ON PRIMITIVE AND IMPRIMITIVE GROUPS

THESIS

Submitted in Partial

Fulfilment of the Requirements for the

Award of the M. Sc. Degree

By

ESAM EL-DEEN MOSTAFA KAMAL ABDEL-LATEEF

Submitted at

Ain Shams University
Faculty of Science

December 1982

C1

M. Sc. COURSES

STUDIED BY THE AUTHOR (1980 - 1981)

AT AIN SHAMS UNIVERSITY

FACULTY OF SCIENCE

1. Abstract Algebra .
2. Algebriac Topology.
3. Functional Analysis.
4. Numerical Analysis.
5. Spectral Theory.

Rg
20/12/1982

بسم الله الرحمن الرحيم

ACKNOWLEDGEMENT

******

I wish to express my deepest gratitude to Prof. Emeritus Dr. Ragy H. Makar, Faculty of Science, Ain Shams University, for his constant encouragement and kind help.

I would like to acknowledge my deepest gratitude and thankfulness to Dr. Abdel-Raouf Omar, Mathematics Department, Faculty of Science, Minia University, for suggesting the topic of the thesis, for his kind supervision and for his invaluable help during the preparation of the thesis.

6

CONTENTS

****

PREFACE

The thesis consists of four chapters:

Chapter (I) is concerned with the fundamental theorems and definitions for the action of a group on a set, transitive, intransitive, primitive, and imprimitive groups.

Chapter (II) is devoted to studying the Mathieu groups, their maximal, and Sylow subgroups.

Chapter (III) deals with the Higman-Sims group, its combinatorial configuration, and the maximal subgroups.

Lastly, in Chapter (IV) we search among all the above subgroups wether they are superimprimitive or not. The final conclusion is that none of the maximal or Sylow subgroups of the Mathieu groups, and the maximal subgroups of the Higman-Sims group are superimprimitive. Yet, there is an example of a superimprimitive subgroup, of M_{12} which is neither a maximal or Sylow subgroup.

CHAPTER (I)

******

GROUP ACTIONS ON SETS

In this chapter, we are concerned with the group which acts transitivity or intransitivity on a finite set. Also for the transitive group, we define the primitive and the imprimitive.

§ (1.1) The action of a group G on a set X : [21]

(1.1.1) Definition:

We say that G acts on X (or that G permutes X) if each $g \in G$ and $x \in X$ there corresponds a unique element $x^g \in X$ such that, for all $x \in X$ and $g_1, g_2 \in G$,

$$x^{(g_1 g_2)} = (x^{g_1})^{g_2}$$

and

$$x^e = x.$$

As an example, if G is a subgroup of the symmetric group on X , $G \leq \$^X$, then we say G acts on X.

(1.1.2) Theorem:

Let G act on X . Then to each $g \in G$ there corresponds a map $\rho_g : X \to X$ defined by $\rho_g : x \to x^g$, and this is a permutation of X. Moreover, the map $\rho : G \to \$^X$ defined by $\rho : g \to \rho_g$ is a homomorphism; it is called the permutation representation of G corresponding to the group action.

(1.1.3) Theorem:

Let σ be a homomorphism of G into $\$^X$. Then G acts on X when we define, for each $g \in G$ and $x \in X$,

$$x^g = (\sigma_g)\, x \quad ;$$

and the permutation representation of G corresponding to this action is σ .

Proof:

For $g_1, g_2 \in G$ and $x \in X$, by definition of composition of maps ,

$$(\sigma g_2)((\sigma g_1)x) = ((\sigma g_2)(\sigma g_1))x$$

$$= (\sigma(g_2 g_1))x ,$$

and $(\sigma e)\, x = x$ since σ must map $e \in G$ to $e' \in \$^X$.

Hence, by setting

$$x^g = (\sigma g)\, x ,$$

we do define an action of G on X . Let the corresponding permutation representation of G be ρ. Then

$$\rho_g\, x = x^g = (\sigma g)\, x \quad ,$$

hence $\rho_g = \sigma g$ for all $g \in G$,

and so $\rho = \sigma$.

Thus in considering group action on a set X , we now look not merely at subgroups of $\$^X$ but at a homomorphism of groups into $\$^X$.

(1.1.4) Lemma:

Let G act on X . We define a relation $\sim$ on X by setting $x_1 \sim x_2$ if and only if $x_1, x_2 \in X$ and there is an element $g \in G$ such that $x_1^g = x_2$. Then $\sim$ is an equivalence relation on X.

The following definition is of fundamental importance.

(1.1.5) Definition:

Let G act on X . Then X is partitioned into disjoint equivalence classes with respect to the equivalence relation $\sim$ of the above Lemma. These equivalence classes are called the orbits of X. For each $x \in X$, the orbit containing x is called the orbit of x : it is the subset $\{x^g : g \in G\}$ of X .

Neumann [18] introduced an algorithm to compute the orbits. Let G act on X. We begin with any element x , of X and apply to it the members $e, g_1, g_2, \ldots$ of G , each in turn untill one has reason to know that no new elements of X result. Then $X_1 = \{x_1, x_1^{g_1}, x_1^{g_2}, \ldots\}$ is an orbit of G. If $X_1 = X$ the process is finished ; other wise we choose x_2 from $X \setminus X_1$ and we list the set $\{x_2, x_2^{g_1}, x_2^{g_2}, \ldots\}$, which will be our second orbit X_2. When X is exhausted the process is complete. In practice, the details of such a calculation must depend on the description of G and of X. There are general purpose programmes for doing it on computers. Most of these assume that G is a group of permutations of X and that generators of it are given. That is, the data consist of certain permutations $g_1, \ldots, g_k$ which generate G in the sence that every element can be obtained as some product $g_{i_1}^{\pm 1} \; g_{i_2}^{\pm 1} \cdots g_{i_m}^{\pm 1}$ of them and their inverses.

(1.1.6) Definition:

Let G act on X, and let $x \in X$. The stabilizer of x in G is the set $\{g \in G : x^g = x\}$.

It is a subgroup of G and is usually abbreviated to G_x.

(1.1.7) Lemma :

Let G act on X, and let $x \in X$. Then

$$|\{\text{the orbit of } x\}| = |G : G_x| .$$

Proof:

We have $x^{g_1} = x^{g_2}$ if and only if $g_1^{-1} g_2 \in G_x$, i.e., $g_2 \in g_1 G_x$. Therefore there are precisely as many points x^{g_1} as there are distinct left cosets $g_1 G_x$. However, this number is $|G : G_x|$.

§ (1.2) Transitivity:

(1.2.1) Definition: [21]

Let G act on X. This action is said to be transitive on X if it has just one orbit. An action which is not transitive is called intransitive.

A transitive group G acting on $X = \{x_1, \ldots, x_n\}$, has elements $g_1, \ldots, g_n$ which replace x_1 by $x_1, x_2, \ldots, x_n$, respectively. Then $g_j g_i^{-1}$ replaces x_i by x_j, so that any symbol in X can be replaced by another by a suitable element in G, [4] .

G is a doubly transitive group if there exists an element in G which replaces any ordered pair of symbols in X by any other ordered pair of symbols in X, [4] .

In general G is said to be <u>k-fold transitive</u>, where k is an integer ≥ 1, if, given any two ordered k-tuples $(x_1,\ldots,x_k)$; $(y_1,\ldots,y_k)$ of distinct symbols of X there is some $g \in G$ such that

$$x_i^g = y_i \quad , \ i = 1,\ldots, k.$$

(1.2.2) <u>Definition</u>: [2]

The rank of the transitive group G on X is the number of orbits of G_x on X.

(1.2.3) <u>Theorem</u>: [4]

The totality of elements of a given k-fold transitive group G each of which leaves fixed a given ordered set of k symbols of X forms a subgroup.

If $G_{[\Delta]}$ denote the elements of the group G that leave each point of the subset Δ of $X, \Delta \subseteq X$, fixed then $G_{[\Delta]}$ is a subgroup.

(1.2.4) <u>Theorem</u>: [24]

Let G be transitive on X and $x \in X$. Then G is $(k+1)$-fold transitive on X if and only if G_x is k-fold transitive on $X \setminus \{x\}$. If G is k-fold transitive on X and $\Delta \subseteq X$ with $|\Delta| = d < k$, then $G_{[\Delta]}$ is $(k-d)$-fold transitive on $X \setminus \Delta$.

Biggs [2] suggested that to determine if a group is highly transitive we examine the successive stabilizers, G_x, $(G_x)_y$, ..., etc.

(1.2.5) Theorem : [2]

If G is k-fold transitive, then $|G|$ is divisible by $n(n-1) \ldots (n-k+1)$ where $n = |X|$.

Proof:

$$|G| = n\,|G_x|$$
$$= n(n-1)\,|(G_{x_1})_{x_2}| = \ldots$$
$$= n(n-1)\ldots(n-k+1)\,|G_{x_1 x_2 \ldots x_k}| .$$

If $|G| = n = |X|$ we say that G is regular on X.

Also we have the following theorem:

(1.2.6) Theorem: [5]

Let G be a k-fold transitive on X, and let $\Delta \subseteq X$, $|\Delta| = k$. Let the subgroup $U \leq G_{[\Delta]}$ be conjugate in $G_{[\Delta]}$ to every group V which lies in $G_{[\Delta]}$ and which is conjugate to U in G. Then the normalizer of U in G , $N_G(U)$, is k-fold transitive on the set of symbols, left fixed by U .

(1.2.7) Theorem: [8]

Let G be a k-fold transitive permutation group of degree n. Let Q be a subgroup of G which fixes the symbols, $1,2,\ldots,k$. Let L be a subgroup of Q with the following property:

If a subgroup M of Q is conjugate to L in G, then it is conjugate to L in Q. (i.e. if there is an $x \in G$ such that $x^{-1}Lx < Q$ then there is an element $q \in Q$ such that $q^{-1}Lq = x^{-1}Lx$).

Then the normalizer of L, $N(L)$ is k-fold transitive on the set of m symbols that are fixed by the subgroup L.

(1.2.8). Lemma: [2]

(i) The symmetric group of degree n , $\$_n$, is n-transitive.

(ii) The alternating group of degree n , A_n, is (n-2)-transitive.

The first part is obvious. In the alternating case, when n =3 , $A_3 = \{e, (123), (132)\}$, which is 1-transitive, so we can formulate a proof by recursion, using the remark of Biggs after Theorem (1.2.4) and the fact that the stabilizer $(A_n)_n$ is A_{n-1}.

§(1.3) Primitivity: [24]

(1.3.1) Definition:

Let G act transively on X . We call a subset B of X a block of G if for each g ε G the image set $B^g = \{b^g : b \in B\}$ either coincides with B or has no point in common with B.

Obviously, the whole set X , the empty set Φ, and the sets {x} consisting of only one symbol, are blocks. We call these trivial blocks.

We say that $B \subseteq X$ is a fixed block of G if $B^G = B$. (We denote by B^G the set of all b^g with b ε B and g ε G). If U ≤ G , then every block of G is also a block of U .

(1.3.2) Lemma:

If B_1 and B_2 are blocks of G , then their intersection $B_1 \cap B_2$ is also a block of G.

For if $\Delta = B_1 \cap B_2$ has a nonempty intersection with

Δ^g for some $g \in G$, then so B_1 with B_1^g and B_2 with B_2^g. Therefore the fact that B_1 and B_2 are blocks implies that

$$\Delta^g = B_1^g \cap B_2^g = B_1 \cap B_2 = \Delta .$$

Hence Δ is also a block.

(1.3.3) <u>Theorem</u>:

If $g \in G$, $U \leq G$, and B is a block of U, then B^g is a block of $g^{-1} U g$.

<u>Proof</u>:

Let $u \in U$. If $B^{g\, u\, g^{-1}.g} \cap B^g \neq \phi$, it follows by application of g^{-1} that $B^u \cap B \neq \phi$, hence since B is a block of U, $B^u = B$. Application of g now shows that $B^{gug^{-1}.g} = B$.

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

(1.3.4) <u>Lemma</u>:

The length of a block of a transitive group G divides the degree of G (order of X).

(1.3.5) <u>Definition</u>:

A transitive group is called <u>imprimitive</u> if there is at least one nontrivial block B. (i.e. $B \neq \phi$, $\{x\}$, X).

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

(1.3.6) <u>Theorem</u>:

If $\Delta \subseteq X$ and $x \in X$, then $B = \bigcap_{x \in \Delta^g} \Delta^g$ is a block of the transitive group G.

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

(1.3.7) <u>Theorem</u>:

Let $x \in X$. The transitive group G on X is imprimitive if and only if there is a group Z which lies properly between G_x and G, i.e., for which $G_x < Z < G$ holds.

<u>Proof</u>:

(i) Let G be imprimitive and B nontrivial block of G. Let Z be the set of those $z \in G$ for which $B=B^z$. Z is clearly a proper subgroup of G because $B \subset X$ and G is transitive. Let $x \in B$. Because B is a block it follows from $x^g = x$ that $B^g=B$. Therefore $G_x \leq Z$. Because $|B| > 1$ there is an $x_1 \neq x$ in B and because of the transitivity of G an $h \in G$ with $x^h = x_1$. We conclude that $h \in Z$, but $h \notin G_x$, hence $G_x < Z$.

(ii) Let Z be given with $G_x < Z < G$. We put $B = x^Z$. First we show that B is a block. Let $b \in B \cap B^g$ with $g \in G$. then $b= x^z = x^{z'g}$ (with $z, z' \in Z$). Therefore $z'gz \in G_x < Z$, i.e., $g \in Z$. Thus $B^g = B$ and B is a block. Because $G_x < Z$, B does not consist of x alone. We have