defined simply isomorphic $m$-groups in §4, and have shown there that the transform of an $m$-group by an element or polyad is an $m$-group simply isomorphic with the given $m$-group. Restricting our attention to the case when the simple isomorphism is an automorphism, i.e., between an $m$-group and itself, we then have conversely, as in the case of ordinary groups, that any automorphism of an $m$-group can be effected by transforming it by an element. This really means that an $m$-group can be found of which the given $m$-group is a subgroup and which has an element so transforming the given $m$-group. This result may be proved as in the ordinary case by representing the given $m$-group as a regular $m$-adic substitution group in accordance with §28. Then, by §16, the principal holomorph of the $m$-group so represented certainly transforms it into each of its possible automorphisms.

Since the abstract containing group of an $m$-group is determined abstractly by the $m$-group, we see that a simple isomorphism between two $m$-groups determines a simple isomorphism between their abstract containing groups. Conversely, any simple isomorphism between the abstract containing groups of two $m$-groups which makes the classes of elements of the $m$-groups correspond determines a simple isomorphism between the $m$-groups. The simple isomorphism theorem of §8 may be considered a refinement of this obvious result. As that theorem is related to the determination theorem preceding it, so the following theorems are related to two of the generation theorems of §25. Their proofs, easily supplied, are therefore here omitted.

*Two $m$-groups of the same order $G'$ and $G''$ are simply isomorphic if their associated ordinary groups $G_0'$ and $G_0''$ contain two simply isomorphic subgroups $H_0'$ and $H_0''$ invariant under $G'$ and $G''$ respectively, while $G'$ and $G''$ are generated by $H_0'$ and $H_0''$ and two elements $s_1$ and $s_2$ such that if $s_1^{\kappa(m-1)}$ is the smallest positive power of $s_1^{m-1}$ that occurs in $H_0'$, then $s_2^{\kappa(m-1)}$ is the smallest positive power of $s_2^{m-1}$ that occurs in $H_0''$, and $s_1^{\kappa(m-1)}$, $s_2^{\kappa(m-1)}$ correspond in the given simple isomorphism of $H_0'$ and $H_0''$. Moreover, it is assumed that $s_1$ and $s_2$ transform corresponding generators of $H_0'$, $H_0''$ into corresponding elements in the given simple isomorphism.*

*Two $m$-groups of the same order $G_1$ and $G_2$ are simply isomorphic if they contain two simply isomorphic invariant subgroups $H_1$ and $H_2$ respectively, and are generated by these subgroups and two elements $s_1$ and $s_2$ such that if $s_1^{\lambda}$ is the smallest positive power of $s_1$ which occurs in the abstract containing group $H_1^*$ of $H_1$, then $s_2^{\lambda}$ is the smallest positive power of $s_2$ which occurs in the abstract containing group $H_2^*$ of $H_2$, and $s_1^{\lambda}$ and $s_2^{\lambda}$ correspond as a consequence of the given simple isomorphism of $H_1$ and $H_2$. Moreover, it is assumed that $s_1$, $s_2$ transform corresponding generators of $H_1$, $H_2$ into corresponding elements in the given simple isomorphism.*

We have observed that cyclic $m$-groups of the same order are simply isomorphic, and, obviously, no noncyclic $m$-group can be simply isomorphic

with a cyclic $m$-group. The following is a rather interesting application of the simple isomorphism theorem of §8. Let $G'$ and $G''$ be two $m$-groups of order $g$ reducible to cyclic polyadic groups, and let element $s_0'$ of $G'$ be of the same $m$-adic order as element $s_0''$ of $G''$. Then element $s_0'^{m-1}$ of $G_0'$ is of the same ordinary order as element $s_0''^{m-1}$ of $G_0''$. Since $G_0'$ and $G_0''$ are ordinary cyclic groups of order $g$, a simple isomorphism can be set up between them which makes $s_0'^{m-1}$ correspond to $s_0''^{m-1}$. The theorem in question then yields the following result. *If two m-groups reducible to cyclic polyadic groups are of the same order, and one m-group has an element of the same order as an element of the other, then the m-groups are simply isomorphic.*

Every automorphism of an $m$-group $G$ permutes the elements of $G$ according to a certain ordinary substitution. These substitutions clearly constitute an ordinary substitution group which may be called the group of isomorphisms of $G$. This terminology may be reconciled with that of §16 by noting that when $G$ is represented as a regular substitution group, the corresponding $(K_0)_{11}$ of §16 is simply isomorphic with the group of isomorphisms of $G$.

On the other hand the substitutions which result merely from transforming $G$ by its own elements need not form a 2-group. In fact, it is readily verified that they do form an ordinary substitution group when and only when $G$ has an invariant element. However they clearly do form an $m$-adic group of ordinary substitutions which may then be called the *group of inner isomorphisms of* $G$. It is easily proved that as in the ordinary theory this $m$-group is *simply isomorphic with the central quotient group of* $G$. Hence it is simply isomorphic with $G$ if and only if the associated central of $G$ is the identity.

By using the fact that every automorphism of $G$ can be obtained by transforming it by some element, it is readily proved that the group of inner isomorphisms of $G$ is an invariant subgroup of the group of isomorphisms of $G$, if not identical with it, when the latter is extended to an $m$-group. On the other hand, the containing group of the group of inner isomorphisms is directly an invariant subgroup of the group of isomorphisms, when not identical with it. This containing group clearly consists of the substitutions according to which the elements of $G$ are permuted when $G$ is transformed by all of its polyads.

In extending the Sylow subgroup property of the group of inner isomorphisms of an ordinary group to $m$-groups, we have to restrict our $m$-adic $G$ to be of order $g$ with $g/p^\alpha$ prime to $m-1$, $p^\alpha$ being the largest power of the prime $p$ dividing $g$. Since the order of $I_{11}$, the $m$-group of inner isomorphisms of $G$, divides $g$, $I_{11}$ has the same order property. We can then show that $I_{11}$ *contains the same number of Sylow subgroups corresponding to* $p$ *as* $G$ *does*, it being understood that if $p$ does not divide the order of $I_{11}$, the corresponding Sylow subgroups of $I_{11}$ are its subgroups of first order. While the proof differs little from the corresponding ordinary group proof, we cannot follow Miller

in dismissing it with a line, and instead present it at least in outline. The elements of $I_{11}$ corresponding to the elements of a subgroup $H$ of $G$ constitute a subgroup $H'$ of $I_{11}$ which may be called $H$'s corresponding subgroup. Let $H$ be a Sylow subgroup of $G$ for the prime $p$ in accordance with our hypothesis. Then, by considering $I_{11}$ to be the central quotient group of $G$, and comparing the largest powers of $p$ dividing the orders of $H$, $I_{11}$, and $C_0$ with those dividing the orders of $H$, $H'$, and the crosscut of $H_0$ and $C_0$, we are enabled to conclude that $H'$ is a Sylow subgroup of $I_{11}$ for the prime $p$. Since corresponding elements of $G$ and $I_{11}$ transform corresponding subgroups into corresponding subgroups, the relation between the Sylow subgroups of $G$ for the prime $p$ and their corresponding subgroups of $I_{11}$ is shown by the complete set of conjugates theorem to be a correspondence between all the Sylow subgroups of $G$, and all the Sylow subgroups of $I_{11}$, for the prime $p$. Finally, since any subgroup of $G$ with given corresponding subgroup of $I_{11}$ would be transformed into itself by any other subgroup of $G$ with that corresponding subgroup of $I_{11}$, the above correspondence must be 1-1.

The fact that the central quotient group of a non-abelian group cannot be cyclic leads in ordinary group theory to the result that the order of the group of inner isomorphisms of a non-abelian group is at least four. In the case of a non-abelian $m$-group, the same theorem, used in conjunction with our determination of the $m$-groups of the first three orders, shows that the least order of the group of inner isomorphisms of $m$-groups is at least two when $m-1$ is even, three when $m-1$ is odd but divisible by 3, four when $m-1$ is neither divisible by 2 nor 3. The following examples show that these actually are the least orders of $I_{11}$ for such $m$'s as well as the fact that the order of $I_{11}$ may have any value from that least order up to and including the order four. First, by extending an ordinary group with $I_1$ of order four to an $m$-group, we see that for any $m$, $I_{11}$ may be of order four. An $I_{11}$ of order three is immediately furnished for $m-1$ even by the non-abelian $m$-group of order three itself. For $m-1$ odd, but divisible by 3, we have the following example with $m-1=3$, and hence by extension for any $m$ with $m-1$ divisible by 3. Let $G_0$ be the ordinary cyclic group of order nine generated by the cyclic substitution $t=(a_1a_2a_3a_4a_5a_6a_7a_8a_9)$. Then $s=(a_2a_5a_8)(a_3a_9a_6)$ transforms $t$ into $t^4$ while $s^3=1$. $G=G_0s$ is then a 4-group of order nine. Since $G_0$ is abelian, the associated central $C_0$ of $G$ consists of the elements of $G_0$ invariant under $s$, i.e., of 1, $t^3$, $t^6$. The $I_{11}$ of $G$ is therefore also of order three. Finally an $I_{11}$ of order two for $m-1=2$, and hence by extension for any even $m-1$, is exhibited by the following 3-group of order four. Let $G_0$ be the axial group 1, $(ab)$, $(cd)$, $(ab)(cd)$, $s$ the substitution $(ac)(bd)$. Since $s$ transforms $G_0$ into itself, while $s^2=1$, $G=G_0s$ is a 3-group of order four. As $s$ transforms but 1 and $(ab)(cd)$ of $G_0$ into themselves, the $C_0$ of $G$, and hence also the $I_{11}$ of $G$, is of order two.

When $I_{11}$ is of order two it can abstractly be but the noncyclic $m$-group of

order two with its two first order elements. $G$ is correspondingly separated into two abelian subgroups of half its order. It is readily proved that every abelian subgroup of $G$ is contained in one of these subgroups. Conversely, if non-abelian $G$ can be separated into two abelian subgroups, its $I_{11}$ is of order two.

When $I_{11}$ is of order three, it can be but the non-abelian group when $m-1$ is of the form $6\mu+2$ and $6\mu+4$, the abelian noncyclic group when $m-1$ is of the form $6\mu+3$, and either of these two when $m-1$ is of the form $6\mu+6$ as shown by extensions of the cases where $m-1=2$ and 3. In any event $I_{11}$ consists of three first order elements, so that $G$ is separated into three abelian subgroups of one-third its order. Again every abelian subgroup of $G$ is contained in one of these three subgroups. We have not however been able to decide the question whether a non-abelian $G$ which can be separated into three abelian subgroups of one-third its order must have $I_{11}$ of order three.

We restrict our discussion of $I_{11}$ of order four to $m$'s for which four is the least order of $I_{11}$, i.e., to $m-1$ not divisible by 2 or 3. Since $m-1$ is then prime to the order of $I_{11}$, while the smallest prime divisor of $m-1$ cannot be less than 5, our seemingly trivial form for the number of first order elements of an $m$-group with $m-1$ prime to $g$ shows that $I_{11}$ has exactly one first order element. $I_{11}$ is therefore reducible to an ordinary group of order four, and indeed to the axial group. Furthermore, the subgroups of $I_{11}$ reduce to the subgroups of the axial group when $I_{11}$ is so reduced. It follows that $G$ then has three abelian subgroups of half its order, while every abelian subgroup of $G$ is contained in one of these subgroups. Conversely, if a non-abelian $m$-group with $m-1$ not divisible by 2 or 3 has more than one abelian subgroup of half its order, its $I_{11}$ is reducible to the axial group.

33. **Extension of Frobenius's theorem to $m$-adic groups.** Thanks to recent work of Hall([89]) on a wide generalization of Frobenius's theorem, the extension of the original theorem of Frobenius to polyadic groups is immediate. A very special case of Theorem III of Hall's paper may be stated as follows. If a subgroup $H$ is transformed into itself by an element $P$, then the number of solutions of $X^N=1$ which lie in the coset $HP$ is congruent to 0 modulo H.C.F.$(N, h)$, where $h$ is the order of $H$. Given, then, an arbitrary $m$-group $G$ of order $g$, express $G$ in the form $G=G_0s_0$ in accordance with our coset theorem. With $n$ a divisor of $g$, the elements $s$ of $G$ whose $m$-adic orders divide $n$ are those for which $s^{[n]}=s$, i.e., $s^{(m-1)n}=1$. Since $G_0$ is transformed into itself under $s_0$, the above special case of Hall's theorem is immediately applicable to yield the following result. *The number of elements of an $m$-group $G$ of order $g$ whose ($m$-adic) orders divide an arbitrary divisor $n$ of $g$ is, if not* 0, *not only a multiple of $n$, but of $n$* H.C.F.$(g/n, m-1)$.

That the number in question may be 0 is shown by a cyclic $m$-group of

([89]) P. Hall, *On a theorem of Frobenius*, Proceedings of the London Mathematical Society, (2), vol. 40 (1935–1936), pp. 468–501.

order $g$ with $g/n$ not prime to $m-1$. If $\gamma$ is any divisor of $n$, $g/\gamma$ will also fail to be prime to $m-1$, and the cyclic group has no elements of orders dividing $n$. Note that when $g$ is prime to $m-1$ this can never occur, for our otherwise arbitrary $G$ must then have at least one first order element. Actually, by applying the above result, restated for $n$ not a divisor of $g$, to the conjugate subgroups of $G$ of §26—and for these subgroups, indeed, the result is easily obtainable with but the help of the ordinary Frobenius theorem—we obtain the following stronger result. *If an $m$-group $G$ is of order $g$ prime to $m-1$, and $n$ is any divisor of $g$, then the number of elements of $G$ whose orders divide $n$ is a multiple not only of $n$, but of $n$* H.C.F.$(g/n, \lambda)$, $\lambda$ *being the number of first order elements of $G$.*

34. **Representation of an abstract $m$-adic group as a transitive $(m, \mu)$ substitution group.** We shall consider the general question of representing an abstract $m$-group $G$ of order $g$ by a transitive $m$-adic group of $\mu$-adic substitutions of degree $n$. (See §17.) The result can then immediately be specialized to the two cases of chief interest, $\mu=m$ and $\mu=2$, as well as to the case $n=g$, i.e., when the representing group is regular.

In the general case it is necessary to introduce polyadic groups intermediate between $G$ and its associated ordinary group $G_0$, groups whose introduction simultaneously with that of $G_0$ could have been used to generalize the theory at a number of points(90). Clearly each coset in the expansion of the abstract containing group $G^*$ of $G$ as regards $G_0$ is a polyadic group of order $g$ under suitable extensions of the dyadic operation of $G^*$. In particular, if $i$ is a divisor of $m-1$, the coset consisting of the $i$-ads of $G$, regarded as members of $G^*$, will thus constitute a group of dimension $(m-1)/i+1$. It will suffice to refer to this group as the polyadic group $G_i$ of the $i$-ads of $G$. In particular $G_1=G$, $G_{m-1}=G_0$. As in the case of the subgroups of $G$, we may identify $(G_i)^*$ with the subgroup of $G^*$ generated by the elements of $G_i$. $(G_i)_0$ is then simply $G_0$. Finally, since the isomorphism between $G^*$ and any other containing group of $G$ established in §6 involves but a 1-1 correspondence between the elements of two corresponding cosets, $G_i$ may similarly be set up by means of any containing group of $G$.

Suppose then that $G$ can be represented by a transitive $(m, \mu)$ group $G'$ of degree $n$, with, of course, $\mu-1$ a divisor of $m-1$. Corresponding to the polyadic group $G_{\mu-1}$ of the $(\mu-1)$-ads of $G$ there will then be the polyadic group $G'_{\mu-1}$ of the $(\mu-1)$-ads of $G'$, conveniently set up by means of the containing group of $G'$ generated by the substitutions of $G'$. $G'_{\mu-1}$ then consists of substitutions carrying each of the $\mu-1$ $\Gamma$'s on which $G'$ is written into themselves(91). Since $G'$ is transitive, at least one substitution of $G'_{\mu-1}$ carries $a_{11}$

(90) E.g., see the end of the last footnote to §7. Likewise the concept of semi-invariant subgroups could correspondingly be generalized.

(91) Note that these will also be the substitutions forming $G'_0$ when and only when the containing group generated by $G'$ is of index $\mu-1$.

into itself. The set of all such substitutions in $G'_{\mu-1}$ then constitutes a subgroup $H'_{\mu-1}$ of $G'_{\mu-1}$ of order $g/n$. The associated ordinary group $H'_0$ of $H'_{\mu-1}$ is a subgroup of the associated ordinary group $G'_0$ of $G'$, and, in fact, consists of the substitutions of $G'_0$ carrying $a_{11}$ into itself. It then follows from the transitivity of $G'$ that neither $H'_0$, if it be not the identity, nor any subgroup of $H'_0$ other than the identity is invariant under $G'$.

It therefore follows that for $G$ to be representable by a transitive $(m, \mu)$ group of degree $n$, $\mu-1$ a divisor of $m-1$, it is necessary that $G_{\mu-1}$ have a subgroup $H_{\mu-1}$ of order $g/n$ such that neither $H_0$, that is, $(H_{\mu-1})_0$, if it be not the identity, nor any subgroup of $H_0$ other than the identity is invariant under $G$. We now prove this condition also sufficient. Each right coset of $G^*$ as regards $H_0$ consists of $g/n$ $i$-ads with fixed $i$. $H^*_{\mu-1}$ consists of $(m-1)/(\mu-1)$ of these cosets, one for each $i$ a multiple of $\mu-1$. Each right coset of $G^*$ as regards $H^*_{\mu-1}$ therefore also consists of $(m-1)/(\mu-1)$ of the right cosets of $G^*$ as regards $H_0$, one for each $i$ differing from a fixed $i=i_0$ by a multiple of $\mu-1$. We may then choose $i_0$ so that $1 \leqq i_0 \leqq \mu-1$. And for each such $i_0$ there will be exactly $n$ right cosets of $G^*$ as regards $H^*_{\mu-1}$ which together exhaust all $i$-ads with $i-i_0$ a multiple of $\mu-1$. Now symbolize the $n$ right cosets of $G^*$ as regards $H^*_{\mu-1}$ with $i_0=1$ by the letters $a_{11}, a_{12}, \cdots, a_{1n}$. These together will form the $\Gamma_1$ of the basis of our representation. Similarly for $\Gamma_2, \cdots, \Gamma_{\mu-1}$, with $i_0$ correspondingly $2, \cdots, \mu-1$. If now we multiply the elements of $G^*$ on the right by an element $s$ of $G$, the effect on the right cosets of $G^*$ as regards $H^*_{\mu-1}$ is merely to permute them as units, the $i_0$ of such a coset becoming $i_0+1$, reduced modulo $\mu-1$ if need be. In terms of the $a$'s therefore, the letters of $\Gamma_1$ go over in 1-1 fashion into those of $\Gamma_2$, of $\Gamma_2$ into those of $\Gamma_3, \cdots$, of $\Gamma_{\mu-1}$ into those of $\Gamma_1$. Corresponding to $s$ there is thus determined a $\mu$-adic substitution $s'$ of degree $n$ on the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_{\mu-1}$. The set of all such $\mu$-adic substitutions corresponding to elements of $G$ clearly constitute an $m$-group $G'$, under the product of $m$ substitutions as operation, isomorphic with $G$. This isomorphism is also simple. For if $s_1$ and $s_2$ are any two elements of $G$ corresponding to the same substitution $s'$ of $G'$, $t=s_1s_2^{-1}$ must be both in $G_0$ and $H^*_{\mu-1}$, and hence in $H_0$. The set of such $t$'s must then be a group contained in $H_0$, and invariant under $G$, and hence consists of the identity only. That is, $s_1=s_2$.

We have thus proved the following theorem. *A necessary and sufficient condition that an abstract m-group G of order g can be represented as a transitive m-adic group of μ-adic substitutions of degree n, μ−1 a divisor of m−1, is that the polyadic group of (μ−1)-ads of G contains a subgroup of order g/n whose associated ordinary group, if not the identity, is not invariant under G, and contains no subgroup besides the identity invariant under G.* For the representation of $G$ by a transitive $m$-adic substitution group of degree $n$ this condition reduces to the condition that *the associated ordinary group of G contains a subgroup of order g/n which, if not the identity, is not invariant under G, and*

*contains no subgroup besides the identity invariant under G*, while for the representation of $G$ by a transitive $m$-group of ordinary substitutions the condition becomes *$G$ contains a subgroup of order $g/n$ whose associated ordinary group has the above property.*

When $g=n$ the non-invariantive property is vacuously satisfied. Hence *a necessary and sufficient condition that an abstract $m$-group $G$ can be represented by a regular $m$-adic group of $\mu$-adic substitutions is that the polyadic group of $(\mu-1)$-ads of $G$ possesses a first order element.* When $\mu=m$ this leads again, through the identity of $G_0$, to the *universal representability* of abstract $m$-groups as regular $m$-adic substitution groups. On the other hand, for the representation of $G$ as a regular $m$-adic group of ordinary substitutions, it is necessary and sufficient that *$G$ possess a first order element.* In particular, every abstract $m$-group of order prime to $m-1$ can be so represented.

## C. Finite $m$-adic linear groups

35. **$m$-adic linear transformations.** An ordinary transformation in $n$ variables may be thought of as transforming an $m$-dimensional space $\Sigma$ into itself. By analogy with $m$-adic substitutions, an $m$-adic transformation in $n$ variables will then transform $m-1$ spaces $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$, of $n$ dimensions each, cyclically into each other, i.e., $\Sigma'\to\Sigma''$, $\Sigma''\to\Sigma'''$, $\cdots$, $\Sigma^{(m-1)}\to\Sigma'$. In particular, if $x_{i1}, x_{i2}, \cdots, x_{in}$ are the old coordinates in $\Sigma^{(i)}$, and $x'_{i1}, x'_{i2}, \cdots, x'_{in}$ the new, *an $m$-adic linear transformation of $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$* will consist of $m-1$ sets of linear homogeneous equations of the form

$$
A:\quad
\begin{aligned}
&\cdots, \ x_{i1} = a^{(i)}_{11} x'_{(i+1)1} + a^{(i)}_{12} x'_{(i+1)2} + \cdots + a^{(i)}_{1n} x'_{(i+1)n}, \ \cdots,\\
&\cdots, \ x_{i2} = a^{(i)}_{21} x'_{(i+1)1} + a^{(i)}_{22} x'_{(i+1)2} + \cdots + a^{(i)}_{2n} x'_{(i+1)n}, \ \cdots,\\
&\cdots, \ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \ \cdots,\\
&\cdots, \ x_{in} = a^{(i)}_{n1} x'_{(i+1)1} + a^{(i)}_{n2} x'_{(i+1)2} + \cdots + a^{(i)}_{nn} x'_{(i+1)n}, \ \cdots,
\end{aligned}
$$

where $i=1, 2, \cdots, m-1$, the $i+1$ in the last case being replaced by 1, and where for each $i$ the determinant of the $n^2$ coefficients is not zero.

As in the case of $m$-adic substitutions, we shall assume for simplicity that the spaces $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ are mutually exclusive. The $m$-adic linear transformation $A$ may then be considered to be an ordinary linear transformation of the $(m-1)n$ variables $x_{11}, \cdots, x_{(m-1)n}$, but of the above special form([92]). The product of $m$ such linear transformations will again be a linear transformation of the same form, and hence serves to define an $m$-adic operation on $m$-adic linear transformations of $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$. It then readily follows that the class of all $m$-adic linear transformations of

([92]) The above requirement that each of the $m-1$ separate determinants be different from zero is equivalent to this ordinary linear transformation's being nonsingular. See the end of the present section.

$\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ with complex coefficients form an $m$-group under this operation. For the associative law follows immediately from this reinterpretation. Furthermore, if in the equation $A_1A_2 \cdots A_m = A_{m+1}$ all but $A_i$ are specified $m$-adic linear transformations, $A_i$ will be determined as an ordinary linear transformation and be given by the equation $A_i = A_{i-1}^{-1} \cdots A_1^{-1}A_{m+1}A_m^{-1} \cdots A_{i+1}^{-1}$. Now each $A^{-1}$ carries $\Sigma_j$ into $\Sigma_{j-1}$. Hence $A_i$ carries $\Sigma_j$ into $\Sigma_k$ where $k \equiv j-(m-1)+1 \pmod{m-1}$, i.e., $k \equiv j+1 \pmod{m-1}$, and $A_i$ is also an $m$-adic linear transformation.

We shall call any set of $m$-adic linear transformations of $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ which constitute an $m$-group under the above operation an *$m$-adic linear group in $n$ variables*. Any such $m$-group will then be a subgroup of the above "complete" $m$-adic linear group in $n$ variables. It follows that the necessary and sufficient condition that a finite set of $m$-adic linear transformations of $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ with complex coefficients form an $m$-adic linear group is that the product of any $m$ members of the set is in the set. Unless otherwise indicated, $m$-adic linear group will mean finite $m$-adic linear group in the present paper. However, the infinite complete $m$-adic linear group is useful in serving as fundamental $m$-group for operations on arbitrary $m$-adic linear transformations. Its members, as ordinary linear transformations in $(m-1)n$ variables, will generate a containing group of index $m-1$ which may therefore be used in place of its abstract containing group. Its ordinary associated group, consisting of the products of $m-1$ $m$-adic linear transformations of $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$, will therefore consist of transformations which carry each $\Sigma^{(i)}$ into itself, and indeed of all linear transformations with complex coefficients which carry each $\Sigma^{(i)}$ into itself. We may therefore refer to such transformations as $(m-1)$-ads of $m$-adic linear transformations, or briefly $(m-1)$-ads.

While it will continue to be useful every so often to consider $m$-adic linear transformations as special forms of ordinary linear transformations, it is as generalization of ordinary linear transformation that they lend themselves to a corresponding generalization of the ordinary theory. For this purpose we return to our arbitrary $m$-adic linear transformation $A$, and as in ordinary theory represent it by the *$m$-adic matrix*

$$A = [A', A'', \cdots, A^{(m-1)}],$$

where the *component* $A^{(i)}$ is the ordinary matrix

$$A^{(i)} = \begin{pmatrix} a_{11}^{(i)} & a_{12}^{(i)} & \cdots & a_{1n}^{(i)} \\ a_{21}^{(i)} & a_{22}^{(i)} & \cdots & a_{2n}^{(i)} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1}^{(i)} & a_{n2}^{(i)} & \cdots & a_{nn}^{(i)} \end{pmatrix}$$

formed from the coefficients in the equations expressing each $x_{ij}$, with fixed $i$, in terms of the $x'_{(i+1)k}$'s. The product of $m$ $m$-adic linear transformations $A_1, A_2, \cdots, A_m$ is the $m$-adic linear transformation $A$ obtained by performing these $m$ transformations in succession. If then the corresponding $m$-adic matrices are $A_1=[A_1', A_1'', \cdots, A_1^{(m-1)}], \cdots, A_m=[A_m', A_m'', \cdots, A_m^{(m-1)}]$, then by following through the $m$ transformations, we find that the $m$-adic matrix $A=[A', A'', \cdots, A^{(m-1)}]$ is given by the following ordinary matrix equations

$$\begin{aligned} A' &= A_1'A_2'' \cdots A_{m-1}^{(m-1)}A_m, \\ &\cdots\cdots\cdots\cdots\cdots, \\ A^{(i)} &= A_1^{(i)}A_2^{(i+1)} \cdots A_{m-1}^{(i-1)}A_m^{(i)}, \\ &\cdots\cdots\cdots\cdots\cdots, \\ A^{(m-1)} &= A_1^{(m-1)}A_2' \cdots A_{m-1}^{(m-2)}A_m^{(m-1)}. \end{aligned}$$

These equations then completely determine an $m$-adic operation on $m$-adic matrices. We shall call $A$ the product of $A_1, A_2, \cdots, A_m$, and write simply $A=A_1A_2 \cdots A_m$. From the correspondence between $m$-adic matrices and $m$-adic linear transformations we then have immediately that the set of all $m$-adic matrices with complex $a$'s and fixed $n$, forms an $m$-group under this $m$-adic operation. Hence also we have the group property criterion for a finite $m$-adic group of $m$-adic matrices. As in ordinary theory, we therefore reinterpret $m$-adic linear group as an $m$-adic group of $m$-adic matrices.

We could correspondingly reinterpret the concrete containing group of the complete $m$-adic linear group. It suffices for our purpose merely to do so for the $(m-1)$-ads of the containing group. If $\alpha^{(i)}$ is the matrix of the coefficients in the transformation thus expressing the $x_{ij}$'s in terms of the $x_{ik}$'s, we shall represent the $(m-1)$-ad $\alpha$ by the sequence of matrices $\alpha=(\alpha', \alpha'', \cdots, \alpha^{(m-1)})$. The dyadic operation on matrix $(m-1)$-ads is then seen from the corresponding transformations to be

$$\begin{aligned} &(\alpha_1', \alpha_1'', \cdots, \alpha_1^{(m-1)})(\alpha_2', \alpha_2'', \cdots, \alpha_2^{(m-1)}) \\ &\qquad = (\alpha_1'\alpha_2', \alpha_1''\alpha_2'', \cdots, \alpha_1^{(m-1)}\alpha_2^{(m-1)}), \end{aligned}$$

while the product of an $(m-1)$-ad and a monad, i.e., a single $m$-adic linear transformation, will be given by

$$\begin{aligned} &(\alpha', \alpha'', \cdots, \alpha^{(m-1)})[A', A'', \cdots, A^{(m-1)}] \\ &\qquad = [\alpha'A', \alpha''A'', \cdots, \alpha^{(m-1)}A^{(m-1)}], \end{aligned}$$

of a monad by an $(m-1)$-ad by

$$[A', A'', \cdots, A^{(m-1)}](\alpha', \alpha'', \cdots, \alpha^{(m-1)}) = [A'\alpha'', A''\alpha''', \cdots, A^{(m-1)}\alpha'].$$

Clearly the identity among $(m-1)$-ads is $(E, E, \cdots, E)$, where $E$ is the ordinary matrix identity, while the inverse of $(\alpha', \alpha'', \cdots, \alpha^{(m-1)})$ is $((\alpha')^{-1}, (\alpha'')^{-1}, \cdots, (\alpha^{(m-1)})^{-1})$.

We consider now the important question of change of variable. Let $S$ be an $m$-adic linear transformation carrying the $x_{ij}$'s into the $x_{(i+1)k}$'s, $T$ an $m$-adic linear transformation expressing the $x_{ij}$'s in terms of $X_{(i+1)k}$'s, and likewise the $x'_j$'s in terms of $X'_{(i+1)k}$'s. As a result, the $X_{ij}$'s are carried into the $X'_{(i+1)k}$'s according to an $m$-adic linear transformation $R$. We shall say that $R$ is the result of $m$-adically changing variables in $S$ according to $T$. Now with $R$, $S$, and $T$ considered to be ordinary linear transformations on $(m-1)n$ variables, $R$ is the result of an ordinary change of variables in $S$ according to $T$, and hence is the transform of $S$ with respect to $T$. If then in the equation $R=T^{-1}ST$ we follow through the successive linear transformations, we obtain the following results on the corresponding $m$-adic matrices. If

$$S = [S', S'', \cdots, S^{(m-1)}], \quad T = [T', T'', \cdots, T^{(m-1)}],$$

then the transform

$$R = [R', R'', \cdots, R^{(m-1)}]$$

of $S$ with respect to $T$, which is the result of $m$-adically changing the variables of $S$ according to $T$, is given by the equations

$$R^{(i)} = [T^{(i-1)}]^{-1}S^{(i-1)}T^{(i)}, \qquad i = 1, 2, \cdots, m-1 \ (^{93}).$$

Closer to the ordinary concept of change of variable would be instituting an ordinary change of variable in each space $\Sigma^{(i)}$. This would then correspond to changing variables according to an $(m-1)$-ad. As before, if $S$ is an $m$-adic linear transformation, $\tau$ equivalent to an $(m-1)$-ad of $m$-adic linear transformations, the result of changing variables in $S$ according to $\tau$ will be an $m$-adic linear transformation $R$ with $R=\tau^{-1}S\tau$. The corresponding formula for transforming the $m$-adic matrix $S=[S', S'', \cdots, S^{(m-1)}]$, by the $(m-1)$-ad $\tau=(\tau', \tau'', \cdots, \tau^{(m-1)})$ to yield the $m$-adic matrix $R=[R', R'', \cdots, R^{(m-1)}]$ may again be obtained by following through the transformations involved, or, perhaps just as easily, by applying our formulas for operations on $(m-1)$-ads. We thus obtain

$$R^{(i)} = [\tau^{(i)}]^{-1}S^{(i)}\tau^{(i+1)}, \qquad i = 1, 2, \cdots, m-1.$$

While our $m$-adic matrix notation is more convenient in most applications, our later generalization of characteristic equation requires rather the matrix of the corresponding ordinary linear transformation in the $(m-1)n$ variables.

---

($^{93}$) These equations can also be obtained from the equations defining the $m$-adic operation on $m$-adic matrices, and the original $m$-adic definition of transform.

With $A=[A', A'', \cdots, A^{(m-1)}]$, the corresponding ordinary matrix then has the following form

$$\begin{pmatrix} 0 & A' & 0 & \cdots & 0 \\ 0 & 0 & A'' & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & A^{(m-2)} \\ A^{(m-1)} & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

If then $D$ is the determinant of this matrix, $D', \cdots, D^{(m-1)}$ of the components $A', \cdots, A^{(m-1)}$ of $A$, it follows that

$$D = (-1)^{mn} D'D'' \cdots D^{(m-1)}.$$

By contrast, for the $(m-1)$-ad $\alpha=(\alpha', \alpha'', \cdots, \alpha^{(m-1)})$, the corresponding ordinary matrix has the components of $\alpha$ along its principal diagonal, zero's elsewhere, and the determinant of the matrix is always the product of the determinants of the components.

36. ***m*-adic collineations and collineation-groups.** If the variables of each space $\Sigma^{(i)}$ be considered homogeneous coordinates in a corresponding space $S^{(i)}$ of dimension $n-1$, our $m$-adic linear transformation $A$ on $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$, may be said to define an *m-adic collineation* on $S', S'', \cdots, S^{(m-1)}$. In fact, if we let the ratios $x_{i1}/x_{in}, \cdots, x_{i(n-1)}/x_{in}$ be denoted by $y_{i1}, \cdots, y_{i(n-1)}$, we are thus led to the *m-adic linear fractional transformation* $i=1, 2, \cdots, m-1$:

$$y_{is} = \frac{a_{s1}^{(i)} y'_{(i+1)1} + \cdots + a_{s(n-1)}^{(i)} y'_{(i+1)(n-1)} + a_{sn}^{(i)}}{a_{n1}^{(i)} y'_{(i+1)1} + \cdots + a_{n(n-1)}^{(i)} y'_{(i+1)(n-1)} + a_{nn}^{(i)}}, \qquad s = 1, 2, \cdots, n-1.$$

Unlike the case of an $m$-adic linear transformation, our $m$-adic linear fractional transformation is in general not a special case of an ordinary linear fractional transformation on all the variables, since the denominators in general are not all the same. On the other hand it justifies our phrase $m$-adic collineation, since the equality of the denominators for each $i$ insures our $m$-adic linear fractional transformation on the nonhomogeneous $y$'s carrying the straight lines of each $S^{(i)}$ into those of $S^{(i+1)}$. Moreover, the product of $m$ $m$-adic linear fractional transformations of $S', S'', \cdots, S^{(m-1)}$ will again be of that form, so that we can expect to have $m$-adic linear fractional groups, and hence $m$-adic collineation-groups.

Two $m$-adic linear transformations $A_1$ and $A_2$ on $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ will yield the same $m$-adic linear fractional transformation on $S', S'', \cdots, S^{(m-1)}$ when and only when their $m$-adic matrices $A_1=[A_1', A_1'', \cdots, A_1^{(m-1)}]$ and $A_2=[A_2', A_2'', \cdots, A_2^{(m-1)}]$ are such that the elements of each component $A_1^{(i)}$ are a constant $k_i$ times the elements of the corresponding component $A_2^{(i)}$.

This then is the condition that $A_1$ and $A_2$ represent the same $m$-adic collineation. Since the $k_i$'s need not be the same, $A_1$ and $A_2$ as ordinary linear transformations need not then represent the same collineation in the ordinary sense. If now we let $\tau$ be the $(m-1)$-ad

$$((k_1, k_1, \cdots, k_1), (k_2, k_2, \cdots, k_2), \cdots, (k_{m-1}, k_{m-1}, \cdots, k_{m-1}))$$

whose components are all ordinary similarity-matrices, we see from the preceding section that $A_1 = \tau A_2$. We shall call an $(m-1)$-ad each of whose components is a similarity-matrix a *similarity-$(m-1)$-ad*. It follows that $A_1$ and $A_2$ represent the same $m$-adic collineation when and only when $A_1 A_2^{-1}$ is a similarity-$(m-1)$-ad.

$A_2^{-1} A_1$ must then also be a similarity-$(m-1)$-ad; but it will equal $A_1 A_2^{-1}$ when and only when the $k_i$'s are all equal. In fact, again by the preceding section, writing the above $\tau = (\tau', \tau'', \cdots, \tau^{(m-1)})$, we find that $A_1 = A_2 \bar{\tau}$, where $\bar{\tau} = (\tau^{(m-1)}, \tau', \cdots, \tau^{(m-2)})$, and hence $A_2^{-1} A_1 = \bar{\tau}$. Comparing these two results, we see that $A_2^{-1} \tau A_2 = \bar{\tau}$. Since $A_2$ is an arbitrary $m$-adic matrix, it follows that every $m$-adic matrix transforms a similarity-$(m-1)$-ad $(\tau', \tau'', \cdots, \tau^{(m-1)})$ into the similarity-$(m-1)$-ad

$$(\tau^{(m-1)}, \tau', \cdots, \tau^{(m-2)}).$$

By contrast, every similarity-$(m-1)$-ad is transformed into itself by an $(m-1)$-ad.

Consider now any $m$-adic linear group $G$. Since the product of two similarity-$(m-1)$-ads is again a similarity-$(m-1)$-ad, the similarity-$(m-1)$-ads of $G_0$, the associated ordinary group of $G$, will constitute a subgroup $H_0$ of $G_0$. Since every $m$-adic matrix transforms a similarity-$(m-1)$-ad into a similarity-$(m-1)$-ad, $H_0$ will be invariant under $G$. We may therefore form the $m$-adic quotient group $K = G/H_0$. Each coset of $G$ as regards $H_0$ can be written $H_0 A$ with $A$ in $G$, and hence consists of elements of $G$ representing the same $m$-adic collineation as $A$, and, in fact, of all such elements of $G$. The elements of $K$ are thus in 1-1 correspondence with the distinct $m$-adic collineations represented by the elements of $G$. $K$ may therefore be called the *$m$-adic collineation-group* corresponding to $G$.

An arbitrary $m$-adic collineation-group $G$ may be given by arbitrarily representing each collineation by an $m$-adic linear transformation(94). If $G$ is of order $g$, and written thus "on $n$ variables," a modification of the ordinary treatment will yield an $m$-adic linear group of order $n^{m-1} g$ which is $(n^{m-1}, 1)$ isomorphic with $G$, and whose transformations have *components of determinant unity*. In fact let $S = [S', S'', \cdots, S^{(m-1)}]$ be in $G$ thus represented, with the determinants of its components $D', D'', \cdots, D^{(m-1)}$ respectively. Let $\theta^{(i)}$ be any solution of the equation $[\theta^{(i)}]^n = [D^{(i)}]^{-1}$, and form the similarity-

(94) The product of $m$ such representatives need not then be in the given set of representatives, but need merely represent the same $m$-adic collineation as some member of the set.

$(m-1)$-ad $\tau=((\theta', \theta', \cdots, \theta'), (\theta'', \theta'', \cdots, \theta''), \cdots, (\theta^{(m-1)}, \theta^{(m-1)}, \cdots, \theta^{(m-1)}))$. Then $A=\tau S=[(\theta', \theta', \cdots, \theta')S', (\theta'', \theta'', \cdots, \theta'')S'', \cdots, (\theta^{(m-1)}, \theta^{(m-1)}, \cdots, \theta^{(m-1)})S^{(m-1)}]$ represents the same $m$-adic collineation as $S$, and has all of its components of determinant unity. For each $S$ there will thus be $n^{m-1}$ $A$'s, and these constitute all of the $m$-adic linear transformations with components of determinant unity representing the same $m$-adic collineation as $S$. It then readily follows that the set of $n^{m-1}g$ $m$-adic linear transformations thus corresponding to the $g$ elements of $G$ constitute a linear $m$-group isomorphic with $G$. For let $S_1, S_2, \cdots, S_m$ be any $m$ transformations in the original representation of $G$, $A_1=\tau_1 S_1$, $A_2=\tau_2 S_2, \cdots, A_m=\tau_m S_m$ corresponding transformations with components of determinant unity. Then

$$A = A_1 A_2 \cdots A_m$$

has for its $i$th component

$$A^{(i)} = A_1^{(i)} A_2^{(i+1)} \cdots A_m^{(i)} = \tau_1^{(i)} \tau_2^{(i+1)} \cdots \tau_m^{(i)} S_1^{(i)} S_2^{(i+1)} \cdots S_m^{(i)} = \tau^{(i)} S^{(i)},$$

where $S=S_1 S_2 \cdots S_m$, and $\tau$ is a similarity-$(m-1)$-ad. $A$ therefore has components of determinant unity, and represents the same $m$-adic collineation as $S$. $A$ is therefore in our set of $n^{m-1}g$ transformations, whence finally our result.

To compare the ordinary treatment with this modification of it, we introduce the following considerations. Given an $m$-adic linear group $G$, those similarity-$(m-1)$-ads of $G_0$ which have equal components themselves constitute a subgroup $H_0'$ of $G_0$ invariant under $G$. We may therefore form the $m$-adic quotient group $K'=G/H_0'$. Each coset of the expansion of $G$ as regards $H_0'$ consists of all transformations in $G$ which as ordinary transformations on $(m-1)n$ variables correspond to the same ordinary collineation. We shall therefore call $K'$ the collineation-$m$-adic group of $G$. If now an arbitrary collineation-$m$-adic group $G$ be given by corresponding representative $m$-adic linear transformations, the ordinary treatment applies without modification; and if $G$ is of order $g$, and on $n$ variables, a linear $m$-adic group of order $(m-1)ng$ is thus obtained which is $[(m-1)n, 1]$ isomorphic with $G$, and whose members as ordinary transformations are of determinant unity. On the other hand, if an arbitrary $m$-adic collineation-group $G$ be thus given, the ordinary unmodified treatment will in general be inapplicable. In fact, otherwise, the given representatives of the members of $G$ must also be representatives of the members of a collineation-$m$-adic group. This will clearly not be so for random representations of the members of $G$. And the following example shows that the $m$-adic collineation-group $G$ may be such that no representation thereof will represent a collineation-$m$-adic group. The triadic collineations corresponding to

$$A: \quad [(1, 1), (1, -1)], \qquad B: \quad \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right]$$

generate a triadic collineation-group $G$ of order 4. The most arbitrary representations of $A$ and $B$ are

$$A: \quad [(a, a), (b, -b)], \qquad B: \quad \left[\begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}, \begin{pmatrix} 0 & d \\ -d & 0 \end{pmatrix}\right].$$

By direct computation we find that $AAA = [(a^2b, -a^2b), (ab^2, ab^2)]$, $BBA = [(-acd, acd), (bcd, bcd)]$. As triadic collineations, $AAA$ and $BBA$ are identical, being the same as $[(1, -1), (1, 1)]$. As ordinary collineations, they can but be identified with $[(a, -a), (b, b)]$, $[(-a, a), (b, b)]$ which are never the same. Since any representation of $G$ can have but one triadic linear transformation for each triadic collineation in $G$, no representation of this triadic collineation-group can also represent a collineation-triadic group.

If however $G$ itself is an $m$-adic linear group, both methods are applicable. The unmodified treatment will then yield an $m$-adic linear group which is $[(m-1)n, 1]$ isomorphic with the collineation-$m$-adic group of $G$, and whose members as ordinary linear transformations have determinants unity. On the other hand, our modified treatment yields an $m$-adic linear group which is $(n^{m-1}, 1)$ isomorphic with the $m$-adic collineation-group of $G$, and whose members have components of determinant unity.

37. **$m$-adic Hermitian invariants.** A set of $m-1$ positive-definite Hermitian forms $J = [J', J'', \cdots, J^{(m-1)}]$, one for each space $\Sigma^{(i)}$, will be said to be an *$m$-adic (positive-definite) Hermitian form.* Now

$$J^{(i)} = \sum_{k=1}^{n} \sum_{l=1}^{n} q_{kl}^{(i)} x_{ik} \bar{x}_{il}, \qquad q_{lk}^{(i)} = \bar{q}_{kl}^{(i)},$$

can be transformed into

$$I^{(i)} = y_{i1}\bar{y}_{i1} + y_{i2}\bar{y}_{i2} + \cdots + y_{in}\bar{y}_{in}$$

by a change of variables of the form

$$y_{ik} = \sum_{l=1}^{k} \rho_{kl}^{(i)} x_{il}, \qquad k = 1, 2, \cdots, n.$$

Hence $J = [J', J'', \cdots, J^{(m-1)}]$ *can be transformed into* $I = [I', I'', \cdots, I^{(m-1)}]$ *by changing variables in* $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ *according to an* $(m-1)$*-ad whose components, with* $i = 1, 2, \cdots, m-1$, *are of the above form.* The $(m-1)$-ad, of course, is that obtained by solving for the $x$'s in terms of the $y$'s. It is further understood that in operating on $J$ by this $(m-1)$-ad, if $x_{ij}$ is replaced by a certain expression, $\bar{x}_{ij}$ is replaced by the conjugate of that expression.

If, on the other hand, $J$ is transformed according to an $m$-adic change of variables, $J^{(i)}$, written on the variables of $\Sigma^{(i)}$, becomes an expression in the new variables not of $\Sigma^{(i)}$ but of $\Sigma^{(i+1)}$. We are thus led to define an *$m$-adic Hermitian invariant* of an $m$-adic linear group as an $m$-adic Hermitian form

$J=[J', J'', \cdots, J^{(m-1)}]$ such that each transformation in the group carries $J'\to J''$, $J''\to J'''$, $\cdots$, $J^{(m-1)}\to J'$. It then readily follows that *every m-adic linear group G has an m-adic Hermitian invariant.* For let $G_0'$ be the $\Sigma'$ constituent group of $G_0$, the complete analogue of the $G_0'$ of an $m$-adic substitution group. The linear group $G_0'$ then has an Hermitian invariant $J'$ on the variables of $\Sigma'$. Let $S$ be in $G$, and let $J''$ be the result of transforming $J'$ according to $S$, $\cdots$, $J^{(m-1)}$ of transforming $J^{(m-2)}$ according to $S$. Then $J=[J', J'', \cdots, J^{(m-1)}]$ will be an $m$-adic Hermitian form on $\Sigma'$, $\Sigma''$, $\cdots$, $\Sigma^{(m-1)}$, and, as in §39 to come, is seen to be an $m$-adic Hermitian invariant of $G$.

By combining the above two results it follows that *the variables of an m-adic linear group G may be so changed according to an* $(m-1)$*-ad that* $I=[I', I'', \cdots, I^{(m-1)}]$, $I^{(i)}=x_{i1}\bar{x}_{i1}+x_{i2}\bar{x}_{i2}+\cdots+x_{in}\bar{x}_{in}$, *is an m-adic Hermitian invariant of the resulting transform of G.*

An $m$-adic linear group $G$ in $n$ variables will be said to be linearly reducible(95) if by a suitable change of variables according to an $(m-1)$-ad there will be in $\Sigma'$, $\Sigma''$, $\cdots$, $\Sigma^{(m-1)}$ subspaces(96) $\Sigma_1'$, $\Sigma_1''$, $\cdots$, $\Sigma_1^{(m-1)}$ respectively on $\nu<n$ variables each such that $\Sigma_1'\to\Sigma_1''\to\cdots\to\Sigma_1^{(m-1)}\to\Sigma_1'$ under every transformation in the resulting transform of $G$. If for some such change of variables the subspaces $\Sigma_2'$, $\Sigma_2''$, $\cdots$, $\Sigma_2^{(m-1)}$ on the remaining $n-\nu$ variables of $\Sigma'$, $\Sigma''$, $\cdots$, $\Sigma^{(m-1)}$ are also each transformed into the next, then $G$ will be said to be intransitive. In the first case $\Sigma_1'$, $\Sigma_1''$, $\cdots$, $\Sigma_1^{(m-1)}$ will be said to be a *reduced set* for $G$, in the second case a *set of intransitivity* of $G$. We then prove the theorem *a linearly reducible m-adic linear group G is intransitive, and a reduced set constitutes one of the sets of intransitivity of G,* subject, of course, to a change of variables in the reduced set according to an $(m-1)$-ad thereon. We may assume the variables in the reduced set to be the first $\nu$ variables of each $\Sigma^{(i)}$. Then $G$ may be further transformed by an $(m-1)$-ad so that it will have the $m$-adic Hermitian invariant $I$ above. And this further change of variables, according to the form given above, merely transforms the reduced set according to an $(m-1)$-ad on its variables. With $G$ in this last form, consider its containing group $G^*$. Then $I^*=I'+I''+\cdots+I^{(m-1)}$ will be an ordinary Hermitian invariant of the ordinary linear group $G^*$, while the $(m-1)\nu$ variables constituting the reduced set for $G$ form a reduced set for $G^*$ without further transformation. But then $G^*$ is in intransitive form with those $(m-1)\nu$ variables constituting a set of intransitivity of $G^*$. The same is then true of $G$.

An $m$-adic matrix $A=[A', A'', \cdots, A^{(m-1)}]$ will be said to be in canonical form if each component $A^{(i)}$ is in the canonical form $(a_1^{(i)}, a_2^{(i)}, \cdots, a_n^{(i)})$. Then the corresponding ordinary theorem generalizes, i.e., *if A is of finite*

(95) To distinguish between this extension of the ordinary concept and the totally unrelated polyadic concept we have termed reducibility.

(96) Strictly, a misnomer, but a convenient one.

*m-adic order, then it can be reduced to canonical form by transformation by an* $(m-1)$*-ad*([97]). We shall prove this result in the next section more expeditiously. However we here give the analogue of the ordinary proof for the sake of the concepts thus introduced.

We prove then that we can always find $m-1$ linear functions

$$y_{i1} = b_1^{(i)} x_{i1} + b_2^{(i)} x_{i2} + \cdots + b_n^{(i)} x_{in}, \qquad i = 1, 2, \cdots, m-1,$$

such that each $y_{i1}$ is transformed into a constant $\theta_i$ times $y_{(i+1)1}$ by $A$. These $m-1$ functions may then be said to constitute a *relative m-adic invariant* of $A$. With $A$ the transformation

$$x_{is} = \sum_{t=1}^{n} a_{st}^{(i)} x'_{(i+1)t}, \qquad s = 1, 2, \cdots, n;\ i = 1, 2, \cdots, m-1,$$

we find that $(y_{i1})A = \theta_i y_{(i+1)1}$ provided the following equations are true:

$$\theta_i b_t^{(i+1)} = \sum_{s=1}^{n} b_s^{(i)} a_{st}^{(i)}, \qquad t = 1, 2, \cdots, n.$$

By successive substitution, with $i = 1, 2, \cdots, m-1$, we obtain from these equations

$$\theta_1\theta_2 \cdots \theta_{m-1} b_t' = \sum_{s=1}^{n} b_s' a_{st}^{(0)}, \qquad t = 1, 2, \cdots, n,$$

where the ordinary matrix $(a_{st}^{(0)}) = A_0 = A'A'' \cdots A^{(m-1)}$([98]). A set of solutions $b_1', b_2', \cdots, b_n'$, not all zero, of this last set of equations can always be found provided $\theta_1\theta_2 \cdots \theta_{m-1}$ is a root of the characteristic equation of $A_0$. The preceding equations, with $i = 1, 2, \cdots, m-2$, then determine the remaining $b$'s, while the equations for $i = m-1$ are then automatically satisfied.

Having thus found a relative $m$-adic invariant of $A$, the remainder of the proof follows the lines of the standard proof. That is, by a change of variables according to an $(m-1)$-ad given in part by our relative $m$-adic invariant of $A$, the new variables $y_{11}, y_{21}, \cdots, y_{(m-1)1}$ are transformed according to the equations $y_{i1} = \theta_i y'_{(i+1)1}$, $i = 1, 2, \cdots, m-1$, and hence constitute a reduced set for the $m$-adic linear group generated by $A$. If then $A$ is of finite $m$-adic order, further change of variables according to an $(m-1)$-ad will

([97]) It might be thought that since $A$ as ordinary linear transformation is then of finite ordinary order, the standard theorem would apply. But note that an $m$-adic matrix in canonical form is not in canonical form as ordinary matrix. And from the contrary point of view, while $A$ as ordinary matrix could thus be reduced to ordinary canonical form, the resulting linear transformation would no longer be an $m$-adic linear transformation; and the transformation used to obtain it would be a linear transformation on all the $(m-1)n$ variables in a form constituting a meaningless jumble from the point of view of $m$-adic linear transformations.

([98]) Or, more expeditiously, from $(y_{11})A^{m-1} = \theta_1\theta_2 \cdots \theta_{m-1} y_{11}$.

change $y_{11}, y_{21}, \cdots, y_{(m-1)1}$ into a set of intransitivity of the group generated by $A$. $A$ then determines an $m$-adic linear transformation on the remaining $n-1$ variables, and the process may be repeated until $A$ appears in canonical form, and, indeed, as the result of a single change of its original variables according to an $(m-1)$-ad.

Our proof of the existence of relative $m$-adic invariants of $A$ might have taken a different turn. Our original $(m-1)n$ homogeneous linear equations in the $(m-1)n$ undetermined $b$'s will have a set of solutions not all zero, and hence, as shown by the equations themselves, not all zero for any $i$, provided the determinant of their coefficients is zero. We are thus led to one equation in the $m-1$ unknowns $\theta_1, \theta_2, \cdots, \theta_{m-1}$ which may be called the *m-adic characteristic equation* of $A$. Its right-hand member is zero; left, the determinant of $A$ as ordinary linear transformation with the elements of the principal diagonal, all zero in $A$, replaced by $-\theta_{m-1}, \cdots, -\theta_{m-1}, -\theta_1, \cdots, -\theta_1, \cdots, -\theta_{m-2}, \cdots, -\theta_{m-2}$. With $\theta_1=\theta_2=\cdots=\theta_{m-1}=\theta$, the $m$-adic characteristic equation of $A$ becomes the ordinary characteristic equation of $A$ as ordinary linear transformation. We are thus, in fact, assured of relative $m$-adic invariants of $A$ with $\theta$'s all equal. However, comparison with the earlier treatment yields the following result. The solutions of the $m$-adic characteristic equation of $A=[A', A'', \cdots, A^{(m-1)}]$ consist of all sets of values $\theta_1, \theta_2, \cdots, \theta_{m-1}$ for which $\theta_1\theta_2\cdots\theta_{m-1}$ is a root of the characteristic equation of $A_0=A'A''\cdots A^{(m-1)}$.

38. **Reduction to canonical form.** If for two $m$-adic linear transformations $A$ and $B$ in $n$ variables there is a third $C$ such that $B=C^{-1}AC$, then $A$ and $B$ will be said to be *conjugate*. This is equivalent to there being an $(m-1)$-ad $\gamma$ such that $B=\gamma^{-1}A\gamma$, since $C$ and $A^{m-2}C$ on the one hand, $\gamma$ and $A\gamma$ on the other, yield the same transform of $A$. It follows that the relation "$A$ and $B$ are conjugate" is an equivalence relation. Likewise for $m$-adic linear groups.

The following easily proved theorem reduces the problem of conjugate $m$-adic linear transformations in $n$ variables to that of conjugate ordinary linear transformations in $n$ variables. *The necessary and sufficient condition that* $A=[A', A'', \cdots, A^{(m-1)}]$ *and* $B=[B', B'', \cdots, B^{(m-1)}]$ *are conjugate is that* $A_0=A'A''\cdots A^{(m-1)}$ *and* $B_0=B'B''\cdots B^{(m-1)}$ *are conjugate.* In fact, if $B=\gamma^{-1}A\gamma$, $\gamma=(\gamma', \gamma'', \cdots, \gamma^{(m-1)})$, then by our formula for change of variables according to an $(m-1)$-ad

$$B' = [\gamma']^{-1}A'\gamma'', B'' = [\gamma'']^{-1}A''\gamma''', \cdots, B^{(m-1)} = [\gamma^{(m-1)}]^{-1}A^{(m-1)}\gamma'.$$

Hence

$$B'B''\cdots B^{(m-1)} = [\gamma']^{-1}A'A''\cdots A^{(m-1)}\gamma',$$

whence the necessity of our condition. Conversely, if $A_0$ and $B_0$ are conjugate, $\gamma'$ may be chosen to satisfy the last of the above equations. If then $\gamma'', \gamma''', \cdots, \gamma^{(m-1)}$ are determined in accordance with the first $m-2$ of the

change of variable equations, the last of those equations will be automatically satisfied. An $(m-1)$-ad $\gamma=(\gamma', \gamma'', \cdots, \gamma^{(m-1)})$ is thus determined which transforms $A$ into $B$.

This result contrasts strongly with the corresponding result for $(m-1)$-ads. We may define two $(m-1)$-ads $\alpha$ and $\beta$ to be conjugate if there is an $(m-1)$-ad $\gamma$ such that $\beta=\gamma^{-1}\alpha\gamma$. From our formula for the product of two $(m-1)$-ads it follows that $\alpha=(\alpha', \alpha'', \cdots, \alpha^{(m-1)})$ and $\beta=(\beta', \beta'', \cdots, \beta^{(m-1)})$ are conjugate when and only when the corresponding components $\alpha^{(i)}$ and $\beta^{(i)}$ are conjugate for each $i$. Hence, while the question of conjugacy for an $m$-adic matrix in $n$ variables depends on but one ordinary matrix in $n$ variables, the same question for an $(m-1)$-ad depends on $m-1$ independent ordinary matrices in $n$ variables each. Intrinsically, therefore, an $m$-adic matrix is far simpler than an $(m-1)$-ad. This is rather surprising in that apart from change of variables they are of equal generality; for if $A$ is a fixed $m$-adic matrix the relation $S=\tau A$ gives a 1-1 correspondence between all $m$-adic matrices $S$ and $(m-1)$-ads $\tau$.

A more symmetrical though less useful condition for the $m$-adic matrices $A$ and $B$ being conjugate is that the $(m-1)$-ads $A^{m-1}$ and $B^{m-1}$ are conjugate. In fact, if $A^{m-1}=\alpha$, the equation $A^m=\alpha A$ yields

$$A^{m-1} = (A'A'' \cdots A^{(m-1)}, A''A''' \cdots A', \cdots, A^{(m-1)}A' \cdots A^{(m-2)}).$$

The first component of $A^{m-1}$ is therefore the $A_0$ of our previous condition, while all the components are conjugate. The present condition then follows. We may note that all the components of an $(m-1)$-ad being conjugate is sufficient as well as necessary for the $(m-1)$-ad being the $(m-1)$-st ordinary power of some $m$-adic matrix. Intrinsically, then, an $m$-adic matrix is of the same degree of generality as an $(m-1)$-ad with conjugate components. Too much emphasis, however, must not be placed on the forms assumed by a single element under transformation, our present concern.

Returning to our first condition for the conjugacy of $m$-adic matrices, we have immediately that $A=[A', A'', \cdots, A^{(m-1)}]$ is conjugate to $[A_0, E, \cdots, E]$, with $A_0=A'A'' \cdots A^{(m-1)}$. If now $A$ is of finite $m$-adic order, then $A^{m-1}$, and hence its first component $A_0$, is of finite order. $A_0$ is then conjugate to a matrix in the canonical form $(a_1, a_2, \cdots, a_n)$. Hence, *if $A$ is of finite $m$-adic order, it is conjugate to an $m$-adic matrix in the canonical form* $[(a_1, a_2, \cdots, a_n), E, \cdots, E]$.

More generally, if $A$ is of finite $m$-adic order, it is conjugate to those $m$-adic matrices in the canonical form $[(a_1', a_2', \cdots, a_n'), (a_1'', a_2'', \cdots, a_n''), \cdots, (a_1^{(m-1)}, a_2^{(m-1)}, \cdots, a_n^{(m-1)})$ for which $a_i' a_i'' \cdots a_i^{(m-1)}=a_{j_i}, a_{j_1}, a_{j_2}, \cdots, a_{j_n}$ a permutation of $a_1, a_2, \cdots, a_n$. Since $a_1, a_2, \cdots, a_n$ are the roots of the characteristic equation of $A_0$, we may say, as a consequence of the last section, that an $m$-adic matrix $A$ of finite order assumes those canonical forms for which each selection of corresponding elements chosen from its components

constitutes a solution of the $m$-adic characteristic equation of $A$, while the corresponding roots of the characteristic equation of $A_0$ are all of its roots each with the correct multiplicity. In particular, we may make $a_i' = a_i'' = \cdots = a_i^{(m-1)}$ for each $i$. Hence the useful special result *if $A$ is of finite $m$-adic order, it is conjugate to an $m$-adic matrix in canonical form having equal components.*

The most satisfactory generalization of an ordinary similarity-matrix is our similarity-$(m-1)$-ad. An $m$-adic matrix each of whose components is a similarity-matrix will not in general remain of that form under transformation by an $m$-adic matrix([99]). We therefore define an *$m$-adic similarity-matrix* as one which is conjugate to an $m$-adic matrix whose components are all similarity-matrices. It readily follows from our criterion for the conjugacy of $m$-adic matrices that $A = [A', A'', \cdots, A^{(m-1)}]$ *is an $m$-adic similarity-matrix when and only when $A'A'' \cdots A^{(m-1)}$ is a similarity-matrix.* In particular, every first order $m$-adic matrix is an $m$-adic similarity-matrix. In fact, $A$ is of $m$-adic order one when and only when $A'A'' \cdots A^{(m-1)} = E$. Hence the first order $m$-adic matrices are the conjugates of $[E, E, \cdots, E]$.

Our chief reason for introducing the above concept is the following theorem. *If an $m$-adic linear group has an $m$-adic similarity-matrix as invariant element, it is conjugate to a group in which each element is an $m$-adic matrix with equal components.* By an $m$-adic change of variable the invariant similarity-matrix can be transformed into an $m$-adic matrix $A$ in canonical form in which the components are now equal similarity-matrices. If the given group is correspondingly transformed, a conjugate group having $A$ as invariant element is obtained. For each element $B$ of the transformed group we thus have $A^{-1}BA = B$, i.e.,

$$B^{(i)} = [A^{(i-1)}]^{-1} B^{(i-1)} A^{(i)}, \qquad i = 1, 2, \cdots, m-1.$$

Since $A^{(i)}$ and $A^{(i-1)}$ are the same similarity matrices, we thus have $B^{(i)} = B^{(i-1)}$ for $i = 1, 2, \cdots, m-1$, whence our theorem.

An $m$-adic linear group which is reducible to a 2-group automatically satisfies the condition of this theorem via its invariant first order element. An interesting property of any $m$-adic linear group thus conjugate to an "equi-component" group is that its $m$-adic collineation-group is identical with its collineation-$m$-adic group. In fact, in the case of an equi-component group itself, the associated ordinary group consists of $(m-1)$-ads with equal com-

([99]) Nevertheless, the set of such $m$-adic matrices of an $m$-adic linear group do constitute a subgroup, if existent, though in general not an invariant subgroup, of the group—likewise, those of these matrices having equal components. On the other hand, the subset of $m$-adic similarity matrices, in the sense about to be defined, while constituting an invariant subset of the $m$-adic linear group by their very definition, do not in general constitute a subgroup thereof. They do, however, when existent, separate into a number of semi-invariant subgroups with the subgroup of similarity-$(m-1)$-ads as common associated group.

ponents, and hence has no other similarity-$(m-1)$-ads than those with equal components; while under transformation by an $(m-1)$-ad the similarity-$(m-1)$-ads are unchanged. An equi-component group clearly has the following two properties: (a), it is simply isomorphic with a group of ordinary matrices in the specified number of variables, (b), no two distinct elements of the group have a pair of corresponding components the same. Now these properties are invariant for transformation by an $(m-1)$-ad; (a), by its very formulation, (b), by our formulas for transformation by an $(m-1)$-ad. Hence they are satisfied by all groups conjugate to equi-component groups. The class of groups satisfying condition (a), as well as the class of groups satisfying condition (b), are therefore each at least as wide as the class of groups conjugate to equi-component groups. Actually each of the first two classes is wider than the third, for the following examples show that neither of the first two contains the other[100]. Let $G_0$ be the axial group with elements $((1, 1), (-1, -1)), ((-1, -1), (1, 1)), ((-1, -1), (-1, -1)), ((1, 1), (1, 1))$; $S_0 = [(1, 1), (1, 1)]$. Then in terms of the present operations the conditions of the construction theorem of §8 are satisfied, and $G = G_0 S_0$ is a triadic linear group in two variables. Now let $\overline{G}_0$ be the axial group with elements $(1, -1)$, $(-1, 1), (-1, -1), (1, 1)$;

$$\overline{S}_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then $\overline{G} = \overline{G}_0 \overline{S}_0$ is a 3-group of ordinary matrices in two variables. With elements of $G_0$ and $\overline{G}_0$ corresponding in order, $S_0$ corresponding to $\overline{S}_0$, the conditions of the simple isomorphism theorem of §8 are satisfied, so that $G$ is simply isomorphic with $\overline{G}$. Hence $G$ satisfies condition (a), but clearly fails to satisfy condition (b), since condition (b) is equivalent to the same condition stated for $G_0$. For our second example we consider the rather trivial case $n = 1$. With $G_0$ the cyclic group whose elements are $((i), (-i))$, $((-1), (-1))$, $((-i), (i))$, $((1), (1))$, and $S_0 = [(1), (1)]$, $G = G_0 S_0$ is a triadic linear group in one variable satisfying condition (b). But it cannot satisfy condition (a); for it is non-abelian, while any polyadic group of ordinary matrices in one variable is readily seen to be abelian.

We conclude this section with a proof of the following generalization of the corresponding ordinary theorem. *Any abelian m-adic linear group is conjugate to a group each of whose elements is in canonical form with equal components.* We first prove this result for the case of an abelian group $G$ having an $m$-adic similarity-matrix $A$. By the proof of the theorem preceding the above digression, $G$ is conjugate to an equi-component group $\overline{G}$ in which $\overline{A}$, the correspondent of $A$, has for its components equal similarity-matrices. Now the constituent $\overline{G}_0'$ of the associated ordinary group $\overline{G}_0$ of $\overline{G}$ will be an ordi-

[100] Clearly these distinctions constitute but a first glance at a probably wide theory.

nary abelian linear group, and hence can be transformed by an ordinary matrix $\alpha'$ so that each of its elements appears in canonical form. Since $\overline{G}_0$ will consist of $(m-1)$-ads with equal components, the $(m-1)$-ad $\alpha=(\alpha', \alpha', \cdots, \alpha')$ will transform $\overline{G}_0$ into a group in which each element appears with equal components in canonical form. As $\alpha$ transforms $\overline{A}$ into itself, it will therefore transform $\overline{G}=\overline{G}_0\overline{A}$ into the conjugate of $G$ of our theorem.

Now let $G$ be an arbitrary abelian $m$-adic linear group, $A$ some fixed element thereof. By a previous result, we may assume the group to have been so transformed by an $(m-1)$-ad that $A$ appears in canonical form with equal components $A'$. The $(m-1)$-ad $A^{m-1}$ then has the equal components $A'^{m-1}$, also in canonical form. It follows from the invariance of any element $B=[B', B'', \cdots, B^{m-1}]$ of $G$ under $A^{m-1}$ that

$$A'^{m-1}B^{(i)} = B^{(i)}A'^{m-1}$$

for each $i$. If then we separate the variables of each space $\Sigma^{(i)}$ into sets $\Sigma_1^{(i)}, \Sigma_2^{(i)}, \cdots, \Sigma_l^{(i)}$ according to their distinct multipliers in $A'^{m-1}$, the proof of the corresponding ordinary theorem shows that $B^{(i)}$ transforms the variables of each $\Sigma_j^{(i)}$ into those of $\Sigma_j^{(i+1)}$. Each element $B$ of $G$ therefore transforms $\Sigma_j' \to \Sigma_j'' \to \cdots \to \Sigma_j^{(m-1)} \to \Sigma_j'$. That is, $G$ appears in intransitive form with the $l$ sets of intransitivity corresponding to $j=1, 2, \cdots, l$. Now for each set of intransitivity the corresponding partial transformations constitute any abelian $m$-adic linear group. Moreover, the corresponding partial transformation of $A$ is an $m$-adic similarity-matrix, since the corresponding partial transformation of $A'^{m-1}$ has but one distinct multiplier. Hence, by our special result, each of these constituent groups can be thrown into the desired form by transformation by an $(m-1)$-ad on the corresponding set of intransitivity. Together, these $l$ partial $(m-1)$-ads constitute an $(m-1)$-ad on $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$ which transforms $G$ into the conjugate group of our theorem.

Clearly, every $m$-adic linear group, each of whose elements is in canonical form with equal components, is abelian. On the other hand, unlike the ordinary case, an $m$-adic linear group each of whose elements is in canonical form need not be abelian. It is readily proved that the necessary and sufficient condition that such a group be abelian is that its associated ordinary group consist of elements with equal components.

39. **$m$-adic invariants.** In the theory of ordinary linear groups in $n$ variables the concept of a function of those variables precedes that of an invariant. In our theory of $m$-adic linear groups $G$ in $n$ variables it is therefore natural to replace the concept of a function by a set of $m-1$ functions, one for each of the spaces $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$. If we transform such a set of functions $[f'(x_{11}, x_{12}, \cdots, x_{1n}), f''(x_{21}, x_{22}, \cdots, x_{2n}), \cdots, f^{(m-1)}(x_{(m-1)1}, x_{(m-1)2}, \cdots, x_{(m-1)n})]$ by an $m$-adic linear transformation $T$ of $\Sigma', \Sigma'', \cdots, \Sigma^{(m-1)}$, each function $f^{(i)}(x_{i1}, x_{i2}, \cdots, x_{in})$ will become a function of $x_{(i+1)1}, x_{(i+1)2}, \cdots, x_{(i+1)n}$.

We therefore define $f=[f', f'', \cdots, f^{(m-1)}]$ to be an (absolute) *m-adic invariant* of $T$ if $T$ transforms $f'\rightarrow f''$, $f''\rightarrow f'''$, $\cdots$, $f^{(m-1)}\rightarrow f'$; of $G$, if $f$ is an $m$-adic invariant of each element of $G$. Actually, the following analysis shows this definition to be too narrow for a real generalization of the ordinary concept. But how to widen it without destroying our basic concept of $m-1$ spaces $\Sigma'$, $\Sigma''$, $\cdots$, $\Sigma^{(m-1)}$ we do not at present know.

Our chief result involves the associated constituent groups $G_0'$, $G_0''$, $\cdots$, $G_0^{(m-1)}$ of $G$ already introduced in §37 as the complete analogues of the corresponding concepts for $m$-adic substitution groups. More specifically, we saw that if $G$ is an $m$-adic linear group of $m$-adic matrices $T=[T', T'', \cdots, T^{(m-1)}]$, $G_0$, the associated ordinary group of $G$, may be concretely given by a group of $(m-1)$-ads $\tau=(\tau', \tau'', \cdots, \tau^{(m-1)})$. For each $\tau$, $\tau^{(i)}$ represents a transformation of the space $\Sigma^{(i)}$ into itself; and the set of $\tau^{(i)}$'s constitute an ordinary group, the *associated constituent group* $G_0^{(i)}$ above. It is then fundamental that, as in the case of $m$-adic substitution groups, the associated constituent groups of $G$ are conjugate, each element $T$ of $G$ in fact transforming $G_0'\rightarrow G_0''$, $G_0''\rightarrow G_0'''$, $\cdots$, $G_0^{(m-1)}\rightarrow G_0'$. To verify this fact we need only observe that $T$ transforms $G_0$ into itself; while if we follow through the operations involved in $T^{-1}\tau T$, we see that the $i$th component of the resulting $(m-1)$-ad is the transform of the $(i-1)$-st component of $\tau$ by $T^{(i-1)}$.

Now let $f=[f', f'', \cdots, f^{(m-1)}]$ be an $m$-adic invariant of $G$; that is, each element of $G$ transforms $f'\rightarrow f''$, $f''\rightarrow f'''$, $\cdots$, $f^{(m-1)}\rightarrow f'$. Each element $\tau$ of $G_0$ may be written as the product $T_1T_2\cdots T_{m-1}$ of $m-1$ elements of $G$. By following through these $m-1$ transformations we see that $\tau$ transforms $f'$ into itself. But $\tau$ can operate on $f'$ only through its first constituent $\tau'$. Hence each $\tau'$ transforms $f'$ into itself, and $f'$ is an ordinary invariant of the associated constituent group $G_0'$.

Conversely, let $f'$ be any invariant of $G_0'$, $T_0$ some element of $G$. $T_0$ will transform $f'$, a function of the variables of $\Sigma'$, into a function of the variables of $\Sigma''$. Call this function $f''$, i.e., $f''=(f')T_0$. Likewise write $f'''=(f'')T_0$, $\cdots$, $f^{(m-2)}=(f^{(m-1)})T_0$. Now $(f^{(m-1)})T_0=(f')T_0^{m-1}$. Since $f'$ is an invariant of $G_0'$, it will actually be transformed into itself by each element of $G_0$, and hence by the $(m-1)$-ad $T_0^{m-1}$. That is $(f^{(m-1)})T_0=f'$, and $f=[f', f'', \cdots, f^{(m-1)}]$ is an $m$-adic invariant of $T_0$. We now show that it is also an $m$-adic invariant of every element $T$ of $G$, that is, of $G$. Since $G_0''$ is the transform of $G_0'$ under $T_0$, it follows that if $\tau''$ is any element of $G_0''$, then for some element $\tau'$ of $G_0'$, $(f'')\tau''=(f')T_0\,T_0^{-1}\tau' T_0=(f')\tau' T_0=(f')T_0=f''$. Hence, $f''$ is an invariant of $G_0''$, and likewise $f'''$ of $G_0'''$, $\cdots$, $f^{(m-1)}$ of $G_0^{(m-1)}$. Each element $\tau=(\tau', \tau'', \cdots, \tau^{(m-1)})$ of $G_0$ will therefore transform each function $f', f'', \cdots, f^{(m-1)}$ into itself. Hence, by writing an arbitrary element $T$ of $G$ in the form $\tau T_0$, with $\tau$ in $G_0$, we see that $T$, along with $T_0$, will transform $f'\rightarrow f''$, $f''\rightarrow f'''$, $\cdots$, $f^{(m-1)}\rightarrow f'$.

We have thus proved the following theorem. *Given an m-adic linear group*

*G with first associated constituent group $G_0'$, then every m-adic invariant $f=[f', f'', \cdots, f^{(m-1)}]$ of G is such that $f'$ is an ordinary invariant of $G_0'$; and, conversely, every ordinary invariant $f'$ of $G_0'$ yields an m-adic invariant $f=[f', f'', \cdots, f^{(m-1)}]$ of G.* Clearly, this correspondence between $m$-adic invariants of $G$ and ordinary invariants of $G_0'$ is 1-1. A like correspondence of course exists between the $m$-adic invariants of $G$ and the ordinary invariants of $G_0^{(i)}$ for any $i$.

The weakness of our concept of $m$-adic invariants, already apparent from this reduction to ordinary invariants, is conclusively demonstrated by a consideration of invariants as group determiners. While the groups in question will in general be infinite, no part of the above discussion involves the hypothesis of finiteness in a linear group. Suppose then that $f=[f', f'', \cdots, f^{(m-1)}]$ is an $m$-adic invariant of at least one $m$-adic linear transformation $T_0$, and let $G$ be the set of all $m$-adic linear transformations with $f$ as $m$-adic invariant. It is then readily verified that $G$ is an $m$-adic linear group. By the proof of the above theorem, $f'$ is an invariant of $G_0'$, and, likewise, $f''$ of $G_0''$, $\cdots$, $f^{(m-1)}$ of $G_0^{(m-1)}$. If then $\tau', \tau'', \cdots, \tau^{(m-1)}$ is any selection from $G_0', G_0'', \cdots, G_0^{(m-1)}$, and $\tau=(\tau', \tau'', \cdots, \tau^{(m-1)})$, then $T=\tau T_0$ has $f$ for $m$-adic invariant. $T$ is therefore in $G$, and hence $\tau$ in $G_0$. That is, the $m$-adic linear group defined by a given $m$-adic invariant is of that special kind in which the associated ordinary group consists of all selections, written as $(m-1)$-ads, that can be made from the associated constituent groups.

When the above definition is extended to relative $m$-adic invariant, entirely corresponding results obtain. However, by a device similar to that which gave us our $m$-adic alternating groups, we can enlarge somewhat the role of relative m-adic invariant as group determiner. $f=[f', f'', \cdots, f^{(m-1)}]$ will be a relative $m$-adic invariant of an $m$-adic linear transformation $T$ if $T$ transforms $f$ so that $f' \to \kappa_1 f'', f'' \to \kappa_2 f''', \cdots, f^{(m-1)} \to \kappa_{m-1} f'$, the $\kappa$'s being constants depending on $T$. Each $T$ having $f$ as relative $m$-adic invariant thus determines a $\kappa$-sequence. Furthermore, if $T_1, T_2, \cdots, T_m$ have $f$ as relative $m$-adic invariant, so also will $T=T_1T_2 \cdots T_m$; and the $\kappa$-sequence of $T$ is determined by the $\kappa$-sequences of $T_1, T_2, \cdots, T_m$ by the same equations that connected the $\delta$-sequences of our alternating group theory. We are thus led to a complete $m$-adic $\kappa$-group; and corresponding to any subgroup thereof, the set of all $T$'s with $\kappa$-sequences in that subgroup will be an $m$-adic linear group. Furthermore, whenever the associated ordinary group of the $\kappa$-subgroup does not consist of all selections from its constituent associated subgroups, the corresponding $m$-adic linear group will also not be of this special type. However, with the $f^{(i)}$'s homogeneous polynomials in the corresponding variables, any $T$ having $f$ for relative $m$-adic invariant can be changed to a $T$ having $f$ for absolute $m$-adic invariant by multiplying it into a suitable similarity-$(m-1)$-ad; and conversely, without qualification. Hence the $T$'s corresponding to any one $\kappa$-sequence represent the same $m$-adic collineations as the

$T$'s having $f$ for absolute invariant. All the $m$-adic linear groups corresponding to the various $\kappa$-subgroups therefore have the same corresponding $m$-adic collineation-group as the $G$ defined by $f$ as absolute invariant, and our seemingly greater freedom is largely illusory.

An obvious, but probably superficial, remedy for the relative triviality of our concept of $m$-adic invariant would be to allow each of the functions $f', f'', \cdots, f^{(m-1)}$ to be functions not of the variables of the corresponding $\Sigma$ alone, but of all of the $\Sigma$'s. It may be mere prejudice that makes us object to thus uniting the $m-1$ spaces of $n$ dimensions each into one space of $(m-1)n$ dimensions; for, certainly, arbitrarily to give $m-1$ points, one for each space, is equivalent to giving one point in the combined space. One qualification does suggest itself. Corresponding to the condition of homogeneity for the polynomial invariants of ordinary theory, §36 suggests that the $f^{(i)}$'s be polynomials homogeneous in the variables of each $\Sigma$ separately. However, a finally acceptable form for a general concept of $m$-adic invariant will probably involve changes in our original idea both more specific and more drastic than here suggested.

40. **Generalization of $m$-adic substitution and transformation groups.** The concept of $m$-adic linear group is readily extended to that of an $(m, \mu)$ linear group, analogous to our earlier $(m, \mu)$ substitution group. However, both concepts admit of a far wider extension. We shall give this extension only for $m$-adic substitution groups, the generalization of $m$-adic linear group being entirely similar([101]). It is of interest to note that this generalization continues to be a generalization even when $m=2$. But the resulting ordinary groups are then essentially realizations of Specht groups, referred to in the introduction, or subgroups thereof([102]).

The concepts of an $m$-adic substitution on the letters of classes $\Gamma_1, \Gamma_2, \cdots, \Gamma_{m-1}$ is associated with the cyclic substitution $(\Gamma_1\Gamma_2 \cdots \Gamma_{m-1})$ on the classes themselves; for, under the $m$-adic substitution, $\Gamma_1 \rightarrow \Gamma_2$, $\Gamma_2 \rightarrow \Gamma_3$, $\cdots$, $\Gamma_{m-1} \rightarrow \Gamma_1$. More generally then let $\Gamma_1, \Gamma_2, \cdots, \Gamma_\nu$ be any finite set of classes, $\sigma$ any substitution on those classes themselves as elements. $s$ will then be said to be a *polyadic substitution corresponding to* $\sigma$ if, whenever $\sigma$ replaces class $\Gamma_i$ by class $\Gamma_j$, $s$ carries the members of $\Gamma_i$ in 1-1 fashion into the members of $\Gamma_j$. Clearly, if polyadic substitutions $s_1, s_2, \cdots, s_m$ on the members of $\Gamma_1, \Gamma_2, \cdots, \Gamma_\nu$ correspond to $\sigma_1, \sigma_2, \cdots, \sigma_m$ respectively, $s_1 s_2 \cdots s_m$, the result of performing these $m$ polyadic substitutions in succession, is itself a

([101]) A corresponding generalization of our narrow concept of $m$-adic invariant immediately suggests itself.

([102]) On the other hand, groups of the permutations of sets of variables considered by L. Weisner (*Generalization of Lagrange's theorem*, Bulletin of the American Mathematical Society, vol. 32 (1926), pp. 629–630) are but a very special case of the present generalization with $m=2$. We may note that the associated and containing ordinary groups of $m$-adic substitution groups, and, indeed, of the present generalization thereof, also come under this generalization with $m=2$, and thus tie up with Specht groups, or subgroups thereof.

polyadic substitution corresponding to $\sigma_1\sigma_2 \cdots \sigma_m$, the product of the $m$ corresponding ordinary substitutions. It follows from our last result on homomorphisms given in §4 that if $G$ is an $m$-group of polyadic substitutions $s$ on the members of $\Gamma_1, \Gamma_2, \cdots, \Gamma_\nu$ under the above $m$-adic operation, the corresponding ordinary substitutions $\sigma$ form an $m$-group $B$ of ordinary substitutions. Moreover, *$G$ is homomorphic to $B$.* We shall call $B$ the *basic $m$-group* corresponding to the *polyadic substitution group $G$.* In the case of our $m$-adic substitution groups, and more generally our $(m, \mu)$ groups, the basic $m$-group is of first order, its sole substitution consisting of a single cycle the number of whose letters is $m-1$ in the first case, a divisor $\mu-1$ of $m-1$ in the second.

As a consequence of the homomorphism between an arbitrary polyadic substitution group $G$ and its basic $m$-group $B$, we see that there are the same number of polyadic substitutions in $G$ for each substitution in $B$. Hence, also, the order of $G$ is always a multiple of the order of $B$. Again, the ordinary substitutions corresponding to the polyadic substitutions forming any subgroup of $G$ will form a subgroup of $B$, if not $B$ itself; while to each subgroup of $B$ there is at least one corresponding subgroup of $G$, i.e., the one consisting of all the elements of $G$ corresponding to the elements of the subgroup of $B$, and hence containing all such subgroups.

For simplicity, we now restrict ourselves to mutually exclusive classes $\Gamma_1, \Gamma_2, \cdots, \Gamma_\nu$ of the same finite number of letters $n$ each([103]). Given any substitution $\sigma$ on those classes as elements, there will then be a total of $(n!)^\nu$ polyadic substitutions corresponding to $\sigma$. If then $B$ is a given $m$-group of substitutions on those classes as elements, and $b$ is the order of $B$, the $(n!)^\nu b$ polyadic substitutions corresponding to the elements of $B$ are readily seen to constitute a polyadic substitution group with $B$ as basic group. It may be called the *$m$-adic symmetric group of degree $n$ with basic $m$-group $B$.* We can now state that any polyadic group with basic $m$-group $B$ is a subgroup of the corresponding $m$-adic symmetric group. On the other hand, a subgroup of that $m$-adic symmetric group may have but a subgroup of $B$ for basic group.

Of the theory of $m$-adic substitution groups we shall redevelop here only the general aspects of the theory leading to $m$-adic alternating groups. Again form the Vandermonde determinants $\Delta_1, \Delta_2, \cdots, \Delta_\nu$ for the letters of $\Gamma_1, \Gamma_2, \cdots, \Gamma_\nu$ respectively. If now a substitution $\sigma$ on the $\Gamma$'s as elements be written in the primitive form

$$\Gamma_1 \Gamma_2 \cdots \Gamma_\nu$$
$$\Gamma_{i_1}\Gamma_{i_2} \cdots \Gamma_{i_\nu},$$

a polyadic substitution corresponding to $\sigma$ will transform the $\Delta$'s as follows:

$$\Delta_1 \to \delta'\Delta_{i_1}, \Delta_2 \to \delta''\Delta_{i_2}, \cdots, \Delta^{(\nu)} \to \delta^{(\nu)}\Delta_{i_\nu}, \qquad \delta', \delta'', \cdots, \delta^{(\nu)} = \pm 1.$$

([103]) When $B$ is transitive, the number of letters in the several $\Gamma$'s must of necessity be the same.

To describe this transformation completely, we must therefore not only specify the $\delta$-sequence $\delta=[\delta', \delta'', \cdots, \delta^{(\nu)}]$, but the substitution $\sigma$. We therefore form the couple $\{\sigma, \delta\}$. Given then a polyadic substitution group $G$, each element thereof uniquely determines a $\{\sigma, \delta\}$ couple. Moreover, if $s_1, s_2, \cdots, s_m$ are any $m$ elements of $G$, $\{\sigma_1, \delta_1\}, \{\sigma_2, \delta_2\}, \cdots, \{\sigma_m, \delta_m\}$ the corresponding couples, then $s=s_1s_2\cdots s_m$ has a couple $\{\sigma, \delta\}$ completely determined by the couples of $s_1, s_2, \cdots, s_m$. For clearly $\sigma=\sigma_1\sigma_2\cdots\sigma_m$. On the other hand, let $\delta=[\delta', \delta'', \cdots, \delta^{\nu}]$, $\delta_i=[\delta_i', \delta_i'', \cdots, \delta_i^{(\nu)}]$. For any substitution $\sigma$ on the $\Gamma$'s as elements, if $\sigma$ carries $\Gamma_i$ into $\Gamma_{i_j}$, write $i_j=i\sigma$. Then we will have

$$\delta^{(i)} = \delta_1^{(i)}\delta_2^{(i\sigma_1)}\cdots\delta_{m-1}^{(i\sigma_1\cdots\sigma_{m-2})}\delta_m^{(i\sigma_1\cdots\sigma_{m-2}\sigma_{m-1})}.$$

It again follows from our last result on homomorphisms that the class of $\{\sigma, \delta\}$ couples corresponding to the elements of $G$ constitutes an $m$-group under the resulting $m$-adic operation on $\{\sigma, \delta\}$ couples, and hence that $G$ is homomorphic to this $m$-group. We shall call the latter the $\{\sigma, \delta\}$ *subgroup* corresponding to $G$. The homomorphism in question then again assures us that there are exactly the same number of elements of $G$ for each $\{\sigma, \delta\}$ couple in its $\{\sigma, \delta\}$ subgroup, and again yields the many-one relation between the subgroups of $G$ and those of its $\{\sigma, \delta\}$ subgroup.

Clearly the relationship between $G$ and its $\{\sigma, \delta\}$ subgroup is intimately bound up with the relationship between $G$ and its basic $m$-group $B$. In fact, the very form of a $\{\sigma, \delta\}$ couple yields a many-one correspondence between the elements of the $\{\sigma, \delta\}$ subgroup corresponding to $G$, and of $B$; while our formulation of the $m$-adic operation on $\{\sigma, \delta\}$ couples shows this correspondence to be a homomorphism—hence again the sameness of the number of $\{\sigma, \delta\}$ couples corresponding to different $\sigma$'s, and the many-one correspondence between the subgroups of the $\{\sigma, \delta\}$ subgroup, and of the basic $m$-group $B$, corresponding to $G$. Much can now be said of the interrelations between $G$, its $\{\sigma, \delta\}$ subgroup, and its basic $m$-group $B$. But they are all implicit in the fact that the above homomorphism between $G$ and $B$ is the one determined by the homomorphism between $G$ and its $\{\sigma, \delta\}$ subgroup, and the homomorphism between that $\{\sigma, \delta\}$ subgroup and $B$.

When $G$ is the polyadic symmetric group of degree $n$ corresponding to a given basic $m$-group $B$, then, as in the case of $m$-adic substitutions, $G$ will have at least one polyadic substitution for each of the $2^{\nu}$ possible $\delta$-sequences, and each substitution $\sigma$ in $B$, provided $n>1$. The "$\{\sigma, \delta\}$ subgroup" may now be called the *complete* $\{\sigma, \delta\}$ *group* corresponding to $B$. With $B$ of order $b$, the corresponding complete $\{\sigma, \delta\}$ group is then of order $2^{\nu}b$. We thus have a division of the corresponding $(n!)^{\nu}b$ polyadic substitutions into $2^{\nu}b$ mutually exclusive classes of consequently $(n!/2)^{\nu}$ members each.

Now in the many-one relations between the subgroups of the polyadic symmetric group of degree $n$, the complete $\{\sigma, \delta\}$ group, and the basic

$m$-group $B$ consider only those (proper) subgroups of the complete $\{\sigma, \delta\}$ group which correspond to $B$ itself. For each of these $\{\sigma, \delta\}$ subgroups there is a unique largest subgroup of the polyadic symmetric group. These may then be called the *polyadic alternating groups* of degree $n$ with basic $m$-group $B$. The corresponding $\{\sigma, \delta\}$ subgroups are of orders $2^{\nu_1}b$, $0 \leqq \nu_1 < \nu$, and the polyadic alternating groups correspondingly of orders $(n!/2)^{\nu}2^{\nu_1}b$, each consisting of all the elements in each of $2^{\nu_1}b$ of the above mutually exclusive classes. Note that if $B$ is considered as a substitution group on the symbols $\Gamma_1, \Gamma_2, \cdots, \Gamma_\nu$ rather than on the classes they symbolize, then one and the same $B$ will serve for arbitrary $n$. Hence also the complete $\{\sigma, \delta\}$ group will be independent of $n$; and for each $n > 1$ there will be as many polyadic alternating groups of degree $n$ and basic $m$-group $B$ as the complete $\{\sigma, \delta\}$ group has subgroups also corresponding to $B$.

By considering an arbitrary polyadic group $G$ of degree $n$, and with basic $m$-group $B$, a subgroup of the corresponding polyadic symmetric group, we see that the $\{\sigma, \delta\}$ subgroup for $G$ is actually a subgroup, proper or improper, of the complete $\{\sigma, \delta\}$ group corresponding to $B$. But that subgroup also must correspond to $B$. That is, we have a many-one relation between all polyadic groups of degree $n$ with basic $m$-group $B$, and those subgroups of the complete $\{\sigma, \delta\}$ group which themselves correspond to $B$.

COLLEGE OF THE CITY OF NEW YORK,
NEW YORK, N.Y.