UNIVERSAL
LIBRARY
OU_148388
UNIVERSAL
LIBRARY

OSMANIA UNIVERSITY LIBRARY

Call No. 512.84/M647 Accession No. 20217

Author Miller and others.

Title Theory and ..... Groups. 1938

This book should be returned on or before the date last marked below.

THEORY AND APPLICATIONS

OF

FINITE GROUPS

BY

G. A. MILLER

PROFESSOR OF MATHEMATICS IN THE UNIVERSITY OF ILLINOIS

H. F. BLICHFELDT

PROFESSOR OF MATHEMATICS IN STANFORD UNIVERSITY

L. E. DICKSON

PROFESSOR OF MATHEMATICS IN THE UNIVERSITY OF CHICAGO

Reprint of 1916 Edition
with corrections.

NEW YORK
G. E. STECHERT & CO.
1938

To

Camille Jordan,

WHOSE FUNDAMENTAL INVESTIGATIONS
ON THE THEORY AND APPLICATIONS OF FINITE GROUPS
ENRICHED THE SUBJECT TO THE EXTENT OF CONVERTING IT
INTO A FUNDAMENTAL BRANCH OF MATHEMATICS
AND FURNISHED IN A LARGE MEASURE THE
INSPIRATION FOR THE SUBSEQUENT
GREAT ACTIVITY IN THIS FIELD,
THIS BOOK IS DEDICATED
(BY PERMISSION)

PREFACE

THE aim of this book is to present in a unified manner the more fundamental aspects of finite groups and their applications, and at the same time to preserve the advantage which arises when each branch of an extensive subject is written by one who has long specialized in that branch.

To secure unification, the three authors planned the book after various conferences and extensive correspondence, while each read and commented upon both the MS. and proof-sheets of the parts by the remaining authors. However, the influence of each author upon the other two has been mainly of editorial character, so that the individuality of the authorship of each part remains intact.

Part I, written by G. A. Miller, gives in the first two chapters various concrete examples of groups and an elementary presentation of the most fundamental theorems on groups of substitutions. These two chapters prepare the way, by easy stages, for the formal developments in the theory of abstract groups, to which the remaining six chapters of Part I are devoted.

A reader who wishes to proceed as early as possible to the phases of group theory presented in Part II or Part III will find that the prerequisites for either of the latter parts are met by these first two chapters of Part I, with the exception that also § 22, § 27, § 48 are needed for the last half of Part II, while § 68 is needed for Part III.

Chapter III is devoted to a development of fundamental theorems of abstract group theory and to the establishment of a logical connection between this theory and the theory of substitution groups. A (1,1) correspondence between the abstract

groups of finite order and the non-conjugate regular substitution groups is established in § 27, where it is proved that every such abstract group can be represented as a regular substitution group and that any two simply isomorphic regular substitution groups must be conjugate. This (1, 1) correspondence is used frequently in the further development of the theory of abstract groups for the sake of furnishing concrete illustrations. The section in which it is established closes with a very simple recent proof of Sylow's theorem, and in § 29 the interesting ϕ-subgroups are considered for the first time in a textbook.

The two most important categories of special abstract groups are doubtless the Abelian groups and the prime-power groups, and these two categories are treated in Chapters IV and V respectively. In the development of a theory of Abelian groups special emphasis has been placed on a determination of all their possible invariants, since these invariants seemed to offer the easiest means for studying various important questions in this theory. The Abelian groups which are groups of isomorphisms of cyclic groups receive especial attention in view of their applications in number theory. Chapter V contains a considerable number of recent theorems. One of the most interesting of these is proved in § 50 and establishes the fact that every possible set of independent generators of any given prime-power group involves the same number of operators.

Chapters VI and VII are more largely devoted to the developments due to the author than any other chapters of Part I. In the former of these two chapters various simple relations between two operators are considered and the categories of groups which can be generated by two operators which satisfy these relations are determined, while the latter chapter is devoted to a study of groups of isomorphisms. The closing Chapter VIII of Part I deals with solvable groups and aims to be especially useful to those who seek a wide knowledge of the Galois theory of algebraic equations treated in Part III.

Some of the exercises of Part I are due to questions asked by students and are intended to remove similar difficulties for the reader. In fact, this Part is based largely on a course of

lectures given by its author at various times and the lecture notes were frequently changed so as to obviate difficulties which presented themselves to the students. Special thanks are due to Dr. E. A. Kircher for assisting the author in preparing these notes for publication, and to Professor W. A. Manning and Dr. Josephine E. Burns for valuable suggestions on the printer's proofs.

Part II, written by H. F. Blichfeldt, seeks to give a more comprehensive outline of the theory of linear groups as developed up to the present moment than is contained in the published texts dealing with this phase of group-theory. At the same time an attempt has been made to present this theory in as simple a manner as possible, consistent with brevity. Thus, in several places it has been deemed sufficient to indicate the method of proof of a general proposition by attending to a concrete case.

From the outset the student is urged to work with the matrix form of a linear transformation (§ 76). The practice thus gained is of great advantage throughout Part II; in particular, the more difficult sections of Chapter XIII will be mastered readily if the student has a clear mental image of the matrix form of the regular groups as depicted in § 136 (M').

The introductory chapter (IX) and the chapter on binary groups (X) presuppose only the rudiments of ordinary group theory as given in §§ 1–4, 6–9, 22, in addition to a few definitions. By the aid of the Hermitian invariant (§ 92), the the determination of the binary groups is here made to depend upon geometrical analysis, entirely with reference to Euclidean space.

The following two chapters (XI, XII), exclusive of §§ 116, 125, are based on articles published by the author, mainly in the *Transactions of the American Mathematical Society*, 1903–1911. Certain proofs have been recast and new theorems added. For the intelligent reading of these chapters and the next following, the principles of §§ 1–22, 27, 48 should be well understood.

The somewhat difficult theory of group-characteristics (Ch. XIII) has been developed along fairly easy lines, differing not only in arrangement, but also in methods of proof, from pre-

TABLE OF CONTENTS

PART I

SUBSTITUTION AND ABSTRACT GROUPS

CHAPTER I

EXAMPLES OF GROUPS AND FUNDAMENTAL DEFINITIONS

SECTION		PAGE
1.	The symmetric group of order six	1
2.	The octic group	4
3.	Generating substitutions of a group	7
4.	The group of movements of plane figures	9
5.	Congruence groups	10
6.	Groups represented by matrices	13
	Exercises	15

CHAPTER II

SUBSTITUTION GROUPS AND SYLOW'S THEOREM

7.	Positive and negative substitutions	16
8.	Commutative substitutions	18
9.	Transforms of a substitution and of a substitution group	20
	Exercises	23
10.	Co-sets and double co-sets	24
11.	Sylow's theorem	27
	Exercises	30
12.	Transitive groups and average number of letters in its substitutions	30
13.	Intransitive substitution groups	32
14.	Substitutions which are commutative with each of the substitutions of a transitive group	35
	Exercises	38
15.	Primitive and imprimitive groups	38
	Exercises	41
16.	Groups involving no more than four letters	41
17.	Simplicity of the alternating group of degree n, $n \neq 4$	43

SECTION PAGE
18. Groups of degree five 45
19. Holomorph of a regular group 46
Exercises 47
20. Class of a substitution group 47
Exercises 50

CHAPTER III

Fundamental Definitions and Theorems of Abstract Groups

21. Introduction 51
22. Definition of an abstract group and a few properties of its elements 52
23. The cyclic group 54
Exercises 57
24. Properties of transforms 57
25. Construction of groups with invariant subgroups 59
26. The dihedral and the dicyclic groups 61
27. Representation of a group as a regular substitution group 63
Cayley's theorem 64
Exercises 65
28. Invariant subgroups and quotient groups 66
29. Commutators, commutator subgroups and the ϕ-sub-groups 68
Exercises 73
30. Simply isomorphic groups 73
Exercises 76
31. Group of inner isomorphisms 76
32. Frobenius's theorem 77
Exercises 81
33. Representation of an abstract group as a transitive substitution group 81
Exercises 84
34. Historical note 84

CHAPTER IV

Abelian Groups

35. Invariants 87
36. Largest and smallest number of possible invariants 90
37. Number of elements of a given order 93
Exercises 94
38. Abelian groups of given orders 94
39. A special class of Abelian groups 95
Exercises 98
40. Sub-groups and quotient groups of any Abelian group 99
Exercises 101
41. Group of isomorphisms of an Abelian group 101
42. Groups of isomorphisms of the groups of order p^2 105
43. Abelian groups which are conformal with non-Abelian groups 107
Exercises 109

SECTION PAGE
44. Characteristic sub-groups of an Abelian group ... 109
Exercises ... 112
45. Non-Abelian groups in which every sub-group is Abelian ... 112
Exercises ... 114
46. Roots of the operators of an Abelian group ... 114
47. Hamilton groups ... 115
Exercises ... 117

CHAPTER V

Groups Whose Orders are Powers of Prime Numbers

48. Introduction ... 118
49. Invariant Abelian sub-groups ... 120
Exercises ... 122
50. Number of sub-groups in a group of order p^m ... 123
Exercises ... 127
51. Number of non-cyclic subgroups in a group of order p^m, $p>2$ ... 128
52. Number of non-cyclic subgroups in a group of order 2^m ... 129
Exercises ... 133
53. Some properties of the group of isomorphisms of a group of order p^m ... 134
Exercises ... 137
54. Maximum order of a Sylow subgroup in the group of isomorphisms of a group of order p^m ... 137
55. Construction of all the possible groups of order p^m ... 138
Exercises ... 141

CHAPTER VI

Groups Having Simple Abstract Definitions

56. Groups generated by two operators having a common square ... 143
Exercises ... 147
57. Groups of the regular polyhedrons ... 147
58. Group of the regular icosahedron ... 150
Exercises ... 151
59. Generalizations of the group of the regular tetrahedron ... 152
60. Generalizations of the octahedron group ... 154
Exercises ... 158

CHAPTER VII

Isomorphisms

61. Relative and intrinsic properties of the operators of a group ... 159
62. Group of isomorphisms as a substitution group ... 160
63. Groups of isomorphisms of non-Abelian groups ... 162
Exercises ... 164
64. Doubly transitive substitution groups of isomorphisms ... 164

SECTION PAGE
65. Groups of isomorphisms of the alternating and the symmetric groups.... 166
Exercises.... 168
66. Several useful theorems relating to groups of isomorphisms.... 168
67. Group of isomorphisms of a transitive substitution group.... 172
Exercises.... 173

CHAPTER VIII

Solvable Groups

68. Introduction.... 174
Exercises.... 177
69. Series of composition.... 17
70. Groups involving no more than one non-cyclic Sylow subgroup.... 181
71. Groups whose nth group of inner isomorphisms is the identity.... 183
Exercises.... 184
72. Arbitrary choice of factors of composition.... 184
73. Groups of order $p^\alpha q^\beta$, p and q being prime numbers.... 185
74. Insolvable groups of low composite orders.... 186
Exercises.... 192

PART II

FINITE GROUPS OF LINEAR HOMOGENEOUS TRANSFORMATIONS

CHAPTER IX

Preliminary Theorems

75–82. Linear transformations; product of linear transformations.... 193
83–7. Groups of linear transformations.... 197
88. Change of variables.... 203
89. Characteristic equation.... 205
90. Transitive and intransitive groups.... 206
91–3. Hermitian invariant; conjugate-imaginary groups; unitary form.... 207
94. Reducible and irreducible groups.... 210
95–6. Canonical form of a linear transformation and of abelian groups.... 212

CHAPTER X

The Linear Groups in Two Variables

97–100. Introduction; geometrical analysis.... 215
101–3. The groups of the regular polyhedra.... 220
104–5. Invariants of the linear groups in two variables.... 224

CHAPTER XI

Some Special Types of Groups

SECTION PAGE
106–7. Primitive and imprimitive groups 228
108–9. Sylow groups 230
110. On the group of similarity-transformations 233

CHAPTER XII

The Linear Groups in Three Variables

111. Introduction 235
112–3. Intransitive and imprimitive groups 236
114–5. Groups having invariant intransitive or imprimitive subgroups 237
116. On roots of unity 239
117–23. Primitive simple groups 241
124. Primitive groups having invariant primitive subgroups 251
125. Invariants of the linear groups in three variables 253
126. Order of a primitive group in n variables; historical note 255

CHAPTER XIII

Group Characteristics

127. Introduction 257
128–30. Number of invariants; conditions for transitivity 258
131–2. Equivalence 262
133–5. The sum of matrices; the product of characteristics 265
136. Number of independent elements in the group-matrix 268
137. Number of non-equivalent isomorphic groups 271
138. Groups of order $p^a q^b$ are composite 272
139. Substitution groups of degree n and class $n-1$ are composite 274

PART III

APPLICATIONS OF FINITE GROUPS

CHAPTER XIV

The Group of an Algebraic Equation for a Given Domain

140–1. Introduction, number domains 279
Exercises 280
142–4. Reducible and irreducible functions 280
Exercises 282

SECTION PAGE
145. Functions with $n!$ values 282
146–7. Galoisian resolvents 283
148. The group G of an equation for a domain 286
149. Characteristic properties of this group G 287
150. Transitive group 289
Exercises 291
151. Definitions of the roots for variable coefficients 292
152. Function domains, equality 293
153. Group of the general equation 294
Exercises 295
154. Rational functions belonging to a group 296
155. Galois' generalization of Lagrange's theorem 298
156. Effect on the group by an adjunction to the domain 299
Exercises 300

CHAPTER XV

Sufficient Condition that an Algebraic Equation be Solvable by Radicals

157. Solvability by radicals 301
158. Solution of a cubic equation 302
159. Resolvent equations and their groups 303
Exercises 305
160. Equations with a regular cyclic group 306
161–3. Cyclotomic equations, Gauss' lemma 308
164. Sufficient condition for solvability by radicals 310
165. Solution of a quartic equation 312
Exercises 314

CHAPTER XVI

Necessary Condition that an Algebraic Equation be solvable by Radicals

166. Galois' criterion for solvability 315
167 Theorems of Galois, Jordan, Hölder 317

CHAPTER XVII

Constructions with Ruler and Compasses

168. Some celebrated problems of Greek origin 321
169. Analytic criterion for constructibility 321
170. Trisection of an angle 323
171. Duplication of a cube 323
172. Regular polygons 323

CHAPTER XVIII

The Inflexion Points of a Plane Cubic Curve

SECTION PAGE
173. Homogeneous coördinates, Euler's theorem, singular points 327
174. Hessian curve 329
175. Inflexion points, inflexion triangles 330
176–8. Group of the equation for the inflexion points 333
179. Real points of inflexion 341

CHAPTER XIX

The 27 Straight Lines on a General Cubic Surface and the 28 Bitangents to a General Quartic Curve

180. Existence of the 27 lines on a cubic surface 343
181. Double-six configuration 345
182. The 45 triangles on a cubic surface 346
183. Group of the equation for the 27 lines 347
184. Relation between cubic surfaces and quartic curves 351
Exercises 353
185. Steiner sets of bitangents to a quartic curve 354
186. Notation of Hesse and Cayley for the bitangents 357
187. Group containing the group for the 28 bitangents 362
188. Number of real bitangents to a quartic curve 365
189. Number of real lines on a cubic surface 366
190. Actual determination of the group for the bitangents 367
191. Symmetrical notation for the bitangents 372
192. Further problems of contacts of curves 375

CHAPTER XX

Monodromie Group

193. Monodromie group M of $F(z, k)=0$ 378
194. M an invariant subgroup of the Galois group of F 378
195. Applications of monodromie, differential equations 379
196. Quintic equations, form problem 381

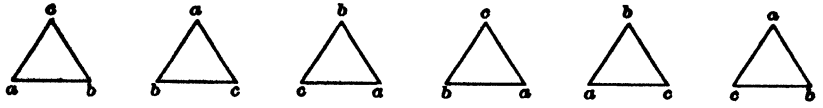
PART I*

SUBSTITUTION AND ABSTRACT GROUPS

CHAPTER I

EXAMPLES OF GROUPS AND FUNDAMENTAL DEFINITIONS

1. The Symmetric Group of Order Six. There are six movements of a plane which transform into itself a given equilateral triangle situated in this plane. These are the rotations about the center of the triangle through angles 0°, 120°, 240°, and the rotations through 180° of the plane about an altitude of the triangle. If we represent the vertices of this triangle by the letters a, b, c, the results of these six movements, which include the identity, are represented by the following figures:



FIGS. 1–6.

All of these figures may be obtained from any one of them by interchanging the letters in every possible manner. Such interchanges of letters are called *substitutions* on these letters.

Various symbols have been employed to represent substitutions. According to one of the oldest and most elementary types of symbols, the given six substitutions are represented as follows:

$$\begin{pmatrix} abc \\ abc \end{pmatrix}, \quad \begin{pmatrix} abc \\ bca \end{pmatrix}, \quad \begin{pmatrix} abc \\ cab \end{pmatrix}, \quad \begin{pmatrix} abc \\ bac \end{pmatrix}, \quad \begin{pmatrix} abc \\ acb \end{pmatrix}, \quad \begin{pmatrix} abc \\ cba \end{pmatrix}.$$

*This part was written by G. A. Miller.

This notation implies that each letter is to be replaced by the one just below it in the same symbol. The same substitutions, in order, are commonly represented by the following briefer symbols: *

$$\| \; 1, \; abc, \; acb, \; ab, \; bc, \; ac.$$

This notation implies that each letter is to be replaced by the one which follows it in the same symbol, the last being replaced by the first. Letters which are not replaced are omitted in this notation, and the symbol for unity is used to represent the *identity;* that is, the substitution in which every letter is replaced by itself.

It is easy to verify the fact that any two of these substitutions, when performed successively, are equivalent to a single one of them. For instance, if we first apply ab and then ac the result is the same as if we had applied abc only once. The process of combining (composing) two substitutions into one is called *multiplication*, and it is denoted by the common symbols for multiplication. Hence abc is said to be the *product* of ab and ac. Since $ac \cdot ab = acb$, and $ab \cdot ac = abc$, it results that the commutative law of multiplication is not always satisfied as regards the multiplication of substitutions.

A set of distinct substitutions, which has the property that no additional substitution can be obtained by multiplying successively each substitution of the set into all the substitutions of the set, is called a *substitution group.*† Hence the given set of six substitutions constitutes a substitution group. The number of the distinct substitutions of a group is called the *order* of the group and the number of the distinct letters in its substitutions is the *degree* of the group. The totality of the possible $n!$ substitutions on n letters evidently constitutes a

* These symbols have been called the *normal forms of substitutions*, J. de Séguier, *Groupes de Substitutions*. 1912, p. 3. They are often inclosed in parentheses.

† The term group in this technical sense is due to E. Galois (1811–32). The statement that the term group was not used before 1870 with its present technical meaning, which is found in the *Encyclopædia Britannica*, eleventh edition, vol. 12, p. 626, is incorrect.

substitution group, and this is known as the *symmetric group of degree n.*

The symmetric group of degree n exists for every value of n, $n>1$, and it includes every possible group on these letters. There may, however, be other groups on n letters. In fact, it is easy to verify that the three substitutions

$$1,\ abc,\ acb$$

constitute a second group on the three given letters. Hence we have found two substitution groups on three letters, and it can be verified that no other groups involving these three letters are possible. That is, if a set of substitutions involving the three letters a, b, c constitutes a group, this group is of order 3 or of order 6, and there is only one such group of each of these orders if we regard two substitution groups identical when they differ only as regards the letters involved. This group of order 3 could have been found by trial combinations of the six possible substitutions on three letters, but it results also directly from the fact that it corresponds to the rotations of the given triangle about its center through the angles 0°, 120° and 240°.

As this group of order 3 is contained in the symmetric group of order 6 it is called a *subgroup* or a divisor of the latter. The identity is a subgroup of every group. The only other subgroups of this symmetric group are of order 2. There are three such subgroups, viz.,

$$1,\ ab;\quad 1,\ ac;\quad 1,\ bc.$$

Hence *the symmetric group of order* 6 *has four subgroups besides the identity.* The last three of these correspond to the groups of movements through the angle π around the lines of symmetry of the given triangle.

The symmetric group of order 6 could also have been found by considering the possible permutations of three variables which do not alter a symmetric function of these variables. A simple instance of such a function is the following:

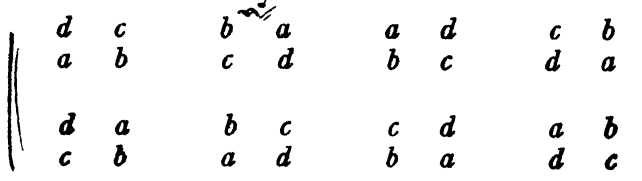
$$x+y+z.$$

The given group of order 3 may be obtained from a consideration of the permutations which leave formally unaltered the function

$$(x-y)(y-z)(z-x)$$

of the independent variables x, y, z.

2. The Octic Group.* There are eight movements of a plane which transform into itself a square situated in this plane. If we represent the vertices of this square by the letters a, b, c, d, the results of these eight movements are represented by the following figures:



FIGS. 7–14.

The corresponding eight substitutions are as follows:

$$1,\ ac\cdot bd,\ abcd,\ adcb,\ ac,\ bd,\ ab\cdot cd,\ ad\cdot bc.$$

It should be observed that three of these substitutions are separately the products of two substitutions on distinct sets of letters. For instance, the substitution $ac\cdot bd$ implies that a and c are replaced by each other, and that b and d are also replaced by each other.

The symmetric group on four letters is composed of 24 substitutions. Hence the octic group is composed of one-third of the possible substitutions on four letters. It contains three subgroups of order 4, viz.,

$$1,\ ac\cdot bd,\ abcd,\ adcb;\quad 1,\ ac\cdot bd,\ ac,\ bd;$$

$$1,\ ac\cdot bd,\ ab\cdot cd,\ ad\cdot bc.$$

The first of these corresponds to the rotations about the center of the square through the angles 0, $\pi/2$, π, and $3\pi/2$. The

*This group is also known as the *group of the square*, and as the *dihedral group of order* 8. It is given in § 108 of the noted article by J. L. Lagrange entitled, "Réflexions sur la résolution algébrique des équations," which was published in the *Nouveaux Mémoires de l'Académie royale de Berlin*, 1771.

second corresponds to the movements through the angle π around the diagonals, and their combinations. The third corresponds to the movements through the angle π around the lines joining the middle points of opposite sides, and their combinations.

The three subgroups of order 4 have the subgroup 1, $ac \cdot bd$ in common. There are four other subgroups of order 2 in the octic group, viz.,

$$1,\ ac;\ 1,\ bd;\ 1,\ ab \cdot cd;\ 1,\ ad \cdot bc.$$

Hence *the octic group has three subgroups of order* 4 *and five subgroups of order* 2 *besides the identity.* It can be verified that no other subgroup exists in this octic group.

Another illustration of this group may be based on the function of four variables

$$x_1x_3 + x_2x_4$$

which is transformed into itself by the following eight substitutions

$$1,\ x_1x_3 \cdot x_2x_4,\ x_1x_2x_3x_4,\ x_1x_4x_3x_2,\ x_1x_3,\ x_2x_4,\ x_1x_2 \cdot x_3x_4,\ x_1x_4 \cdot x_2x_3.$$

These substitutions constitute the octic group, since they can be changed or transformed into those of the given octic group by the substitution

$$x_1a \cdot x_2b \cdot x_3c \cdot x_4d.$$

Substitutions and substitution groups which can be transformed into each other by an interchange of letters are said to be *conjugate.*

The remaining sixteen substitutions on these four variables transform the function $x_1x_3 + x_2x_4$ into one of the following two functions:

$$x_1x_2 + x_3x_4,\quad x_1x_4 + x_2x_3.$$

Each of these two functions belongs to the group of all the substitutions on these four letters which transform the function into itself. These two groups are distinct from each other and also from the octic group obtained above. In fact,

the three groups are conjugate,* and they have in common the following subgroup of order four:

$$1,\quad x_1x_2\cdot x_3x_4,\quad x_1x_3\cdot x_2x_4,\quad x_1x_4\cdot x_2x_3.$$

Hence *the symmetric group of degree four contains three conjugate octic groups.* These octic groups have four substitutions in common, and therefore they involve sixteen distinct substitutions.

An interesting illustration of the applications of the octic group in elementary trigonometry is furnished by the operations of finding the complement and the supplement of an angle α, and of the angles obtained from α by these operations. We thus obtain the following eight geometric angles and no more:

$$\alpha,\ 90°-\alpha,\ 180°-\alpha,\ 90°+\alpha\ \ 270°+\alpha,\ -\alpha,\ 270°-\alpha,\ 180°+\alpha.$$

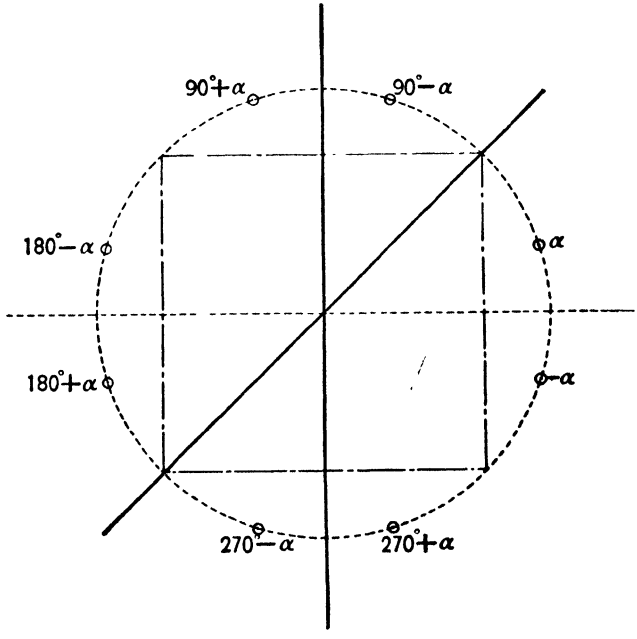


FIG. 15.

* Two conjugate substitution groups are often regarded as the same group, but when they are subgroups of a given group they are often said to be distinct whenever one contains at least one substitution which is not in the other. In listing the possible substitution groups on a given number of letters conjugate groups are regarded as identical.

Each of these eight angles may be regarded as representing also the operation by means of which it can be derived from α. From this point of view these angles constitute a group of order 8. That this is actually the octic group may be seen as follows:

If the angle α is represented by a point on a unit circle, the process of finding the complement of α is equivalent to reflecting α on the bisector of the first and third quadrants, since the geometric meaning of subtraction is a reflection on the point midway between 0 and the minuend. Hence the process of finding the supplement of any angle α is equivalent to reflecting on the Y-axis the point representing α. Since these two kinds of reflections transform into itself the square whose sides are parallel to the coordinate axes, inscribed in the unit circle, it results that the group represented by the eight angles which may be obtained from α by the operations of finding the complement and the supplement is the octic group.

One important difference between the group of movements of the triangle and the group of movements of the square should be emphasized here. In the former case we obtain exactly the same substitution group on the letters a, b, c no matter how these letters are arranged so as to represent the vertices. In the latter case, some possible rearrangements give rise to a different substitution group. In fact, by starting with different arrangements we may obtain three possible conjugate octic groups on the letters a, b, c, d by movements which transform the figure as a whole into itself. We thus obtain another elementary illustration of the important concept of conjugate substitution groups, or of subgroups conjugate under the symmetric group.

3. Generating Substitutions of a Group. The different distinct powers of any substitution constitute a group, which is called *cyclic*. If it is not possible to find at least one substitution in a group such that all the others are powers of it, the group is *non-cyclic*. The symmetric group of order 6 and the given conjugate octic groups are non-cyclic. Each of the latter groups involves one cyclic and two non-cyclic subgroups of order 4.

A substitution whose powers give all the substitutions of a group is said to *generate* this cyclic group, and the order of this cyclic group is equal to the *order of the substitution*. It is always possible to select such a generating substitution in more than one way except when the order of the cyclic group is 1 or 2. For instance, the cyclic group of order 4

$$1,\ ac\cdot bd,\ abcd,\ adcb$$

is generated by *abcd* as well as by *adcb*, and the cyclic group of order 3

$$1,\ abc,\ acb$$

has also two generating substitutions.

In general, a substitution group is said to be *generated by a set of substitutions* provided all of the substitutions of the group can be obtained by combining those of the set. The least number of substitutions that can generate a non-cyclic group is two. Each of the non-cyclic groups which have been considered thus far can be generated by two of its substitutions. For instance, the symmetric group of order 6 can be generated by any one of its three possible pairs of two distinct substitutions of order 2. It can also be generated by any one of the six distinct pairs composed of one substitution of order 2 and one of order 3. Hence the symmetric group of order 6 has nine distinct pairs of generating substitutions.

The octic group cannot be generated by every possible pair of distinct substitutions of order 2, since some such pairs generate only four substitutions. In fact, it is easy to verify that only four out of these ten possible pairs generate this group, while each of the remaining six generate a group of order 4. The square of the substitutions of order 4 cannot be used as one of a pair of generating substitutions of the octic group, but every other substitution besides the identity of this group occurs in such a pair. Hence it is not difficult to verify that there are exactly 12 possible pairs of generating substitutions of the octic group.

Any set of substitutions on n letters generates some substitution group on these letters, which is contained in the sym-

metric group of degree n. It is not necessary that each of these substitutions should actually involve all of these n letters. For instance, it may be found by trial that the two substitutions abc and abd generate a group of order 12, while the two substitutions abc and ad generate the symmetric group of order 24. There is no upper limit for the order of a group which can be generated by two substitutions if these substitutions be chosen arbitrarily and their degrees are not limited.

A set of λ substitutions $s_1, s_2, \ldots, s_\lambda$ of a finite substitution group G is called a *set of generators of* G provided there is no subgroup in G which includes each of these substitutions. When these substitutions satisfy the additional condition that G can be generated by no $\lambda-1$ of them, the set is said to be a *set of independent generators of* G. Such a set can usually be chosen in many different ways.

4. The Groups of Movements of Plane Figures. The symmetric group of order 6 and the octic group are special cases of the groups of movements of regular polygons. The regular polygons of n sides are evidently transformed into themselves by the cyclic group of order n which is generated by the substitution corresponding to the permutation of the vertices when the polygon is rotated around the center through the angle $2\pi/n$. They are also transformed into themselves by n substitutions of order 2 which correspond to the permutation of the vertices when the polygons are rotated successively through the angle π around their different lines of symmetry. As no other movements transform these polygons into themselves, it results that the group of movements of a regular polygon of n sides is of order $2n$.

According to a common definition of regular polygons there is only one regular polygon of 3, 4, or 6 sides, but there are two regular polygons of five sides, as may be seen by connecting alternate vertices, and there are three such polygons of 7 sides. In fact, it is not difficult to see that the number of such regular polygons of n sides is equal to one-half the number of generating substitutions of the cyclic group of order n. All of these regular polygons of n sides belong to the same

substitution group, but this group can be most easily studied by means of the polygon obtained by connecting successive points dividing the unit circle into n equal parts. It contains n or $n+1$ substitutions of order 2 according as n is odd or even.

If we consider the general problem of transforming a system of n, $n>2$, non-collinear points in the rigid plane among themselves, it is important to observe that all such transformations leave a given point invariant, viz., the center of the smallest circle that circumscribes the system of points in question. Hence the possible movements are restricted to rotations around this center, or rotations through the angle π on a line passing through this invariant point. The former rotations must constitute either exactly half or all of the possible movements. In the case of the general parallelogram they evidently constitute all of the possible movements, while they constitute exactly half of the possible four movements in the case of the general rectangle. This result may also be expressed as follows: A plane figure either has no line of symmetry or it has as many lines of symmetry as it admits different plane rotations around the center of its smallest circumscribing circle. In the former case its group of movements is cyclic, while it is non-cyclic in the latter case.

5. Congruence Groups. It will be proved later that every finite group can be represented as a substitution group. Many groups present themselves naturally in different forms and hence it is desirable to study groups represented in different ways. For the present we shall, however, study these groups by means of substitution groups.

Suppose that the first $m-1$ positive integers, together with zero, are combined by addition, and the sums are replaced by their least positive or zero residues modulo m. It is clear that no new numbers are obtained in this way. If any number is added separately to itself and to each of the others, the m numbers will be permuted according to a substitution which may be associated with this added number. The substitutions which are thus associated with all these numbers constitute the cyclic group of order m.

The substitution which is associated with 0 is the identity, while the one which is associated with 1 must be a generating substitution of the cyclic group of order m. If k is any one of these m numbers, the substitution which corresponds to k will be of order m/d, where d is the highest common factor of m and k. Two substitutions whose product is the identity are said to be the *inverses* of each other. Hence the inverse of the substitution which corresponds to k is the one which corresponds to $m-k$.

Moreover, if the $\phi(m)$* positive integers which are prime to m and not greater than m are combined by multiplication, and the products are reduced modulo m, no additional numbers are obtained by this operation. For instance, if $m=8$ and we multiply the four numbers

$$1,\ 3,\ 5,\ 7$$

in succession by 1, 3, 5, 7, we obtain the following non-cyclic substitution group of order 4:

$$1,\ 13\cdot 57,\ 15\cdot 37,\ 17\cdot 35$$

If $m=5$ and we combine the numbers 1, 2, 3, 4, by multiplication, there results the following cyclic group of order 4:

$$1,\ 1243,\ 1342,\ 14\cdot 23$$

The two given types of groups furnish illustrations of the following very important category of congruence groups, where p is a prime number, viz., the groups formed by all the possible linear substitutions of the following form:

$$x' \equiv ax+b \pmod{p}\dagger \qquad \begin{matrix} a=1,\ 2,\ 3,\ \ldots,\ p-1, \\ b=0,\ 1,\ 2,\ \ldots,\ p-1. \end{matrix}$$

* This symbol was first used by Gauss to represent the present concept. It is called the *toticnt of m* according to Sylvester. The French called it the *indicator of m*, and the Germans commonly call it the *Euler ϕ-function of m*.

† This group is sometimes represented by the following general substitution:

$$\begin{pmatrix} 0 & 1 & 2 & \ldots & p-1 \\ b & a+b & 2a+b & \ldots & (p-1)a+b \end{pmatrix}$$

It is easy to find the order of such a substitution as follows:

Let s represent the substitution $x' \equiv ax+b$.

Then s^2 is $x' \equiv a^2x+(a+1)b$,

s^3 is $x' \equiv a^3x+(a^2+a+1)b$,

. . . . . .

and s^r is $x' \equiv a^rx+(a^{r-1}+a^{r-2}+ \ldots +a+1)b$.

If $s^r=1$, it is necessary that $a^r \equiv 1 \pmod{p}$. This is equivalent to

$$a^r-1=(a-1)(a^{r-1}+a^{r-2}+ \ldots +a+1) \equiv 0 \pmod{p}.$$

When $a \not\equiv 1 \pmod{p}$, it results that a necessary and sufficient condition that $s^r=1$ is that $a^r \equiv 1 \pmod{p}$. That is, the order of s is the exponent to which a belongs (mod p) except when $a \equiv 1 \pmod{p}$. In the latter special case, s is clearly of order p when b is not zero.

It should be observed that the order of s is independent of the value of b except when $a \equiv 1 \pmod{p}$. Hence the congruence group under consideration has $p-1$ substitutions of order p, and $p\phi(d)$ substitutions of order d, d being any divisor of $p-1$, including $p-1$ but excluding 1. The order of this group is therefore $p(p-1)$, as is also evident from its definition. It is commonly known as the *metacyclic* group of order $p(p-1)$. The term metacyclic has also been used by H. Weber in his *Lehrbuch der Algebra*, 1895, page 598, to define a more general category of groups, but the definition given here is the older one and is still commonly used.

A particular type of linear groups considered by E. Galois consists of the m^k operations which may be represented by

$$| \; z_1, z_2, \ldots, z_k \quad z_1+c_1, \; z_2+c_2, \ldots, z_k+c_k \; | \pmod{m}$$

where each z_i is replaced by $z_i+c_i \pmod{m}$. In a more explicit notation, we have

$$z'_i \equiv z_i+c_i \pmod{m}, \quad i=1, 2, \ldots, k.$$

This group of order m^k was called by A. L. Cauchy the *group of arithmetic substitutions*. In particular, when $m=k=2$ we

obtain the non-cyclic group of order 4 noted above. This general group is clearly generated by the k substitutions of which the ith (for $i=2, 3, \ldots, k-1$) is

$$z'_1=z_1, \ldots, z'_{i-1}=z_{i-1}, z'_i=z_i+1, z'_{i+1}=z_{i+1}, \ldots, z'_k=z_k \pmod m.$$

For $i=1$ and $i=k$ this substitution becomes respectively

$$z'_1=z_1+1,\ z'_2=z_2,\ \ldots,\ z'_k=z_k$$

and

$$z'_1=z_1,\ \ldots,\ z'_{k-1}=z_{k-1}, z'_k=z_k+1 \pmod m.$$

Each of these k substitutions generates a cyclic group of order m, and the entire group is said to be the *direct product* of these k independent cyclic groups.

6. Groups Represented by Matrices. If two matrices of order n are multiplied together in the ordinary manner * there results a matrix of order n. It may happen that the elements of the matrices are of such a nature that only a finite number of different matrices result when a given set of them are combined by multiplication in every possible order. For instance, the six matrices

$$\left\|\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right\|,\ \left\|\begin{matrix}-1 & 1\\ -1 & 0\end{matrix}\right\|,\ \left\|\begin{matrix}0 & -1\\ 1 & -1\end{matrix}\right\|,\ \left\|\begin{matrix}0 & 1\\ 1 & 0\end{matrix}\right\|,\ \left\|\begin{matrix}-1 & 0\\ -1 & 1\end{matrix}\right\|,\ \left\|\begin{matrix}1 & -1\\ 0 & -1\end{matrix}\right\|,$$

and the six substitutions

$$1,\ abc,\ \ acb,\ \ ab,\ \ ac,\ \ bc$$

may be put into a (1, 1) correspondence in the given order so that like products always correspond. That is, the given matrices combined under multiplication constitute the symmetric group of order six, or the group of an equilateral triangle. We thus meet this group in another very important and extensive field of mathematics, viz., the theory of matrices. It may be observed that the first three of these matrices constitute the subgroup of order three and they can therefore be put into a (1, 1) correspondence, as regards multiplication, with the cube roots of unity.

* For a definition of the product of two matrices cf. Bôcher, *Introduction to Higher Algebra*, 1907, p. 62.

It is not difficult to verify that the following six matrices also constitute a group of order six as regards multiplication:

$$\left\|\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right\|, \left\|\begin{matrix}-1 & 1\\ -1 & 0\end{matrix}\right\|, \left\|\begin{matrix}0 & -1\\ 1 & -1\end{matrix}\right\|, \left\|\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}\right\|, \left\|\begin{matrix}1 & -1\\ 1 & 0\end{matrix}\right\|, \left\|\begin{matrix}0 & 1\\ -1 & 1\end{matrix}\right\|.$$

This group of order six can, however, not be put in a (1, 1) correspondence with the one considered in the preceding paragraph, although the first three matrices are the same in the two groups. The present group of order six is generated by a single matrix and hence it is cyclic. As a generating matrix we may use either one of the last two matrices. It may also be observed that multiplication is commutative in the present group, while this is not the case in the group of the preceding paragraph. The matrices of the present group can be placed in a (1, 1) correspondence with the six sixth roots of unity as regards the operation multiplication.

The four matrices

$$\left\|\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right\|, \left\|\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}\right\|, \left\|\begin{matrix}1 & 0\\ 0 & -1\end{matrix}\right\|, \left\|\begin{matrix}-1 & 0\\ 0 & 1\end{matrix}\right\|$$

evidently serve as another illustration of the non-cyclic group of order 4 when they are combined by multiplication, while the four matrices

$$\left\|\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right\|, \left\|\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}\right\|, \left\|\begin{matrix}0 & 1\\ -1 & 0\end{matrix}\right\|, \left\|\begin{matrix}0 & -1\\ 1 & 0\end{matrix}\right\|,$$

combined according to the same operation, constitute the cyclic group of order 4. As an instance of matrices which constitute a cyclic group of an arbitrary order we may observe that the matrices

$$\left\|\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right\|, \left\|\begin{matrix}1 & 1\\ 0 & 1\end{matrix}\right\|, \left\|\begin{matrix}1 & 2\\ 0 & 1\end{matrix}\right\|, \left\|\begin{matrix}1 & 3\\ 0 & 1\end{matrix}\right\|, \cdots, \left\|\begin{matrix}1 & m-1\\ 0 & 1\end{matrix}\right\|$$

constitute the cyclic group of order m when they are combined as to multiplication, and the elements are reduced modulo m.

EXERCISES

1. In a letter to C. Hermite [Paris *Comptes Rendus*, vol. 49 (1859), p. 115], E. Betti states that the following substitutions:

$$z' = 4z, \quad z' = \frac{1}{z}, \quad z' = 3\frac{z+1}{z-1} \pmod 5$$

generate a group of order 12. Verify this statement, and prove that the first two of these substitutions generate the non-cyclic group of order 4. Either of the first two of the three given generating substitutions could be omitted without affecting the resulting group.

2. Prove that the transformations of the form $z' = \frac{\alpha z+\beta}{\gamma z+\delta} \pmod 3$, α, β, γ, δ being integers such that $\alpha\delta-\beta\gamma \equiv 1 \pmod 3$, constitute a group of order 12 which has the same number of elements of each order as the one in Example 1. Cf. F. Klein, *Mathematische Annalen*, vol. 14 (1879), p. 418.

3. By subtracting a given number n from unity and dividing unity by n, and then performing the same operations successively on the resulting numbers, it is possible to obtain, in general, six different numbers. The only exceptions occur when n has one of the following 8 values: -1, 2, $\frac{1}{2}$; 1, 0, ∞; $\frac{1}{2}(1\pm\sqrt{-3})$. If n represents an anharmonic ratio of four points, then the six values of n obtained by the given operations represent all the values of this ratio.

CHAPTER II

SUBSTITUTION GROUPS AND SYLOW'S THEOREM *

7. Positive and Negative Substitutions. The symbol $a_1a_2 \ldots a_n$ is called a *cyclic substitution* of degree n, and it implies that each of these letters is replaced by the one which follows it, and that a_n is replaced by a_1. That is, it implies a cyclic interchange of its letters, and any one of these letters may be written first without changing the meaning of the substitution. Any permutation of a set of m distinct letters can evidently be effected by one or more cyclic substitutions on these letters. If a substitution consists of more than one cycle it is said to be non-cyclic and its various cycles are usually separated by periods, and the number of letters in all these cycles is the *degree* of the substitution. For instance, $a_1a_2a_3 \cdot a_4a_5$ denotes a substitution of degree 5 which implies a cyclic interchange of the letters a_1, a_2, a_3 in order, and also an interchange of the letters a_4, a_5.

A cyclic substitution which involves only two letters is called a *transposition*. The fact that every possible substitution is a product of transpositions results directly from each of the following equations:

$$a_1a_2a_3 \ldots a_n = a_1a_2 \cdot a_1a_3 \cdot \ldots \cdot a_1a_n$$

$$= a_1a_n \cdot a_na_{n-1} \cdot \ldots \cdot a_3a_2$$

A given substitution can be factored into transpositions in an infinite number of different ways, but the number of the transpositions into which a particular substitution can be

* The general theory of substitutions and substitution groups is developed from the beginning in the present chapter. A few definitions given in the preceding chapter are, however, not repeated.

factored is either always even or it is always odd. We proceed to prove this important elementary theorem.

Let s represent any substitution on m letters and suppose that s has been factored into transpositions in various ways. Each of these transpositions changes the sign of the following determinant: *

$$\Delta = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{m-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{m-1} \\ \cdots & & \cdots & & \\ 1 & a_m & a_m^2 & \cdots & a_m^{m-1} \end{vmatrix}$$

which is not identically zero. As the various sets of transpositions which are equivalent to s must have the same effect on Δ as s has, it results that the number of transpositions in every set is odd if s transforms Δ into $-\Delta$, and this number is even if s transforms Δ into itself.

A substitution is said to be *positive* if it can be factored nto an even number of transpositions. If it can be factored nto an odd number of transpositions it is called *negative*. For nstance, $abc = ab \cdot ac$ is positive, and $abcd = ab \cdot ac \cdot ad$ is negative. The product of two positive substitutions is positive and the product of two negative substitutions is also positive. Hence a product of a set of substitutions is positive or negative according as it involves an even or an odd number of negative substitutions.

If a substitution group involves a negative substitution then exactly one-half of its substitutions are negative. In fact, if all its positive substitutions are multiplied into this negative substitution, all of these products are distinct and negative. Hence it has at least as many negative substitutions as positive ones. On the other hand, if this negative substitution is multiplied into all of its negative substitutions, all these products are distinct and positive. Hence it has at least as many positive substitutions as negative ones. In other

* This determinant is known as the determinant of Vandermonde or of Cauchy. It is equal to the product

$$\Pi(a_i - a_k); \quad i, \ k = 1, \ 2, \ \ldots, \ m; \quad i > k.$$

words, *either all the substitutions of a substitution group are positive or exactly half of them are positive.*

Whenever a group contains negative substitutions it contains a subgroup of half its own order, composed of its positive substitutions. In particular, the symmetric group of degree n contains a subgroup of order $n!/2$ which is composed of its positive substitutions. This subgroup is called *the alternating group of degree n*. Hence there are at least three distinct groups of degree n whenever $n>3$, viz., the group generated by a cyclic substitution on n letters, the alternating group, and the symmetric group. It will be proved that other groups of degree n exist for every value of $n>3$. The cyclic substitution of degree n is positive or negative according as n is odd or even.

The product of two transpositions which have a common letter is always of the form abc. A positive cyclic substitution is always the product of substitutions of the form abc, since it is the product of an even number of transpositions having a common letter. A substitution composed of two negative cyclic substitutions is also the product of substitutions of the form abc. In fact, such a substitution may be regarded as the product of two distinct sets of transpositions such that all the transpositions of each set have a common letter and such that each set involves an odd number of transpositions. Hence it remains only to observe that a substitution composed of two transpositions having no letter in common is the product of substitutions of the form abc. This fact results directly from the product

$$ab \cdot cd = acb \cdot bdc.$$

That is, *every possible positive substitution is the product of substitutions of the form abc.*

8. Commutative Substitutions. Let s and t represent two substitutions. If $st=ts$, these two substitutions are said to be *commutative*. For instance, if $s=ab \cdot cd$ and $t=ac \cdot bd$, it is easy to verify that $st=ts=ad \cdot bc$. On the other hand, if $s=ab \cdot cd$ and $t_1=bc$, it results that $st_1=acdb$ while $t_1 s=abdc$. Hence

the two substitutions $ab \cdot cd$, $ac \cdot bd$ are commutative, but $ab \cdot cd$ is not commutative with bc. Two substitutions which have no letter in common are always commutative.

It is often necessary to find all the substitutions on certain letters which are commutative with a given substitution. The solution of this problem is based on finding all the substitutions on the letters $a_1, a_2, \ldots, a_n$ which are commutative with the cyclic substitution $s_1 = a_1 a_2 \ldots a_n$. It is clear that s_1 is commutative with all of its powers, and hence s_1 is commutative with at least n substitutions, including the identity, on the letters $a_1, a_2, \ldots, a_n$.

All substitutions which are commutative with s_1 must also be commutative with $s_1^{\alpha_1}$, where α_1 is any positive integer. Suppose that t_2 is a substitution on the letters $a_1, a_2, \ldots, a_n$ which is commutative with s_1 but is not a power of s_1. It is evident that t_2 must involve each of the letters $a_1, a_2, \ldots, a_n$. Hence we may suppose that $t_2 = a_1 a_\alpha \ldots$, where α is one of the numbers $2, 3, \ldots, n$. Since $s_1^{\alpha-1} = a_1 a_\alpha \ldots$, it results that $t_2 s_1^{n+1-\alpha}$ is a substitution which is commutative with s_1, does not involve a_1, and is not the identity. That is, we arrive at an absurdity by assuming that more than n substitutions on the letters $a_1, a_2, \ldots, a_n$ are commutative with s_1. This proves the theorem: *The only substitutions on n letters which are commutative with a cyclic substitution on these letters are the powers of this cyclic substitution.*

If a substitution s_2 is composed of λ cycles such that no two of these cycles involve the same number of letters, then all the substitutions on the letters of s_2, which are commutative with s_2 must also be commutative with each cycle of s_2. The number of the substitutions which are commutative with s_2, and involve only letters contained in s_2, is therefore equal to the product of the orders of the cycles of s_2. For instance, the substitutions which are commutative with the following substitution

$$abcde \cdot fgh,$$

and involve only its eight letters, constitute a substitution group of order 15.

A substitution s_3 which involves k equal cycles is commutative with substitutions which permute these cycles according to the symmetric group of degree k. If each of these cycles involves n letters, the substitutions on these kn letters which are commutative with s_3 must therefore constitute a substitution group of order $n^k \cdot k!$. For instance, the substitutions on the nine letters involved in the following substitution

$$abc \cdot def \cdot ghi,$$

and which are commutative with this substitution, constitute a group of order $27 \cdot 6 = 162$.

9. Transforms of a Substitution and of a Substitution Group. If s and t represent any two substitutions, it is possible to find a third substitution by means of the operation $s^{-1}ts = t_1$, where s^{-1} represents the inverse of s. The substitution t_1 is called the *transform* * of t as regards s. There is a very simple rule for deriving t_1 if s and t are given. We proceed to develop this rule.

Suppose that

$$t = \ldots a_\alpha a_\beta \ldots$$

$$s = \ldots a_\alpha a_\alpha' \ldots a_\beta a'_\beta \ldots$$

It is not assumed that a_α or a_β actually appears in s when s is written in the normal form, since a'_α may be identically equal to a_α and a'_β may be identically equal to a_β. Hence the given notation is entirely general. It is easy to see that

$$t_1 = \ldots a'_\alpha a'_\beta \ldots$$

That is, *to obtain the transform of t as regards s we simply replace each letter in t by the one by which s replaces this letter.*† For instance, if $s = abcd \cdot ef$ and $t = ab \cdot ce$, then $\cdot s^{-1}ts = bc \cdot df$. In

* This transformation is fundamental in the theory of groups. Many of its properties were developed by E. Betti in 1852; *Annali di Scienze matematiche e fisiche*, vol. 3, p. 55.

† This simple method to find the transform of a substitution is found in C. Jordan's thesis, Paris, 1860, p. 14.

particular, if a substitution contains a certain number of cycles of a given order, each of its transforms contains the same number of cycles of this order.

A necessary and sufficient condition that $t=t_1$ is that s and t are commutative, since the equation $s^{-1}ts=t$ implies that $ts=st$ and conversely. Each of two commutative substitutions is transformed into itself by the other. If a substitution is transformed into itself by all the substitutions of a group it is said to be *invariant* under this group. When this substitution belongs to the group it is said to be an invariant substitution of the group. The identity is invariant under every group and is an invariant substitution of every group. As an instance of another invariant substitution it may be observed that $ac\cdot bd$ is invariant under the following octic group:

$$1,\ ab\cdot cd,\ ac\cdot bd,\ ad\cdot bc,\ ac,\ bd,\ abcd,\ adcb.$$

The symmetric group of order 6 contains no invariant substitution besides the identity.

If each substitution of a group G is transformed by means of a substitution s there results a group G_1 which is called the *transform of* G with respect to s, or the *conjugate* of G with respect to s, and is represented by the symbol

$$s^{-1}Gs=G_1.$$

Conjugate substitutions and conjugate groups are also called *similar*. When $G_1=G$ the substitution s is said to transform G into itself, and G is said to be invariant under s. Every group is invariant under its own substitutions. A subgroup which is invariant under all the substitutions of a group is called an *invariant*, or *self-conjugate*, *subgroup*. If a group involves negative substitutions all of its positive substitutions constitute an invariant subgroup. In particular, the alternating group of degree n is an invariant subgroup of the symmetric group of this degree.

Suppose that s is transformed into itself by some but not by all of the substitutions of a group G. The substitutions

of G which transform s into itself form a subgroup H of G. If t is any substitution of G which is not in H then all the substitutions obtained by multiplying t on the left by a substitution of H will transform s into the same substitution. For, if t_1 is any substitution of H, we have the equation

$$(t_1 t)^{-1} s t_1 t = t^{-1} t_1^{-1} s t_1 t = t^{-1} s t.$$

Moreover, if $t'^{-1} s t' = t^{-1} s t$, it results that $s = t' t^{-1} s t t'^{-1}$. That is, $t t'^{-1}$ is in H. Hence its inverse $t' t^{-1}$ is also in H. That is, t' is one of the substitutions obtained by multiplying t on the left by some substitution of H.

From what precedes it results that all the substitutions of G can be divided into equal sets such that each set is composed of all the substitutions of G which transform s into the same substitution. The totality of the substitutions into which s is transformed under G forms a *complete set of conjugates of s under G.* The number of different substitutions in a complete set of conjugates under a group is a divisor of the order of the group. A complete set of conjugate subgroups under G is defined in a similar manner.

Incidentally we proved above that the order of G is divisible by the order of its subgroup H. We proceed to prove that the order g of G is divisible by the order k of any subgroup K.* In fact, all the substitutions of G can be written in the form of a rectangle, whose first line is composed of the substitutions of K, as follows:

$$\begin{array}{l} 1, \quad s_2, \quad s_3, \quad \ldots, \quad s_k \\ t_2, \quad s_2 t_2, \quad s_3 t_2, \quad \ldots, \quad s_k t_2 \\ \cdots\cdots\cdots\cdots\cdots \\ t_\lambda, \quad s_2 t_\lambda, \quad s_3 t_\lambda, \quad \ldots, \quad s_k t_\lambda \end{array}$$

In this rectangular array the substitutions $t_2, \ldots, t_\lambda$ are any substitutions of G which do not occur in any of the preceding rows.

* If a group is represented by a capital letter the corresponding small letter usually represents the order of the group.

To prove that k is a divisor of g it is only necessary to prove that no substitution of G can occur twice in such an array. This fact can be easily proved as follows:

If $s_\alpha t_\gamma = s_\beta t_\gamma (\alpha, \beta \leqq k)$, then $s_\alpha = s_\beta$;

and

if $s_\alpha t_\gamma = s_\beta t_\delta (\delta > \gamma)$, then $s_\beta^{-1} s_\alpha t_\gamma = s_{\alpha'} t_\gamma = t_\delta (\alpha' \leqq k)$.

Hence it results that no substitution of G can occur twice in such an array and we have established a fundamental theorem, known as the *theorem of Lagrange*, which may be stated as follows:

The order of a group is divisible by the order of each one of its subgroups.

This may be regarded as the most important theorem of group theory. It will appear that a subgroup has properties similar to those of a modulus in number theory. Hence a subgroup is sometimes called a modulus of the group. The quotient obtained by dividing the order of a group by the order of a subgroup is called the *index* of this subgroup under the group. The index of a subgroup is therefore always a positive integer.

EXERCISES

1. The order of a group is divisible by the order of each of its substitutions. (Cauchy.)

2. The order of every substitution group on n letters is a divisor of $n!$. (Cauchy.)

3. All the substitutions which are common to two groups constitute a group. This is known as the *cross-cut* of these two groups.

4. The number of substitutions in a complete set of conjugate substitutions under a group cannot exceed the quotient obtained by dividing the order of the group by the order of one of these substitutions.

5. The symmetric group of degree n, $n>2$, does not contain any invariant substitution besides the identity.

6. The alternating group of degree n, $n>3$, does not contain an invariant substitution besides the identity.

7. Find the following products:

$abcde \times bdc =$, $ac \cdot bd \times bcfe =$

$ade \times abc \times acbed =$, $ac \times cd \times de =$

8. Find a value of t in the form of a product of transpositions such that $abcdefg = ae \times af \times ag \times bh \times ek \times cd \times t$.

9. Transform $ace \cdot gf$ by bef, and also by $ab \cdot cd$.

10. Write the 12 positive substitutions on four letters, and find the groups composed of all the substitutions on these four letters which transform into itself each of these 12 positive substitutions.

10. Co-sets and Double Co-sets. From the arrangement of all the substitutions of a group in the form of a rectangle in which the first line is composed of all the substitutions of a subgroup (§ 9), it results directly that, if H is any subgroup of the group G, all the substitutions of G can be written in the following form: *

$$G \equiv H + Ht_2 + \ldots + Ht_\lambda.$$

In this notation, $Ht_\alpha (\alpha = 2, \ldots, \lambda)$ stands for all the products formed by multiplying every substitution of H into t_α. The sets of substitutions represented by Ht_α are called *co-sets* † of G as regards H. It is important to observe that t_α may be replaced by any one of the substitutions of the co-set to which it belongs without changing the co-set. In other words, if two such co-sets have one substitution in common they are identical co-sets.

It is sometimes desirable to include the subgroup H among the co-sets as regards H. In this case, the given λ sets are called the *augmented co-sets* of G as regards H. Unless the contrary is stated, it will be assumed that these co-sets are distinct, so that every substitution of G appears once and only once in the co-sets. The set of multiplying substitutions $t_2, \ldots, t_\lambda$ can be chosen in $h^{\lambda-1}$ ways, h being the order of H.

Instead of multiplying H on the right we could have multiplied on the left. Hence all the substitutions of G can also be written in the form

$$G \equiv H + t'_2 H + \ldots + t'_\lambda H.$$

* This notation is due to Galois.

† The concept of co-sets was used by E. Galois, but he did not use a special name for it. H. Weber used the term *Nebengruppen* to represent what we her call co-sets. The latter term seems not to have been used for this concept before 1910, *Quarterly Journal of Mathematics*, vol. 41 (1910), p. 382.

It will be proved later (§ 33) that it is always possible to select the $\lambda-1$ multipliers in such a manner that $t'_\alpha = t_\alpha$, $\alpha = 2, \ldots, \lambda$. By taking the inverses of each of the co-sets in the formula of the first paragraph of this section, it results that

$$G \equiv H + t_2^{-1}H + \ldots + t_\lambda^{-1}H.$$

Hence it is also possible to replace t'_α by t_α^{-1} in the preceding formula.

If H_1 and H_2 are any two subgroups of G, the symbol

$$H_1 t_\alpha H_2$$

is called a *double co-set** of G as regards H_1 and H_2. It implies that each of the substitutions of $H_1 t_\alpha$ is multiplied on the right by every substitution of H_2. All of these products are represented by the single symbol $H_1 t_\alpha H_2$. While all of the substitutions of a co-set are distinct, those of a double co-set need not be distinct. If one substitution of G occurs exactly k times in such a double co-set, every substitution of the double co-set occurs exactly k times among the products represented by this double co-set. We proceed to prove this statement.

Consider the product of the two groups $H_1 \cdot H_2$, that is, all the products obtained by multiplying every substitution of H_1 on the right by all the substitutions of H_2. If H_1 and H_2 have exactly ρ substitutions in common, it is clear that each substitution of H_1 and each of H_2 will appear exactly ρ times in $H_1 \cdot H_2$. In fact, if t_1 is any substitution of H_1, the ρ substitutions obtained by multiplying t_1 on the right by the substitutions which are common to H_1 and H_2 will yield the same products when they are multiplied on the right by H_2. As no other substitution of H_1 can yield any of these products, being in the same co-set of G as regards H_2, it results that *the product $H_1 \cdot H_2$ involves each one of its substitutions exactly*

* Double co-sets were first used by A. L. Cauchy, Paris *Comptes Rendus*, vol. 22 (1846), p. 630. They were more fully developed by Frobenius, *Crelle*, vol. 101 (1887), p. 273. The term double co-set was first used with this meaning in *Bulletin of the American Mathematical Society*, vol. 17 (1911), p. 292.

ρ times, ρ being the number of the substitutions which are common to H_1 and H_2.

It is now very easy to find the number of times that a given substitution of the product $H_1 t_\alpha H_2$ appears in this product. In fact, $H_1 t_\alpha H_2 = t_\alpha \cdot t_\alpha^{-1} H_1 t_\alpha \cdot H_2$, and hence $H_1 t_\alpha H_2$ is the product of t_α and two groups. If a substitution s occurs exactly k times in $t_\alpha^{-1} H_1 t_\alpha \cdot H_2$, the substitution $t_\alpha s$ must occur exactly k times in $H_1 t_\alpha H_2$. That is, *each of the substitutions of $H_1 t_\alpha H_2$ occurs exactly k times in this double co-set, k being the number of the substitutions common to the two groups $t_\alpha^{-1} H_1 t_\alpha$ and H_2.*

The following special case of this theorem is often useful.

The number of the distinct substitutions in the double co-set $H_1 t_\alpha H_2$ is equal to the product of the orders of H_1 and H_2, divided by a number which is the common order of two subgroups contained in H_1 and H_2 respectively.

The double co-set $H_1 t_\alpha H_2$ is not changed if t_α is replaced by any one of the other substitutions of this double co-set, since the co-sets $H_1 t_\alpha$ is not altered when t_α is replaced by any other substitution of this co-set, and likewise for the co-set $t_\alpha H_2$. Hence two such double co-sets of G have either no substitution in common or they are identical. The possible double co-sets of G as regards the two subgroups H_1 and H_2, in the given order, are therefore completely determined by these subgroups. If we count only the distinct substitutions of these double co-sets we may write G in the following form:

$$G \equiv H_1 \cdot H_2 + H_1 t_2 H_2 + \ \ldots \ + H_1 t_\gamma H_2.$$

Each substitution of G appears once and only once in the second member of this identity, if these symbols are used to represent only the distinct substitutions which occur among the possible products represented by the symbols. Double co-sets are commonly used with this restricted meaning, and we shall hereafter use them in this sense unless the contrary is stated. Hence two of these double co-sets do not necessarily represent the same number of substitutions, but these numbers are always in accord with the theorem expressed above.

11. Sylow's Theorem.* The theorem of the preceding section may be used to prove another very fundamental theorem known as *Sylow's theorem*, which asserts that every group whose order is divisible by p^m but not by p^{m+1}, p being a prime number, contains a subgroup of order p^m. Such a subgroup is called a *Sylow subgroup* of the group. E. Galois made the remark in his *Manuscripts*, published by Jules Tannery in 1908, page 39, that a group whose order is divisible by p contains a subgroup of order p. This theorem was proved by A. L. Cauchy in 1845. It was extended to the case mentioned above by L. Sylow, in an article published in the *Mathematische Annalen*, volume 5, 1872, page 584. We shall establish this theorem, treating first the special case when the group G is symmetric and of prime power degree.

It is evident that the symmetric group of degree p, p being any prime number, contains a subgroup of order p. As $p!$ is not divisible by p^2 this establishes Sylow's theorem for this special case. We proceed to establish the theorem for the symmetric group G of degree $p^{\alpha+1}$. This group contains the following substitution composed of p^α cycles:

$$s = a_1 \ldots a_p \cdot a_{p+1} \ldots a_{2p} \cdot \ldots \cdot a_{p^{\alpha+1}-p+1} \ldots a_{p^{\alpha+1}}.$$

It contains also the subgroup H composed of all the substitutions on these $p^{\alpha+1}$ letters which transform s into itself. We proceed to prove that H includes a Sylow subgroup of G.

The subgroup H includes a subgroup K composed of all the substitutions obtained by multiplying in every possible way all the substitutions generated by the separate cycles of s. Since each cycle is of order p and there are p^α cycles in s, it results that the order of K is

$$p^{p^\alpha}.$$

These p^α cycles are permuted under H according to the symmetric group G' of degree p^α which transforms K into itself. As G' is of a smaller degree than G, and as the symmetric group of degree p contains a Sylow subgroup, we may assume, in a

* A different proof of this theorem will be given in § 27.

proof by complete induction, that G' contains a Sylow subgroup of order $p^{m'}$, where

$$m' = \frac{p^\alpha - 1}{p-1}.*$$

Since the p^α cycles of s are transformed under H according to a group of order $p^{m'}$, and since the substitutions of H which permute these cycles according to these various substitutions transform K into itself, it results that H involves a subgroup H_2 of order

$$p^{m'} \cdot p^{p^\alpha} = p^m, \text{ where } m = \frac{p^{\alpha+1} - 1}{p-1}.$$

As p^m is the highest power of p which divides the order of G, in accord with the well-known theorem in number theory which has just been used, it results that G contains a Sylow subgroup of order p^m whenever G' contains such a subgroup of order $p^{m'}$. That is, Sylow's theorem has been established, by the method of complete induction, for every symmetric group whose degree is a power of p.

It is now easy to establish Sylow's theorem for every possible substitution group. Let H_1 be any such group. As the symmetric group of degree n includes the symmetric group of degree $n-1$, it results that it is possible to find a value for α such that H_1 is contained in the symmetric group G of degree $p^{\alpha+1}$. Let H_2 represent any Sylow subgroup of order p^m contained in G, and write the substitutions of G in the form of double co-sets as regards the two subgroups H_1 and H_2, as follows:

$$G \equiv H_1 \cdot H_2 + H_1 t_2 H_2 + \ldots + H_1 t_\gamma H_2.$$

Let p^β be the highest power of p which divides the order of H_1. The number of distinct substitutions in each of these double co-sets is a multiple of $p^{m+\beta} \div p^\beta$, according to a theorem of the preceding section. This number cannot be divisible by p^{m+1} for every one of these double co-sets, since the order

* This result is contained in the well-known formula for the highest power of a prime which divides $n!$. Cf. *Encyclopédie des Sciences Mathématiques*, tome 1, vol. 3, p. 4; R. D. Carmichael, *Theory of Numbers*, 1914, p. 26.

of G is not divisible by p^{m+1}. Hence there must be at least one of these double co-sets in which $\delta=\beta$. As p^δ is the order of a subgroup of H_1, it follows that H_1 must contain a Sylow subgroup. Hence *every possible substitution group contains at least one Sylow subgroup corresponding to every prime number which divides the order of the group.*

If H_1 contains more than one subgroup of order p^β, let

$$K_1,\ K_2,\ \ldots\ ,\ K_\lambda$$

represent all its subgroups of this order. A substitution s of K_1 which is not also in K_2 cannot transform K_2 into itself, otherwise s and K_2 would generate a group whose order would be divisible by $p^{\beta+1}$. Hence the substitutions of K_1 must transform K_2 into a complete set of conjugates under K_1 and this set contains p^{α_1} of these λ subgroups. If p^{α_1} is less than $\lambda-1$, this process can be repeated until all of these groups are exhausted. It is therefore necessary that $\lambda-1$ be divisible by p. That is, *the number of the Sylow subgroups of order p^β contained in any group is always of the form*

$$1+kp.$$

In other words, this number is always $\equiv 1 \pmod{p}$.

From this theorem it results directly that every subgroup of order p^γ of a group G is contained in a Sylow subgroup of G, or is itself a Sylow subgroup of G. In fact, such a subgroup must transform into itself at least one of the Sylow subgroups of G. If it were not contained in this Sylow subgroup, G would involve a subgroup whose order would be a higher power of p than the order of its Sylow subgroup. It is also clear that every operator of order p^δ which is in G and transforms into itself a Sylow subgroup of order p^β must be contained in this Sylow subgroup.

Another important elementary result in regard to the Sylow subgroups should be observed here. Suppose that the given λ Sylow subgroups were such that they could not all be transformed into each other by the substitutions of these subgroups. There would therefore be a set of h which would be transformed only among themselves by all these substitutions. By trans-

forming these h subgroups by the substitutions of one of their own number it would result that h would be of the form $1+k_1p$, and by transforming the same subgroups by the substitutions of a subgroup of order p^β which is not included among these h subgroups, it would result that h would be divisible by p. Hence *all the Sylow subgroups of order p^β in any substitution group constitute a single complete set of conjugates under this group.* In fact, they constitute such a complete set under these Sylow subgroups.

The three results: that Sylow subgroups of order p^β always exist, that their number is of the form $1+kp$, and that they form a single set of conjugates under the group, are very closely related. Generally these three results are implied by the expression "Sylow's theorem." All of them are of fundamental importance. In fact, if the theorems of group theory were arranged in order of their importance Sylow's theorem might reasonably occupy the second place—coming next to Lagrange's theorem in such an arrangement.

EXERCISES

1. By means of Sylow's theorem prove that every substitution group of order 20 contains only one subgroup of order 5, and either one or five subgroups of order 4.

2. Every group of order pq, p and q being distinct primes and $p>q$, contains only one subgroup of order p.

3. A group of order 15 contains only one subgroup of each of the orders 3 and 5. Hence a group of order 15 is cyclic.

4. Find two substitutions of order 2 such that their product is of order 7, and verify that they generate a substitution group of order 14.

5. The number of subgroups of order p in the symmetric group of degree p is $(p-2)!$, p being any prime number. Hence $(p-2)!\equiv 1 \pmod{p}$.

6. The number of the subgroups which are generated by cyclic substitutions of order n and are contained in the symmetric group of degree n is $\frac{(n-1)!}{\phi(n)}$, $\phi(n)$ being the totient of n.

7. The symmetric group of degree n, $n>3$, contains more than one Sylow subgroup of order p^α, whenever $n!$ is divisible by p.

12. Transitive Groups, and Average Number of Letters in its Substitutions. The two substitution groups of order 4

$$1,\ ab\cdot cd,\ \ ac\cdot bd,\ \ ad\cdot bc;\quad 1,\ ab,\ \ cd,\ \ ab\cdot cd$$

represent two very important types of groups. In the former each letter of the group is replaced by every other letter by the various substitutions of the group. Such a group is said to be *transitive*. In the latter of these two groups, there is a letter which is not replaced by every other letter, and hence this group is called *intransitive*. Every substitution group evidently belongs to one and only one of these two types. Every symmetric group and every alternating group is transitive.

Suppose that G is a transitive group on the n letters $a_1, a_2, \ldots, a_n$. There is at least one substitution in G which does not involve the letter a_1, viz., the identity. In general, the substitutions of G which omit a_1 constitute a subgroup G_1 of order g_1. As G is transitive it must involve a substitution which replaces a_1 by a_2, and this substitution transforms G_1 into G_2, G_2 being composed of all the substitutions of G which omit a_2. Hence G contains n conjugate subgroups $G_1, G_2, \ldots, G_n$, each of which is composed of all the substitutions of G which omit a letter. It is not necessary that all of these n subgroups be distinct. In fact, in the octic group they form two pairs of identical subgroups.

All the substitutions of G can be arranged in a rectangle as follows, the substitutions of G_1 forming the first row:

$$\begin{array}{l} 1, \ s_2, \ s_3, \ \ldots, \ s_{g_1} \\ t_2, \ s_2t_2, \ s_3t_2, \ \ldots, \ s_{g_1}t_2 \\ t_3, \ s_2t_3, \ s_3t_3, \ \ldots, \ s_{g_1}t_3 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ t_\lambda, \ s_2t_\lambda, \ s_3t_\lambda, \ \ldots, \ s_{g_1}t_\lambda \end{array}$$

where $\lambda = g/g_1$. If t_2 replaces a_1 by a_2 then all the g_1 substitutions of the row involving t_2 have this property. If any other substitution of G should replace a_1 by a_2, all the distinct products, obtained by multiplying its inverse into itself and into all the substitutions of the row involving t_2, would transform a_2 into itself. As this would give more than g_1 distinct substitutions, the row which involves t_2 contains all the substitutions of G which replace a_1 by a_2.

Since similar remarks apply to every other row, it results that $\lambda = n$. That is, *the order of the subgroup formed by all the substitutions of a transitive group which omit a given letter is equal to the order of the group divided by its degree.* From the given rectangle it follows that each letter occurs $g_1(n-1)$ times in the substitutions of G. Hence these substitutions involve $g_1 n(n-1) = g(n-1)$ letters. That is, *the average number of letters in the substitutions of a transitive group is equal to the degree of the group diminished by unity.** In particular, the average number of letters in all the possible substitutions on n letters is $n-1$, and this is also the average number in all the positive substitutions on these letters when $n > 2$.

13. Intransitive Substitution Groups. One of the simplest examples of an intransitive substitution group may be obtained by multiplying together transpositions on distinct sets of letters. For instance, the intransitive group generated by the following three transpositions,

$$ab,\ cd,\ ef,$$

is of order eight and contains seven substitutions of order 2, besides the identity. This is a special case of the elementary theorem which affirms that h transpositions on h distinct pairs of letters generate a group of order 2^h and of degree $2h$. This group is intransitive when $h > 1$.

By multiplying all the substitutions of any transitive group by all those of another transitive group, represented on a distinct set of letters, there results an intransitive group whose order is the product of the orders of these two transitive groups, and whose degree is the sum of their degrees. Hence it is clear that it is possible to construct an unlimited number of different groups from any given group by representing the group on distinct sets of letters and then multiplying the substitutions in every possible manner. Groups obtained in this manner are sometimes called *powers* of the given group, an index being used to indicate the number of times the group was used

* This interesting theorem was given explicitly for the first time by G. Frobenius, *Crelle*, vol. 101 (1887), p. 287.

as a factor. The groups considered in the preceding paragraph constitute a special class of such powers.

Another way of forming an unlimited number of non-conjugate substitution groups from a given substitution group is by a process called establishing a (1, 1) correspondence or a *simple isomorphism*. For instance, the following three substitution groups of order 2:

$$1,\ ab\cdot cd;\ 1,\ ab\cdot cd\cdot ef;\ 1,\ ab\cdot cd\cdot ef\cdot gh$$

are obtained by establishing simple isomorphisms between the groups 1, ab and 1, cd; 1, ab, 1, cd, and 1, ef; 1, ab, 1, cd, 1, ef, and 1, gh, respectively. It is clear that we can establish such simple isomorphisms between any number of groups, obtained by writing a given transitive group on distinct sets of letters. All the groups thus obtained are merely different ways of representing the same group of order 2 considered abstractly, and these isomorphisms show that there is no upper limit to the number of letters of the substitution groups which represent such a group.

The two given methods of constructing intransitive substitution groups are called the *direct product method* and the *simple isomorphism method*. They are the simplest methods for constructing such groups and the other possible methods are based upon them.* Before entering upon a consideration of other methods it should be observed that every intransitive group is composed of *transitive constituent groups*, and that it can be constructed by establishing some correspondence between these constituent groups.

Let G be any intransitive group, and consider the letters which replace a given letter a in the substitutions of this group. If a is replaced by b in some substitution s_1 and there is also a substitution s_2 in which b is replaced by c, then there must be a third substitution $s_3 = s_1 s_2$ in which a is replaced by c. Hence a and all the letters by which a is replaced constitute the letters of a transitive constituent group.

If $1, s_2, \ldots, s_k$ represent the substitutions of this con-

* Cf. Bolza, *American Journal of Mathematics*, vol. 11 (1889), p. 195.

stituent group K, then each of these k substitutions is found in the same number of the substitutions of G, and hence k is a divisor of g, where g is the order of G. In the simple isomorphism method, $k=g$. All the substitutions of G which involve only the identity from K constitute an invariant subgroup H of G, and K is said to be a *quotient group* of G as regards H. This quotient group is commonly represented by the following symbol: *

$$G/H=K.$$

For instance, consider the following intransitive group G:

$$1,\ cde,\ ced,\ ab\cdot cd,\ ab\cdot de,\ ab\cdot ce.$$

One of the transitive constituent groups is $1,\ ab\equiv K$, and the invariant subgroup of G, which involves only the identity of this constituent group, is as follows:

$$H\equiv 1,\ cde,\ ced.$$

The quotient group $G/H\equiv K$ may also be regarded as a group in which the three substitutions of H are regarded as one substitution, while the remaining three substitutions constitute the other substitution. The other transitive constituent of G is simply isomorphic with G, and the given correspondence is sometimes represented by the following symbol:

1	
cde	1
ced	
cd	
de	ab
ce	

As an instance of a more general correspondence, we may consider the group of order 18 composed of all the positive substitutions in the direct product of the symmetric group of degree 3 represented on two distinct sets of letters. This group is represented as follows:

* This symbol was used by C. Jordan, *Bulletin de la Société Mathématique de France*, vol. 1 (1872), p. 46. The symbol is often credited to Hölder, who used it in 1889. Cf. H. Weber, *Kleines Lehrbuch der Algebra*, 1912, p. 192.

1	1
abc	*def*
acb	*dfe*
ab	*de*
bc	*ef*
ac	*df*

If we let K represent the former of these two constituent groups it is clear that $H \equiv 1$, *def*, *dfe*, and that $G/H \equiv K$ can be regarded as a group in which three substitutions of G are considered as a single substitution.

14. Substitutions which are Commutative with Each of the Substitutions of a Transitive Group. When G_1, the subgroup composed of all the substitutions which omit a given letter, reduces to the identity, the transitive group G is said to be a *regular group*. Regular groups are especially important since every possible group of finite order can be represented as a regular substitution group, as will be proved later. We proceed to prove the important theorem, which we shall call *Jordan's theorem*,* that the total number of substitutions on n letters which are commutative with every substitution of a regular group G on the same n letters constitutes a group G' which is conjugate or similar to G; i.e., it can be transformed into G by some substitution. This theorem results almost immediately if we multiply all the substitutions of $G \equiv 1$, $s_2, s_3, \ldots, s_g$ successively on the right and on the left as follows: †

$$G = \begin{cases} 1, & s_2, & s_3, & \ldots, & s_g \\ s_2, & s_2^2, & s_3 s_2, & \ldots, & s_g s_2 \\ s_3, & s_2 s_3, & s_3^2, & \ldots, & s_g s_3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_g, & s_2 s_g, & s_3 s_g, & \ldots, & s_g^2 \end{cases} \qquad G' = \begin{cases} 1, & s_2, & s_3, & \ldots, & s_g \\ s_2, & s_2^2, & s_2 s_3, & \ldots, & s_2 s_g \\ s_3, & s_3 s_2, & s_3^2, & \ldots, & s_3 s_g \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_g, & s_g s_2, & s_g s_3, & \ldots, & s_g^2 \end{cases}$$

* This theorem was first proved in Jordan's thesis, Paris, 1860, p. 39.

† The two simply isomorphic regular substitution groups which are represented by these square arrays have been called *potential* and *antipotential* groups respectively. G. Frattini, *Atti della R. Accademia dei Lincei. Memoria*, vol. 14 (1883), p. 144.

The permutation of the substitutions of each of these rows as regards the first row represents a substitution, and we may assume, without loss of generality, that the substitutions represented by the first square, when the various rows are associated successively with the first row, are the substitutions of G. Any one of these rows, say the one involving s_α, represents a substitution obtained by multiplying all the substitutions of G on the right by s_α; while any row of G', say the one involving s_β, represents a substitution obtained by multiplying all the substitutions of G on the left by s_β. Since we get the same result when we multiply all the substitutions of G first on the right by s_α and then on the left by s_β, as when we multiply them first on the left by s_β and then on the right by s_α, as a consequence of the associative law, it follows that each substitution of G is commutative with every substitution of G', and vice versa. Moreover, G' includes all the substitutions on these letters, which are commutative with every substitution of G, since every such substitution must involve all the letters of G and the totality of these substitutions forms a group.

As G and G' are different ways of representing the group G they must be simply isomorphic. It remains to prove that they are conjugate. If we establish a simple isomorphism between G and G' in such a way that all the substitutions begin with the same letter, the second letters in all the substitutions of these groups represent the substitution by means of which G may be transformed so that the first two letters in each one of its substitutions are the same as the first two letters of the corresponding substitution in G'. Since this transformation will lead to simply isomorphic groups, and since two simply isomorphic regular groups have the property that the corresponding substitutions are identical whenever the first two letters of all these substitutions are the same, we have proved Jordan's theorem; viz., *with every regular group of order n there is associated another regular group of order n such that each of these groups is composed of the total number of substitutions on these n letters which are commutative with every substitution of the other group.*

The two groups G and G' which are defined by Jordan's theorem are called *conjoints*. When G is abelian it coincides with its conjoint and vice versa. A special case of this theorem relating to a cyclic group was proved above in § 8. Suppose that G is transitive and of degree n, but not regular, and that all the substitutions of G which omit a_1 omit also $a_2, \ldots, a_\alpha$. Hence G_1, which is composed of all the substitutions of G which omit a_1, is transformed into itself by all the substitutions of G which replace a_1 by $a_2, \ldots, a_\alpha$. That is, G_1 is transformed into itself by a subgroup H of order αg_1. All of the substitutions of H, except those of G_1, must involve each of the letters $a_1, a_2, \ldots, a_\alpha$. Hence H is an intransitive group, and the components of its substitutions involving the letters $a_1, a_2, \ldots, a_\alpha$ must form a regular group. This regular group is a transitive constituent of H and the subgroup G_1, which is transformed into itself by H, corresponds to the identity of this transitive constituent. Let C_1 be the conjoint of this constituent, and consider the n/α transforms of C_1 under G.

A (1, 1) correspondence can be established between the substitutions of these n/α transforms such that each substitution is of degree n and is transformed into itself by G. To do this it is only necessary to regard as one substitution all the transforms of a single substitution of C_1. This proves a theorem due to H. W. Kuhn,* which is a generalization of Jordan's theorem and may be stated as follows:

A necessary and sufficient condition that there are α substitutions on the letters of a transitive group; which are commutative with every substitution of the group, is that its subgroup which is composed of all its substitutions which omit one letter omits exactly α letters.

If G_1 is of degree $n-1$, the identity is therefore the only substitution on these n letters which is commutative with every substitution of G, as is also otherwise evident.

* *American Journal of Mathematics*, vol. 26 (1904), p. 67.

EXERCISES

1. Every transitive group of degree n involves at least $n-1$ substitutions which separately involve all the letters of the group; if it contains also substitutions of degree $n-\alpha$, $1<\alpha<n$, it must contain more than $n-1$ substitutions of degree n.

Suggestion. The average number of letters in the substitutions is $n-1$.

2. If all the substitutions which omit a given letter of a transitive group of degree n constitute a group of degree $n-1$, then the n conjugates of the latter are transformed under the transitive group in exactly the same way as its letters are transformed.

3. A transitive group composed of invariant substitutions is necessarily regular.

4. If the order of a transitive group is p^m, p being a prime number, the subgroup composed of all its substitutions which omit a given letter omits p^{m_0} letters, where $m_0>0$.

5. All the substitutions of highest degree (n) in any transitive group generate a transitive group of degree n, which either coincides with the original group or differs from it merely with regard to substitutions of degree $n-1$.

Suggestion. Use the theorem that the average number of letters in all the substitutions of a transitive group of degree n is $n-1$, while in an intransitive group this number is smaller.

6. The total number of the substitutions which are conjugate to a given substitution of a group must generate either the entire group or an invariant subgroup. This theorem remains true if the word conjugate is replaced by the word similar.

7. The number of the substitutions of degree p^β and of order p in the symmetric group of degree n is prime to p whenever p^β is the highest power of p which does not exceed n. Cf. *Annals of Mathematics*, vol. 16 (1915), p. 169.

15. Primitive and Imprimitive Groups. When the subgroup G_1, composed of all the substitutions of a transitive group G which omit a given letter, is of degree $n-\alpha$, n being the degree of G, we have seen that the letters of G may be divided into n/α sets, each set involving α distinct letters, such that these sets are transformed as units by all the substitutions of G. Such a substitution group is said to be *imprimitive* whenever $\alpha>1$, and the sets of α letters are called its *systems of imprimitivity*. These systems of imprimitivity are transformed under G according to a transitive group which has a

$(1, m)$ correspondence with G. If $m>1$, G must therefore contain an invariant subgroup of order m which transforms each of these systems of imprimitivity into itself. If $m=1$, each substitution of G, besides the identity, must transform at least one of these systems of imprimitivity into another.

While every transitive group whose G_1 omits more than one letter is necessarily imprimitive, it does not follow that the G_1 of an imprimitive group must omit more than one letter. We proceed to prove that *a necessary and sufficient condition that G is imprimitive is that G_1 is contained in a larger subgroup of G.* In other words, a necessary and sufficient condition that G is imprimitive is that G_1 is a *non-maximal* subgroup of G. It should be observed that this theorem connects the theory of imprimitivity with the theory of abstract groups. Every transitive substitution group which is not imprimitive is said to be primitive.

The given theorem is contained in a more general theorem which may be stated as follows: *A necessary and sufficient condition that a complete set of conjugate substitutions or subgroups of G is transformed under G according to an imprimitive substitution group is that the largest subgroup of G which transforms into itself one of these substitutions or subgroups is contained in a larger subgroup of G.* That this condition is sufficient results from the fact that if this largest subgroup K, which transforms into itself a substitution or subgroup L, is contained in a larger subgroup H, then the number of the conjugates of L under H is equal to the quotient obtained by dividing the order of H by the order of K, and H involves all the substitutions of G which transform these conjugates among themselves.

Every substitution of G which is not in H must therefore transform the set of conjugates of L under H into an entirely new set of conjugates, and therefore this set of conjugates is transformed as a unit. Hence all the conjugates of L can be divided into sets such that they are all transformed as units and such that no two sets have a common substitution or subgroup. On the other hand, if the complete set of conjugates

to which L belongs is transformed according to an imprimitive group there must be such a group as H which includes K, since all the substitutions which transform among themselves the substitutions or subgroups, corresponding to a system of imprimitivity, must constitute a group. Hence the given general theorem is established.

To deduce the special case relating to the primitivity of G when G_1 is of degree $n-1$, we have only to observe that a necessary and sufficient condition that G_1 is transformed into itself by only its own substitutions, is that its degree is $n-1$. As G transforms the conjugates of G_1 in exactly the same way as it transforms its letters, whenever the degree of G_1 is $n-1$, and as we assume in the present case that the degree of G_1 is exactly $n-1$, it results directly from the given theorem that G transforms the conjugates of G_1, and hence also its letters, according to a primitive group whenever G_1 is maximal, and only then.

If G_1 is a transitive group on $n-1$ letters, G is said to be *doubly transitive*, and every pair of letters of G is transformed into every other pair by the substitutions of G. In general, G is said to be *r-fold transitive*, whenever G_1 is $(r-1)$-fold transitive and of degree $n-1$. Since the order of a transitive group is always a multiple of its degree, it results that the order of an r-fold transitive group is a multiple of $n(n-1) \ldots (n-r+1)$. A group which is more than simply transitive is said to be *multiply transitive*. The alternating group of degree n is $(n-2)$-fold transitive and the symmetric group of degree n is said to be either n-fold or $(n-1)$-fold transitive. We shall generally say that this group is $(n-1)$-fold transitive. With the exception of the alternating and the symmetric groups no group is known which is more than five-fold transitive and only two such five-fold transitive groups are known. These groups are of degrees 12 and 24 respectively and were discovered by E. Mathieu in 1861. The theory of multiply transitive groups has not yet been extensively developed, and it seems to offer great difficulties.

EXERCISES

1. If all the substitutions of order m, $m>2$, in a group are conjugate, they must be transformed under the group according to an imprimitive group.

Suggestion: The generating substitutions of one cyclic subgroup are transformed into all of those of another.

2. If an imprimitive group contains substitutions besides the identity which do not interchange any of its systems of imprimitivity, in a given set of systems of imprimitivity, all such substitutions constitute an invariant subgroup.

3. Every regular group of composite order is imprimitive, and involves as many different sets of systems as it has subgroups, excluding the identity.

4. A transitive group of order p^α, p being a prime number and $\alpha>1$, is always imprimitive.

Suggestion: Consider its complete sets of congjuate substitutions and observe that each of these sets involves p^β distinct substitutions.

5. Every invariant subgroup besides the identity of a primitive group is transitive.

6. The total number of substitutions which are commutative with every substitution of the intransitive group obtained by establishing a simple isomorphism between n, $n>2$, symmetric groups of degree n, written in distinct sets of letters, constitute a conjugate intransitive group.

16. Groups Involving no More than Four Letters. The only possible substitution group on two letters is 1, ab. Since every system of intransitivity must involve at least two letters, a group of degree 3 is necessarily transitive. It is also included in $(abc)all$,* and hence its order is a divisor of 6. Therefore $(abc)all$ and (abc) are the only two possible groups of degree 3. If a group of degree 4 is intransitive, each of its two systems of intransitivity must be of degree 2. The largest intransitive group of degree 4 is therefore the direct product of (ab), (cd). The other possible intransitive group is a simple isomorphism between the substitutions of these transitive groups of degree 2. Hence *there are two and only two intransitive groups of degree* 4;

* The notation $(a_1a_2 \ldots a_n)all$ is used to represent the symmetric group of degree n, while $(a_1a_2 \ldots a_n)$ represents the group generated by the cyclic substitution $a_1a_2 \ldots a_n$. It should, however, be emphasized that the symbol $(a_1a_2 \ldots a_n)$ is also often employed to denote the substitution $a_1a_2 \ldots a_n$. Since there is no uniformity of usage along this line, the reader is frequently obliged to determine the meaning from the context.

one of these is of order 4 while the other is of order 2. Their substitutions are as follows:

$$1,\ ab,\ cd,\ ab\cdot cd;\ 1,\ ab\cdot cd.$$

According to Sylow's theorem, $(abcd)all$ involves at least one subgroup of order 8 and all its subgroups of this order are conjugate. Since all conjugate groups are regarded as identical in the enumeration of groups, there is one and only one substitution group of degree 4 and of order 8. This is known to be transitive (§ 2). We shall represent it by the symbol $(abcd)_8$. Since the order of every transitive group is a multiple of its degree, and since a group must be included in the symmetric group of its own degree, it results that the order of a transitive group of degree four is 4, 8, 12 or 24.

As there is one and only one such group of each of the orders 8 and 24, it remains to determine all the possible groups of orders 4 and 12. We know that there are two transitive groups of the former order; viz., the subgroups of the octic group considered in § 2, and there is one group of the latter order; viz., $(abcd)pos$.* We proceed to prove that no other groups of these orders are possible. Another transitive group of order 4 would also be regular, since the average number of letters in its substitutions is 3. It could not be cyclic, since there is one and only one cyclic group of each order, and two simply isomorphic regular groups are conjugate. If it were non-cyclic it would involve all the possible substitutions of the form $ab\cdot cd$ in the symmetric group of degree 4. This proves that there are only two regular groups of degree 4. One of these has three conjugates under the symmetric group while the other is invariant under this group.

To prove that there is only one group of order 12 and degree 4, we observe that every such group would have to contain a subgroup of order 3 according to Sylow's theorem. As all the subgroups of order 3 in $(abcd)all$ are conjugate, we may assume that every group of order 12 and degree 4 includes (abc). Since this subgroup could not be invariant under a tran-

* The symbol $(a_1a_2 \ldots a_n)pos$ represents the alternating group of degree n.

sitive group of degree 4, every group of this degree and of order 12 must involve the 4 subgroups of order 3 in $(abcd)all$, and hence it must be identical with $(abcd)pos$. That is, *there are exactly five transitive groups of degree* 4,—*one of each of the orders* 24, 12, 8, *and two of order* 4. Each of these possible transitive groups has at least two substitutions in common with the non-cyclic regular group.

It has been observed that $(abcd)pos$ cannot involve a subgroup of order 6, since its Sylow subgroups of order 3 are transformed into themselves by their own substitutions only under $(abcd)pos$. We have here an instance where a group whose order is divisible by 6 does not contain a group of order 6. That is, while the order of every subgroup is a divisor of the order of the group *there is not neccessarily a subgroup for each divisor of the order of a group*. The ten groups whose degrees do not exceed 4 may be represented as follows: *

$$(ab),\ (abc)all,\ (abc),\ (abcd)all,\ (abcd)pos,$$
$$(abcd)_8,\ (abcd),\ (abcd)_4,\ (ab)(cd),\ (ab\cdot cd).$$

17. Simplicity of the Alternating Group of Degree n, $n \neq 4$. If a group does not contain any invariant subgroup besides the identity it is said to be a *simple group*. All other groups are said to be *composite*. We proceed to prove that the alternating group is simple except when its degree is 4. Suppose that s_1, s_2 are two cyclic substitutions of order greater than 2, such that one can be obtained from the other by interchanging two adjacent letters. That is,

$$s_1 = \ldots a_\gamma a_\alpha a_\beta \ldots, \quad s_2 = \ldots a_\gamma a_\beta a_\alpha \ldots$$

Hence $s_1 s_2^{-1} = a_\alpha a_\gamma a_\beta$. That is, *if the order of a substitution exceeds* 2 *it is always possible to find another substitution similar to it such that the product of the two is a cycle of order* 3. By means of this elementary theorem and the fact that every posi-

* A fundamental problem of substitution groups is the determination of all the substitution groups of degree n. This problem has been completely solved when n does not exceed 11. The noted French mathematician A. L. Cauchy was the first to do serious work along this line; Paris *Comptes Rendus*, vol. 21 (1845), p. 1363.

tive substitution is the product of cycles of order 3, it is easy to prove that every alternating group whose degree exceeds 4 is simple.

Assume that G is the alternating group of degree n, $n>4$, and that it involves an invariant subgroup H. As H involves all the substitutions of G, which are conjugate with any one of its substitutions under G, it cannot involve any substitutions of order 2 without also containing substitutions whose orders exceed 2. This results immediately from the fact that the positive substitution $ab\cdot cd$ . . . of order 2 is transformed by bde into a substitution which is not commutative with it, and hence the product of these two substitutions has an order which exceeds 2. If H is not the identity, it must therefore involve either substitutions of an odd prime order, or substitutions involving cycles of even order greater than 2. As the cyclic groups generated by such substitutions are evidently transformed into themselves by negative substitutions, these cyclic groups are transformed into all their conjugates under the symmetric group of degree n by substitutions of G. That is, H must involve all these conjugates, and hence it must involve all the substitutions of the form abc in G. In other words, H coincides with G whenever it exceeds the identity. This proves the important theorem: *the alternating group of degree n is simple whenever* $n>4$.

The alternating group of degree 3 is evidently simple, but the alternating group of degree 4 contains 1, $ab\cdot cd$, $ac\cdot bd$, $ad\cdot bc$ as an invariant subgroup, as was observed above. Hence every alternating group, with the exception of the alternating group of degree 4, is simple. In this special case the alternating group contains a group of order 4 as an invariant subgroup. From what precedes, it results immediately that the symmetric group of degree n contains only one subgroup of order $n!/2$. If it contained two such subgroups, one would contain only $n!/4$ positive substitutions, and these would constitute a subgroup of the alternating group. This is impossible, since such a subgroup would contain all the substitutions of odd order and hence all the substitutions of the form abc.

18. Groups of Degree Five. The intransitive groups on five letters must involve transitive constituents of degrees 3 and 2, and hence all of them are contained in the direct product of $(abc)all$, (de). Consequently there are three such groups—one of order 12 and two of order 6. They may be represented as follows:

$$(abc)all(de),\ (abc)(de),\ \{(abc)all(de)\}pos.$$

All the transitive groups of degree 5 are primitive, and they involve either only one, or six subgroups of order 5. As these six groups must generate the alternating group, according to the preceding section, it follows that the alternating and the symmetric groups of degree 5 are the only ones which involve six subgroups of order 5. If such a group contains only one subgroup of order 5, its order divides 20, since a generating substitution of the subgroup of order 5 is transformed into itself by only five substitutions on these 5 letters. We may evidently suppose that each of the possible groups involves the same subgroup of order 5 since all these subgroups are conjugate. Hence there is only one such group of each of the orders 20, 10, 5. The five transitive groups of degree 5 may be represented as follows:

$$(abcde),\ (abcde)_{10},\ (abcde)_{20},\ (abcde)pos,\ (abcde)all.$$

The group $(abcde)pos$ is especially interesting since it is the simple group which has the smallest possible composite order. This group is simply isomorphic with the total number of movements which transform the icosahedron into itself, as we shall see later, and hence it is frequently called the *icosahedron group*. Galois was the first to observe that it is simple, and he also observed that it is the smallest simple group of composite order. Sir W. R. Hamilton observed, in 1856, that this group may be defined abstractly as the group generated by two substitutions of orders 2 and 3 respectively whose product is of order 5. That is, every pair of substitutions which satisfy these conditions generates a group of order 60, which is simply isomorphic with $(abcde)pos$.

19. Holomorph of a Regular Group. If G is a regular group of order n, all the substitutions on these n letters which transform G into itself constitute a group which has been called the *holomorph* * of G. For instance, the symmetric group of degree 3 is the holomorph of its subgroup of order 3, $(abcd)_8$ is the holomorph of $(abcd)$, and $(abcde)_{20}$ is the holomorph of $(abcde)$. The holomorph of G includes the conjoint of G, and hence it is also the holomorph of this conjoint. If this conjoint is not identical with G, it is conjugate with G under a substitution of order 2 which transforms the holomorph of G into itself. This substitution and G generate a group known as the *double holomorph* of G. Every non-abelian group has a double holomorph.

Since the holomorph K of G involves exactly n substitutions which are commutative with every substitution of G, it must transform the substitutions of G in k/n different ways, k being the order of K. The largest subgroup of degree $n-1$ contained in K must also transform the substitutions of G in k/n different ways. This subgroup is known as the *group of isomorphisms* of G.† Hence *the order of the holomorph of a group is the product of the order of the group and the order of its group of isomorphisms.* Since any two simply isomorphic regular groups are conjugate, the group of isomorphisms of G transforms G into every possible simple isomorphism with itself. That is, it transforms it into all its possible *automorphisms.*

If a group involves substitutions which transform it into every possible automorphism, but does not contain any invariant substitution besides the identity, it is said to be a *complete group.* The symmetric group of degree 3 is evidently a complete group. The holomorph of a complete group is the product of the group and its conjoint. It is easy to prove that the

* The concept of holomorph was used by many early writers, but the term was introduced by W. Burnside in the first edition of his Theory of Groups, 1897, p. 228.

† The statement relating to this matter in the *Encyklopädie der Mathematischen Wissenschaften*, vol. 1, p. 221, note 103, is inaccurate. The group of isomorphisms is one of the most important and also one of the most far-reaching concepts in group theory.

symmetric group of degree 4 is also complete. In fact, this group is generated by any two of its cyclic subgroups of order 4. One of the generators of such a cyclic group can be selected in six different ways, and after it has been selected, a generator of the second cyclic group can be selected in four different ways. The two generators can therefore be selected in 24 different ways. Since *(abcd)all* contains no invariant substitution besides the identity, it must transform its own substitutions in these 24 possible different ways. Hence the holomorph of *(abcd)all* is the direct product of this group and its conjoint. The order of this holomorph is therefore 576.

EXERCISES

1. The symmetric group of degree n does not contain any subgroup of index ρ, if ρ is greater than 2 but less than the largest prime factor of n. (Cauchy, 1815.)

Suggestion: Such a subgroup could not involve all the substitutions whose order is this prime factor, since these substitutions would generate the alternating group.

2. Prove that the symmetric group of degree n is generated by a cyclic substitution of degree $n-1$ and a transposition which connects any one of these letters with the remaining letter.

3. The group of order 48 on $x_1, \ldots, x_6$, which transforms the function $x_1x_2+x_3x_4+x_5x_6$ into itself is imprimitive and involves an invariant subgroup of order 8.

4. The polynomial $(x_1+\omega x_2+\omega^2 x_3+ \ldots +\omega^{r-1}x_r)^r$ is transformed into itself by the cyclic group of order r on these variables, if ω represents a number whose powers give all the rth roots of unity.

Suggestion: If we multiply the polynomial within the parenthesis, which is known as the Lagrangian resolvent, by a power of ω, we interchange the variables cyclically.

5. Construct all the possible substitution groups that can be represented on six letters. Cf. *American Journal of Mathematics*, vol. 21 (1899), page 327.

20. Class of a Substitution Group. A substitution group G of degree n is said to be of class $n-\alpha$, $\alpha<n$, if it contains at least one substitution of degree $n-\alpha$ but does not contain any substitutions besides the identity whose degree is less than $n-\alpha$. For instance, every symmetric group is of class 2 while every alternating group is of class 3. It is easy to prove that

these two infinite systems are composed of all the possible primitive groups which are of class 2 and class 3 respectively. A substitution which actually contains exactly k letters is sometimes said to be of *class k*.

To prove that a primitive group G which is of class 2 and of degree n is symmetric, it is only necessary to observe that such a group contains at least two transpositions having a letter in common, otherwise G would be imprimitive. Hence G involves the symmetric group of degree 3. It must therefore contain two such symmetric groups which have two letters in common. Hence G contains the symmetric group of degree 4. By continuing this process, it results that G is the symmetric group of degree n. In exactly the same manner, it can be proved that if a primitive group of degree n contains a substitution of the form abc it includes the alternating group of degree n. That is, *if a primitive substitution group involves a transposition it is a symmetric group, and if it involves a substitution of the form abc without also involving a transposition, it is an alternating group.*

Suppose that G is a primitive group which contains a substitution of degree and of order p, $p>3$, and that G is of degree n, $n>p$, p being a prime number. There must be at least two substitutions in G which are of degree and of order p, and which have some but not all their letters in common. Let s_1 and s_2 be two such substitutions. If s_2 involves more than one letter which is not also contained in s_1, there is some power of s_1 in which two such letters are adjacent. The transform of s_1 by this power will then be a substitution which has more letters in common with s_1 than s_2 has; but this transform involves at least one letter which is not contained in s_1. Hence we may assume that G contains two substitutions of degree p and of order p such that these substitutions contain exactly $p-1$ common letters. These two substitutions generate a doubly transitive group of degree $p+1$. By continuing these considerations it results that *if a primitive group of degree n contains a substitution of degree p and of order p, p being any prime number, this primitive group is at least* $(n-p+1)$*-fold transitive.*

It is now easy to prove that a primitive group of class p, $p>3$, cannot have a degree which exceeds $p+2$. In fact, if such a group were of degree $p+3$, it would be at least four-fold, or four times, transitive. Since any set of four letters of such a group can be replaced by an arbitrary set of four letters, it results that any four times transitive group must involve an intransitive subgroup H which has the symmetric group of degree 3 for one constituent, and a transitive group on the remaining letters for the other constituent. In the present case the latter group is of degree p.

In any transitive group of degree p, the subgroups of order p generate a simple group, since an invariant subgroup of a primitive group is transitive. If this simple group is not the entire group, it must be invariant under the entire group and the corresponding quotient group must be cyclic, since it is a subgroup of the group of isomorphisms of a group of order p, and this group of isomorphisms is cyclic, since p has primitive roots. Hence it results that H includes substitutions of the form abc whenever G is of degree $p+3$, since its transitive constituent of degree p cannot give rise to a quotient group which is simply isomorphic with the symmetric group of degree 3 when $p>3$. That is, *if a primitive group is of class p, p being a prime number greater than* 3, *the degree of this primitive group is at most* $p+2$.

There is evidently one and only one primitive group of degree p and of class p; viz., the group of order p. In order that a primitive group of degree $p+1$ be of class p, it is clearly necessary that this group be of order $p(p+1)$, and that it contain $(p+1)(p-1)$ substitutions of order p. Hence $p+1$ must be of the form 2^m, and if $p+1$ is of this form there is one and only one such group. A primitive group of degree $p+2$ which is of class p must therefore include this primitive group of degree $p+1$. It must also contain a substitution of order 2 and of degree $p+1$ which transforms into its inverse one of the substitutions of order p in this group of degree $p+1$. Hence there cannot be more than one primitive group of degree $p+2$ and of class p.

The fact that this primitive group actually exists was proved by C. Jordan,* but we shall not give the proof here. We have, however, established the following theorem:

When the prime number p, $p>3$, is not of the form 2^n-1 there is one and only one primitive group of class p. When p is of the form 2^n-1 there cannot be more than three primitive groups of class p.

The study of primitive substitution groups by means of their classes was begun by C. Jordan, who proved that there is a finite number of such groups of every class. In recent years W. A. Manning has contributed new theorems on this interesting but difficult subject.†

EXERCISES

1. If a primitive substitution group contains two transitive subgroups which can be transformed into each other by a transposition, the primitive group is alternating or symmetric.

2. Prove that the two substitutions $abe\cdot cdf$ and $ag\cdot bf$ generate a group of order 168, and that this group is simple.

3. It is known that the simple group of order 504 can be represented as a transitive substitution group on 9 letters. Hence prove that it contains the abelian group of order 8 which is composed of seven substitutions of order 2 and the identity.

* *Journal de Mathématiques* (2), vol. 17 (1872), p. 351.

† W. A. Manning, *Transactions of the American Mathematical Society*, vol. 11 (1912), p. 375.

CHAPTER III

FUNDAMENTAL DEFINITIONS AND THEOREMS OF ABSTRACT GROUPS

21. Introduction. In the preceding chapters we gave several examples of groups which were either in the form of substitution groups or could readily be associated with such groups. Some of the fundamental theorems of substitution groups were also developed. As the theory of groups is applicable to many different subjects, it became a matter of economy of thought to develop and to state the main theorems of this theory in a language which is common to these various subjects. The efforts to accomplish this end led gradually to what is known as abstract group theory.

Many of the theorems proved in the preceding chapter can be used directly in the theory of abstract groups. In fact, we shall find that the theory of substitutions is a very useful means to study the abstract properties of groups. It has already been observed, § 15, that the question of primitivity and imprimitivity of a substitution group has an abstract meaning, even if these terms apparently relate only to the notation of substitution groups.

Some of the definitions used in the theory of substitution groups are not directly available for the study of abstract groups, and hence it will be necessary to re-define some of the terms used in the preceding chapter. This is due to the fact that substitutions have inherent properties. For instance, the associative law is always satisfied when substitutions are multiplied, and hence we did not need to specify this law in defining a substitution group. On the contrary, this law should be included in a definition of an abstract group.

22. Definition of an Abstract Group and a Few Properties of its Elements. In the theory of finite abstract groups we deal with a set of distinct symbols $G \equiv s_1, s_2, \ldots, s_g$, and we assume that any two of them can be combined according to some law which is called *multiplication*, and which is denoted in the same way as multiplication is commonly denoted. This set of symbols represents a *group* provided the symbols satisfy the following conditions:

1. If any two of the three symbols in an equation of the form

$$s_\alpha s_\beta = s_\gamma$$

are contained in G, then the third is also contained in G, and it is completely determined by this equation. It is assumed that this statement includes the case when the two symbols which are contained in G are identically equal to each other.

2. The symbols of G obey the associative law. That is,

$$(s_\alpha s_\beta) s_\gamma = s_\alpha (s_\beta s_\gamma).$$

From the former of these conditions it results that if one of the three symbols in

$$s_\alpha s_\beta = s_\gamma$$

remains fixed while another assumes successively all the values of the symbols or *elements* of G, the third will also run through all these elements. In particular, there must be an element s_1 such that

$$s_1 s_\beta = s_\beta.$$

Such an element is called the left-hand identity of s_β. This left-hand identity is the same for all the elements of G. To see this fact we multiply the last equation on the right by s_γ, and then let s_γ run through all the elements of G. In exactly the same way it may be observed that G contains only one right-hand identity s_1'.

To prove that $s_1' = s_1$ it may be observed that if we replace s_β by s_1' in the last equation it results that

$$s_1 s_1' = s_1'.$$

Similarly, by letting $s_\alpha = s_1$ in the following equation

$$s_\alpha s_1' = s_\alpha$$

it results that

$$s_1 s_1' = s_1.$$

That is, $s_1 = s_1'$; in other words, *every group contains one and only one element which does not alter the value of any element when it is used as a multiplier on the right or on the left. This element is called the identity of the group, and it is denoted by the symbol* 1. Every other element changes *all* the elements into which or by which it is multiplied.

Since g is finite there must be some finite power of s_α ($\alpha = 1, 2, \ldots, g$) which is equal to some other power of this element. That is, the series

$$s_\alpha,\ s_\alpha^2,\ s_\alpha^3,\ \ldots,\ s_\alpha^n\ *$$

must involve a term which is equal to a preceding term when n is taken sufficiently large. Let s_α^r be the lowest power of s_α which satisfies the equation

$$s_\alpha^r = s_\alpha^{r-k}, \text{ or } s_\alpha^{r+k} = s_\alpha^r,\ 0 < k < r.$$

Since

$$s_\alpha^r s_\alpha^k = s_\alpha^r$$

and since G involves only one identity, it results that $s_\alpha^k = 1 = s_\alpha^0$. That is, the lowest power of s_α which is equal to a lower power occurs after the identity appeared in the series of successive positive powers. On the other hand, since

$$s_\alpha^{k+1} = s_\alpha$$

it results that $r = k+1$. That is, *the first power which is equal to a lower power in a series of successive powers of an element is the one following the identity in this series.* Hence the series is periodic and the number of different elements in each period is k. This number is called the *order* or *period* of s.

Two powers of s_α whose exponents are of the form $l+mk$ are equivalent whenever m is any positive integer or zero. Negative exponents are introduced by assuming that this

* The symbol s_α^n indicates the product $s_\alpha \cdot s_\alpha \cdot s_\alpha \ldots$ taken n times as a factor; s_α^0 is defined as equal to the identity.

equivalence remains true when m is any negative integer. In particular, two elements of G which satisfy the equation

$$s_\alpha s_\beta = 1$$

are said to be the *inverses of each other*, and $s_\beta = s_\alpha^{k-1}$ is denoted by s_α^{-1}. Elements of order 2 are their own inverses; but all other elements, besides the identity, go in pairs, composed of an element and its inverse. In particular, *every possible group contains an even number of elements, which may be zero, of every order which exceeds* 2.

Since

$$s_\alpha s_\beta \ldots s_\lambda \cdot s_\lambda^{-1} \ldots s_\beta^{-1} s_\alpha^{-1} = 1,$$

it results that the inverse of $s_\alpha s_\beta \ldots s_\lambda$ is $s_\lambda^{-1} \ldots s_\beta^{-1} s_\alpha^{-1}$, and that

$$(s_\alpha s_\beta \ldots s_\lambda)^{-1} = (s_\lambda^{-1} \ldots s_\beta^{-1} s_\alpha^{-1})^1.$$

If all of the elements $s_\alpha, s_\beta, \ldots, s_\lambda$ are of order 2, then

$$(s_\alpha s_\beta \ldots s_\lambda)^{-1} = s_\lambda \ldots s_\beta s_\alpha.$$

In particular, *if the product of two elements, s_α, s_β of order* 2 *is also of order* 2 *the elements are commutative,* that is $s_\alpha s_\beta = s_\beta s_\alpha$.

If the elements $s_\alpha, s_\alpha^2, \ldots, s_\alpha^k = 1$ do not include all the elements of G, they represent a subgroup of G. By exactly the same arguments as were used to prove that the order of a substitution group is divisible by the order of each of its subgroups (§ 9), it can be proved that the order of an abstract group is divisible by the order of each one of its subgroups. Hence it results that k is a divisor of g.

23. The Cyclic Group.* By definition the cyclic group is generated by a single element, and every group which can be generated by a single element is cyclic. If the order of such a group is g, it contains at least one element s of the order g. The order of s^m, m being an arbitrary positive integer, is g/d, d being the greatest common divisor of m and g. If $\phi(g)$ repre-

* Many of the results of this section can be deduced from properties of the n roots of unity. In fact, these n roots form a cyclic group with respect to multiplication.

sents, as usual, the number of natural numbers prime to g and not greater than g, then G involves exactly $\phi(g)$ elements of order g, and hence it involves $\phi(g)$ generators. All cyclic groups of the same order are simply isomorphic, and hence we shall say *there is one and only one cyclic group whose order is an arbitrary natural number.* This group of order g may be represented by the g gth roots of unity, when they are combined by multiplication.

If m is prime to g, then s^m generates s; that is, *every element is generated by any one of its powers whose index is prime to the order of the element.* This theorem is included in the statement that if k is any number such that the highest common factor of g and k is d, then will s^k generate the cyclic subgroup of order g/d, which is also generated by s^d. It should be observed that a necessary and sufficient condition that two elements of G generate each other is that they have the same order, and a necessary and sufficient condition that one of these elements generates the other is that the order of the former is divisible by that of the latter.

Let t be an element of any group such that t^m is of order n. If all the prime factors of m are also in n, it results from this that the order of t is equal to mn. In general, the given condition implies that the order of t is a divisor of mn and a multiple of $m'n$, where m' is the quotient obtained by dividing m by its largest factor that is prime to n. By means of substitutions it is easy to show that t may be so determined that its order is any arbitrary multiple of $m'n$ that divides mn, whenever the only restriction on t is that the order of t^m is n.

If k is any divisor of g, so that $kh=g$, there must be at least one subgroup of order k in the cyclic group G. This contains $\phi(k)$ generators. The theorem that G cannot contain more than one subgroup of order k results immediately from the fact that the elements of such a subgroup must be as follows:

$$s^h,\ s^{2h},\ \ldots,\ s^{kh}=1$$

since their kth powers are equal to the identity. Hence *a cyclic group contains one and only one subgroup whose order is any*

given divisor of the order of the group. In particular, every subgroup of a cyclic group is cyclic.

When g is even, G contains an element of order 2, and every element of G which is the square of another element of G is the square of exactly two such elements. When g is odd, every element of G is the square of only one element of G. In general, the kth powers of all the elements of G are the elements of a group G' whose order g' is the quotient obtained by dividing g by the highest common factor h of g and k. Each element of G' is the kth power of exactly h elements of G. The continued product of all the elements of G is of order 2 or the identity according as g is even or odd.

If g is the product of two numbers which are relatively prime, then G is the product of two cyclic subgroups whose orders are these two numbers, and the number of elements of highest order in G is the product of the numbers of the elements of highest orders in these two cyclic subgroups. This is equivalent to the well-known formula that $\phi(m)=\phi(m_1)\phi(m_2)$, whenever m_1, m_2 are relatively prime and $m_1m_2=m$. The determination of all the subgroups of G is equivalent to the determination of all the factors of g. If g be written in the form $g=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_\rho^{\alpha_\rho}$, p_1, p_2, . . ., p_ρ being distinct primes, the number of subgroups of G, including the identity, must therefore be

$$(\alpha_1+1)(\alpha_2+1)\ \ldots\ (\alpha_\rho+1)-1.$$

Since each element of a group generates a cyclic group, it is clear that cyclic groups are of fundamental importance. When g is a prime number p, every element of G besides the identity generates G, and hence this G does not involve any subgroup besides the identity. The cyclic group of order p is therefore the only possible group of this order. That is, while there is one and only one cyclic group of every possible order, there are orders for which no non-cyclic group exists. These orders include all prime numbers. The smallest composite number which is not the order of any non-cyclic group is 15 (cf. Ex. 3, § 11). This is a special case of the theorem (which will be proved in § 70) that two necessary and sufficient

conditions that there is only one group of order g are that g is not divisible by the square of a prime number and that none of its prime factors is a divisor of the number obtained by diminishing by unity another such factor.

EXERCISES

1. Prove that the 8 natural numbers which are less than 15 and prime to 15 constitute a group with respect to multiplication (mod 15), which is not simply isomorphic with the group formed similarly by the numbers which are less than 24 and prime to 24.

2. The smallest group of multiplication which involves the two matrices

$$\begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}$$

is of order 8. Is this group simply isomorphic with either of the groups of Exercise 1? Find the six other matrices of this group.

3. To which of the three groups of the preceding exercises is the group of movements of the square simply isomorphic? To which is the group formed by the 8 numbers less than 20 and prime to 20, with respect to multiplication (mod 20), simply isomorphic?

4. Find two groups whose product is the cyclic group of order 36, and determine the number of elements of each order in this group.

5. Including the identity there are five complete sets of conjugate elements in the group of movements of the square. Determine the elements of each of these sets.

6. Do the numbers 2, 4, 6, 8 form a group with respect to multiplication (mod 10)? If so, is this group simply isomorphic with the group formed by 1, -1, $\sqrt{-1}$, $-\sqrt{-1}$? Which of the four numbers 2, 4, 6, 8 corresponds to the identity?

7. If s^6 is of order 2 find two substitutions of orders 12 and 4 respectively which may be used for s.

8. Give the orders of all the possible cyclic groups having only two distinct generators.

24. Properties of Transforms. In § 9 we considered the transform of a substitution. As the concept of transforming is very useful we shall develop the properties of this operation more fully at this place. Suppose that

$$s^{-1}ts = t^{\alpha}.$$

By raising each member of this equation to the βth power there results the equation

$$s^{-1}t^{\beta}s = t^{\alpha\beta} = (t^{\beta})^{\alpha}.$$

Hence the theorem: *if an element transforms a generator of a cyclic group into its* αth *power it transforms every element of this cyclic group into its* αth *power.*

From the first equation we can also deduce the equation

$$s^{-\beta}ts^{\beta} = t^{\alpha^{\beta}}.$$

Since an element and its transform are of the same order, it is necessary that α be prime to the order k of t. Hence t^{α} generates t, and from Euler's generalization of Fermat's theorem it results that if m is the lowest power of α such that

$$\alpha^{m} \equiv 1 (\text{mod } k)$$

then m is a divisor of $\phi(k)$. Since s^{m} is the lowest power of s which is commutative with t, it follows that m divides the order of s. For instance, an element of order 3 could not transform an element of order 5 into any power of itself, except the first power, since the numbers 2, 3, 4 belong to the exponents 4, 4, 2 respectively modulo 5.

If we form the successive transforms

$$s^{-1}t_0s = t_1, \quad s^{-1}t_1s = t_2, \quad \ldots, \quad s^{-1}t_{n-1}s = t_n,$$

it results that for a sufficiently large value of n we have

$$t_n = t_k, \quad k < n$$

since the order of s is finite. This implies that $t_{n+\alpha} = t_{k+\alpha}$, α being any positive integer, and if n is the smallest subscript for which this relation is true then $k = 0$. That is, the transforms

$$t_1, \quad t_2, \quad \ldots, \quad t_{n-1}, \quad t_0$$

repeat themselves in the given order if the powers of s transform t_0 into n distinct elements. Since

$$s^{-n}t_0s^{n} = t_0$$

it results that n must divide the order of s. If this order is a prime number p, n is either 1 or p. That is, *if* s *is not com-*

mutative with t it transforms t into n distinct elements where n divides the order of s; whenever this order is a prime number, n is equal to the same prime.

Instead of transforming t_0 by the different powers of s we may transform it by all the elements of a group G. If this is done, there results a set of elements, each of which has the same order, and each is transformed into all the others by the elements of G. This set is called a complete set of conjugates of t_0 under G. In particular, *all the elements of G can be separated into distinct complete sets of conjugates as regards G, and this separation can be performed in only one manner.* The elements of G which transform t_0 into itself form a subgroup of G, and the number of the elements in the complete set of conjugates to which t_0 belongs is equal to the order of G divided by the order of this subgroup.

By transforming all the elements of a group G by the same element t there results a group which is simply isomorphic with G, since we obtain a (1, 1) correspondence by making each element correspond to its transform with respect to t. If t transforms G into itself the resulting simple isomorphism is an automorphism of G.

25. Construction of Groups with Invariant Subgroups. Let $s_1, s_2, \ldots, s_\varrho \equiv G$ be any group and suppose that t transforms all the elements of G into elements of G (i.e., t transforms G into itself), and that t^γ is the lowest power of t which occurs in G. The following rectangle

$$\begin{array}{llll} 1, & s_2, & \ldots, & s_\varrho \\ t, & s_2 t, & \ldots, & s_\varrho t \\ \ldots & \ldots & \ldots & \ldots \\ t^{\gamma-1}, & s_2 t^{\gamma-1}, & \ldots, & s_\varrho t^{\gamma-1} \end{array}$$

is composed of distinct elements since t^δ cannot be an element of the form $s_\alpha t^{\delta_1}$, where $\delta_1 < \delta < \gamma$, and all the elements of a row are distinct from each other and also from the elements of each of the preceding rows.

In order to prove that the elements of this rectangle represent a group, it remains only to show that no additional element

can be obtained by combining the elements in every possible manner. This fact results from the equation

$$s_\alpha t^\beta s_\gamma t^{\delta_1} = s_\alpha t^\beta s_\gamma t^{-\beta} t^{\delta_1+\beta} = s_\epsilon t^{\delta_2}.$$

Hence the theorem: *If t transforms a group G into itself and if t^δ is the lowest power of t which occurs in G, then t and G generate a group whose order is δ times the order of G.* This theorem is very useful in the construction of groups.

The theorem which has just been proved can be readily extended by replacing the cyclic group generated by t by any group H. It has been observed that all the common elements of G and H constitute a subgroup of both of these groups, viz., the cross-cut of G and H. By replacing the first column of the given rectangle by elements from the different co-sets of H as regards this cross-cut, we arrive at a more general theorem which may be stated as follows: *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 cross-cut of G and H.* It is easy to verify that all the elements of the group generated by G and H transform G into itself. Hence G is an invariant subgroup of this group.

It was observed in § 10 that when $1, s_2, s_3, \ldots, s_\gamma$ is a subgroup of the group G it is always possible to arrange all the elements of G in both of the following ways so that no element is repeated:

$$\begin{array}{llll} 1, & s_2, & s_3, & \ldots, s_\gamma \\ t_2, & s_2t_2, & s_3t_2, & \ldots, s_\gamma t_2 \\ \cdot & \cdot & \cdot & \cdot \\ t_\lambda, & s_2t_\lambda, & s_3t_\lambda, & \ldots, s_\gamma t_\lambda \end{array} \qquad \begin{array}{llll} 1, & s_2, & s_3, & \ldots, s_\gamma \\ t_2, & t_2s_2, & t_2s_3, & \ldots, t_2s_\gamma \\ \cdot & \cdot & \cdot & \cdot \\ t_\lambda, & t_\lambda s_2, & t_\lambda s_3, & \ldots, t_\lambda s_\gamma \end{array}$$

In these arrangements the elements of the first column do not necessarily constitute a group. By interchanging rows and columns it becomes evident that such an arrangement is possible when the elements of the first row do not form a group.

The question arises whether all the elements of G can be arranged in the given manner even when neither the first row nor the first column is a subgroup of G. That such an arrange-

ment is sometimes possible follows from the fact that when G is the symmetric group of degree 4, we may use for the first row the elements of any two Sylow subgroups of order 8, and for t_2 one of the substitutions of order 4 in the remaining Sylow subgroups of order 8. Hence the given rectangular arrangement does not always imply that either the first column or the first row is composed of the elements of a subgroup.

26. The Dihedral and the Dicyclic Groups. Let s_1 and s_2 represent any two elements of order 2. Their product s_1s_2 is transformed into its inverse by each of the elements s_1 and s_2. Each of the elements of the cyclic group generated by s_1s_2 is therefore transformed into its inverse by each of the two generators s_1 and s_2. In particular, this cyclic group is transformed into itself by each of these generators. Hence *two elements of order* 2 *generate a group whose order is twice the order of the product of these elements.* This group is called the *dihedral group.* When s_1s_2 is of order 2 the group generated by s_1 and s_2 is the non-cyclic group of order 4.

There is at least one dihedral group of every even order greater than 4, since the group of movements of the regular polygon of n sides is clearly such a group. Moreover, there is only one abstract dihedral group of order $2n$, $n>1$. In fact, if there were two such groups their cyclic subgroups of order n could be made simply isomorphic. Since each of the remaining elements of both groups would be of order 2 and would transform each element of this cyclic subgroup of order n into its inverse, any two of these remaining elements could also be made to correspond, and thus a simple isomorphism between the two groups could be established. Hence *there is one and only one dihedral group of every even order greater than* 2.

The fact that there is at least one dihedral group of order $2n$ can also be easily established by means of substitutions. In fact, if n is even we may let

$$s_1 = a_1a_2 \cdot a_3a_4 \cdot \ \ldots \ \cdot a_{n-1}a_n,$$

$$s_2 = a_2a_3 \cdot \ \ldots \ \cdot a_{n-2}a_{n-1}.$$

If n is odd, these substitutions can be selected as follows:

$$s_1 = a_1a_2 \cdot a_3a_4 \cdot \ \ldots \ \cdot a_{n-2}a_{n-1},$$

$$s_2 = a_2a_3 \cdot \ \ldots \ \cdot a_{n-3}a_{n-2} \cdot a_{n-1}a_n.$$

Since the product of s_1s_2 in each case is a cyclic substitution of order n it results that s_1 and s_2 generate the dihedral group of order $2n$.

The non-cyclic group of order 4 is the only dihedral group which does not involve non-commutative elements. A group which contains no non-commutative elements is called *commutative* or *abelian*. Since there is one cyclic group of every order and one dihedral group of every even order greater than 2, there must be at least two groups of every even order greater than 2. When this order exceeds 4 one of these two groups, whose existence has been proved here, is abelian while the other is non-abelian.

Instead of defining the dihedral group of order $2n$ as the group generated by two elements of order 2 whose product is of order n, it could also have been defined as the group generated by a cyclic group H of order n and an element of order 2 which transforms every element of H into its inverse. Both of these definitions of the dihedral group are very useful, If n is even we can find an element t of order 4 which transforms every element of H into its inverse and has its square in H. The group of order $2n$ generated by H and this t is called the *dicyclic* group whenever $n>2$, and there is one and only one such group of every order which is divisible by 4 and exceeds 4. The smallest dicyclic group is the group of order 8 generated by the four quaternion units 1, i, j, k. This is known as the *quaternion group*. Its properties were studied by W. R. Hamilton.

The fact that there is no more than one dicyclic group of a given order can be at once proved by proving that two such groups of the same order are simply isomorphic. The existence of this group for every even value of n may be proved by means of substitution groups as follows: Write a transitive dihedral group of order $2n$ on two distinct sets of letters and

establish a (1, 1) correspondence between the substitutions. Let t be a substitution of order 2 which is commutative with each substitution of this dihedral group and transforms the two systems of intransitivity into each other.

The required dicyclic group of order $2n$ may now be constructed by extending the cyclic subgroup of order n in the given dihedral group by means of a substitution of order 4 which is the continued product of t, one of two generating substitutions of order 2 of this dihedral group, and the substitution of order 2 which is generated by the cyclic group of order n in one of the two transitive constituents of this group. Hence *there exists one and only one dicyclic group of order* $4n$, *where* n *is any positive integer exceeding unity.*

Every dicyclic group is non-abelian. We have now established the existence of three distinct groups of every order which exceeds 4 and is divisible by 4. One of the fundamental problems of abstract group theory is a determination of all the possible groups of a given order. A considerable number of special cases have been solved, but the general solution of this problem seems to lie far beyond the present developments of this subject. As early as 1859 Cayley determined the five possible groups of order 8.

27. Representation of a Group as a Regular Substitution Group. Cayley's Theorem. We proceed to prove that every abstract group G of finite order can be represented as a regular substitution group. Let $G \equiv 1, s_2, \ldots, s_g$ and consider the square array of g^2 elements formed as follows:

$$\begin{array}{llll}
1, & s_2, & s_3, & \ldots, s_g \\
s_2, & s_2^2, & s_3 s_2, & \ldots, s_g s_2 \\
s_3, & s_2 s_3, & s_3^2, & \ldots, s_g s_3 \\
\cdot & \cdot & \cdot & \cdot \\
s_g, & s_2 s_g, & s_3 s_g, & \ldots, s_g^2
\end{array}$$

If we regard the substitutions by means of which each of these lines may be obtained from the first, we obtain a substitution group on g letters, and each substitution besides the identity involves all of these letters. As no two of these substitutions

are identical, this substitution group is of order g and it is simply isomorphic with G. Since each letter of this group is replaced once and only once by every other letter, the substitution group is regular. By combining these facts with those of § 14 there results the following theorem: *Every group of finite order can be represented as a regular substitution group, and two regular substitution groups which are simply isomorphic are also conjugate.**

The fact that every abstract group of finite order can be represented as a substitution group enables us to use, in the theory of abstract groups, all the theorems of substitution groups which are confined to group properties; for instance, the theorems relating to subgroups, quotient groups, sets of conjugates, etc. Many of these properties can, however, be studied to advantage from the standpoint of abstract groups, since we are thus led to fix our attention on the essentials and are not distracted by the notation. In some cases, on the contrary, this notation appears to be the simplest means to establish abstract properties. In fact, we shall see later that linear substitution groups also enable us to prove some important abstract group properties very readily.

From the fact that every group can be represented as a regular substitution group it is very easy to derive a simple proof of Sylow's theorem. This proof is as follows:

Let G be any group whose order g is divisible by p^α but not by $p^{\alpha+1}$, and represent G as a regular substitution group. Suppose that p^β is the highest power of p which is less than g, and that $g \neq p^\alpha$ since the case when g is a power of p does not require consideration, and consider all the possible substitutions on the g letters of G which are of degree p^β and of order p. Since G is transitive, it cannot transform any of these substi-

* This theorem is fundamental, as it reduces the study of abstract groups uniquely to that of regular substitution groups. The rectangular array by means of which it was proved is often called *Cayley's Table*, and it was used by Cayley in his first article on group theory, *Philosophical Magazine*, vol. 7 (1854), p. 40. The theorem may be called *Cayley's theorem*, and it might reasonably be regarded as third in order of importance, being preceded only by the theorems of Lagrange and Sylow.

tutions into itself. It must therefore transform all of them into complete sets of conjugates under G such that each of these sets is composed of more than one substitution. As the total number of these substitutions is prime to p, according to § 14, Ex. 7, at least one of these sets of conjugates involves a number m of substitutions, where m is prime to p.

Each of these m substitutions is transformed into itself by a subgroup of G whose order is g/m, where $m>1$. Hence G contains a subgroup whose order is divisible by p^α. If this subgroup is of order p^α, our theorem is established. If it is not of this order, we have reduced our problem to that of a smaller group whose order is divisible by p^α. In case Sylow's theorem were not universally true it would clearly be possible to find a smallest group G for which it would not be satisfied. As the preceding considerations establish the fact that such a smallest group does not exist, they constitute a proof of Sylow's theorem.

EXERCISES

1. If a group involves a subgroup whose order is one-half the order of the group this subgroup is invariant.

2. If the order of a group is pq, p and q being prime numbers and $p>q$, this group is cyclic unless $p-1$ is divisible by q. In the latter case there are exactly two groups of order pq.

3. Every simple group of composite order can be represented as a non-regular transitive substitution group.

Suggestion: Consider the substitutions according to which any complete set of conjugate substitutions or subgroups are transformed under the group.

4. There are exactly two abstract groups of order 4.*

Suggestion: Represent the possible groups as regular substitution groups.

* The non-cyclic group of order 4 is known under various names. Among these are the following: Axial group, four-group, fours group (Vierergruppe), quadratic group, anharmonic group, and group of the general rectangle. For the use of these terms, in order, the reader may consult the following: Pierpont, *Annals of Mathematics*, vol. 1 (1900), p. 140; Bolza, *American Journal of Mathematics*, vol. 13 (1891), p. 75; Bôcher, *Introduction to Higher Algebra*, 1907, p. 87; Burnside, *Theory of Groups of Finite Order*, 1912, p. 444; Capelli, *Istituzioni di analisi algebrica*, 1909, p. 111; Miller, *American Mathematical Monthly*, vol. 10 (1903), p. 217.

5. Every group of order p^2, p being any prime number, is abelian, and hence there are exactly two such groups for every prime.

Suggestion: If such a group is non-cyclic it contains $p+1$ subgroups of order p. These could not constitute a complete set of conjugates.

6. If the order of a group is the double of an odd number, the group contains an invariant subgroup of half its own order.

Suggestion: Write the group as a regular group and observe that it contains negative substitutions.

28. Invariant Subgroups and Quotient Groups. In § 13 we gave examples of invariant subgroups and of quotient groups as related to intransitive substitution groups. The term invariant subgroup was defined in § 9. Another but equivalent definition is based on the following considerations: If H is any subgroup of G, then G can be represented in either of the following two forms:

$$G \equiv H + Hs_2 + \ldots + Hs_\lambda$$
$$\equiv H + s_2^{-1}H + \ldots + s_\lambda^{-1}H.$$

The co-sets Hs_α, $\alpha = 2, \ldots, \lambda$, are called *right co-sets*, while those of the form $s_\alpha^{-1}H$ are called *left co-sets*. A necessary and sufficient condition that H is an invariant subgroup of G is that every right co-set of G as regards H is equal to some left co-set of G as regards H. If this condition is satisfied the totality of the left co-sets is identical with the totality of the right co-sets.

This theorem may be stated more generally as follows: A necessary and sufficient condition that H is invariant under the substitutions of the right co-set Hs_α is that $Hs_\alpha \equiv s_\alpha H$. When H is an invariant subgroup of G, the augmented co-sets of G as regards H may therefore be regarded as elements of a new group Q, H being the identity of Q.* This group Q is the quotient group G/H of G as regards H (cf. § 13).

There is an $(h, 1)$ isomorphism between G and Q, h being the order of H. When H is the identity this isomorphism reduces to a simple isomorphism, and G and Q are the same

* E. Galois first directed attention to the invariant subgroups and their important properties. The fact that each invariant subgroup gives rise to a quotient group is fundamental.

abstract group. Whenever $h>1$ the isomorphism is said to be multiple. The groups H and Q are called *complementary groups* as regards G, and the product of their orders is equal to the order of G. The fact that two different groups may have the same complementary groups results directly from the dihedral and the dicyclic groups.

Let q be any element of Q and let s be any one of the elements of the corresponding co-set. The order of s must be divisible by the order m of q, since s^m is the lowest power of s that occurs in H. If m is a power of a prime p then there is an element in the corresponding co-set whose order is also a power of p, since the group generated by H and this co-set must involve a larger subgroup whose order is a power of p than H does. Hence the theorem: *The order of any element of a quotient group divides the orders of all the elements of the corresponding co-set, and if this order is a power of a prime number the given co-set involves an element whose order is a power of the same prime.*

As a special case of this theorem it may be observed that every invariant subgroup of index 2 under any group includes all the elements of odd order contained in this group. Two elements which belong to the same co-set as regards an invariant subgroup are sometimes called *equivalent* with respect to this invariant subgroup. They are also said to be *congruent* with respect to this invariant subgroup as a modulus. It should be observed that an invariant subgroup has many of the properties of a modulus in elementary number theory. To a smaller extent these properties belong to all subgroups, and the terms equivalent and congruent are sometimes used in connection with any subgroup.

From the separation of the elements of a group into co-sets it results directly that every subgroup of index ρ under any group includes a ρ'th, $\rho' \leqq \rho$, part of the elements of every other subgroup of G. We proceed to prove that $\rho'<\rho$ whenever the two distinct subgroups G_1, G_2 in question are conjugate under G. Suppose that $\rho'=\rho$. It must therefore be possible to write all the elements of G in the form $s_1 s_2$, where s_1 is any element of G_1 and s_2 is any element of G_2. Hence all the con-

jugates of G_1 under G are also conjugates under G_2. This is, however, impossible, when H_1 and H_2 are conjugate since the elements of G_2 cannot transform G_1 into G_2. As the assumption that $\rho' = \rho$ has led to an absurdity, it has been proved that *the index of the cross-cut of any two distinct conjugate subgroups under one of these subgroups is always less than the index of these subgroups under the entire group.*

To find a simple illustration of this fundamental theorem, suppose that the index of G_1 under G is 2. It follows then directly from this theorem that if G_1 and G_2 are two conjugate subgroups, the cross-cut of G_1 and G_2 must have an index which is less than 2 under each of these subgroups. Hence this index is 1, and G_1, G_2 are identical. Hence the given theorem includes as a special case the theorem that a subgroup of index 2 under any group is invariant. This fact can also be readily proved in other ways. Cf. preceding Exercises.

If the invariant subgroup H is composed of all the invariant elements of G it is called the *central* of G and its complementary group is known as the *central quotient group* of G. When this central quotient group is abelian G is said to be *metabelian.** The central quotient group is also called the *group of congredient isomorphisms* of G. It is clear that the central of G is always abelian. For instance, 1, -1 constitute the central of the quaternion group, and the central of an abelian group coincides with the group. In a non-abelian group the order of the central cannot exceed the order of the group divided by 4, and if this is the order of the central of G, the central quotient group is the axial group. It is easy to prove that *the central quotient group is always non-cyclic.*

29. Commutators, Commutator Subgroup, and the ϕ-subgroup. The element or operator † $s^{-1}t^{-1}st$ is called the *commutator* of s and t, while its inverse is the commutator of t and s. When s and t are commutative their commutator is

* W. B. Fite, *Proceedings of the American Association for the Advancement of Science*, vol. 49 (1901), p. 41.

† The elements of a group are also called operators or operations. We shall hereafter use the terms element, operator, and operation interchangeably, since all of these terms are commonly found in the modern literature of group theory.

the identity and vice versa. By writing the commutator of s and t in the form $s^{-1}t^{-1}st=c$, or $t^{-1}st=sc$, it is clear that the commutator represents an operator which must be multiplied into another operator to obtain its conjugate. A group G of order g has g^2 commutators, but no more than g of them can be distinct. In general, these g^2 commutators generate a subgroup of G, known as the *commutator subgroup** of G, or the *first derived group of* G. When G coincides with its commutator subgroup it is said to be a *perfect group*.

To prove that the commutator subgroup of G is invariant under G it is only necessary to prove that the transform of a commutator of G as regards any element of G is also a commutator of G. This fact results immediately from the equation

$$r^{-1}s^{-1}t^{-1}str=r^{-1}s^{-1}r\cdot r^{-1}t^{-1}r\cdot r^{-1}sr\cdot r^{-1}tr=s_1{}^{-1}t_1{}^{-1}s_1t_1.$$

It should be emphasized that a group may have many invariant subgroups, but it has only one commutator subgroup. The quotient group which corresponds to the commutator subgroup is known as the *commutator quotient group*. This quotient group is always abelian, since the commutator of two of its elements must correspond to the commutator of any two of the corresponding elements of G and hence it must be the identity.

As the commutator quotient group is abelian, and as every invariant subgroup which is complementary to an abelian quotient group must include the commutator subgroup, it results that this subgroup is the smallest invariant subgroup that is complementary to an abelian quotient group. In fact, *every invariant subgroup which is complementary to an abelian quotient group includes the commutator subgroup.* From the given definition of a perfect group it results also that every simple group of composite order is a perfect group, but the con-

* The term commutator subgroup is due to R. Dedekind, but the fundamental properties of these subgroups were first published by G. A. Miller, *Quarterly Journal of Mathematics*, vol. 28 (1896), p. 266. Their usefulness was quickly recognized, and they have entered largely into the recent group theory literature.

verse is not necessarily true. That is, there are perfect groups which are not also simple, as we shall see later.

If the elements of a commutator belong to two invariant subgroups of a group G, this commutator is contained in the cross-cut of these invariant subgroups. Hence it results that *if two invariant subgroups of G have only the identity in common, every element of each one of these subgroups is commutative with every element of the other.*

If the elements of the commutator $s^{-1}t^{-1}st$ are permuted in every possible manner, there result eight operators which may be distinct and may all differ from the identity. These eight operators are: $s^{-1}t^{-1}st$, $t^{-1}sts^{-1}$, $sts^{-1}t^{-1}$, $ts^{-1}t^{-1}s$, $t^{-1}s^{-1}ts$, $st^{-1}s^{-1}t$, $tst^{-1}s^{-1}$, $s^{-1}tst^{-1}$. All of them can be obtained from any one of them by means of the substitution group of order 8 on the four factors. It is evident that each of these 8 commutators has the same order.

To prove this it may first be observed that *the order of any product of n operators is invariant as regards the cyclic group of permutations of these factors*, since such permutations are equivalent to transforming by elements. If reversing the order of these n factors does not affect the order of the product, this order is invariant as regards the dihedral group of permutation of its n factors. In particular, *the order of the product of n elements of order* 2 *is always invariant as regards the dihedral group of permutations of the n elements.* Reversing the order of the factors of a commutator cannot affect the order of this commutator, since it is equivalent to a cyclic permutation of the factors of its inverse.

The given eight commutators, involving s, t and their inverses, are contained in the commutator subgroup of the group generated by s and t, but they do not necessarily generate this subgroup. Since four of them are the inverses of the other four, it is clear that no more than four of them are distinct when their common order is 2. The most general definition of a commutator is, "the product of the transform of an element and its inverse." Whenever an element can be written as such a product, it may be called a commutator. When we speak

of the commutator of a group it is assumed that the elements of the commutator are elements of the group in question, and hence it may happen that only a small number of the elements of the group are commutators. For instance, the identity is the only commutator in an abelian group. We shall see later that every possible group element may be regarded as a commutator of some two elements. When s and t are both of order 2 their commutator is the square of their product and is transformed into its inverse by both of its elements.

The importance of the concept of commutator is largely due to the fact that the commutators of a group represent those operators which must be multiplied on the right into a given one of a complete set of conjugate operators to obtain all the others. Hence the order of the commutator subgroup of a group cannot be less than the number of conjugate operators in its largest complete set of conjugates. Since the commutator subgroup is unique, it must evidently correspond to itself in every possible automorphism of the group. A subgroup which has this property is said to be a *characteristic subgroup.** Hence it results that *if a group is not perfect, its commutator subgroup is a characteristic subgroup.*

It was observed in § 3 that any set of operators belonging to any group G of finite order is called a set of independent generators of G provided that these operators generate G and that none of them is contained in the group generated by the rest of them. All the operators of G can be divided into two categories, having no common operator, by putting into one category all those which occur in at least one of the possible sets of independent generators of G, and into the other category those which do not have this property. The operators of the second category constitute a characteristic subgroup of G, which has been called by G. Frattini the *ϕ-subgroup of G.*†

If H is any maximal subgroup of G it is evidently always possible to select at least one set of independent generators

* G. Frobenius, *Berliner Sitzungsberichte*, 1895, p. 183.

† G. Frattini, *Atti della Reale Accademia dei Lincei, Rendiconti*, ser. 4, vol. 1 (1885), p. 281.

of G in such a manner that it includes any arbitrary one of the operators of G which are not contained in H, while the remaining operators of the set belong to H. Moreover, there is at least one maximal subgroup of G which does not include any given one of the independent generators of a particular set of independent generators of G. Hence it results that the ϕ-subgroup of G is the cross-cut of all the maximal subgroups of G. This useful second definition of the ϕ-subgroup is also due to Frattini.

If a ϕ-subgroup of the group G involves a non-invariant subgroup or a non-invariant operator, this subgroup or operator cannot be transformed into all its conjugates under G by the operators of the ϕ-subgroup. That is, every complete set of conjugates of the ϕ-subgroup is an incomplete set of conjugates under G whenever the former set involves more than one element. If this were not the case all the operators of G which would transform one of these elements into itself would form a subgroup which would not involve all the operators of the ϕ-subgroup of G. This subgroup could not be maximal, since it does not involve the ϕ-subgroup. As any maximal subgroup obtained by extending this subgroup by means of operators of G could also not involve the ϕ-subgroup, we have proved the theorem: *If the ϕ-subgroup of a group G involves a non-invariant operator or subgroup, the number of conjugates under G of this operator or subgroup is greater than the number of the corresponding conjugates under the ϕ-subgroup.*

An important special case of this theorem was noted by Frattini, who observed that the ϕ-subgroup of any group involves only one Sylow subgroup for every prime which divides the order of the ϕ-subgroup. In other words, every ϕ-subgroup is the direct product of its Sylow subgroups, and hence we can always reach the identity by forming successive ϕ-subgroups, starting with any given group. If a group can be represented as a non-regular primitive substitution group of degree n, its n subgroups of degree $n-1$, each being composed of all its substitutions which omit a letter, are maximal and have only the identity in common. Hence it results that *the ϕ-subgroup of every primitive substitution group is the identity.*

EXERCISES

1. If an intransitive group of degree n contains exactly k transitive constituents, the average number of letters in all its substitutions is $n-k$.

2. Prove that the group of the square involves an invariant subgroup leading to the four-group as a quotient group and that this invariant subgroup is its commutator subgroup.

3. All the elements which are common to all the subgroups of a complete set of conjugate subgroups constitute an invariant subgroup.

4. To every invariant subgroup of a quotient group there corresponds an invariant subgroup of the group, and to every subgroup which involves a given invariant subgroup there corresponds a subgroup in the quotient group corresponding to this invariant subgroup.

5. If every element of a group is raised to the same power and if this power is prime to the order of the group, each element of the group is found once and only once among these powers.

6. The commutator subgroup of the symmetric group of degree n is the alternating group of this degree, and the alternating group of degree n is perfect whenever $n>4$.

7. A necessary and sufficient condition that the ϕ-subgroup of a cyclic group is the identity is that the order of this group is not divisible by the square of a prime number.

30. Simply Isomorphic Groups. One of the most important and most difficult problems in group theory is to determine whether two given groups of the same order are simply isomorphic or not. If they are simply isomorphic they are identical as abstract groups and vice versa. Two cyclic groups of the same order are always simply isomorphic and a cyclic group cannot be simply isomorphic with a non-cyclic group. One of the most useful theorems as regards simply isomorphic groups may be stated as follows: *Two groups of the same order G_1, G_2 are simply isomorphic if they contain two simply isomorphic invariant subgroups H_1, H_2 respectively, and are generated by these subgroups and two elements t_1, t_2 such that if t_1^α is the lowest power of t_1 which occurs in H_1, then t_2^α is the lowest power of t_2 that occurs in H_2, and t_1^α, t_2^α correspond in the given simple isomorphism of H_1, H_2. Moreover, it is assumed that t_1, t_2 transform corresponding generators of H_1, H_2 into corresponding elements in the given simple isomorphism.*

To illustrate the use of this theorem, let G_1, G_2 represent two

dihedral groups of order $2n$ and let H_1, H_2 represent their cyclic subgroups of order n. Let t_1, t_2 represent any two elements of G_1, G_2 respectively but not contained in H_1, H_2. The common order of t_1, t_2 is 2, and t_1, t_2 transform corresponding generators of H_1, H_2 respectively into corresponding elements, since they transform all the elements of these subgroups into their inverses. Hence this theorem includes the known theorem that two dihedral groups of the same order are always simply isomorphic.

The given illustrative example of the use of the theorem in question may also serve to point out the way toward a proof. In fact, if H_1, H_2 are arranged in a simple isomorphism and if the products obtained by multiplying corresponding operators by t_1^β, t_2^β respectively, $\beta = 1, 2, \ldots, \alpha - 1$, are placed in correspondence, we obtain a simple isomorphism between G_1, G_2. In fact, t_1^β, t_2^β transform all the corresponding operators of H_1, H_2 into corresponding operators because they transform generators of H_1, H_2 in this manner. It may be observed that this theorem may be employed to prove that two cyclic groups of the same composite order are simply isomorphic if it is assumed that two cyclic groups of the same prime order have this property.

It results immediately from the given theorem that if two abelian groups of the same order involve only operators of the same prime order besides the identity, they must be simply isomorphic. Among the most important simple isomorphisms are those in which the operators of the same group G are placed into a (1, 1) correspondence in such a way that an automorphism of G is obtained. We have seen (§ 24) that any operator which transforms G into itself effects an automorphism on its elements. Moreover, any automorphism of G can always be brought about by transforming G by some operator which transforms G into itself. To prove this statement we shall employ a method which has been illustrated in § 14 but which we desire to exhibit more fully.

Represent G as a regular substitution group and establish an arbitrary automorphism of G. We may suppose that all the substitutions begin with the same letter, so that the second

letters of the corresponding substitutions exhibit a substitution by means of which we can transform one of these groups in such a way that the first two letters of all the corresponding substitutions are identical. After this has been done all the corresponding letters of the corresponding substitutions must be identical, so that the given substitution may be used to effect the given automorphism. This follows immediately from the fact that the two regular groups in which all of the corresponding substitutions have the first two letters in common are still simply isomorphic, and if in a given substitution c is replaced by d, this substitution is the product of the inverse of the substitution in which a is replaced by c and the substitution in which a is replaced by d. Hence in the corresponding substitution of this automorphism c must also be replaced by d, since a regular group contains only one substitution in which a given letter is replaced by another given letter.

In view of the importance of this theorem we shall give an illustrative example. Consider the following automorphism of the symmetric group of order 6:

1	1
$abc \cdot def$	$acb \cdot dfe$
$acb \cdot dfe$	$abc \cdot def$
$ad \cdot bf \cdot ce$	$ad \cdot bf \cdot ce$
$ae \cdot bd \cdot cf$	$af \cdot be \cdot cd$
$af \cdot be \cdot cd$	$ae \cdot bd \cdot cf$

The substitution which transforms the former of these two groups so that the first two letters in each pair of corresponding substitutions are identical is $bc \cdot ef$. This substitution also transforms the former of these corresponding groups into the latter. The theorem that *every automorphism of G may be obtained by transforming G by operators which transform G into itself* is not only useful in finding the possible automorphisms, but it may also be used to determine the totality of the substitutions which transform a given group into itself.

EXERCISES

1. The substitutions which represent the transformations of the symmetric group of order 6 into all its possible automorphisms constitutes a group which is simply isomorphic with this symmetric group.

2. If a substitution of order 2 transforms G_1 into G_2 it must also transform G_2 into G_1.

3. Any group G of order g that involves an invariant operator s of order h can be extended by means of an operator t of order nh which is commutative with every operator of G and satisfies the equation $t^n = s$ so as to obtain a group of order gn.

Suggestion: Write G as a regular group on n distinct sets of letters and establish a simple isomorphism between these groups. Let t_1 be a substitution of order n which permutes the corresponding letters of this intransitive group and is commutative with each of its substitutions. For t we may use the product of t_1 and the substitution s in one of the regular constituents.

31. Group of Inner Isomorphisms. If all the elements of a non-abelian group G are transformed by any one of its own elements, the elements of G are permuted according to a certain substitution. By transforming the elements of G successively by all the elements of G there result a series of substitutions which constitute a group known as the *group of inner isomorphisms of G.* This group is also called the group of *cogredient isomorphisms* of G, and it is simply isomorphic with the central quotient group of G (§ 28). A necessary and sufficient condition that G is simply isomorphic with its group of inner isomorphisms is that the central of G is the identity.

If G admits isomorphisms which cannot be obtained by transforming all the elements of G by its own elements, they are called *outer*, or *contragredient, isomorphisms.* In this case the group of inner isomorphisms is clearly an invariant subgroup of the group of isomorphisms of G.

One of the most useful properties of the group of inner isomorphisms I_1 of G is that I_1 *contains the same number of Sylow subgroups of every order as G does,* provided we call the identity a Sylow subgroup of order p^m whenever the order of the group I_1 is not divisible by p. The truth of this fact becomes evident if we observe that a Sylow subgroup of I_1 has exactly the same number of conjugates under I_1 as the corresponding Sylow

subgroup of G has under G. In particular, an abelian group contains only one Sylow subgroup of every order.

In § 13 we defined the term direct product as regards substitution groups. In general, a group is said to be the *direct product* of two subgroups which generate it, provided these two subgroups have only the identity in common and every element of the one is commutative with every element of the other. For instance, *the holomorph of a complete group is the direct product of the group and its conjoint* (§ 19). This holomorph is also said to be the square of this complete group. A simpler illustration of a direct product is furnished by the axial group, which is the direct product of any two of its subgroups of order 2.

As the group of inner isomorphisms of G cannot be cyclic it cannot have a smaller order than 4. If it is of order 4, G contains exactly three abelian subgroups of half its own order; and vice versa. When G is non-abelian and contains more than one abelian subgroup of half its order, then G has the four-group for its group of inner isomorphisms. As instances of groups which have the four-group for their group of inner isomorphisms we may cite the octic group and the quaternion group.

32. Frobenius's Theorem. In an article published in the *Berliner Sitzungsberichte*, 1895, page 984, Professor G. Frobenius developed a very fundamental theorem which may be stated as follows:

If n is any factor of the order g of a group G, the number of the operators in G, including the identity, whose orders divide n, is a multiple of n.

This theorem is evidently true when g is a prime number, and also when $n=g$. Hence, in a proof by complete induction, we may assume that the theorem holds for all the groups whose orders involve a fewer number of factors than g does, and also for all factors of g which are larger than n. If we can prove that it remains true for G and n provided these assumptions are made, then the theorem will follow by complete induction for an arbitrary group G and any divisor n of its order.

The theorem is clearly true for every cyclic group, since such a group has one and only one subgroup whose order is any divisor of the group, and this subgroup includes all the operators of this cyclic group whose orders divide this divisor. To simplify the general considerations which follow, we shall first prove that the theorem applies also to the non-cyclic group of order pq, p and q being distinct primes and $p>q$. Let N_x represent the number of operators of G whose orders divide x, while $\overline{N}_x$ represents the number of those operators of G whose orders do not divide x. Hence, in the special case when G is the non-cyclic group of order pq,

$$N_{pq}=N_p+\overline{N}_p.$$

As N_{pq} is divisible by p we can prove that N_p is divisible by p by proving that $\overline{N}_p$ is divisible by p. The fact that $\overline{N}_p$ is divisible by p results directly from the fact that all of these operators are of order q, since G is non-cyclic, and they must occur in complete sets of conjugates under a subgroup of order p, such that each set involves p of these conjugates.

We shall now prove, by means of the two given assumptions, the general theorem stated above. If p represents any prime divisor of g/n, G involves, by hypothesis, a multiple of np operators whose orders divide np. As

$$N_{np}=N_n+\overline{N}'_n,$$

where $\overline{N}'_n$ represents the number of operators of G whose orders divide np but do not divide n, it is evident that we have only to prove that $\overline{N}'_n$ is divisible by n in order to prove our theorem.

The totality of these $\overline{N}'_n$ operators will be represented by A. Suppose that $n=p^{\lambda-1}s$ where s is prime to p. It is clear that A is composed of operators whose orders are divisible by p^λ, and hence it is very easy to see that $\overline{N}'_n$ is divisible by $p^{\lambda-1}$. In fact, every cyclic group whose order is divisible by p^λ must have a multiple of $p^{\lambda-1}$ distinct generators, since $\phi(p^\lambda)=p^{\lambda-1}(p-1)$, $\phi(m)$ being the totient of m. Hence it remains only to prove that $\overline{N}'_n$ is also divisible by s.

Among the operators of A there may be several which have the same constituent P of order p^λ. All such operators are the direct product of P and operators whose orders are divisors of s, and all the operators of A may be divided into distinct sets such that each set is composed of all the operators of A which have the same constituent of order p^λ. We proceed to prove that the number of operators in the combined sets which involve all the conjugates of P under G is divisible by s, and hence that the total number of operators in A is divisible by s.

To prove this fact, we consider all the operators of G which are commutative with P. These form a subgroup H of order $p^\lambda r$, and the quotient group of H with respect to the cyclic group generated by P is of order r. The orders of the operators of this quotient group which divide s must also divide the highest common factor (t) of s and r. As the order of this quotient group involves fewer factors than g does we may assume that the number of its operators whose orders divide t is kt. Hence A contains exactly kt operators which have the same constituent P.

The combined sets which involve no operator of order p^λ, except the conjugates of P under G, must therefore involve $gkt/(p^\lambda r)$ distinct operators, since P has $g/(p^\lambda r)$ conjugates under G. Since g is divisible by s and r, it follows that gt is divisible by rs, t being the highest common factor of r and s. Hence s is a divisor of gkt/r. As s and p^λ are relatively prime, s must also be a divisor of $gkt/(p^\lambda r)$, and the theorem in question has been proved.

While the number of the operators of G whose orders divide any divisor n of g is always a multiple of n, it does not follow that groups exist in which the number of these operators is an arbitrary multiple of n. For instance, if p^α is the highest power of the prime p which divides g, G contains at least one subgroup of order p^α, according to Sylow's theorem. If G contains only one such subgroup this must be invariant and hence G involves only p^α operators whose orders divide p^α.

If G contains more than one subgroup of order p^α, it must contain at least $p+1$ such subgroups, since one such subgroup

must transform any other into at least p distinct subgroups. If G contains exactly $p+1$ such subgroups they must have in common $p^{\alpha-1}$ operators and hence they involve exactly

$$(p+1)(p^{\alpha}-p^{\alpha-1})+p^{\alpha-1}=p^{\alpha+1}$$

different operators. Hence G contains exactly p^{α} operators whose orders divide p^{α} whenever it contains only one subgroup of order p^{α}, and it contains exactly $p^{\alpha+1}$ operators whose orders divide p^{α} whenever it contains exactly $p+1$ such subgroups.

We proceed to prove that when G involves more than $p+1$ subgroups of order p^{α}, it must also involve more than $p^{\alpha+1}$ operators whose orders divide p^{α}.

To prove this fact we may assume that p^{β} is the largest number of operators in common to two subgroups (H_1, H_2) of order p^{α}. Then H_1 will transform H_2 into $p^{\alpha-\beta}$ distinct subgroups. At least $p+1$ of these have the same subgroup of order p^{β} in common, according to the evident theorem that every non-invariant subgroup of a group of order p^{α} is transformed into itself by at least one of its conjugates. If $\beta<\alpha-1$, these $p+1$ subgroups involve more than $p^{\alpha+1}$ operators whose orders divide p^{α}. If $\beta=\alpha-1$ they must involve exactly $p^{\alpha+1}$ operators whose orders divide p^{α}. If these $p+1$ subgroups are such that they are not transformed among themselves by all their operators, there must be another subgroup of order p^{α} in G which involves the $p^{\alpha-1}$ operators common to the given $p+1$ subgroups, and hence G would involve more than $p^{\alpha+1}$ operators whose orders divide p^{α}.

It remains only to consider the case when each of the given $p+1$ subgroups transforms the remaining p subgroups among themselves, and when G contains at least one more subgroup of order p^{α}. In this case, this additional subgroup of order p^{α} would contain operators which would not transform the given $p+1$ subgroups among themselves, and hence G *must contain more than* $p^{\alpha+1}$ *operators whose orders divide* p^{α} *whenever it contains more than* $p+1$ *subgroups of order* p^{α}.

This proves that whenever the number of operators in G whose orders divide p^{α} exceeds p^{α} it must be at least $p^{\alpha+1}$, and

hence it establishes the fact that it is impossible to construct a group G such that its order g is divisible by p^α, but not by $p^{\alpha+1}$ and such that the number of its operators whose orders divide p^α lies between p^α and $p^{\alpha+1}$.

EXERCISES

1. If the number of the operators of a group G, whose orders divide an arbitrary divisor d of the order of G, is exactly d, then G must be cyclic.

2. There are no groups with the property that every cyclic subgroup besides the identity is transformed into itself by only its own operators. Cf. Dyck, *Mathematische Annalen*, vol. 22 (1883), p. 101.

3. Let x_1 and n represent two arbitrary numbers, and denote by s_1 and s_2 the operations of subtracting n from x_1 and dividing x_2 by n respectively. If n is replaced successively by all the numbers resulting from these operations, then s_1 and s_2 will, in general, generate the symmetric group of order 6 when $x_1^2 = x_2$. When $x_1^2 = 2x_2$, and when $x_1^2 = 3x_2$, these operations will generate the octic group and the dihedral group of order 12 respectively.*

33. Representation of an Abstract Group as a Transitive Substitution Group. In § 27 it was observed that every group of finite order can be represented in one and only one way as a regular substitution group. It is often very useful to represent a given abstract group as a transitive substitution group on the smallest possible number of letters. Many of the abstract properties of a group can often be most readily determined if the group is written in this form. Hence we proceed to consider the general question of representing an abstract group G as a non-regular transitive substitution group of degree n.

In § 12 it was observed that when G is thus represented, it involves n conjugate subgroups $G_1, G_2, \ldots, G_n$ each of which is composed of all the substitutions of G which omit a given letter. If the subgroup of G_1, composed of all its substitutions which omit a given letter, is of degree $n-\alpha$, these n conjugate subgroups are identical in sets such that each set involves α of them. As G is non-regular, there must be at least two such sets, and hence we see directly that G cannot be represented

* These groups, together with the four group, have been called groups of subtraction and division, *Quarterly Journal of Mathematics*, vol. 37 (1906), p. 80.

as a non-regular transitive substitution group unless it contains a non-invariant subgroup H which involves no invariant subgroup of G besides the identity.

This condition is sufficient as well as necessary in order that G can be represented as a non-regular transitive substitution group. In fact, if the elements of G are arranged in a rectangle, where those of such a subgroup H appear as the first row, as follows:

$$\begin{array}{llll} s_1, & s_2, & \ldots, & s_h \\ s_1t_2, & s_2t_2, & \ldots, & s_ht_2 \\ \cdot & \cdot & \cdot & \cdot \\ s_1t_n, & s_2t_n, & \ldots, & s_ht_n \end{array}$$

the lines are permuted as units if all the elements are multiplied on the right by any element of G, since these lines are the co-sets of G as regards H.

Hence each element of G may be denoted by the substitution according to which it permutes these co-sets when it is used as a multiplier in the given manner. No two elements of G could permute these co-sets according to the same substitution, since H is non-invariant under G and does not involve any invariant subgroup, besides the identity, of G. This proves the following theorem: *A necessary and sufficient condition that an abstract group G of order g can be represented as a transitive substitution group of degree n is that G contains a non-invariant subgroup of order g/n which does not include any invariant subgroup of G besides the identity.*

In the given method of representing G as a transitive substitution group of degree n it is clear that H corresponds to the subgroup composed of all the substitutions which omit a given letter of this transitive group. All the subgroups of G which correspond to H in one of the possible automorphisms of G give rise to the same transitive substitution group, but no other subgroup can have this property. Hence G gives rise to as many different transitive groups of degree n as it has sets of subgroups of order g/n such that each set includes all those subgroups which correspond in some one of the possible auto-

morphisms of G, and such that these subgroups do not include any invariant subgroup of G besides the identity.*

For instance, the symmetric group of order 24 contains three conjugate cyclic subgroups of order 4 and also three conjugate noncyclic subgroups of this order. It contains no other non-invariant subgroup of order 4. Hence this symmetric group appears twice among the transitive substitution groups of degree 6. As the alternating group of degree 4 contains two sets of conjugate subgroups, of orders 2 and 3 respectively, this group can be represented transitively in only two ways besides the regular form. That is, it appears as a transitive group of degree 4 and also as a transitive group of degree 6. It should be observed that these considerations establish another very close contact between the theory of abstract groups and that of transitive substitution groups.

It is now easy to prove the theorem, to which we referred in § 10, that the co-set multipliers may be so selected that they are the same on the right as on the left. When the subgroup H is invariant this requires no proof. When H does not involve any invariant subgroup of G besides the identity, and G is represented as a transitive substitution group of degree n with respect to H, it may be supposed that H is composed of all the substitutions of G which omit a given letter a. The right co-sets will then be composed separately of all the substitutions of G in which a is replaced by a given letter. In the left co-sets a is replaced by all the letters of a transitive constituent of H if H is intransitive on $n-1$ letters. If H is transitive on $n-1$ letters the theorem is evident.

Hence it remains only to consider the case when H is intransitive. In this case it is evidently possible to select a certain number of left co-sets involving all the substitutions of the same number of right co-sets, and in these the multipliers may be made the same in the left co-sets as in the corresponding right co-sets. Hence the theorem is established in case H contains no invariant subgroup of G besides the identity.

If H involves such an invariant subgroup but is not itself

* *Bulletin of the American Mathematical Society*, vol. 3 (1897), p. 215.

invariant under G, H will correspond to a subgroup in a quotient group, such that this quotient group can be represented transitively with respect to this subgroup. Hence the theorem is also true in this case. For an abstract proof of this theorem the reader may consult H. W. Chapman, *Messenger of Mathematics*, vol. 42 (1913), page 132.

EXERCISES

1. If a dicyclic group is represented as a transitive substitution group it must be regular.

2. A dihedral group of order $2n$, $n>2$, can be represented in two and in only two ways as a transitive substitution group.

3. Only one of the five possible groups of order 8 can be represented as a non-regular transitive substitution group.

4. If a simple group of composite order is represented as a transitive group of lowest possible degree it must be primitive.

5. There are five and only five abstract groups of order 12.

34. Historical Note.* The concept of group is one of the oldest mathematical concepts. Even in the development of elementary geometry by the Greeks this concept played a fundamental rôle, as was pointed out by H. Poincaré in an article entitled "On the foundations of Geometry," *Monist*, volume 9 (1898), pages 1–43. It was, however, not developed into an extensive theory until a comparatively recent period.

In the latter half of the eighteenth century various writers, especially J. L. Lagrange and A. T. Vandermonde, began to lay stress, in their algebraic investigations, upon the elements of the theory of substitutions. On the other hand, L. Euler brought some properties of abelian groups into prominence, especially by his work on power residues. Towards the close of the eighteenth and at the beginning of the nineteenth century, two Italian mathematicians, P. Ruffini and P. Abbati, entered more directly on the study of substitution groups by proving that there are no three or four-valued rational functions of more than four variables, and that a two-valued function must be alternating.

During the first half of the nineteenth century a number of other investigators entered this field. Foremost among

* Cf. *Bibliotheca Mathematica*, vol. 10 (1910), p. 317.

these were C. F. Gauss, A. L. Cauchy, N. H. Abel, and E. Galois. The first of these helped to lay a foundation for abelian groups by his investigations in number theory, while the other three contributed directly towards the development of the general theory of substitution groups. Abel and Galois solved two fundamental problems in the theory of equations by means of substitution groups, and thus they directed attention to the usefulness of this subject (Cf. Part III). On the other hand, Cauchy ordered and extended the results obtained by his predecessors and contemporaries, and laid a broad foundation for the general theory of substitution groups. Hence Cauchy is frequently called the founder of this theory.

The theory of abstract groups grew gradually out of that of substitution groups. In fact, we find even in Cauchy's later writings a tendency to state some results independently of the notation. Cayley's table and Cayley's theorem are very fundamental in this theory, and hence A. Cayley is sometimes called the founder of the abstract theory of groups. In 1856 W. R. Hamilton gave abstract definitions of the groups which are simply isomorphic with the groups of movements of the five ancient regular solids. By these definitions, and the fact that his quaternion units and their negatives form an important non-abelian group of order 8, he contributed considerably towards an interest in this theory.

A solid foundation for an abstract theory implies, however, clear abstract definitions of the terms used. Among the earlier writers one fails to find such definitions. According to E. V. Huntington, *Transactions of the American Mathematical Society*, volume 6 (1905), page 181, the earliest explicit set of postulates for abstract groups were given by L. Kronecker in 1870. Even at the present time the term group is sometimes used with different meanings as a mathematical technical term.*

The earliest separate text-book devoted to group theory is Jordan's *Traité des substitutions et des équations algébriques*, Paris, 1870. This work has become a classic. It was written, however, before the abstract theory was well estab-

* Cf. *Encyclopédie des Sciences Mathématiques*, tome 1, vol. 1, p. 576; vol. 2, p. 243.

lished. Even Sylow's theorem appeared two years later, and a number of other more recent theorems make it possible to present many subjects in a simpler manner than could be done at the time when Jordan wrote this *Traité*. The only other separate text-books on groups of finite orders which appeared before the present century are Netto's *Substitutionentheorie*, 1882, Burnside's *Theory of Groups of Finite Order*, 1897, and Bianchi's *Lezioni sulla theoria dei gruppi di sostituzioni*, 1897 (lithographed). Netto's book was translated into Italian by G. Battaglini in 1885, and into English by F. N. Cole in 1892.

In the older writings on groups, and in some of the more recent ones, a set of distinct elements considered with respect to only one formal law of combination is said to form a group whenever every element obtained by combining an element with itself or with any other element of the set is again in the set. In most cases it is, however, tacitly assumed that these elements obey the other laws which were imposed in our definition of a group. If this is not assumed the set may be said to have "the group property." Cf. M. Bôcher, *Introduction to Higher Algebra*, 1907, page 82.

Since the beginning of the present century a considerable number of separate treatises on groups of finite order have appeared. The literature on this subject has been made more accessible by the publication of two somewhat extensive bibliographies, viz., *The Constructive Development of Group-Theory* by B. S. Easton, University of Pennsylvania, 1902, and the "Essai d'une bibliographie sur la théorie des groupes" by C. Alasia, published in the *Rivista di fisica, mathematica e scienze naturali*, Pavia, 1908–10.

The main theorems of the theory of finite groups, together with numerous historical data relating to their development, may be found in the *Encyclopédie des Sciences Mathématiques*, tome 1, volume 1, page 532, and in the second edition of Pascal's *Repertorium der höheren Mathematik*, volume 1, page 168. A list of remarks on the bearing of the theory of groups, exhibiting the wide application of this subject, was published in volume 6 (1914), of the *Tôhoku Mathematical Journal*.

CHAPTER IV

ABELIAN GROUPS *

35. Invariants. A group is said to be abelian when each of its elements is commutative with every element of the group, § 26. Since all the Sylow subgroups of the same order are conjugate under every group, it results that an abelian group can have only one Sylow subgroup of a given order, and hence *every abelian group is the direct product of its Sylow subgroups whenever its order is divisible by more than one prime number.* This implies that a necessary and sufficient condition that two abelian groups are simply isomorphic is that all their Sylow subgroups are simply isomorphic, and hence the study of abelian groups is reduced to the study of such groups whose orders are powers of a single prime number. In particular, if the order of an abelian group is not divisible by the square of a prime number the group must be cyclic.

Suppose that G is an abelian group of order p^m, p being any prime number. If G is cyclic, all of its elements are generated by a single one of them s_1, where s_1 may be selected in $p^m - p^{m-1}$ ways. Moreover, every element of order p^α, $m > \alpha > 0$, in G is the pth power of p distinct elements of order $p^{\alpha+1}$, the p^2th power of p^2 distinct elements of order $p^{\alpha+2}$; the $p^{(m-\alpha)}$th power of $p^{m-\alpha}$ distinct elements of order p^m. When G is not cyclic we may choose for s_1 any one of its elements of highest order. Some power of every other element of G is contained in the group (s_1) generated by s_1. We represent by s_2' one of those elements which have to be raised to the highest power p^{α_2} to obtain an

* A number of the theorems on abelian or commutative groups were first developed by L. Euler and C. F. Gauss in connection with their studies in number theory. The earliest extensive exposition of the properties of these groups is due to G. Frobenius and L. Stickelberger, *Crelle*, vol. 86, p. 217.

element of (s_1). That is, the p^{α_2}th power of every element of G is in (s_1) but the p^{α_2-1} power of s_2' is not in (s_1). We proceed to prove that s_2' may be so selected that the cyclic groups (s_1) and (s'_2) have only the identity in common; that is,

$$s_2'^{p^{\alpha_2}} = 1.$$

Since $s_2'^{p^{\alpha_2}}$ is in (s_1), and the order of s_2' does not exceed that of s_1, there must be an element in (s_1) whose p^{α_2}th power is the inverse of $s_2'^{p^{\alpha_2}}$. The product of s_2' and this element is therefore of order p^{α_2}. Moreover, the p^{α_2-1}th power of this product is not contained in (s_1) since one of its factors is in (s_1), while the other does not have this property. In what follows we shall denote this product, of order p^{α_2}, by s_2. If the order of G is the product of the orders of s_1 and s_2 it is clear that G is the direct product of (s_1) and (s_2). We proceed to prove that G is always the direct product of cyclic groups.* The orders of these cyclic groups are called the *invariants* † of G. In particular, if s_1 is of order p^{α_1} and if G is the direct product of (s_1), (s_2), the invariants of G are p^{α_1}, p^{α_2}.

If G contains elements which are not included in the group (s_1, s_2), generated by s_1 and s_2, we may suppose that the p^{α_2}th power of every other element is in (s_1, s_2) while the p^{α_2-1}th powers of some of the elements are not in this subgroup. We proceed to prove that at least one of the latter elements is of order p^{α_2}. Let s_3' be any one of these elements. As

$$s_3'^{p^{\alpha_2}}$$

is in (s_1, s_2), and as $\alpha_3 \leqq \alpha_2 \leqq \alpha_1$, there must be some element in (s_1, s_2) whose p^{α_2}th power is the inverse of $s_3'^{p^{\alpha_2}}$. The product, s_3, of this element and s'_3 is therefore of order p^{α_2}, and G involves the direct product of the three groups (s_1), (s_2), (s_3). As this process may clearly be continued until all

* It is implied that each of these cyclic groups has only the identity in common with the group generated by all the others. In other words, they are independent cyclic groups.

† The invariants of an abelian group have also been called the elementary divisors of the order of this group. Frobenius and Stickelberger, *Crelle*, vol. 86 (1878), p. 238.

the elements of G have been exhausted, it has been proved that *every non-cyclic abelian group of order p^m is the direct product of independent cyclic groups*. This is the most important theorem relating to abelian groups.*

These independent cyclic groups may be represented as substitution groups on distinct sets of letters. Moreover, it is clear that a group can be constructed such that the orders of such substitution groups are arbitrary, and hence the product is an abelian group of arbitrary order. That is, *the number of distinct abelian groups of order p^m is equal to the number of the possible partitions of m as regards addition*, and each of these groups may be completely defined by the value of p and the symbol $(m_1, m_2, \ldots, m_\lambda)$ where $m_1, m_2, \ldots, m_\lambda$ represent positive integers such that $m_1+m_2+\ldots+m_\lambda=m$. The group G is completely defined by p and the values of the integers $m_1, m_2, \ldots, m_\lambda$, and it is not affected by the order in which these integers are arranged. It is said to be of order p^m and of *type* $(m_1, m_2, \ldots, m_\lambda)$. We may therefore suppose that the numbers $m_1, m_2, \ldots, m_\lambda$ are always arranged in order of magnitude, beginning with the largest. It may be added that the determination of the number of possible abelian groups of order p^m is reduced by these theorems to a problem in the theory of numbers; viz., the determination of the total number of possible partitions of m as regards addition. This problem has received considerable attention, but it still involves many unsolved difficulties.

Suppose that an abelian group G of order p^m has α invariants. All of its elements whose orders divide p must constitute a subgroup of order p^α; and, conversely, whenever these elements constitute a group of order p^α, G has exactly α invariants. The

* A set of independent generating elements can generally be selected in a large number of ways. Such a set is often called a *base* of the abelian group, and the operators $s_1, s_2, s_3, \ldots$ are called elements of the base. The fundamental theorem that every abelian group is a direct product of independent cyclic groups is implicitly contained in the works of C. F. Gauss and E. Schering, but L. Kronecker gave the first satisfactory proof of it in 1870. It should perhaps be placed next after Cayley's theorem among the most fundamental theorems of group theory.

elements of G whose orders divide p^2 constitute a group of order $p^{2\alpha-\beta}$, where β is the number of invariants of G which are equal to p. In general, let $x_1, x_2, \ldots, x_\lambda$ represent the number of the invariants of G which are equal to $p, p^2, \ldots, p^\lambda$ respectively, and suppose that they include all the invariants of G. The number N of the elements of G whose orders divide p^k, $k \leqq \lambda$, is then given by the formula

$$N = p^{x_1+2x_2+\ldots+(k-1)x_{k-1}+k(x_k+x_{k+1}\ldots+x_\lambda)}.$$

It should be observed that the orders of the independent cyclic groups which generate a given group G are completely determined by G when G is of order p^m. In general, G is the direct product of Sylow subgroups and hence it is also the direct product of a series of cyclic independent subgroups $C_1, C_2, \ldots, Cm'$, each of which has for its order a power of a prime number. Unless the contrary is stated it will be assumed that the order of each of these subgroups exceeds unity, and hence their number and their orders are completely determined by G; and, in turn, they determine G completely. That is, if these orders are the same for two groups these groups are simply isomorphic. These orders are therefore invariants of G, but they are not the only numbers which are known as invariants of G. Their number constitutes the largest possible number of orders of independent cyclic groups in G; that is, neither G nor any of its subgroups can have more than m' independent generators.

It is important to note that the term *set of independent generators* as regards abelian groups is usually employed to represent a set of independent generators which is such that the group generated by an arbitrary number of them has only the identity in common with the group generated by the remaining ones. In dealing with abelian groups we shall always use this term with this special meaning and not with its general meaning given in § 3.

36. Largest and Smallest Number of Possible Invariants. We proceed to find the smallest number of independent generators of G. The given subgroups $C_1, C_2, \ldots, Cm'$ can be

arranged in rows such that the orders of all those in one row are powers of the same prime, and such that the order of each is equal to or greater than the order of the one which follows it in the same row. In case the rows do not contain the same number, the vacant places may be filled by the identity. Arranging these rows in the form of a rectangle, we have

$$\begin{array}{llll} C_1, & C_2, & \ldots, & C_a \\ C_{a+1}, & C_{a+2}, & \ldots, & C_{2a} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

By forming the products of all those in each column we obtain a independent cyclic subgroups such that the order of each is divisible by the orders of all those which follow it. *These subgroups form the smallest possible number of generating cyclic subgroups of* G. The orders of these subgroups are commonly called the *invariants of* G, since any other system of independent generating subgroups in which the order of every group is divisible by the order of every following group is composed of groups which are simply isomorphic with these products. It may be observed that a is the largest number of invariants in a Sylow subgroup of G, while m' is equal to the sum of the numbers of invariants of all the Sylow subgroups of G. It is clear that the independent generators of G can be so selected that their number has any arbitrary value from a to m', but this number can have no other value. Moreover, G cannot be generated by less than a cyclic subgroups even if these subgroups are not independent.

Whenever the independent generators of G are so chosen that the order of each of them is divisible by the orders of all those which follow it, their number must be a, and when the order of each is a power of a single prime their number must be m', but it is not true that the independent generators can be so arranged that the order of each is divisible by the order of all those which follow it whenever the number of these generators is a. The two numbers a and m' are only equal when the order of G is a power of a single prime. Since the former method leads to the smallest number of invariants it seems appro-

priate to call the orders of these independent generators the invariants of G, although the latter method has some advantages. The choice of invariants such that their number lies between a and m' seems less natural. We evidently arrive at the a invariants if we choose the independent generators in the following way. Start with an element of highest order and then select any other element such that the two generate the largest possible subgroup. The orders of two independent generators of this subgroup are the first two invariants of G. If we add to this subgroup another element so that the three generate the largest possible subgroup, we arrive at the third invariant, etc.

A marked difference between the two given methods of arriving at the invariants of G should perhaps be emphasized; viz., the orders of the independent generators of G are completely determined by m', but not by a. That is, if two sets of m' independent generating cyclic subgroups of G were given, the orders of the subgroups of one set would be the same as those of the other; but if two sets of a independent generating cyclic subgroups of G were given, the orders of those of one set could generally vary a great deal from the orders of those of the other. A necessary and sufficient condition that the orders of these two sets *must* be the same is that the a invariants of each of the Sylow subgroups of G, with one possible exception, are equal. The number a is said to be the *rank* of G.

If G is the direct product of a series of subgroups $G_1, G_2, \ldots, G_\lambda$, we may select a set of independent generators of G by combining arbitrary sets of independent generators of each of these subgroups. Suppose that $G_1, G_2, \ldots, G_\lambda$ are the Sylow subgroups of G. Any element t of G will have a constituent, which may be the identity, from each one of these subgroups, and the order of t will be the product of the orders of these constituents. To determine the number of the elements of a given order in G it is only necessary to determine the number of elements of a given order in each of the Sylow subgroups. That is, if the order of t is $p_1^{a_1}p_2^{a_2} \ldots p_\lambda^{a_\lambda}$ ($p_1, p_2, \ldots, p_\lambda$ being prime numbers), the number of elements of G whose

order is equal to the order of t is the product of the numbers of the elements of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_\lambda^{\alpha_\lambda}$ in the respective Sylow subgroups of G. We proceed to determine this number.

37. Number of Elements of a Given Order. Let G be any abelian group of order p^m whose invariants are $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_\lambda}(a_1 \geqq a_2 \geqq a_3 \geqq \ldots \geqq a_\lambda > 0)$. Let $m'_1 = \lambda$ represent the number of invariants $\geqq p$, m'_2 the number of those $\geqq p^2, \ldots,$ and m'_{a_1} the number of those $= p^{a_1}$. To determine the number of the elements of order $p^\beta (1 \leqq \beta \leqq a_1)$, it is only necessary to find the order of the group generated by all the elements whose orders divide p^β and to subtract from this number the order of the group formed by all the elements whose orders divide $p^{\beta-1}$. That is, the number of elements of order p^β in G is equal to *

$$p^{m'_1+m'_2+\ldots+m'_\beta} - p^{m'_1+m'_2+\ldots+m'_{\beta-1}} = (p^{m'_\beta}-1)p^{m'_1+m'_2+\ldots+m'_{\beta-1}}.$$

To obtain the number of the elements of a given order n in any abelian group we may write n in the form $2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\lambda^{\alpha_\lambda}$, and find the number of the elements of order 2^{α_0} in the Sylow subgroup of even order, then find the number of the elements of order $p_1^{\alpha_1}$ in the Sylow subgroup whose order is divisible by p_1, etc. The product of all the numbers obtained in this way is equal to n. For instance, to find the number of the elements of order 12 in the abelian group whose invariants are 24, 6, 2, we observe that the invariants of the Sylow subgroups are 8, 2, 2 and 3, 3 respectively. The number of the elements of order 4 in the former Sylow subgroup is 8, $(m'_1 = 3, m'_2 = 1, m'_3 = 1)$, and the number of those of order 3 in the latter is also 8. Hence there are exactly 64 elements of order 12 in the given abelian group.

The number of the elements of order p^β in the group G of order p^m may also be obtained by observing that if $s_1, s_2, \ldots, s_\lambda$ represent a set of base elements of G, a set of base elements of the subgroup of G generated by all its elements whose

* Heffter, *Crelle*, vol. 119 (1898), p. 261; Netto, *Vorlesungen über Algebra*, vol. 2 (1900), p. 248.

orders divide p^β may be obtained by raising all those of the given set whose orders exceed p^β to a power sufficient to reduce their orders to p^β. The elements whose orders divide $p^{\beta-1}$ constitute a subgroup of index $p^{m'\beta}$ under the given subgroup of G. Hence the number of elements of order p^β is $p^{m'\beta}-1$ times the order of the subgroup of G which is composed of all its elements whose orders divide $p^{\beta-1}$.

EXERCISES

1. Determine the number of elements of each order in the four abelian groups of order 100.

2. The smallest number of letters on which an abelian group can be represented as a substitution group is the sum of its invariants, if all these invariants are powers of prime numbers.

3. A group of order p^2q must be abelian when q is a prime number which is less than the prime number p and does not divide p^2-1.

4. If all the elements besides the identity of a group are of order 2 the group is abelian.

5. The order of the ϕ-subgroup of any abelian group of order g is equal to g divided by the order of the subgroup generated by all the operators of prime orders contained in this abelian group.

38. Abelian Groups of Given Orders. The number of the different possible abelian groups of order $n=2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_\lambda^{\alpha_\lambda}$ ($p_1, p_2, \ldots, p_\lambda$ being distinct odd primes) is equal to the product obtained by multiplying together the numbers which separately represent the total numbers of partitions, as to addition, of the separate exponents $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_\lambda$ which exceed zero. In particular, if none of these exponents exceeds 3 the number of distinct abelian groups of order n is equal to the product of those exponents which exceed zero. For instance, the number of abelian groups of order $3^2\cdot5^3\cdot7^3$ is 18, while the number of those of order $2^5\cdot3^2\cdot5^4$ is $7\cdot2\cdot5=70$.

From the preceding paragraph it results that it is very easy to determine the number of the possible abelian groups of a given order. It may be observed that two abelian groups which involve the same number of elements of each order are simply isomorphic, but this is not true as regards non-abelian groups. In fact, we can easily construct non-abelian groups which have the same number of elements of each order as

certain abelian groups. For instance, if s is an element of order 8 while t is of order 2, the two groups of order 16 generated by s and t, when these elements satisfy one of the following equations

$$tst = s, \quad tst = s^5,$$

evidently contain the same number of elements of each order.

To prove that two abelian groups which have the same number of elements of each order are always simply isomorphic, it is clearly only necessary to consider the case when their order is a power of a prime. In this case, it is easy to see that any change in the invariants will affect the number of elements of given orders. In fact, if the order of such a group is p^m, it has been observed that the elements of order p generate a group of order p^α, where α is the number of its invariants. The elements of order p^2, if there are such, generate a group of order $p^{2\alpha-\beta}$ where β is equal to the number of invariants which are equal to p, etc. Hence it results that *two abelian groups which have the same number of elements of each order are simply isomorphic.*

39. A Special Class of Abelian Groups. We gave, in § 5, illustrations of abelian groups which are generated by the $\phi(g)$ *totitives* of g, that is, by the $\phi(g)$ natural numbers which do not exceed g and are prime to g, and we shall now enter upon a more detailed study of these important abelian groups.* It is easy to see that they constitute the *groups of isomorphisms* of cyclic groups; that is, the groups according to which the elements of cyclic groups are permuted when these cyclic groups are made simply isomorphic with themselves in every possible manner. For the sake of simplicity we begin with two illustrative examples. Let $1, \alpha, \alpha^2, \alpha^3, \alpha^4$, represent the five fifth roots of unity. These may be put into a (1, 1) correspondence, or they can be made simply isomorphic with each other, in the following four ways, but in no other way:

* In the second edition of vol. 2 of Weber's *Lehrbuch der Algebra*, 1899, p. 60, these groups are called the most important example of abelian groups of finite order.

1 1	1 1	1 1	1 1
$\alpha\ \alpha$	$\alpha\ \alpha^2$	$\alpha\ \alpha^3$	$\alpha\ \alpha^4$
$\alpha^2\alpha^2$	$\alpha^2\alpha^4$	$\alpha^2\alpha$	$\alpha^2\alpha^3$
$\alpha^3\alpha^3$	$\alpha^3\alpha$	$\alpha^3\alpha^4$	$\alpha^3\alpha^2$
$\alpha^4\alpha^4$	$\alpha^4\alpha^3$	$\alpha^4\alpha^2$	$\alpha^4\alpha$

As the different ways in which a group can be made simply isomorphic with itself clearly correspond to the substitutions of a group, it results that the group of isomorphisms of the group of order 5 is of order 4. As a substitution group whose elements are the numbers 1, 2, 3, 4 the given group of isomorphisms may be represented in the following manner:

$$1, \qquad 1243, \qquad 1342, \qquad 14\cdot 23.$$

That is, the group of isomorphisms of the group of order 5 is the cyclic group of order 4. The same abstract group of order 4 is evidently generated by the following four numbers, when they are combined by multiplication:

$$1 \qquad 2 \qquad 3 \qquad 4 \qquad (\text{mod } 5).$$

As a second illustrative example we consider all the possible simple isomorphisms between the eight eighth roots of unity represented by the following symbols: $1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7$, where β is any root of the equation $x^4+1=0$. These isomorphisms may be represented as follows:

1 1	1 1	1 1	1 1
$\beta\ \beta$	$\beta\ \beta^3$	$\beta\ \beta^5$	$\beta\ \beta^7$
$\beta^2\beta^2$	$\beta^2\beta^6$	$\beta^2\beta^2$	$\beta^2\beta^6$
$\beta^3\beta^3$	$\beta^3\beta$	$\beta^3\beta^7$	$\beta^3\beta^5$
$\beta^4\beta^4$	$\beta^4\beta^4$	$\beta^4\beta^4$	$\beta^4\beta^4$
$\beta^5\beta^5$	$\beta^5\beta^7$	$\beta^5\beta$	$\beta^5\beta^3$
$\beta^6\beta^6$	$\beta^6\beta^2$	$\beta^6\beta^6$	$\beta^6\beta^2$
$\beta^7\beta^7$	$\beta^7\beta^5$	$\beta^7\beta^3$	$\beta^7\beta$

This group of isomorphisms, as a substitution group on the numbers 1, 2, . . . , 7, is as follows:

$$1 \qquad 13\cdot 57\cdot 26 \qquad 15\cdot 37 \qquad 17\cdot 35\cdot 26.$$

This group could have been equally well represented by

$$1 \qquad 13\cdot 57 \qquad 15\cdot 37 \qquad 17\cdot 35$$

and it is clear that it is simply isomorphic with the group formed by the following numbers, when they are combined by multiplication:

$$1 \qquad 3 \qquad 5 \qquad 7 \qquad (\text{mod } 8).$$

These examples may suffice to illustrate the fact that the group formed by the $\phi(m)$ totitives, with respect to multiplication (mod m), is the group of isomorphisms of the cyclic group of order m. To prove this fact it is only necessary to observe that the correspondence of the operators of lower orders in a cyclic group is completely determined by the correspondence of the operators of highest order, and that all of the latter may be obtained from any one of them by raising it to all the various powers which are prime to the order of the cyclic group. In particular, a necessary and sufficient condition that the number m has a primitive root is that the group formed by the $\phi(m)$ totitives (mod m) be cyclic. While the group formed by the totitives is always abelian, there are many abelian groups which cannot be represented in this way. Hence these groups form a special class of abelian groups.

We proceed to determine some conditions which must be satisfied in order that an abelian group G may belong to this class. When G is cyclic the matter is quite simple. It is necessary and sufficient that its order g be the exponent to which a primitive root of some number belongs. That is, whenever $g=p^a(p-1)$,* p being an odd prime number, and a being any positive integer or zero, the cyclic group G belongs to the given class, and only then. The lowest two even numbers which are not of the form $p^a(p-1)$ are 8 and 14; hence these numbers are the lowest orders of cyclic groups of an even order that cannot be the groups of isomorphisms of any cyclic groups whatever, and hence the cyclic groups of these two orders cannot be represented as groups of totitives.

* Cf. Dirichlet-Dedekind, *Zahlentheorie*, 1879, p. 340.

If g is written in the form $g=2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\ldots$ ($p_1, p_2, \ldots$ being different odd prime numbers), G is the direct product of its subgroups of orders 2^{α_0}, $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, . . . , and its group of isomorphisms I is evidently the direct product of the groups of isomorphisms of these subgroups. Since the group of isomorphisms of a cyclic group whose order is a power of an odd prime number is cyclic, it follows from the above that I is the direct product of the cyclic groups of orders $p_1^{\alpha_1-1}(p_1-1)$, $p_2^{\alpha_2-1}(p_2-1)$, . . . , when $\alpha_0=0$ or 1. When $\alpha_0>1$, we have to add a group of order 2 and a cyclic group of order 2^{α_0-2} to these factor groups in order to obtain I, since there are numbers which belong to the exponent 2^{α_0-2} (mod 2^α), but none which belong to a higher exponent.*

Since I is the direct product of groups of even orders, the order of I is always even when $g>2$. It can clearly be any even number of the form $2^{\beta_0}p_1^{\beta_1}p_2^{\beta_2}\ldots(p_1-1)(p_2-1)\ldots$ The smallest two natural numbers which are not of this form are 14 and 26;† hence these numbers are the lowest orders of groups that cannot be groups of isomorphisms of any cyclic group whatever. It is evident that the highest prime factor of the order of I can not exceed the highest prime factor of g.

EXERCISES

1. Determine the invariants of the group formed by the $40=\phi(100)$ totitives of 100 (mod 100).

2. The number of invariants in the group of the totitives of m (mod m) is equal to the number of the distinct odd prime factors of m whenever m is either odd or double an odd number. It is equal to the number of distinct prime factors of m, whenever m is divisible by 4 but not by 8; when m is divisible by 8, the number of these invariants is one more than the number of the distinct prime factors of m. Cf. Weber, *Lehrbuch der Algebra*, vol. 2, 1896, p. 59.

3. Find the three possible cyclic groups whose group of isomorphisms has the invariants 6, 2, 2.

4. If the operators of order 2 in the group of isomorphisms of the cyclic group of order m generate a group of order 2^α, what is the maximum number of the distinct primes which divide m? What is the minimum number of such divisors of m?

* Cf. H. Weber, *Lehrbuch der Algebra*, 2d ed., vol. 2, 1899, p. 64.

† Lucas, *Théorie des nombres*, 1891, p. 394.

5. If the group of totitives of m has for its order a power of a prime this order is of the form 2^α.

6. Every possible abelian group is a subgroup of some group of totitives.

Suggestion: If the invariants of the given abelian group are so chosen that each is a power of a prime number, it is clearly possible to choose m so that the group of totitives of m involves the same invariants.

40. Subgroups and Quotient Groups of any Abelian Group. It has been proved that every abelian group may be regarded as the direct product of cyclic groups and hence it is completely determined by the orders of these groups. As every subgroup of an abelian group is abelian, it results that these subgroups are also completely determined by the orders of the cyclic groups of which they are the direct products. Hence it follows immediately that *a necessary and sufficient condition that an abelian group G whose invariants are $i_1, i_2, \ldots, i_\rho$ contains a subgroup whose invariants are $j_1, j_2, \ldots, j_t$ is that it be possible to associate the t j's with t distinct i's so that each i is is divisible by the corresponding j.*

If such an arrangement were not possible the subgroup would involve more operators of a certain order than the entire group. The condition imposed upon the invariants of a subgroup is clearly equally applicable as regards the invariants of a quotient group. Hence we have the important theorem: *The invariants of any subgroup of an abelian group are invariants of a quotient group, and the invariants of any quotient group are also invariants of a subgroup.* In other words, each subgroup is simply isomorphic with a quotient group and vice versa. A like theorem is not always true as regards non-abelian groups.

If a group is cyclic all of its subgroups may be obtained by raising successively all of its operators to the same power, but this method cannot give all the subgroups of a non-cyclic group. The kth power of each operator of an abelian group G gives a group which is simply isomorphic with G whenever k is prime to g. If k is not prime to g, these kth powers constitute a quotient group of G, whose order is g divided by the total number of the operators of G whose orders divide k.

While it is not difficult to find, by means of the theorem stated above, the total number of the different types of subgroups in a given abelian group whose invariants are known, it is a problem of considerable difficulty to determine all the possible subgroups of the same type. To illustrate this fact we consider the subgroups of the important class of abelian groups of order p^m and of type (1, 1, . . . , to m units). In this case there are evidently $m-1$ different types of subgroups, excluding the identity. That is, there is one and only one type of subgroups of order p^α, $\alpha=1, 2, \ldots, m-1$, separately.

In this case it is also not very difficult to determine the number of the different subgroups of order p^α. In fact, this number is clearly equal to the quotient obtained by dividing the total number of ways in which generating operators of such a subgroup can be selected from the operators of the group by the number of ways in which such generators can be selected from the operators of the subgroup. Hence this number is

$$\frac{(p^m-1)(p^m-p)(p^m-p^2)\ \ldots\ (p^m-p^{\alpha-1})}{(p^\alpha-1)(p^\alpha-p)(p^\alpha-p)\ \ldots\ (p^\alpha-p^{\alpha-1})} = \frac{(p^m-1)(p^{m-1}-1)\ \ldots\ (p^{m-\alpha+1}-1)}{(p^\alpha-1)(p^{\alpha-1}-1)\ \ldots\ (p-1)}.$$

In the particular case when $\alpha=m-1$, this formula reduces to

$$\frac{p^m-1}{p-1}.$$

Hence there are as many subgroups of order p^{m-1} in an abelian group of order p^m and of type (1, 1, 1, . . .), *as there are subgroups of order p.* For instance, the group of order 8 and of type (1, 1, 1) has seven subgroups of order 2 and also seven subgroups of order 4, while the group of order 16 and of type (1, 1, 1, 1) has fifteen subgroups of order 2 and fifteen subgroups of order 8.

EXERCISES

1. A necessary and sufficient condition that a group be abelian is that each operator corresponds to its inverse in one of the possible automorphisms of the group.*

2. Find the number of subgroups with invariants 6, 2 in the abelian group whose invariants are 12, 6, 2.

3. Determine the number of the subgroups of each possible order in all the abelian groups of order p^3, p being a prime.

4. Every abelian group is generated by its operators of highest order.

5. Give an instance of a non-abelian group which is not generated by its operators of highest order.

41. Group of Isomorphisms of an Abelian Group.† Some of the most useful properties of an abelian group are exhibited by its group of isomorphisms. We have already considered the group of isomorphisms of a cyclic group and found that it is an abelian group. We shall see that a necessary and sufficient condition that the group of isomorphisms of an abelian group G be abelian is that G be cyclic, and hence it results that the groups of totitives are the only abelian groups of isomorphisms of abelian groups. This fact is a special case of the theorem that *the invariant operators of the group of isomorphisms of any abelian group constitute a group which is simply isomorphic with the group of the totitives of the largest possible invariant of this abelian group.* For instance, if an abelian group has the invariants 10, 10, 2, the invariant operators of its group of isomorphisms constitute the cyclic group of order 4. We proceed to prove the stated theorem.

We shall first prove that if an operator t of the group of isomorphisms of an abelian group G transforms every operator of G into the same power (γth) of itself it must be commutative with every operator of the group of isomorphisms of G. Let t_1 be any other operator of this group of isomorphisms and suppose that

$$t_1^{-1} s_\alpha t_1 = s_\beta, \quad t^{-1} s_\alpha t = s_\alpha^{\gamma},$$

* This includes the theorem that every group which involves no operator whose order exceeds 2 is abelian.

† Cf. A. Ranum, *Transactions of the American Mathematical Society*, vol. 8 (1907), p. 83.

s_α being an arbitrary operator of G. Since

$$t^{-1}t_1^{-1}s_\alpha t_1 t = s_\beta^{\gamma} = t_1^{-1}t^{-1}s_\alpha t t_1$$

it results that t and t_1 are commutative. On the other hand, suppose that t is commutative with every operator in the group of isomorphisms of G. We shall first prove that t must transform every operator of highest order in G into a power of itself. For, if s_α is such an operator and

$$t^{-1}s_\alpha t = s_\delta s_\alpha,$$

where s_δ is not a power of s_α, it is clearly possible to find an operator t_1 in the group of isomorphisms of G such that t_1 is commutative with s_α but not with s_δ. As it is necessary then that

$$t^{-1}t_1^{-1}s_\alpha t_1 t = s_\delta s_\alpha, \quad t_1^{-1}t^{-1}s_\alpha t t_1 \neq s_\delta s_\alpha,$$

it results that t is not commutative with every operator of the group of isomorphisms of G unless it transforms every operator of highest order of G into a power of itself.

We shall now show that t must transform into the same power every operator of highest order in G, and hence it must transform every operator of G into this power, since these operators of highest order generate G. It results from the manner in which the invariants of any abelian group were determined that the group of isomorphisms of G transforms its operators of highest order transitively. That is, the group of isomorphisms of G may be represented as a transitive substitution group in which each letter stands for an operator of highest order in G. If s_α, s_β represent two operators of highest order in G and if

$$t^{-1}s_\alpha t = s_\alpha^{\gamma}, \quad t^{-1}s_\beta t = s_\beta^{\delta}, \quad \gamma \neq \delta,$$

we can find an operator t_2 in the group of isomorphisms of G such that

$$t_2^{-1}s_\alpha t_2 = s_\beta.$$

Hence it results that

$$t^{-1}t_2^{-1}s_\alpha t_2 t = s_\beta^{\delta}, \quad t_2^{-1}t^{-1}s_\alpha t t_2 = s_\beta^{\gamma}$$

That is, t, t_2 are not commutative unless $\gamma = \delta$. This completes a proof of the theorem: *A necessary and sufficient con-*

*dition that an operator of the group of isomorphisms of an abelian group be invariant under this group, is that it should transform every operator of this abelian group into the same power of itself.**

Since two abelian groups having the same invariants can be made simply isomorphic, and two simply isomorphic groups have the same invariants, it results that the order of the group of isomorphisms expresses also the number of different ways of choosing the independent generators of the group. It should be observed that while every operator of highest order in an abelian group may be used as an independent generator, and hence each operator of highest order must correspond to every other operator of this order in some simple isomorphism of the group with itself, it is not generally true that every operator of lower order corresponds to every operator of its own order in some simple isomorphism of the group.

This fact may be illustrated by means of the abelian group whose invariants are p^2 and p. It is evident that this group contains a characteristic subgroup of order p; viz., the subgroup of order p which is generated by its operators of order p^2. The remaining p subgroups of order p in the given group of order p^3 are conjugate under the group of isomorphisms of this group.

In any automorphism of any abelian group G each operator of G corresponds to itself multiplied by some operator of G. The totality of these multiplying operators evidently constitutes a group T which is either G itself or a subgroup of G, and the automorphism may be obtained by making G isomorphic with T and multiplying corresponding operators. In this isomorphism no operator except the identity can correspond to its inverse. As this condition is necessary as well as sufficient we have arrived at the following fundamental

THEOREM: *Every automorphism of an abelian group G may be obtained by* (1) *making G isomorphic with one of its subgroups or with itself in such a manner that no operator besides the identity corresponds to its inverse, and* (2) *making each operator of G*

* *Transactions of the American Mathematical Society*, vol. 1 (1900), p. 397; vol. 2 (1901), p. 260.

correspond to itself multiplied by the operator which corresponds to it in this isomorphism.

The simplest case that can present itself is the one in which the subgroup of G which corresponds to the identity of T includes T. The resulting simple isomorphism of G with itself must correspond to an operator in the group of isomorphisms of G, whose order is equal to the order of the operator of highest order in T. When the order of T is an odd prime number p, or double such a number, only one other case can present itself; viz., the case in which T, or its subgroup of odd order, corresponds to itself in the given isomorphism between G and T. In this case the isomorphism corresponds to an operator whose order divides $p-1$, in the group of isomorphisms of G. These results give rise to the following theorem: *If we make an abelian group G simply isomorphic with itself by multiplying its operators by those of a subgroup whose order is p, or $2p$ (p being an odd prime), the resulting automorphism of G corresponds to an operator of order p, $2p$, or $(p-1)/\alpha$ (α being a divisor of $p-1$), in the group of isomorphisms of G.*

The determination of all the possible orders of the corresponding operators in the group of isomorphisms of any abelian group, when T is a given subgroup, seems to be a problem of considerable difficulty. When the order of T is small the number of cases that have to be considered is also small. In addition to the orders included in the given theorems, we have the following, when the order of T does not exceed 8: If T is the cyclic group of order four, the resulting isomorphism may also correspond to an operator of order two in the group of isomorphisms, and when T is the non-cyclic group of this order, it may also correspond to operators of orders 3 and 4. When T is the cyclic group of order 8, the orders of these operators may be 2, 4, and 8; when T is the direct product of the cyclic group of order 4 and an operator of order 2, the orders of the corresponding operators in the group of isomorphisms may be 2 and 4; finally, when T is the direct product of three operators of order 2, the given operators may be of orders 2, 3, 4, 6, and 7. While all of the possible cases for a given T may present themselves in

the same group, it is evident that this does not always happen.

For the sake of illustration we consider the group of isomorphism of the group of order 8 which is the direct product of three operators of order 2.* Each of its 7 subgroups of order 4 leads to three operators of order 2. We thus obtain the 21 operators of order 2 of the required group of isomorphisms when we consider all the possible instances in which the order of T is 2. If the order of T is 4, two cases present themselves, in one case just two of the operators of T (including identity) correspond to operators of T, and in the other case each one of the operators of T corresponds to some operator of T. The former case leads to the 42 operators of order 4, and the latter to the 56 operators of order 3 of the required group of isomorphisms. Finally, we obtain 48 operators of order 7 when we consider all the possible instances in which the order of T is 8. Hence the group of isomorphisms in question is the well-known group of degree 7 and of order 168.

42. Groups of Isomorphisms of the Groups of Order p^2. A group of order p^2 is abelian and there are two such groups. The group of isomorphisms I of the cyclic group of order p^2 is the cyclic group of order $p(p-1)$. If s is a generator of this group of order p^2, we may select for a generator of its I any operator t of order $p(p-1)$ such that $t^{-1}st=s^\alpha$, where α is any primitive root of p^2. If the order of the multiplying subgroup T in such an isomorphism is p, the corresponding operators of I constitute its subgroup of order p. The remaining operators of I result when T is of order p^2, p being an odd prime number.

When the group G of order p^2 is non-cyclic, the order of its I is clearly $(p^2-1)(p^2-p)$, and this I is isomorphic with a transitive group of degree $p+1$ corresponding to the transformations of the $p+1$ subgroups of order p contained in G. There is clearly a $(p-1, 1)$ isomorphism between I and this transitive group of degree $p+1$, since the $p-1$ invariant operators of I are the only ones which transform every subgroup of G into itself.

* Cf. E. H. Moore, *Bulletin of the American Mathematical Society*, vol. 1 (1894), p. 63.

If we regard I as a substitution group on p^2-1 letters it is transitive, its subgroup composed of all its substitutions which omit one letter omits $p-1$ letters, and it is a regular group on the remaining p^2-p letters. This subgroup contains a single Sylow subgroup of order p, which corresponds to the cases when the multiplying subgroup T is composed of the invariant operators of G under the isomorphisms in question. The orders of all its other operators divide $p-1$ as they correspond to the cases when T, under the isomorphism in question, is a non-invariant subgroup of order p; and this subgroup of order $p(p-1)$ is simply isomorphic with the metacyclic group of degree p, which represents the transformations of p Sylow subgroups of G under this subgroup of I. As a substitution group on p^2-1 letters the group I is clearly imprimitive when p is odd, and its $p+1$ systems of imprimitivity are permuted according to a triply transitive group of degree $p+1$ and of order $p(p^2-1)$, discovered by Mathieu.*

It is easy to determine the number and the orders of all the substitutions of I whose degrees are less than p^2-1. In fact, since the subgroup of I which is composed of all its substitutions omitting one letter is regular, and of order p^2-p, it follows directly that I involves $(p^2-p-1)(p+1)$ different substitutions each of which omits exactly $p-1$ letters. The order of p^2-1 of these is p, while the orders of all the others are divisors of $p-1$. If d represents any divisor of $p-1$, then the number of these substitutions which are of order d is $p(p+1)\phi(d)$. All the substitutions of order p are conjugate, but there are $\phi(d)$ equal sets of conjugate substitutions of order d and of degree p^2-p. The isomorphic group of degree $p+1$ and of order $p(p^2-1)$, according to which the $p+1$ subgroups of G are transformed, contains also p^2-1 conjugate substitutions of order p, and all its substitutions whose degree is less than p are of degree $p-1$ and have orders which divide $p-1$. The number of these substitutions whose order is d is $\frac{1}{2}p(p+1)\phi(d)$.

* E. Mathieu, Paris *Comptes Rendus*, vol. 47 (1858), p. 698.

43. Abelian Groups which are Conformal with Non-abelian Groups. Two distinct groups are said to be *conformal* when they contain the same number of operators of each order.* We proceed to determine all the abelian groups which are conformal with non-abelian groups. The complete solution of the converse of this problem, viz., the determination of all the non-abelian groups which are conformal with abelian ones, is much more difficult, since a large number of distinct non-abelian groups may be conformal with the same abelian group, while no more than one abelian group can be conformal with one non-abelian group. In fact, it was observed in § 37 that two distinct abelian groups cannot be conformal.

It is evident that there is only one group of order 2^m which does not include any operator of order 4, viz., the abelian group of type (1, 1, 1, . . .). Moreover, there is only one cyclic group of order 2^m, and when $m<4$ no two groups of order 2^m are conformal. We proceed to prove that every abelian group G of order 2^m which does not satisfy one of these conditions is conformal with at least one non-abelian group.

Let H be the subgroup of G which is generated by the square of one of its independent generators s of lowest order, together with all the other independent generators of G. The order of H is 2^{m-1}. Since $m>3$ there is an operator t of order 2 which has the following properties: It transforms H into itself, it is commutative with half of the operators of H (including all those which are not of highest order), and it transforms the rest into themselves multiplied by an operator of order 2 which is not the square of a non-invariant operator of H; i.e., t does not transform an operator of order 4 contained in H into its inverse. The non-abelian group generated by H and t is conformal with G whenever $s^2=1$.

When the order of s exceeds two, the group generated by t and H (written as a regular substitution group) may be made simply isomorphic with itself by writing it on two distinct sets of letters. If in this intransitive group t is replaced by the continued product of t, the substitution of order two

* *Quarterly Journal of Mathematics*, vol. 28 (1896), p. 270.

which merely permutes corresponding letters of the two systems of intransitivity, and s^2 in one of the systems of letters, there results a transitive group which is conformal with G. That is, any abelian group of order 2^m, $m>3$, which is neither cyclic nor of type (1, 1, 1, . . .), is conformal with at least one non-abelian group.

It will now be assumed that the order of G is p^m (p being an odd prime number and $m>2$), and that G is non-cyclic. Let H be the subgroup generated by s^p (s being one of the independent generators of lowest order in G) together with all the other independent generators of G. There is an operator t of order p which transforms H into itself, is commutative with each of its operators contained in a subgroup of order p^{m-2}, and transforms the rest into themselves multiplied by invariant operators of order p. This t and H generate a group which is conformal with G whenever $s^p=1$; for, if s_1 is any substitution of H that is not commutative with t, it is easy to see that

$$(ts_1)^p = ts_1ts_1 \ . \ . \ . \ (p \text{ times})$$
$$= ts_1t^{-1}t^2s_1t^{-2}t^3s_1t^{-3}t^4 \ . \ . \ . \ t^{1-p}t^ps_1 = s_1{}^p.*$$

When s^p differs from identity the group generated by H and t, written as a regular group, may be made simply isomorphic with itself $p-1$ times, by writing each substitution in p distinct sets of letters; and t may be replaced by the continued product of t, the substitution of order p which merely permutes the corresponding letters of these systems of intransitivity, and the pth power of s in one of these systems. In the resulting group the pth power of the operators will be the same as those of G taken in the same order, and hence this group will be conformal with G.

If a non-abelian group whose order is not some power of a prime is conformal with an abelian group G, it must be the direct product of its Sylow subgroups, and hence each of these subgroups is conformal with an abelian group, and at least one of them is non-abelian. From what precedes, it may be observed that necessary and sufficient conditions that any abelian group

* *Transactions of the American Mathematical Society*, vol. 2 (1901), p. 262.

of order $2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\ldots$ (p_1, p_2, . . . being distinct odd primes) be conformal with at least one non-abelian group are: 1^0 at least one of its subgroups of orders 2^{α_0}, $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, . . . is non-cyclic; 2^0 if the order $p_\beta^{\alpha_\beta}$ of this subgroup is odd, then $\alpha_\beta > 2$; if the order is even (2^{α_0}), then the subgroup must involve operators of order 4 and $\alpha_0 > 3$. Since any number of these factors may be non-abelian, there cannot be an upper limit to the number of non-abelian groups which can be conformal with an arbitrary abelian group. This fact may be seen in many other ways.

EXERCISES

1. Let s be of order 16 and let t represent an operator of order 2 such that $tst = s^9$; prove that (s, t) is conformal with the abelian group whose invariants are 16, 2.

2. Find the group of isomorphisms of the abelian group whose invariants are 8, 2 and determine its invariant operators.

3. If p is an odd number, there is at least one non-abelian group of order p^m, $m > 2$, which is conformal with the abelian group of type (1, 1, . . . to m units). The number of such possible groups increases with m and has no upper limit.

4. Any operator of order p^δ in any abelian group whatever can be used as an independent generator provided its $p^{\delta-1}$th power is not included in a cyclic subgroup of order $p^{\delta+1}$.

5. Every possible group of finite order is a subgroup of the group of isomorphisms of an abelian group of order 2^m and of type (1, 1, 1, . . .).

Suggestions: Observe that this group of isomorphisms contains a subgroup which is simply isomorphic with the symmetric group of degree m.

44. Characteristic Subgroups of an Abelian Group. In § 29 a characteristic subgroup was defined as a subgroup which corresponds to itself in every possible automorphism of the group. An operator which corresponds to itself in every possible automorphism of the group is likewise called a *characteristic operator*. It is clear that every characteristic subgroup is also an invariant subgroup, and that every characteristic operator is also an invariant operator; but invariant subgroups and invariant operators are not necessarily characteristic. The Sylow subgroups of an abelian group whose order is not a power of a single prime are evidently characteristic subgroups.

If G is an abelian group of order p^m and of type $(1, 1, 1, \ldots)$, it contains no characteristic subgroup besides the identity; but every other abelian group contains at least one characteristic subgroup besides the identity. Suppose that G is an abelian group of order p^m but not of type $(1, 1, 1, \ldots)$, and let p^{α_1} be one of its largest invariants. If exactly λ_1 of the invariants of G are equal to p^{α_1}, then G contains a characteristic subgroup of order p^{λ_1} and of type $(1, 1, 1, \ldots)$. This characteristic subgroup C_1 has been called the *fundamental characteristic subgroup* * of G, since it is contained in every possible characteristic subgroup of G besides the identity, as we shall prove in the following paragraph.

It is evident that the subgroup of order p^{λ_1}, which is composed of the identity and of all the operators of order p which are generated by the operators of highest order contained in G, is the characteristic subgroup C_1. Moreover, the conjugates under the group of isomorphisms I of every operator of order p, which is found in G but not in C_1, generate a characteristic subgroup of G which includes C_1 as a subgroup. This fact results immediately from the different possible ways of selecting the independent generators of G. If the second largest invariants of G are p^{α_2}, and if there are exactly λ_2 such invariants in G, then G contains also a characteristic subgroup C_2 of order $p^{\lambda_1+\lambda_2}$, which is composed of the identity and of the operators of order p which are generated by the operators of order p^{α_2} contained in G. By continuing this process we clearly arrive at the following

THEOREM. *If a group G of order p^m has λ_1 invariants which are equal to p^{α_1}, λ_2 which are equal to p^{α_2}, $\ldots$, λ_β which are equal to p^{α_β}, where $\alpha_1 > \alpha_2 > \ldots > \alpha_\beta$, then G has β characteristic subgroups $C_1, C_2, \ldots, C_\beta$, besides the identity, such that each of them is generated by operators of order p. Their orders are $p^{\lambda_1}, p^{\lambda_1+\lambda_2}, \ldots, p^{\lambda_1+\lambda_2+\cdots+\lambda_\beta}$, respectively, and each is included in all of those which follow it.*

Since every operator of highest order contained in an abelian group can be used as an independent generator of the group,

* *American Journal of Mathematics*, vol. 27 (1905), p. 15.

it is clear that a characteristic subgroup of G cannot involve any of its operators of order p^{α_1}. All the operators of G whose orders divide $p^{\alpha_1-\beta_1}$, where β_1 has any value from 1 to α_1-1, constitute a characteristic subgroup of G. The characteristic subgroup C_β of the preceding theorem corresponds to the case when $\beta_1=\alpha_1-1$. If all the invariants of G are equal, there is only one characteristic subgroup of G, besides the identity, which involves operators of order p^{β_1} but none of higher order. It is also evident that the p^{β_1}th powers of all the operators of G constitute a characteristic subgroup of G.

If s is any independent generator of G, the conjugates of s under the group of isomorphisms of G generate a group which involves all the operators of G whose orders do not exceed the order of s. In other words, *if a characteristic subgroup involves an independent generator of an abelian group, it also involves all the operators of this abelian group whose orders divide the order of this independent generator.* This theorem clearly includes the theorem stated above, to the effect that a characteristic subgroup cannot involve any of the operators of highest order contained in G. In the following paragraph we shall establish a still more general theorem in case $p>2$.

For a study of the special properties of the characteristic subgroups it is convenient to let $H_1, H_2, \ldots, H_\beta$ represent the subgroups of G which are generated respectively by a set of λ_1 independent generators of order p^{α_1}, a set of λ_2 independent generators of order p^{α_2}, . . . , a set of λ_β independent generators of order p^{α_β}. Suppose that $p>2$ and that s_1 is some operator of order p^δ, $\alpha_1>\delta$, which is contained in G. If $\alpha_\gamma>\delta\geqq\alpha_{\gamma+1}$, and if s_1 is the product of an operator of highest order in $H_{\gamma+1}$ and an operator of order p^δ from H_γ, then the conjugates of s_1 under I generate a group which involves all the operators of order p^δ that are contained in G. In fact, this group clearly involves an independent generator of $H_{\gamma+1}$ since $p>2$, and it involves all the operators of order p^δ in the direct product of the subgroups $H_1, \ldots, H_\gamma$.

By means of the preceding theorems it is not difficult to determine the characteristic subgroups of any given abelian

group of order p^m. If the order of an abelian group is not a power of a single prime number its characteristic subgroups are found by forming the direct product of the characteristic subgroups of its Sylow subgroups, and all such direct products are characteristic subgroups of G.

EXERCISES

1. If an abelian group G of order p^m has only two distinct invariants p^{α_1}, p^{α_2}, and if $\alpha_1-\alpha_2=n$, then the number of the characteristic subgroups which are generated by the operators of order p^δ is 2, when $n=1$ and δ has any one of the values from 1 to α_1-1. The number of these subgroups cannot exceed the smaller of the two numbers $n+1$, α_2+1 for any value of δ.

2. Find all the characteristic subgroups of the abelian group of order p^6 and of type (1, 2, 3).

3. The abelian group of order 16 and of type (1, 3) has the property that no single set of operators of order 4, which are conjugate under its group of isomorphisms, generates all its operators of this order. Prove that whenever $p>2$ all the operators of order p^2 in the abelian group of order p^4 and of type (1, 3) are generated by a single set of operators of order p^2 which are conjugate under its I.

45. Non-abelian Groups in which Every Subgroup is Abelian. Let G represent any non-abelian group all of whose subgroups are abelian. As instances of such groups we may cite the octic and quaternion groups. We shall first prove that G must contain an invariant subgroup of prime index p. Suppose that G is represented as a transitive substitution group of the smallest possible degree. If this group is imprimitive it must transform a set of systems of imprimitivity according to a primitive group which has a $(1, \alpha)$ isomorphism with G.

This primitive group must be such that each of its subgroups is abelian, and hence we have only to prove that every primitive group which contains only abelian subgroups has an invariant subgroup of index p. If this primitive group were regular it would be of order p. If it were non-regular and of degree n, a maximal subgroup of degree $n-1$ would be abelian and hence all of its substitutions besides the identity would be of degree $n-1$; for, if the degree of such a substitution were less than $n-1$, this substitution would occur in two maximal

abelian subgroups and hence it would be invariant under the entire group. Consequently this primitive group of degree n would involve exactly $n-1$ substitutions of degree n, while each of its remaining substitutions besides the identity would be of degree $n-1$.

The substitution groups which have these properties have been studied extensively. Frobenius * proved that such a group must have an invariant subgroup of order n. This important fact will be proved in § 139. If we assume this theorem for the present, it results that G must contain an invariant subgroup of index p, since the quotient group with respect to the given subgroup of order n is abelian.

We shall now prove that the order g of G cannot be divisible by more than two distinct prime numbers. Suppose that $g = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\lambda^{\alpha_\lambda}$, where $p_1, p_2, \ldots, p_\lambda$ are distinct prime numbers. Since G contains an invariant abelian subgroup of prime index, we may suppose that it contains an invariant subgroup H of order h, where h is given by the formula

$$h = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_\lambda^{\alpha_\lambda}.$$

As H is the direct product of its Sylow subgroups and as every operator of G which is not in H has an order which is divisible by p_1, it results directly that G contains only one Sylow subgroup of each of the orders $p_2^{\alpha_2}, \ldots, p_\lambda^{\alpha_\lambda}$.

Let s be any operator, which is found in G but not in H and whose order is of the form p_1^{β}. As s transforms each of the Sylow subgroups of H into itself, and as G is non-abelian, s must be non-commutative with some of the operators in one of these Sylow subgroups. This Sylow subgroup and s must generate G, otherwise G would involve a non-abelian subgroup. This completes the proof of the fact that *the order of a non-abelian group which contains only abelian subgroups cannot be divisible by more than two distinct prime numbers.*

Suppose that the order of G is $p_1^{\alpha_1} p_2^{\alpha_2}$, $\alpha_2 > 0$, and that G contains an invariant subgroup of order $p_1^{\alpha_1 - 1} p_2^{\alpha_2}$, and represent the Sylow subgroups of orders $p_1^{\alpha_1}$ and $p_2^{\alpha_2}$ by P_1 and P_2 respec-

* Frobenius, *Berliner Sitzungsberichte*, 1902, p. 455.

tively. We proceed to prove that P_1 is cyclic and that P_2 is of type (1, 1, 1, . . .). That P_1 is cyclic follows directly from the fact that s transforms P_2 into itself and that G is generated by s and P_2. In fact, it is evident that $\alpha_1 = \beta$. If P_2 were not of type (1, 1, 1, . . .), it would contain characteristic subgroups generated by its operators whose orders are divisors of $p_2, p_2^2, \ldots, p_2^{r-1}$, where p_2^r is the order of its operators of highest order. All of the operators of these characteristic subgroups would be composed of operators which would be commutative with s, since G cannot contain a non-abelian subgroup. Hence s would have to transform among themselves all the operators of order p_2^r in P_2 which have the same p_2th power. As the number of these operators is a power of p_2, this is impossible. That is, we have arrived at an absurdity by assuming that $r > 1$, and hence we have established the theorem: *If a non-abelian group which contains only abelian subgroups has more than one Sylow subgroup, one of these subgroups is of the type* (1, 1, 1, . . .) *and the others are cyclic.*

EXERCISES

1. If all the subgroups of a non-abelian group of order p^m, p being a prime number, are abelian, its commutator subgroup is of order p and the pth power of each of its operators is invariant.*

2. Every subgroup of the dicyclic group of order $4p$ is abelian.

3. If every subgroup of order p^{m-1} in a non-abelian group of order p^m is abelian, there must be exactly $p+1$ such subgroups.

4. The group of order 56 which contains 8 subgroups of order 7 does not involve any non-abelian subgroup.

46. Roots of the Operators of an Abelian Group. If $s_1, s_2, \ldots, s_\theta$ are the operators of an abelian group G, and if G contains two operators s_α, s_β which are such that $s_\alpha^n = s_\beta$, then s_α is said to be an nth root of s_β. In particular, every operator of G is a gth root of the identity, so that the identity has g gth roots under G. If n is prime to g every operator of G has one and only one nth root. On the other hand, if n is a divisor of g, the total number of the operators of G whose orders divide

* Cf. G. A. Miller and H. C. Moreno, *Transactions of the American Mathematical Society*, vol. 4 (1903), p. 403.

n is always divisible by n. These operators constitute a subgroup H_1 of G. If an operator of G has one nth root it must have h_1 such roots, h_1 being the order of H_1.

Whenever n is a divisor of g all the operators of G may be divided into two classes according as they have nth roots or do not have this property. As each operator of the first class has exactly h_1 nth roots, the number of the operators in this class is g/h_1. The number of the operators in the second class is therefore $g-g/h_1$. When G is cyclic, $h_1=n$.

If d is the highest common factor of n and g every operator of G which has one nth root must have either d or a multiple of d such roots, since the total number of the operators of G whose orders divide d is divisible by d. The number of the operators which have nth roots is evidently equal to g/h_2, h_2 being the order of the subgroup H_2 which is composed of all the operators of G whose orders divide d.

The h_2 operators of G which are nth roots of the same operator correspond to the same operator in the quotient group G/H_2. Every operator of G is clearly an nth root of one and of only one operator of G, but a given operator may have a number of different nth roots. If a group is non-abelian two operators which have nth roots need not have the same number of such roots.

For instance, in the symmetric group of order 6 the identity has three square roots while each of the two operators of order 3 has only one such root.

47. Hamilton Groups. A non-abelian group G is said to be a *Hamilton group*, or a Hamiltonian group, if each of its subgroups is invariant. While these groups are not abelian, they have in common with the abelian groups the property that every subgroup is invariant. They were thus named by Dedekind in honor of Sir W. R. Hamilton, and some of their fundamental properties were first studied by Dedekind in view of their usefulness in the study of the number realms which belong to such groups.*

Since every subgroup of G is invariant, G must be the direct

* R. Dedekind, *Mathematische Annalen*, vol. 48 (1897), p. 548.

product of its Sylow subgroups. *If all the subgroups of a Sylow subgroup of odd order are invariant, this Sylow subgroup must be abelian.* In fact, if the order of such a subgroup P_m is p^m, then each of its operators of order p must be invariant, since the group of isomorphisms of the cyclic group of order p is of order $p-1$. Suppose that P_m contains a cyclic subgroup C_α of order p^α such that C_α involves non-invariant operators.

If this were possible P_m would contain an operator s which would transform C_α into itself without being commutative with every operator of C_α. As the operators of C_α would also transform into itself the cyclic group S_β generated by s, it follows that the commutators, involving elements from C_α and S_β, would be in both of these cyclic groups. These commutators would therefore be in the central of the group generated by C_α and S_β. We may suppose that s was so selected that s^p is commutative with every operator of C_α. As the group generated by C_α and this s would contain non-invariant operators which would not generate the commutator subgroup of order p, it results that P_m must be abelian.

We have now proved that every Hamilton group is the direct product of a Hamilton group of order 2^m and some abelian group of odd order. Hence it remains only to determine the possible Hamilton groups of order 2^m. As an instance of such a group we may cite the quaternion group. We shall first prove that such a group H cannot involve any operator whose order exceeds 4.

In fact, if H contained an operator s whose order exceeds 4, we could find a subgroup in H, by the method used above, which would contain a non-invariant operator which would not generate the commutator of this subgroup. Hence we can assume that the order of every operator of H is either 2 or 4. Moreover, the operators of order 2 are contained in the central of H, while each operator of order 4 is transformed either into itself or into its inverse by every operator of H. Two of these non-commutative operators of order 4 must have a common square, and hence any two such operators must generate the quaternion group.

The group generated by any one such quaternion group and the operators of order 2 contained in H must coincide with H. In fact, if an operator s of H were not contained in this group, this operator and this group would generate a group which would involve more operators of order 2. As this is contrary to the hypothesis, we have established the following theorem: *Every possible Hamilton group is the direct product of a quaternion group, an abelian group of order* 2^m *and of type* (1, 1, 1, . . .), *and an abelian group of odd order.**

A group which is a direct product of two groups is sometimes called a *divisible* group. If it is not a direct product it is said to be *indivisible*. Hence the quaternion group is the only indivisible Hamiltonian group. The only indivisible abelian groups are the cyclic groups whose orders are powers of prime numbers. If an abelian group is written as the product of indivisible groups, the orders of these groups constitute the largest possible set of invariants of the abelian group.

EXERCISES

1. The commutator quotient group of a Hamilton group of order 2^m is abelian and of type (1, 1, 1, . . .).

2. The number of the possible Hamilton groups of order $2^m k$, k being any odd number, is equal to the number of the abelian groups of order k.

3. Every Hamilton group has the four-group as a group of inner isomorphisms.

4. Two and only two of the operators of a Hamilton group are characteristic.

5. Let $g = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}$, where $p_1, p_2, \ldots, p_\lambda$ are distinct primes. Necessary and sufficient conditions that all existing groups of order g shall be abelian are: (1) each $\alpha_j \leqq 2$; (2) no $p_j^{\alpha_j} - 1$ is divisible by one of the primes $p_1, p_2, \ldots, p_\lambda$. Cf. L. E. Dickson, *Transactions of the American Mathematical Society*, vol. 6 (1905), p. 201.

* This theorem, together with various other theorems relating to Hamilton groups, was proved by G. A. Miller, *Bulletin of the American Mathematical Society*, vol. 4 (1898), p. 510. Some of these theorems were proved several years later by E. Wendt, *Mathematische Annalen*, vol. 59 (1904), p. 187. In the following volume of this journal Wendt corrected this oversight.

CHAPTER V

GROUPS WHOSE ORDERS ARE POWERS OF PRIME NUMBERS

48. Introduction. It has been observed in § 11 that if p^α is the highest power of the prime p which divides the order of a group G then G must involve at least one subgroup of order p^α, and if G involves more than one such subgroup, all the subgroups of this order (Sylow subgroups) form a complete set of conjugates. These facts indicate that it is especially important to know the fundamental properties of *Sylow's groups;* * that is, of groups whose orders are powers of prime numbers. Fortunately all these Sylow groups have unusually interesting properties in common and they offer more easy avenues of penetration than the groups whose orders are arbitrary numbers.

A strong instrument of attack here, as well as in many other places in group theory, is the concept of complete sets of conjugates. Each non-invariant operator of a non-abelian group G of order p^m belongs to a complete set of p^α conjugates, since such an operator is transformed into itself by all the operators of a subgroup whose order is p^β, $\beta < m$. Hence all the non-invariant operators of G occur in sets, such that each set involves a power of p conjugate operators, and each non-invariant operator occurs in one and in only one set. The total number of the non-invariant operators must therefore be of the form pk; and, as there are $p^m - 1$ operators besides the identity in G, *there must be an invariant operator of order p in G.* This

* The groups whose orders are powers of prime numbers are also known as primary groups. G. Frobenius and L. Stickelberger, *Journal reine angew. Math.*, vol. 86 (1879), p. 219. They are sometimes called prime-power groups. In view of the unusually large number of useful theorems in this field these groups have been said to constitute the El Dorado of the theory of groups. *Bulletin of the American Mathematical Society*, vol. 6 (1900), p. 393.

theorem was first proved by L. Sylow * and it may be regarded as the most important theorem relating to the prime-power groups.

It has been observed that the totality of the invariant operators of any non-abelian group constitutes an important subgroup known as the central. With respect to its central, G is isomorphic to a group of order $p^{m'}$, $m' < m$. This quotient group must also have a central subgroup, if it is non-abelian, and this gives rise to a second quotient group of order $p^{m''}$, $m'' < m'$. By continuing this process we must arrive at an abelian quotient group. It is a matter of considerable importance to observe that this abelian group is never cyclic. In fact, this is a special case of the theorem proved in § 28 that the central quotient group of a non-abelian group is always non-cyclic.

The subgroup of G which corresponds to an invariant subgroup of order p in the central quotient group of G is abelian, but includes operators which are not in the central of G. Hence it results that *every non-abelian group of order p^m contains an invariant abelian subgroup whose operators are not separately invariant under the group.*

Since we can always arrive at the identity by forming successive central quotient groups of G it results that G must have at least one invariant subgroup whose order is an arbitrary divisor of the order of G. Suppose that $H_1, H_2, \ldots, H_\rho$ represent any complete set of conjugate subgroups of G. Since each of these subgroups is transformed into itself by a subgroup of G whose order is a power of p, it results that ρ is also a power of p. Hence each of these H's must transform into itself each one of at least $p-1$ of the other H's, since it transforms itself into itself, and since it must transform a multiple of p of these conjugates among themselves. That is, *each one of a complete set of conjugate subgroups of a group of order p^m is transformed into itself by at least $p-1$ others of the set, if the set includes more than one subgroup.* In particular, *every subgroup of order p^{m-1} in a group of order p^m is invariant under*

* *Mathematische Annalen*, vol. 5 (1872), p. 584.

this group. As has been observed in § 28, this theorem is also a special case of the following theorem: If H_1 and H_2 are two conjugate subgroups of G, then the index of H_1 or H_2 under G is greater than the index under H_1 or H_2 of the cross-cut of H_1 and H_2.

49. Invariant Abelian Subgroups. From the fact that every group of order p^m contains at least p invariant operators and that its central quotient group has the same property, it results that every group of order p^m, $m>2$, contains a subgroup of order p^{m-1} which involves p^2 invariant operators. In a similar way we observe that every group of order p^m, $m>5$, contains a subgroup of order p^{m-1-2} which involves p^3 invariant operators. In general, every group of order p^m, $m>(\alpha+2)(\alpha-1)/2$, contains a subgroup of order

$$p^{m-1-2-3-\cdots-(\alpha-1)}=p^{m-\alpha(\alpha-1)/2}$$

which involves p^α invariant operators. As the group formed by these invariant operators corresponds to an invariant subgroup in the quotient group, it results that it is invariant under the entire group. Since *every invariant subgroup of order p^α in a group of order p^m is contained in an invariant subgroup of order $p^{\alpha+1}$*, it results from the above that every group of order p^m, $m>\alpha(\alpha+1)/2$, contains an invariant abelian group of order $p^{\alpha+1}$. In other words, *every group of order p^m, $m>\beta(\beta-1)/2$ contains an invariant abelian subgroup of order p^β*.

In the special case when $p=2$ this theorem may be expressed in a little more general form as follows:

Every group of order 2^m, $m\geqq\beta(\beta-1)/2$, $\beta>3$, contains an abelian subgroup of order 2^β *. The proof of this extended theorem is short if the preceding developments are employed. In fact, it has been proved that G involves a subgroup of order

$$p^{m-1-2-\cdots-(\beta-3)}=p^{m-(\beta-2)(\beta-3)/2},\quad \beta>3,$$

* In fact, there is always an *invariant* abelian subgroup of order 2^β when the given conditions are satisfied. Cf. *Messenger of Mathematics*, vol. 41 (1912), p. 28.

whose central is of order at least $p^{\beta-2}$, whenever $m \gtreqless (\beta-1)(\beta-2)/2$. When $m=\beta(\beta-1)/2$ the order of this subgroup is

$$p^{\beta(\beta-1)/2-(\beta-2)(\beta-3)/2}=p^{2\beta-3}.$$

The quotient group with respect to the given central is of order $p^{\beta-1}$. If this quotient group contains operators of order p^2, G must evidently involve an abelian group of order p^β. It remains therefore to consider the case when this quotient group does not involve any operator of order p^2. If $p=2$ we may assume that this quotient group is abelian, and hence we shall confine our attention, in what follows, to this special case.

We are thus led to consider the possibility of constructing a group K of order $2^{2\beta-3}$, having a central C of order $2^{\beta-2}$ which leads to an abelian quotient group of type (1, 1, 1, . . .). If we arrive at a contradiction by assuming that K does not include an abelian subgroup of order 2^β our theorem is proved. If K existed, all the operators of C besides the identity would be of order 2, since all of these operators would be commutators of K. Moreover, each of the non-invariant operators of K would be transformed under K into itself multiplied by all the operators of C.

Let K_1 represent any subgroup of order $2^{2\beta-4}$ and involving C. Each of the non-invariant operators of K_1 is transformed under K_1 into itself multiplied by all the operators of a subgroup of order $2^{\beta-3}$ contained in C. The multiplying subgroups for two distinct operators (mod C) of K_1 must be distinct, otherwise the operators of the group of order 4 (mod C) generated by these two operators would have to be transformed, by an operator of K which is not also in K_1, into themselves multiplied by the operators of a group of order 4 which has only the identity in common with the given subgroup of order $2^{\beta-3}$ in C. As this is clearly impossible it results that all the different non-invariant operators of K_1 are transformed under K_1 into themselves multiplied by all the different subgroups of order $2^{\beta-3}$ in C.

From the preceding paragraph it results that there is a (1, 1) correspondence between the operators of K_1 and the subgroups

of order $2^{\beta-3}$ in C such that each operator of K_1 is transformed under K_1 into itself multiplied by the various operators of the corresponding subgroup. Let t_1 be any non-invariant operator of K_1 and consider all the possible subgroups of order 4 in the quotient group of K_1 with respect to C, such that each of these subgroups involves the operator corresponding to t_1. Any operator (ρ) of K which is not also in K_1 transforms each of these subgroups into itself multiplied into a subgroup of order 4 contained in C. Let $t_1, t_2, \ldots, t_{\beta-2}$ represent a set of operators of K_1 which correspond to a set of independent generating operators in the given quotient group and assume that

$$t_1^{-1}s_2t_1 = s_1t_2,\ t_1^{-1}s_3t_1 = s_2t_3,\ \ldots,\ t_1^{-1}s_{\beta-2}t_1 = s_{\beta-3}t_{\beta-2}.$$

The subgroup (t_1, t_2) is transformed by ρ into itself multiplied by a group of order 4 which does not involve s_1. In general, the subgroup (t_1, t_α), $\alpha = 2, 3, \ldots, \beta-2$, is transformed by ρ into itself multiplied by a subgroup of order 4 of C which does not involve $s_{\alpha-1}$, and $(t_1, t_{\alpha_1}t_{\alpha_2} \ldots t_{\alpha_\lambda})$ is transformed by ρ into itself multiplied by a subgroup of order 4 which does not involve $s_{\alpha_1-1}s_{\alpha_2-1} \ldots s_{\alpha_\lambda-1}, \alpha_1, \alpha_2, \ldots, \alpha_\lambda = 1, 2, \ldots, \beta-2$. As ρ must transform t_1 into itself multiplied by an operator which is common to all of these subgroups of order 4 and as $s_1, s_2, \ldots, s_{\beta-3}$ are independent generators of a group of order $2^{\beta-3}$, it results that $\rho t_1 = t_1\rho$, which is contrary to the hypothesis. That is, we have arrived at a contradiction by assuming that K does not involve an abelian subgroup of order 2^β and hence the theorem under consideration has been proved.

EXERCISES

1. In a group of order p^m the order of the commutator subgroup cannot be greater than p^{m-2}.

2. In a non-abelian group of order p^3 each of the non-invariant operators belongs to a complete system of p conjugates.

3. There is one and only one non-abelian group of order p^3, $p>2$, which is conformal with the abelian group of type (1, 1, 1).

4. If a non-abelian group of order p^m, $p>2$, contains an operator of order p^{m-1} its commutator subgroup is of order p and there is only one such group.

5. Every non-abelian group of order p^m contains an invariant commutator of order p.

6. If a group of order 3^m contains no operator of order 9 all of its operators in any complete set of conjugates are commutative.*

Suggestion: If s_1, s_2 are any two operators of such a group it results that $(s_1s_2)^3 = s_1 \cdot s_2s_1s_2^2 \cdot s_2^2s_1s_2 = (s_1s_2^2)^3 = s_1 \cdot s_2^2s_1s_2 \cdot s_2s_1s_2^2 = 1$.

7. A necessary and sufficient condition that a group of order p^m is abelian is that more than $p^{m-1}\left(\frac{p^{\lambda}-1}{2}\right)$ of its operators corresponds to their inverses in some automorphism of the group

8. If two non-commutative operators of a group of order p^m, $p>2$, correspond to their inverses in an automorphism of the group their commutator cannot correspond to its inverse in this automorphism.

50. Number of Subgroups in a Group of Order p^m. We shall first determine the form of the number of subgroups of order p^{m-1} in a group G of order p^m. Any two subgroups of order p^{m-1} must have p^{m-2} operators in common, and these common operators constitute a group which is invariant under G. They must therefore include all the commutators of G and also the pth powers of every operator of G. If H is composed of all the operators which are common to all the subgroups of order p^{m-1} contained in G it must include all the commutators of G as well as the pth powers of all its operators. From this it results that the quotient group corresponding to H is abelian and of type (1, 1, 1, . . .). Each subgroup of order p^{m-1} in G must correspond to a subgroup of index p in this quotient group. In Chapter IV, § 40, we proved that the number of these subgroups of index p is equal to the number of the subgroups of order p in this quotient group. Hence the theorem:

The number of subgroups of order p^{m-1} contained in a group G of order p^m is always of the form

$$\frac{p^{\lambda}-1}{p-1}.$$

To obtain the exact number of these subgroups it is necessary to observe that p^{λ} is the order of the quotient group of G with respect to the group formed by all of its operators

* W. Burnside, *Quarterly Journal of Mathematics*, vol. 33 (1901), p. 231.

which are common to all of its subgroups of order p^{m-1}. In the special case when G is abelian and of type (1, 1, 1, . . .), $\lambda=m$; but in all other cases, $m>\lambda$. Since in any group every subgroup which involves half the operators is invariant, it results from the above that the number of subgroups whose order is one-half the order of the group is always of the form $2^\alpha-1$. In particular, there is no group which involves exactly 5 or 9 subgroups of half its order. The last two statements are evidently not restricted to groups whose orders are powers of a single prime. In fact, it results from the given method of proof that the number of the invariant subgroups of index p in any group whatever which contains at least one such invariant subgroup is of the form $(p^\lambda-1)/(p-1)$. This is known as *Bauer's theorem.**

Having found the number of the subgroups of order p^{m-1} in G, we shall now consider the other extreme case and determine some property of the number of its subgroups of order p. The invariant subgroups of order p which are contained in G clearly generate a group of order p^β which contains $(p^\beta-1)/(p-1)$ distinct subgroups of order p, where $\beta\geqq 1$. The non-invariant subgroups of order p may be divided into complete sets of conjugates, each set containing p^γ, $\gamma>0$, distinct groups. Hence the total number of subgroups of order p in any group whose order is a power of p is always of the form $1+kp$. From this theorem it results immediately that the number of the subgroups of order p^{n+1} which contain a given subgroup of order p^n is always of the form $1+kp$.

We proceed now to consider the number of subgroups of order p^α in G, where p^α is an arbitrary divisor of p^m. We assume at first that $\alpha<m$, and denote by r_α the number of subgroups of order p^α in G and by $r_{\alpha+1}$ the number of these subgroups of order $p^{\alpha+1}$. Let s_x represent the number of the subgroups of order $p^{\alpha+1}$ in which a given subgroup of order p^α occurs, and let s_y denote the number of subgroups of order p^α contained in a given subgroup of order $p^{\alpha+1}$. We then count each sub-

* H. Hilton, *Introduction to the Theory of Groups of Finite Order*, Oxford, 1908, p. 145.

group of order $p^{\alpha+1}$ as many times as it contains different subgroups of order p^α and thus arrive at the following equation:

$$\sum_{x=1}^{x=r_\alpha} s_x = \sum_{y=1}^{y=r_{\alpha+1}} s_y.$$

As both s_x and s_y are congruent to unity modulo p it results that $r_\alpha \equiv r_{\alpha+1} \pmod{p}$. As $r_1 \equiv 1 \pmod{p}$ it results that $r_\alpha \equiv 1 \pmod{p}$ and hence *the number of the subgroups of order p^α in a group of order p^m is always of the form $1+kp$.*

It is now very easy to prove that the number of the subgroups of order p^α in any group G' whose order is divisible by p^α is always of the form $1+kp$, even if the order of G' is not a power of p. If a subgroup of order p^α in G' is not invariant under some one of the Sylow subgroups of order p^m in G' it evidently belongs to a complete set of ps conjugates. Hence we may confine ourselves to these subgroups of order p^α in G' which are invariant under a particular subgroup of order p^m in G'. All of these must occur in this Sylow subgroup of order p^m and hence their number is of the form $1+kp$. This proves that the total number of the subgroups of order p^α must also be of this form, so that we have proved the following theorem due to Frobenius:

The total number of the subgroups of order p^α in any group whose order is divisible by p^α is of the form $1+kp$.

This theorem holds whether the order of the group is or is not a power of a single prime, and it may be regarded as an extension of Sylow's theorem. It should, however, be observed that the subgroups of order p^α are not always conjugate when they are not Sylow subgroups.

If the group G of order p^m contains at least one abelian subgroup of order p^3 it is easy to prove that the number of its abelian subgroups of order p^3 is of the form $1+kp$. We proceed to prove this theorem. If G contains an abelian subgroup H of order p^α the totality of the operators of G which are commutative with every operator of H forms a group H' which includes all the abelian groups of order $p^{\alpha+1}$ that are contained in G and include H. Hence the abelian subgroups of

order $p^{\alpha+1}$ in G which include H correspond to the subgroups of order p in the quotient group of H' with respect to H. As the number of these subgroups of order p is of the form $1+kp$ whenever H and H' are not identical, we have proved that an abelian group of order p^α contained in G is found in $1+kp$ abelian subgroups of order $p^{\alpha+1}$ whenever it is found in at least one abelian subgroup of this order.

Suppose that G contains at least one abelian subgroup of order $p^{\alpha+1}$ and let $r_{\alpha+1}$ represent the number of its abelian subgroups of this order, while r_α represents the number of the abelian subgroups of order p^α contained in G and included in abelian subgroups of order $p^{\alpha+1}$. By counting each abelian subgroup of order $p^{\alpha+1}$ as many times as it contains subgroups of order p^α and denoting by s_x and s_y respectively the number of the abelian subgroups of order $p^{\alpha+1}$ in which a given subgroup of order p^α occurs, and the number of subgroups of order p^α in a given abelian subgroup of order $p^{\alpha+1}$, we obtain, as before, the equation

$$\sum_{x=1}^{x=r_\alpha} s_x = \sum_{y=1}^{y=r_{\alpha+1}} s_y.$$

Since both s_x and s_y are congruent to unity modulo p we have proved that $r_\alpha \equiv r_{\alpha+1} \pmod{p}$. As $r_1 \equiv 1 \pmod{p}$ and $r_2 \equiv 1 \pmod{p}$ whenever G contains an abelian subgroup of order p^3, there results the theorem:

The number of the abelian subgroups of order p^3 in any group of order p^m is either zero or of the form $1+kp$.

It should not be inferred that the number of the abelian subgroups of a group of order p^m is always either 0, or of the form $1+kp$. The number of the abelian subgroups of index p in a non-abelian group of order p^m is either 1 or $1+p$, if this number exceeds zero, according to example 3 of the following exercises; but there are non-abelian groups of order p^m which contain exactly two abelian subgroups of index p^2. The possible numbers of abelian subgroups in a non-abelian group of order p^m have not yet been determined.

By means of Bauer's theorem and the properties of the ϕ-subgroups it is easy to prove a fundamental theorem relating

to the various possible sets of independent generators of any prime power group. As every maximal subgroup of a group of order p^m is of order p^{m-1}, it results directly from the definition, that the ϕ-subgroup of any group of order p^m is the cross-cut of all its subgroups of index p. Hence the ϕ-subgroup of a group of order p^m can also be defined as its smallest invariant subgroup which gives rise to an abelian quotient group of type $(1, 1, 1, \ldots)$. If the order of this quotient group is p^α, it follows that α is the number of independent generators in every possible set of such generators of this group of order p^m. In particular, *every possible set of independent generators of any prime power group involves the same number of operators.* That is, the number of operators in each of the possible sets of independent generators of a Sylow group is an *invariant* of this group.

From the preceding paragraph it results directly that a necessary and sufficient condition that the ϕ-subgroup of a given group of order p^m be the identity is that this group be the abelian group of type $(1, 1, 1, \ldots)$. Hence there is one and only one group of order p^m, p being any prime number and m being any positive integer, which has the identity for its ϕ-subgroup. The number of operators in every set of independent generators of this group is m. In every other group of order p^m the number of these independent generators is less than m, and there is at least one group of order p^m in which this number is any arbitrary positive integer from 1 to m.

EXERCISES

1. The number of abelian subgroups of order p^s in any group is either 0 or of the form $1+kp$, even if the order of the group is not a power of p.

2. If an abelian group of order p^m has p^2 for one invariant while all of its other invariants are equal to p, the number of its subgroups of order p^{m-1} is $\dfrac{p^{m-1}-1}{p-1}$.

3. A non-abelian group of order p^{s+1} contains 0, 1, or $p+1$ abelian subgroups of order p^s; in the last case it contains p^{s-1} invariant operators.

4. If a group of order 2^m contains only one subgroup of order 2 it is either cyclic or dicyclic, and if a group of order p^m, $p>2$, contains only one subgroup of order p it must be cyclic.*

* W. Burnside, *Theory of Groups*, 1911, p. 132.

5. If a group G of order p^m contain only one subgroup of order p^α, $1<\alpha<m$, the group is cyclic.

Suggestion: Every operator of G which is not in the subgroup of order p^α must generate this subgroup, since every subgroup of order p^α in a group of order p^m is contained in a subgroup of order $p^{\alpha+1}$.

6. The number of the invariant subgroups of order p^α in any group of order p^m is of the form $1+kp$ whenever $m \geqq \alpha$.

7. There are just four non-abelian groups of order 2^m involving a cyclic group of order 2^{m-1}, $m>3$.

8. Prove that the number of the subgroups of order p in any group of order p^m is of the form $1+kp$, by observing that the number of operators of order p^α in such a group is of the form $k_\alpha p^{\alpha-1}(p-1)$, so that

$$p^m-1=\sum_{\alpha=1}^{\alpha=m} k_\alpha p^{\alpha-1}(p-1).$$

9. Find a group of order 18 which contains only two invariant subgroups of order 3, and hence prove that the number of invariant subgroups of order p^α in a group need not be either 0 or of the form $1+kp$.

51. Number of Non-cyclic Subgroups in a Group of Order p^m, $p>2$. It has been observed that the total number of the subgroups of order p^α in any group G of order p^m is of the form $1+kp$ whenever $m>\alpha$, and hence the number of the invariant subgroups is always of this form. The number of the abelian subgroups is again of this form whenever $\alpha<4$ and this number is greater than zero. We proceed to prove that the number of the non-cyclic subgroups is always of the form $1+kp$ whenever $p>2$. This proof can easily be effected by a method employed above. It is easy to prove that the number of the non-cyclic subgroups of order p^α in a group of order $p^{\alpha+1}$ is of the form $1+kp$ whenever this number is not zero and $p>2$ by showing that there must be p cyclic subgroups of order p^α whenever there is one such subgroup. The number of the subgroups of order $p^{\alpha+1}$, which contain a given non-cyclic group of order p^α and are themselves contained in a group of order p^m, is also of the form $1+kp$.

Let r_α and $r_{\alpha+1}$ represent respectively the numbers of the non-cyclic subgroups of order p^α and $p^{\alpha+1}$, and let s_x represent the number of the subgroups of order $p^{\alpha+1}$ in which a given non-cyclic subgroup of order p^α occurs while s_y denotes the num-

ber of non-cyclic subgroups of order p^α contained in a given subgroup of order $p^{\alpha+1}$. We then count each subgroup of order $p^{\alpha+1}$ as many times as it contains a non-cyclic subgroup of order p^α and thus arrive at the equation

$$\sum_{s=1}^{s=r_\alpha} s_s = \sum_{y=1}^{y=r_{\alpha+1}} s_y.$$

Since both s_s and s_y are congruent to unity modulo p, it results that $r_\alpha \equiv r_{\alpha+1} \pmod{p}$ whenever G contains at least one non-cyclic group of order p^α and $m > \alpha$. Since every non-cyclic group of order p^m contains at least one invariant non-cyclic group of order p^2 whenever $p > 2$, there results the theorem:

*The number of the non-cyclic subgroups of order p^α in any non-cyclic group of order p^m is of the form $1+kp$ whenever $1<\alpha<m$ and $p>2$.**

52. Number of Non-cyclic Subgroups in a Group of Order 2^m. It is known that there are three non-cyclic groups of order 2^m which contain a single cyclic subgroup of order 2^α, $2<\alpha<m$; viz., the three groups of order 2^m which involve a cyclic subgroup of order 2^{m-1} and transform a generator of this subgroup into its inverse or into its $(2^{m-2}-1)$th power. It is not difficult to prove that these are the only possible non-cyclic groups of order 2^m that contain an odd number of cyclic subgroups of order 2^α. If a non-cyclic group G of order 2^m contains an odd number of cyclic subgroups of order 2^α, at least one of these is invariant under G. If this were the only cyclic subgroup of order 2^α in G there could not occur in G two cyclic subgroups of order $2^{\alpha+\beta}$, $\beta>0$, since one of these would be transformed into itself by one of its conjugates, and hence one of these and some operator in a conjugate subgroup would generate a group of order $2^{\alpha+\beta+1}$ which would be conformal with the abelian group of type $(\alpha+\beta, 1)$. As this group would involve two cyclic groups of order 2^α, it has been proved that *if G contains only one cyclic subgroup of order 2^α, it contains no more than one cyclic subgroup of order $2^{\alpha+\beta}$, $a+\beta<m$, $\beta \gtrless 0$.*

* *Proceedings of the London Mathematical Society*, vol. 2 (1904), p. 142.

Suppose that G contains one and only one cyclic subgroup of order 2^α and that its largest cyclic subgroup H' is of order 2^{α_1}. Since every subgroup of order 4 in the group of isomorphisms of H' involves the operator of order 2 which is commutative with just half of the operators of H', it results that $a_1 = m-1$, otherwise G would involve a subgroup which would be conformal with the abelian group of type $(\alpha_1, 1)$. From the known properties of the groups of order 2^m which involve operators of order 2^{m-1} and the result just obtained, it follows that G must be one of the three groups mentioned above whenever it contains one and only one cyclic subgroup of order 2^α. It remains to prove that G can involve only one such subgroup whenever it involves an odd number of cyclic subgroups of this order.

Suppose that G contains $2n+1$ cyclic subgroups of order 2^α. At least one of them, H_1, is invariant under G. Let H_2 represent any other and let H'_2 be a subgroup of H_2 such that the group (H_1, H'_2) is of order $2^{\alpha+1}$. Hence (H_1, H_2') has just two cyclic subgroups of order 2^α and at least $2^{\alpha-1}$ invariant operators. These two cyclic subgroups have just $2^{\alpha-1}$ common operators and we proceed to prove that there is an even number of cyclic subgroups of order 2^α in G such that they all have $2^{\alpha-1}$ operators in common.

If there is in G another cyclic subgroup of order 2^α which has exactly $2^{\alpha-1}$ operators in common with H_1, it is transformed either into itself by (H_1, H'_2) or it is transformed into a power of two distinct conjugates such that all of these have $2^{\alpha-1}$ operators in common with H_1. In the former case its generators are either invariant under all the operators of order 2^α in (H_1, H'_2) or they are transformed by at least some of these operators into themselves multiplied by the operators of order 2 in H_1, while the remaining operators of (H_1, H'_2) transform each of these generators into themselves. In this case (H_1, H'_2) is therefore invariant under these subgroups, that is, (H_1, H'_2) is invariant under all the subgroups of order 2^α, contained in G, which have $2^{\alpha-1}$ operators in common with H_1 and are transformed into themselves by (H_1, H'_2).

If H_3 is such a subgroup it is clear that (H_1, H'_2, H_3) is conformal with an abelian group and hence involves an even number of cyclic subgroups of order 2^α. We consider now all the other cyclic subgroups of order 2^α contained in G, which have $2^{\alpha-1}$ operators in common with H_1 and are transformed into themselves by (H_1, H'_2, H_3). If such a subgroup H_4 exists it is clear that (H_1, H'_2, H_3, H_4) must again be conformal with an abelian group and hence it involves an even number of cyclic subgroups of order 2^α. By continuing this process it results that an even number of cyclic subgroups of order 2^α, contained in G, have $2^{\alpha-1}$ operators in common with H_1.

All of these cyclic subgroups of order 2^α form a set. If G contains a cyclic subgroup of order 2^α which is not in this set, this subgroup must belong to another set which involves an even number of distinct cyclic subgroups of order 2^α; that is, these cyclic subgroups of order 2^α are found in distinct sets such that no two have a subgroup in common and such that each set involves an even number of cyclic subgroups. This completes the proof of the theorem: *if a group of order* 2^m *involves an odd number of cyclic subgroups of order* 2^α, $a>2$, *this number is unity.* Combining this with the theorem proved above, it results that if we include the cyclic group *there are just four groups of order* 2^m *such that each involves an odd number of cyclic subgroups of order* 2^α, $\alpha>2$.* In each of these groups there is only one such subgroup.

The four groups mentioned in the last theorem contain one, $2^{m-2}+1$ or $2^{m-3}+1$ cyclic subgroups of order 4. We proceed to prove that these are the only groups of order 2^m which contain an odd number of cyclic subgroups of order 4. The method of proof is similar to the one employed above.

Let G be any group of order 2^m which contains an odd number of cyclic subgroups of order 4. At least one of these subgroups (K_1) is invariant under G, and at least half the operators of G are commutative with a generator (s) of K_1. It will be proved that the subgroup G_1 formed by these 2^{m-1} operators must be cyclic. If G_1 were not cyclic, K_1 would be

* *Transactions of the American Mathematical Society*, vol. 6 (1905), p. 58.

contained in an abelian subgroup of type (2, 1). This subgroup would contain two cyclic subgroups K_1 and K_2 of order 4, having a common square. It will now be proved that G would then contain an even number of cyclic subgroups of order 4 having s^2 in common.

If this number were odd, (K_1, K_2) would transform at least one of the remaining ones (K_3) into itself. The commutator subgroup of (K_1, K_2, K_3) is generated by s^2 and hence this group contains an even number of cyclic subgroups of order 4 and all of these subgroups contain s^2. Hence there would be another invariant cyclic subgroup K_4 involving s^2. The number of cyclic subgroups of order 4 in (K_1, K_2, K_3, K_4) is again even, since the commutator subgroup is still generated by s^2 and all of these subgroups include s^2. This follows almost directly from the fact that the product of an operator of order 4 in (K_1, K_2, K_3, K_4) into an operator of order 2 is of order 4 when the two factors are commutative, and of order 2 when they are not commutative, while the converse is true if the second operator is of order 4.

As this process could be continued indefinitely if there were an odd number of cyclic subgroups of order 4 which contained s^2, it results that the number of these subgroups is even. If there were an odd number of cyclic subgroups of order 4 in G, which did not contain s^2, one of these and s^2 would again generate the abelian group of type (2, 1), and the number of those involving the same subgroup of order 2 would again be even. As similar remarks would apply to all the other possible cyclic subgroups of order 4 we have proved that G_1 *is cyclic whenever* G *contains an odd number of cyclic subgroups of order* 4. This proves the statement in the first paragraph of this section, since the other non-cyclic group of order 2^m which contains a cyclic subgroup of order 2^{m-1} contains an even number of cyclic subgroups of order 4.

Combining the results of this section we conclude that every group of order 2^m, $m>3$, which contains an odd number of cyclic subgroups of order 4, contains just one cyclic subgroup of order 2^α, where α can have any value from 3 to $m-1$; and

every group which contains only one cyclic subgroup of order 2^α contains an odd number of cyclic subgroups of order 4. For each value of α and m there are three such groups; hence there is an infinite system of groups of order 2^m which contain an odd number of cyclic subgroups of composite order. When $m=3$ there are only two groups having this property, viz., the quaternion group and the group of movements of the square. If all the non-cyclic groups of order $p^m (m>3$, p an arbitrary prime) were determined, there would be just three among them in which the number of cyclic subgroups of composite order would not always be a multiple of p. In these three special cases the number of cyclic subgroups of every composite order is not divisible by p.

In the exceptional groups noted above the number of the subgroups of order 2 is $\equiv 1 \pmod 4$. That this number is $\equiv 3 \pmod 4$ in every other non-cyclic group of order 2^m is a direct consequence of the fact that the number of cyclic subgroups of order 4 in all these groups is even. From this fact it results that the number of operators whose order exceeds 2 is divisible by 4, since every cyclic subgroup of order 2^σ contains $2^{\sigma-1}$ operators which are not found in any other subgroup whose order is $\leqq 2^\sigma$. Hence the given system of groups is composed of all the groups of order p^m in which the number of subgroups of order p is not $\equiv 1+p \pmod{p^2}$. That is, the groups of order p^m in which the number of cyclic subgroups of composite order is not divisible by p coincide with those in which the number of subgroups of order p is not of the form $1+p+kp^2$.

EXERCISES

1. The number of subgroups of order p in any non-cyclic group of order p^m, $p>2$, is of the form $1+p+kp^2$.

Suggestion: Consider the forms of the number of the operators of orders p^2, p^3, etc.

2. The number of cyclic groups of order p^β, $p>2$ and $\beta>1$, is of the form kp whenever the Sylow subgroups of order p^m are non-cyclic.

3. If a group G of order p^m contains exactly p cyclic subgroups of order p^α, these subgroups generate a characteristic subgroup of order $p^{\alpha+1}$ under G, and this subgroup is either abelian and of type $(\alpha, 1)$ or it is the non-abelian group which is conformal with this abelian group.

4. There are just three groups of order 3^4 each of which contains only three cyclic subgroups of order 9.

53. Some Properties of the Group of Isomorphisms of a Group of Order p^m. If G_α is any invariant subgroup of G, then G_α contains at least one invariant subgroup of G whose order is an arbitrary divisor of the order of G_α. Let

$$G_0,\ G_1,\ G_2,\ \ldots,\ G_m$$

be a series of invariant subgroups of G whose orders are respectively $1, p, p^2, \ldots, p^m$, so that $G_m \equiv G$; and suppose that each of these subgroups except the last is included in the one which follows it. Let t be any operator whose order is a power of p in the group of isomorphisms of G. Such an operator is said to effect a *p-isomorphism* of G. Since t and G generate a group whose order is a power of p, we may suppose that t transforms all of the operators of each one of the given series of subgroups into themselves multiplied by those of the preceding subgroup. That is, the commutator of t and any operator of G_β is in $G_{\beta-1}$, $\beta = 1, 2, \ldots, m$.

We proceed to prove that the order of t cannot exceed p^{m-1}. In fact, if t_β is any operator of G_β in the above series, it results from the given conditions that

$$t^{-1}t_\beta t = t_{\beta-1}t_\beta, \quad t^{-p}t_\beta t^p = t_{\beta-2}t_\beta.$$

Hence $t^{p^{m-1}}$ must be commutative with every operator of G, and, as t is an operator in the group of isomorphisms of G, it results from this that the order of t is a divisor of p^{m-1}. In other words, *the p^{m-1} power of every operator whose order is a power of p in the group of isomorphisms of a group of order p^m is the identity.* When G is the cyclic group of order p^m, $p>2$, it is known that the group of isomorphisms of G involves operators of order p^{m-1}, viz., those operators which give rise to commutators of order p^{m-1}.

We proceed to prove that the group of isomorphisms of a non-cyclic group of order p^m, $p>2$ and $m>3$, cannot involve any operator of order p^{m-1}. If G is such a group it follows from the preceding section that we may assume that G_2, in the above

series of invariant subgroups, is non-cyclic. If t is an operator in the group of isomorphisms of G and if the order of t is a power of p, it results that t^p is commutative with every operator of G_2 and that it transforms the operators of G into themselves multiplied by operators in G_{m-2}. Similarly t^{p^2} is commutative with every operator in G_3 and transforms every operator in G_m into itself multiplied by an operator in G_{m-3}. In general, t^{p^a} transforms every operator in G into itself multiplied by operators in G_{m-a-1}. As $t^{p^{m-3}}$ transforms the operators of G into itself multiplied by operators in G_2 and as these operators are commutative under this power of t, it results that

$$t^{p^{m-2}}=1.$$

That is, *the order of every operator in a Sylow subgroup of order p^m of the group of isomorphisms of a group of order p^m is a divisor of p^{m-2} whenever $p>2$ and $m>3$.*

The last theorem evidently also applies to all groups of order 2^m which involve a non-cyclic invariant subgroup of order 4, and it is well known to be true as regards the cyclic group of order 2^m. It is, however, not true as regards the dihedral or the dicyclic group of order 2^m, since there is evidently an operator of order 2^{m-1} in the group of isomorphisms of each of these groups; viz., the operator which is commutative with each operator of the cyclic subgroup of order 2^{m-1} but transforms the non-invariant operators of orders 2 and 4 respectively into themselves multiplied by an operator of order 2^{m-1}. These two infinite systems of groups therefore are instances of groups whose groups of isomorphisms contain operators of the largest possible order in accord with the theorem of the second paragraph of the present section.

As the remaining group of order 2^m which does not involve an invariant non-cyclic subgroup of order 4 involves 2^{m-3} non-invariant cyclic subgroups of order 4, its group of isomorphisms may be represented as an intransitive substitution group on 2^{m-2} letters. From this it follows directly that its group of isomorphisms cannot involve any operator of order 2^{m-1}, $m>3$. Hence we have proved the theorem:

The only groups of order p^m, $m>3$, whose groups of isomorphisms involve operators of order p^{m-1} are the cyclic group when $p>2$, and the dihedral and the dicyclic groups when $p=2$.

Every operator whose order is a power of p in the group of isomorphisms of G generates with G a group whose order is a power of p. As G is an invariant subgroup of this group it results that this group involves a series of invariant subgroups

$$G_0,\ G_1,\ G_2,\ \ldots,\ G_m$$

which are such that t transforms the operators of each of these subgroups into themselves multiplied by those of a preceding subgroup. Moreover, whenever t has this property its order is a power of p. Hence the existence of such a series of subgroups is a necessary and sufficient condition that an operator t in the group of isomorphisms of G has for its order a power of p. In other words,

A necessary and sufficient condition that an operator t in the group of isomorphisms of a group G of order p^m has for its order a power of p is that t transform every operator in the series of subgroups

$$G_0,\ G_1,\ G_2,\ \ldots,\ G_m=G$$

of orders $1,\ p,\ p^2,\ \ldots,\ p^m$ *respectively, into itself multiplied by an operator in the preceding subgroup.*

Hence t^{p^α} transforms every operator of G_β into itself multiplied by an operator in $G_{\beta-\alpha-1}$, where $\beta-\alpha-1$ is to be replaced by 0 whenever $\beta\leqq\alpha+1$.

From this theorem it is easy to deduce the following useful corollary: *The order of the commutator of two operators, neither of which is the identity, of a group G of order p^m is less than the order of the smallest invariant subgroup of G in which either of these two operators occurs.* In particular, if one of these two operators is of order p and generates an invariant subgroup, it must be commutative with every operator of G. This special case may also be regarded as a special case of the theorem that every invariant subgroup, besides the identity, in a group of order p^m involves invariant operators of order p.

The group of isomorphisms of the group of order p is the cyclic group of order $p-1$, and hence it does not involve any operator of order p. It is easy to prove that the group of isomorphisms of every group G of order p^m, $m>1$, involves operators of order p. In fact, when G is non-abelian its group of cogredient isomorphisms involves such operators and when G is abelian we may select any subgroup of order p^{m-1}, and multiply the operators of the corresponding quotient group by those of an invariant subgroup of order p which is contained in the given subgroup of order p^{m-1}. It is evident that the latter isomorphisms are also possible even when the group of order p^m is non-abelian. Hence the group of order p is the only group of order p^m whose group of isomorphisms does not involve operators of order p.

EXERCISES

1. If G is the abelian group of order p^m and of type $(1, 1, \ldots)$, its group of isomorphisms cannot involve any operator whose order is a power of p and exceeds $p^{m/2}$ when m is even or $p^{(m+1)/2}$ when m is odd.

Suggestion: When a power of t transforms G into itself multiplied only by operators which are commutative with t, the pth power of this power of t will be the identity.

2. The group of isomorphisms of the dihedral group of order $2n$, $n>2$, is the holomorph of the cyclic group of order n.

Suggestion. The group of isomorphisms of this dihedral group may be represented as a transitive substitution group of degree n, and it involves an invariant cyclic subgroup of order n composed of all its operators which are commutative with every operator of the cyclic subgroup of order n.

3. Find the group of isomorphisms of the dicyclic group of order 2^n, $n>3$.

4. If a group of order 2^m contains exactly two cyclic subgroups of order 2^β, but no cyclic subgroup of any higher order, then $m \leqq \beta+2$.

54. Maximal Order of a Sylow Subgroup in the Group of Isomorphism of a Group of Order p^m. We proceed to determine the maximal order of a Sylow subgroup of order p^n contained in the group of isomorphisms of a group of order p^m. To do this we assume again that a set of invariant subgroups

of orders 1, p, p^2, . . . , p^m respectively of such a group G is represented by the symbols

$$G_0, G_1, G_2, \ldots, G_m,$$

and that these invariant subgroups have the property that each one except the last is included in the one which follows it. The operators of G_m which are not also in G_{m-1} may be transformed into themselves multiplied by at most p^{m-1} different operators. In general, the operators of G_α which are not in $G_{\alpha-1}$ are transformed into themselves multiplied by at most $p^{\alpha-1}$ operators. Hence the order of a Sylow subgroup of order p^n in the group of isomorphisms of G cannot exceed

$$p \cdot p^2 \cdot \ldots \cdot p^{m-1} = p^{m(m-1)/2}.$$

It is evident that when G is abelian and of type (1, 1, . . .), its group of isomorphisms involves Sylow subgroups of order p^n, where n has the maximal value given above. This is also the case when G is abelian and of type (2, 1, 1, . . .). It is not difficult to prove that these are the only abelian groups whose groups of isomorphisms contain Sylow subgroups of the given maximal order.*

55. Construction of all the Possible Groups of Order p^m In view of the simple properties of the group of order p^m various efforts have been made to determine all these groups for given values of m. When $m=1$ there is evidently only one such group, and when $m=2$ there are two possible groups. Each of these groups is abelian. Moreover, it has been observed that for any value of m the number of abelian groups is equal to the number of different partitions of m as regards addition. Hence the only difficulty in the determination of all these groups for small values of m relates to the possible non-abelian groups. In case $m<5$ there is very little difficulty here, but for larger values of m this difficulty increases very rapidly with m.

As an abstract group is simply isomorphic with one and only one regular substitution group, we can determine all the

* Cf. G. A. Miller, *Transactions of the American Mathematical Society*, vol. 12 (1911) p. 396.

possible groups of order p^m by determining all the regular substitution groups of this order. We proceed to indicate a method for constructing all the possible regular groups of order p^m on condition that all those of order p^{m-1} are known. Since every regular group of order p^m contains an invariant intransitive subgroup of order p^{m-1} which is formed by a simple isomorphism between p regular groups of this order, we may first determine all the possible regular groups of order p^m which involve a given group H of order p^{m-1}.

Let the p transitive constituents of H be $H_1, H_2, \ldots, H_p$. A group G of order p^m which contains H is generated by H and some substitution t_1 which permutes the p systems of intransitivity of H cyclically, has its pth power in H, and transforms H into itself. Let t be a substitution of order p which permutes the systems of H transitively and is commutative with every substitution of H. As it may be assumed that t_1 and t permute these systems in the same way, we conclude that $t_1 t^{-1}$ is a substitution s which does not permute any of the p transitive constituents of H. That is, $t_1 = st$, where it may be assumed that t transforms the corresponding letters of each of the p systems among themselves. As t can readily be obtained from the p constituents belonging to $H_1, H_2, \ldots, H_p$ of any substitution in H it remains only to determine $s = s_1 s_2 \ldots s_p$, where $s_1, s_2, \ldots, s_p$ are the constituents of s belonging to $H_1, H_2, \ldots, H_p$ respectively. As $s_1, s_2, \ldots, s_p$ transform each of the constituents $H_1, H_2, \ldots, H_p$ into itself they must be found in the holomorphs of $H_1, H_2, \ldots, H_p$, respectively.

We proceed to prove that $s_2, s_3, \ldots, s_p$ may be assumed to be corresponding substitutions in the groups of isomorphisms of $H_2, H_3, \ldots, H_p$, respectively, while s_1 is one of the p^{m-1} substitutions obtained by multiplying the substitution in the group of isomorphisms of H_1 which corresponds to $s_2, s_3, \ldots, s_p$ by the p^{m-1} substitutions which are commutative with H_1 and involve only letters of H_1. This theorem follows almost directly from the fact that the conjoint of a regular group has the same group of isomorphisms as the regular group itself, since both are invariant subgroups of the holomorph of

this regular group, and the group of isomorphisms of a regular group is the subgroup composed of all the substitutions which omit a given letter in its holomorph. Hence we may reduce each of the substitutions which transform H in a certain way to one of the given form by transforming by a substitution in the direct product of the conjoints of $H_1, H_2, \ldots, H_p$.

From the preceding paragraph it results that the number of groups of order p^m which contain a given group H of order p^{m-1} cannot exceed the order of the product of H and the order of its group of isomorphisms. Hence the number of the groups of order p^m is always finite when p is finite. We shall be able, however, to reduce this apparently possible number very greatly. In the first place it should be observed that if s_1' is so selected that $s_1's_2s_3 \ldots s_p$ is commutative with t, while s_1' involves only letters in H_1, then $s_1 = s_1''s_1'$ where s_1'' is commutative with s_1'; otherwise $(s_1s_2 \ldots s_pt)^p$ would not be in H. This restricts the number of choices of s_1'' to the number of operators in H which are both in its conjoint and also invariant under s_1. Another important restriction is that we evidently need to consider only one of the first $p-1$ powers of $s_1's_2s_3 \ldots s_p$, since t may be transformed into any power without affecting $s_1s_2 \ldots s_p$ by permuting the constituents $H_2, H_3, \ldots, H_p$ cyclically. When H is abelian, all the groups obtained by replacing s_1'' by any of its powers prime to its order are conjugate, since the operators in the group of isomorphisms of an abelian group which transform each operator of this group into the same power are invariant under this group of isomorphisms.

To illustrate the method outlined above we proceed to determine the possible non-abelian groups of order p^3, $p>2$. It has been observed that each of these groups involves a non-cyclic group of order p^2, and hence we may use this for H. As the group of isomorphisms of H involves only one set of conjugate subgroups of order p, the two substitutions $s_1's_2s_3 \ldots s_p$ and t may be supposed to be the same for all these groups. Moreover, s_1'' is restricted to a single subgroup, and hence it is necessary to consider only two cases, viz., the case when

s_1'' is the identity and the case when its order is p. That is, there cannot be more than two non-abelian groups of order p^3, $p>2$, in accord with the general theory which precedes this paragraph. From the present paragraph it results that one of these groups involves operators of order p^2 while the other does not have this property. Hence there are two and only two non-abelian groups of order p^3, $p>2$. It was proved in § 33 that there are also only two such groups when $p=2$.

Among the groups of order p^m which involve H the one generated by H and t is of especial interest in view of its simple structure. In fact, it is abstractly the direct product of H and the group of order p. If we transform this group by

$$r_1^{p-1} r_3 r_4^2 \ldots r_p^{p-2},$$

where r_1 is any invariant substitution of H_1 while r_α, $\alpha=3, \ldots, p$, is the transform of r_1 with respect to t^α, there results a group generated by H and $r_1^{-p}t$. From this and the preceding theory it results that we need to use only two values for s_1'' when H is cyclic and the entire group is abelian, as results also directly from the theory of the abelian groups. This general method can easily be extended so as to reduce the amount of labor necessary to determine all the possible groups of order p^m which involve a given subgroup of order p^{m-1} *; but the preceding developments may suffice to point the way towards a penetration into this difficult subject. From the given illustration it results that we do not always need to use all the possible groups of order p^{m-1} for H in order to determine all the groups of order p^m. In fact, when $m=4$ we need to consider only the abelian groups of order p^3 for H, since every group of order p^4 contains an abelian subgroup of order p^3.

EXERCISES

1. Determine the fourteen possible groups of order 16.

2. Determine the non-abelian groups of order p^4, $p>2$, which involve no operator of order p^2. Show that $s_1''=1$ in these cases and that there are two such groups when $p>3$, one having a commutator subgroup of

* *American Journal of Mathematics*, vol. 24 (1902), p. 395.

order p and the other having such a subgroup of order p^2. When $p=3$ there is only one such group.

3. There are four distinct non-abelian groups of order p^5, $p \geq 3$, which involve an abelian group of order p^4, but do not contain any operator of order p^2. When $p=3$ there are only two such groups.

4. The number m can be so chosen that the number of the distinct groups of order p^m, $p>2$, which do not involve any operator of order p^2 is greater than any given number.

5. Every intransitive Sylow subgroup of a symmetric group is the direct product of its transitive constituents, and each of these transitive constituents has a central of prime order.

6. If the degree of a symmetric group is $n=k_1p^\alpha+k_2p^{\alpha-1}+\ldots+k_{\alpha+1}$; $k_1, k_2, \ldots, k_{\alpha+1}$ being positive integers less than p, then the central of its Sylow subgroup of order p^m is of order $p^{k_1+k_2+\cdots+k_\alpha}$.

CHAPTER VI

GROUPS HAVING SIMPLE ABSTRACT DEFINITIONS

56. Groups Generated by Two Operators Having a Common Square. If s_1, s_2 represent two operators of order 2 they evidently satisfy the equation $s_1^2 = s_2^2$, and the cyclic group $(s_1 s_2)$ generated by $s_1 s_2$ is invariant under s_1 and s_2. In fact, $s_1 s_2$ is transformed into its inverse by each of the two operators s_1, s_2, and hence (s_1, s_2) is the dihedral group whose order is the double of the order of $s_1 s_2$, as has been observed in § 26. Hence the equations

$$s_1^2 = s_2^2 = 1, \quad (s_1 s_2)^n = 1$$

serve as a complete definition of the dihedral group of order $2n$, if we assume that the order of $s_1 s_2$ is exactly n. Throughout the present chapter it will be assumed, unless the contrary is stated, that the condition $s_1^n = 1$ implies that the order of s_1 is exactly n. This fact is sometimes expressed by saying that s_1 *fulfils* the condition $s_1^n = 1$, while the statement s_1 *satisfies* the condition $s_1^n = 1$ may imply merely that the order of s_1 is a divisor of n.* We shall employ the terms fulfil and satisfy with these meanings throughout the present chapter, so that the equation $s_1^n = 1$ implies that s_1 fulfils this condition unless the contrary is stated.

If s_1, s_2 are any two operators which satisfy the equation

$$s_1^2 = s_2^2,$$

they generate a group G under which s_1^2 is invariant. That is, the cyclic group generated by s_1^2 is composed of operators which are invariant under G, since s_1^2 is commutative with each

* *Quarterly Journal of Mathematics*, vol. 41 (1909–10), p. 169.

of the operators s_1 and s_2. From the fact that $s_1^2 = s_2^2$, it results that

$$s_1 s_2^{-1} = s_1^{-1} s_1^2 s_2^{-1} = s_1^{-1} s_2, \quad s_2 s_1^{-1} = s_2^{-1} s_1 = (s_1 s_2^{-1})^{-1}.$$

Each of the operators $s_1 s_2^{-1}$, $s_2 s_1^{-1}$ is therefore transformed into the other by each of the two operators s_1, s_2. That is, the cyclic group generated by either of these operators is invariant under G, and each of its operators is transformed into its inverse by s_1 as well as by s_2. The abelian group generated by the two operators s_1^2, $s_1 s_2^{-1}$ must therefore be invariant under G, and it involves either all, or just half of the operators of G.

When each of the two operators s_1, s_2 is of odd order, G is cyclic, since each of these operators is equal to the other, and G is generated by s_1^2 in this case. When one of these operators is of odd order while the other is of even order, G is generated by the operator of even order and $s_1 s_2^{-1}$ is of order 2. The only case which requires further consideration is therefore the one in which the common order of s_1, s_2 is an even number $2n$. A necessary and sufficient condition that G be abelian is that the order of $s_1 s_2^{-1}$ divide 2. If $s_1 s_2^{-1} = 1$, $s_1 = s_2$ and G is the cyclic group generated by s_1. If the order of $s_1 s_2^{-1}$ is 2, G is either the cyclic group of order $2n$ or the abelian group whose invariants are 2 and $2n$. It remains only to consider the cases when G is non-abelian; that is, when the order of $s_1 s_2^{-1}$ exceeds 2, and hence s_1, s_2 have the same even order $2n$.

It is evident that the common order of s_1, s_2 is not limited by the relation $s_1^2 = s_2^2$. That is, for an arbitrary value of n we can find two operators s_1, s_2 of order $2n$ such that they satisfy the equation $s_1^2 = s_2^2$. In fact, the value of n is not limited if we impose the additional condition that the order of $s_1 s_2^{-1}$ shall be an arbitrary number m, since two generators of order 2 of the dihedral group of order $2m$ may be multiplied by an operator of order $2n$ which is commutative with both of these generators such that the products satisfy both of these conditions. In other words, for any arbitrary number pair m, n, we can find two operators s_1, s_2 of order $2n$ such that they

have a common square and that the order of $s_1 s_2^{-1}$ is m. The order of the group generated by these two operators is always a divisor of $2mn$ and a multiple of mn, since s_1^2 and $s_1 s_2^{-1}$, are of orders n and m respectively and the cyclic group generated by these operators cannot have more than two common operators.

It results from the preceding paragraph that G is completely defined by the three conditions

$$s_1^2 = s_2^2, \quad (s_1 s_2^{-1})^m = 1, \quad s_1^{2n} = 1$$

whenever either m or n is odd. In fact, when s_1, s_2 fulfil these conditions and either m or n is an odd number, G is the group of order $2mn$ obtained by establishing an (m, n) isomorphism between the dihedral group of order $2m$ and the cyclic group of order $2n$. If m and n are both even, G may again be constructed by establishing such an (m, n) isomorphism when the order of G is $2mn$. When this order is only mn, G may be constructed by establishing a simple isomorphism between n cyclic groups of degree and order m, and then extending this group by means of an operator of order $2n$ which transforms into its inverse each operator of this cyclic subgroup, permutes its systems of intransitivity, and has its nth power in this subgroup. That is, *the two operators* s_1, s_2 *may be so selected as to fulfil the three conditions*

$$s_1^2 = s_2^2, \quad (s_1 s_2^{-1})^m = 1, \quad s_1^{2n} = 1$$

and to generate either of two groups when m *and* n *are both given even numbers. When at least one of them is a given odd number, the group generated by* s_1, s_2 *is completely determined by the three given relations.*

To illustrate this theorem we begin with the case when $m=4$ and $n=2$. The group of order mn in this case is clearly the quaternion group, while the group of order $2mn$ may be constructed by establishing a (4, 2) isomorphism between the octic group and the cyclic group of order 4 so as to obtain the group of order 16 involving 12 operators of order 4 which have only two distinct squares. This group has the quaternion

group for a quotient group but not for a subgroup. If a set of generating operators satisfy certain conditions, the largest group which they may generate has all the other groups which they may generate for quotient groups. This follows directly from the theory of the quotient group. When $m=n=2$, G is clearly abelian and is of order 4 or 8. In the former case it is cyclic and in the latter it is of type (2, 1). When $m=3$ and $n=2$, G is the dicyclic group of order 12.

When $n=1$, the category of groups under consideration clearly coincides with the dihedral groups. When $n=2$ and m is odd it coincides with all the dicyclic groups whose orders are not divisible by 8, and when $n=2$ and m is even, the groups of order mn coincide with the totality of the dicyclic groups, while those of order $2mn$ may be obtained by establishing an $(m, 2)$ isomorphism between either the dihedral group of order $2m$ or the dicyclic group of order $2m$ and the cyclic group of order 4. Hence the dihedral groups and the dicyclic groups may both be regarded as special cases of groups generated by two operators having a common square. Since $s_1s_2 = s_1s_2^{-1}s_2^2$, it results that the order of the product of the two operators s_1 and s_2 is either the least common multiple between m and n, or it is exactly half this least common multiple. That is, the order of the product of two operators is not restricted by the fact that they have a common square, and the order of the group which they generate is always a divisor of the double of the square of the order of this product.

If we let $t_1=s_1$ and $t_2=s_1s_2^{-1}$, it results that the group (t_1, t_2) is identical with (s_1, s_2). That is, *every group that can be generated by two operators having a common square can also be generated by two operators such that the one transforms the other into its inverse, and vice versa.* Hence we have two abstract definitions for this category of groups. The latter definition is more convenient than the former for the purpose of obtaining directly the abstract properties of these groups, but in the abstract theory these groups frequently present themselves under the former definition, and hence it is very important to know that the two given definitions apply to the same cate-

gory of groups. It results directly from the given equation that $s_2 = t_2^{-1} t_1$. That is, if $t_1^{-1} t_2 t_1 = t_2^{-1}$ then $t_1^2 = (t_2^{-1} t_1)^2$. In the special case of the dihedral groups the two equivalent definitions reduce to

$$s_1^2 = s_2^2 = 1; \quad t_1^2 = 1, \quad t_1 t_2 t_1 = t_2^{-1}.$$

EXERCISES

1. If s_1, s_2 are two operators, neither of which is the identity, which satisfy both of the conditions:

$$s_1^{-1} s_2 s_1 = s_2^{-1}, \quad s_2^{-1} s_1 s_2 = s_1^{-1},$$

they must also satisfy the conditions:

$$s_1^{-1} s_2 s_1 = s_2^3, \quad s_2^{-1} s_1 s_2 = s_1^3;$$

and they generate either the quaternion group or the four-group.

2. Find the number of operators of order 6 in the group of order g which is generated by s_1, s_2 subject to the following conditions: $s_1^6 = 1$, $s_1^{-1} s_2 s_1 = s_2^{-1}$. Prove that the central of this group is either of order 3 or of order 6, and that g may be an arbitrary multiple of 6.

57. Groups of the Regular Polyhedrons.* The regular tetrahedron evidently admits two movements of order 3 whose product is of order 2. If we represent these movements by s_1, s_2 respectively, these operators must fulfil the conditions

$$s_1^3 = s_2^3 = (s_1 s_2)^2 = 1, \quad \text{or} \quad s_1^3 = s_2^3 = 1, \quad s_1 s_2 = s_2^2 s_1^2.$$

We proceed to prove that these conditions define a group of order 12; whence, as the group of movements of the regular tetrahedron is evidently of order 12, the group defined by the given two equivalent sets of conditions must be the group of the regular tetrahedron. To prove that (s_1, s_2) is of order 12 we may proceed as follows: The three conjugate operators of order 2

$$s_1 s_2, \quad s_2 s_1, \quad s_1^2 s_2 s_1^2$$

are commutative, since

$$s_2 s_1^2 s_2 = s_1^2 s_2^2 \cdot s_2^2 s_1^2 = s_1^2 s_2 s_1^2.$$

* These groups were first studied by means of abstract definitions by W. R. Hamilton, cf. *Bibliotheca Mathematica*, vol. 11 (1910–11), p. 314.

As two operators of order 2 whose product is of order 2 generate the four-group, it results that (s_1, s_2) involves the four-group represented by the operators

$$1, \quad s_1s_2, \quad s_2s_1, \quad s_1^2s_2s_1^2.$$

As this subgroup is invariant under s_1 as well as under s_1s_2, it must be invariant under s_2, and therefore also under (s_1, s_2). Hence the group generated by s_1 and this subgroup of order 4 is of order 12. Since this group involves s_1 and s_1s_2, it must also involve s_2; that is, it must be (s_1, s_2). This proves the theorem:

If the order of the product of two operators of order 3 *is of order* 2 *they generate the tetrahedral group.*

If we replace s_1 by t_1 and s_1s_2 by t_2, it results that t_1, $t_1^{-1}t_2$ are two operators of order 3 whose product is of order 2; hence $(t_1, t_1^{-1}t_2)$ is the tetrahedral group. Since $(t_1, t_1^{-1}t_2) \equiv (t_1, t_2)$ it results also that if the order of the product of two operators of orders 2 and 3 respectively is 3, then these operators must generate the tetrahedral group. That is, s_1, s_2 generate the tetrahedral group if they fulfil either one of the following two sets of conditions:

$$s_1^3 = s_2^3 = (s_1s_2)^2 = 1, \quad s_1^2 = s_2^3 = (s_1s_2)^3 = 1.$$

These two sets of equations furnish two very useful definitions of this important group. The group could also be defined by the facts that its order is 12 and that it does not involve a subgroup of order 6, as well as by the facts that it is of order 12 and contains four subgroups of order 3.

The cube is clearly transformed into itself by 24 movements of rigid space, and the order of each of these movements is equal to one of the four numbers 1, 2, 3, and 4. It is not difficult to find, among these 24 movements, two of orders 3 and 4 respectively whose product is of order 2. If we represent these two movements by s_1, s_2, they must therefore satisfy the equations

$$s_1^3 = s_2^4 = (s_1s_2)^2 = 1.$$

We proceed to prove that these conditional equations define a group of order 24, and hence they must define the group of the cube. To prove that they define a group of order 24 we may proceed as follows: The group (s_1, s_2^2) is the tetrahedral group, as results directly from the fact that

$$(s_1 s_2^2)^3 = s_1 s_2 \cdot s_2 s_1 s_2 \cdot s_2 s_1 s_2 \cdot s_2 = s_1 s_2 \cdot s_1^2 \cdot s_1^2 \cdot s_2 = 1.$$

This tetrahedral group is invariant under s_2, since

$$s_2^{-1} s_1 s_2 = s_2^3 s_1 s_2 = s_2^2 \cdot s_2 s_1 s_2 = s_2^2 s_1^2.$$

As (s_1, s_2^2) is invariant under s_2 and involves s_2^2, it follows that (s_1, s_2) is of order 24. That is,

Two operators of orders 3 *and* 4 *respectively whose product is of order* 2 *generate the group of the cube.*

From the given equations it results directly that this theorem may also be stated in either of the following two ways: Two operators of orders 2 and 3 respectively whose product is of order 4 generate the group of the cube, or two operators of orders 2 and 4 respectively whose product is of order 3 generate the group of the cube. The group of the cube may therefore be defined as the group generated by s_1, s_2 when these operators fulfil any one of the following four sets of equations:

$$s_1^3 = s_2^4 = (s_1 s_2)^2 = 1; \quad s_1^3 = s_2^4 = 1, \; s_1 s_2 = s_2^3 s_1^2;$$
$$s_1^2 = s_2^3 = (s_1 s_2)^4 = 1; \quad s_1^2 = s_2^4 = (s_1 s_2)^3 = 1.$$

The group of the cube is also known as the octahedron group, in view of the fact that the group of movements of the regular octahedron coincides with that of the cube. This group presents itself in many investigations and has been defined abstractly in a number of other ways. Among these are the following: Two operators of order 4 generate the octahedron group provided their product is of order 3 and one of them is transformed into its inverse by the square of the other. The octahedron group is the smallest group that can be generated by two operators whose orders exceed 2 and which are such that each is transformed into its inverse by the square of the other.*

* *Annals of Mathematics*, vol. 21 (1907), p. 50.

The octahedron group is completely defined by the fact that it can be generated by three cyclic non-invariant subgroups of order 4 which do not involve a common subgroup of order 2 nor generate other operators of order 4.* The octahedron group may be defined as the group which contains exactly 9 operators of order 2 such that the order of the product of any two does not exceed 4, while there are at least two such operators whose product is of order 4.†

58. Group of the Regular Icosahedron. Both the regular icosahedron and the regular duodecahedron admit two movements of orders 2 and 5 respectively whose product is of order 3. If we let s_1, s_2 represent these movements it results that these solids are transformed into themselves by operators which fulfil the following equations:

$$s_1^2 = s_2^5 = (s_1 s_2)^3 = 1.$$

It is not difficult to prove that these equations define the simple group of order 60.‡ As the regular icosahedron and the regular duodecahedron admit exactly 60 movements, it will result from this proof that their group of movements must be the simple group of order 60. Hence this group is frequently called the icosahedron group. To prove that (s_1, s_2) is of order 60 if no restrictions are placed on these operators except those implied in the given equations, we may proceed as follows:

The operators $s_1 s_2^2 s_1 s_2^3 s_1$, $s_1 s_2^3 s_1 s_2^2 s_1$ are of order 2, since they coincide with their inverses. They transform s_2 into its inverse, since the product of s_2 and either one of these operators is of order 2, as may be seen directly if we employ the equation $s_1 s_2 s_1 = s_2^4 s_1 s_2^4$, resulting from $(s_1 s_2)^3 = 1$. From this equation it results also that

$$(s_1 s_2^3)^5 = (s_1 s_2^2)^5 = 1.$$

In fact,

$$(s_1 s_2 s_1)^5 = s_2^4 (s_1 s_2^3)^5 s_2 = 1, \quad \text{since} \quad (s_1 s_2 s_1)^\alpha = s_1 s_2^\alpha s_1.$$

* *Mathematische Annalen*, vol. 64 (1907), p. 344.

† *American Journal of Mathematics*, vol. 29 (1907), p. 8.

‡ Hamilton, *Philosophical Magazine*, vol. 12 (1856), p. 446.

As $s_1s_2^2$ is the transform of the inverse of $s_1s_2^3$, the given statement is proved. The most general product that can be formed with the operators s_1, s_2 is of the form

$$s_2^{\alpha_1}s_1s_2^{\alpha_2}s_1s_2^{\alpha_3}s_1 \ . \ . \ . \ s_2^{\alpha_\lambda}.$$

If the number of factors in this product exceeds six it can evidently be reduced by means of one or more of the following equations:

$$s_1s_2s_1 = s_2^4s_1s_2^4, \quad s_1s_2^4s_1 = s_2s_1s_2, \quad (s_1s_2^3)^5 = 1,$$

$$s_1s_2^2s_1 = s_2^4s_1s_2^3s_1s_2^4, \quad s_1s_2^3s_1 = s_2s_1s_2^2s_1s_2.$$

From these equations and from the fact that

$$s_1s_2^2s_1s_2^3s_1s_2^{\alpha} = s_2^{-\alpha}s_1s_2^2s_1s_2^3s_1$$

it results that all the distinct operators of (s_1, s_2) can be written in one of the following forms:

$$s_2^m, \ s_2^ms_1s_2^n, \ s_2^ms_1s_2^2s_1s_2^n, \ s_2^ms_1s_2^2s_1s_2^3s_1 (m, n = 1, 2, \ . \ . \ . \ , 5).$$

Hence (s_1, s_2) is of order 60 if we assume that s_1, s_2 fulfil the equations given above.

The three sets of equations

$$s_1^2 = s_2^5 = (s_1s_2)^3 = 1, \quad s_1^2 = s_2^3 = (s_1s_2)^5 = 1, \quad s_1^3 = s_2^5 = (s_1s_2)^2 = 1$$

are evidently equivalent and hence each of them defines the icosahedral group. In fact, if we should assume that the operators s_1, s_2 merely *satisfy* any one of these sets of equations, they would generate the icosahedron group unless both of them were the identity. Hence we have the theorem:

If the three numbers 2, 3, 5 *are the orders of two operators and of their product, these operators must generate the icosahedron group irrespective of which of these three numbers is the order of the product.*

EXERCISES

1. If two operators merely satisfy the equations defining the tetrahedral group they may generate the cyclic group of order 3, and if they merely satisfy the equations defining the octahedral group they may generate the symmetric group of order 6 or the group of order 2.

2. If a group of order 12 contains no invariant operator of order 2 it must be tetrahedral.

3. If two operators of order 3 have a product of order $2n$ whose square is invariant under both of these operators, they generate a group of order $12n$ whose group of cogredient isomorphisms is the tetrahedral group.

59. Generalizations of the Group of the Regular Tetrahedron.* An immediate generalization of the tetrahedral group is given by the equations

$$s_1^3 = s_2^3, \quad (s_1 s_2)^2 = 1.$$

It results directly that $s_1^3 = t$ is invariant under (s_1, s_2) and that the group of cogredient isomorphisms of (s_1, s_2) is the tetrahedral group. From the fact that $s_1 s_2$ and $s_2 s_1$ are two operators of order 2 it results that $s_1 s_2^2 s_1$ is transformed into its inverse by each of the operators $s_1 s_2$ and $s_2 s_1$. Moreover,

$$(s_1 s_2^2 s_1)^2 = s_1 s_2^2 s_1^2 s_2^2 s_1^2 s_1^{-1} = s_1 . s_2^{-1} s_1^{-1} s_2^{-1} s_1^{-1} . s_1^{-1} s_1^{12} = t^4$$

is both invariant and also transformed into its inverse under (s_1, s_2). Hence the order of t is a divisor of 8. If this order is 8, the order of G is 96. That there is such a group of order 96 may readily be seen by means of the two substitutions

$$s_1 = ac'ce'eg'ga' \cdot bm'nf'oj'hk'ld'mp'fi'jb'kn'do'ph'il',$$

$$s_2 = am'je'on'gk'pc'ml'ei'na'kj'co'lg'ip' \cdot bd'df'fh'hb'.$$

The existence of this group of order 96 and some of its properties may also be established abstractly as follows: Let s'_1, s'_2 be two operators of order 3 whose product is of order 4, and suppose that they have been so chosen that (s_1', s_2') is the group of order 24 which does not involve any subgroup of order 12, i.e., the non-twelve † G_{24}. If we extend this group by means of an operator t of order 8 which is commutative with each of its operators and generates its operators of order 2, it is clear that $s_1't$, $s_2't$ may be used for s_1, s_2 respectively. That such an operator of order 8 actually exists can readily

* Some of these developments could have been presented more briefly by employing the theorem that if the square of an element of a commutator is commutative with the other element it transforms this other element into its inverse. The presentation adopted seems a little more elementary.

† *American Journal of Mathematics*, vol. 32 (1910), p. 65.

be seen if the non-twelve G_{24} is written in the regular form in four distinct sets of letters, and a simple isomorphism is established between these groups. The operator of order 4 which merely permutes cyclically the corresponding letters in these four constituent groups, multiplied by the operator of order 2 in one of these constituents, is clearly the operator of order 8 in question.

When t is of order 4, G is the direct product of the tetrahedral group and the cyclic group of order 4, since s_1^4, s_2^4 are two operators of order 3 whose product is of order 2. When t is of order 2, G is the direct product of the tetrahedral group and the group of order 2, since $(s_1^2 s_2^2)^2 = s_1^{12} = 1$. Combining these results we arrive at the theorem:

If two non-commutative operators s_1, s_2 *satisfy the equations* $s_1^3 = s_2^3$, $(s_1 s_2)^2 = 1$, *they generate a group of order* 96, *or the direct product of the tetrahedral group and one of the following three groups: the cyclic group of order* 4, *the group of order* 2, *the identity.*

Hence there are four and only 4 non-abelian groups which may be generated by two operators which satisfy these two conditions. The cyclic group of order 12 and its subgroups are evidently the only abelian groups which can be generated by two operators satisfying these conditions, and all of these groups can be generated by two such operators.

Another generalization of the tetrahedral group is furnished by the equations

$$s_1^3 = s_2^2, \quad (s_1 s_2)^3 = 1.$$

The cyclic group generated by $s_1^3 = t$ is again invariant under G, and, as $(s_1^{-1} s_2 s_1 \cdot s_2^{-1})^2 = (s_1 s_2 s_1^2 s_1^{-1} 2)^2 = s_1^{-15}$ is both invariant under G and also transformed into its inverse by s_2, it results that the order of t is a divisor of 10. If we assume that t is of order 10, G is of order 120. We proceed to prove that this G is the direct product of the non-twelve group of order 24 and the group of order 5. If t is of order 10 the order of s_1 may be assumed to be 30, since G would be abelian if the order of s_1 were not divisible by 3. Hence we may assume

that s_1, s_2 are of orders 30 and 20 respectively while s_1^5, s_2^5 are two operators of orders 6 and 4 respectively whose product is of order 6, since

$$s_2^5 s_1^5 = s_2 s_1^2 \cdot s_1^9 = s_2^{-1} s_1^{-1} \cdot s_1^{15}.$$

As $(s_1^5)^3 = (s_2^5)^2 = (s_1^5 s_2^5)^3$ is an operator of order 2, it results that (s_1^5, s_2^5) is the non-twelve group of order 24, and that G is the direct product of this group and the group of order 5.

When t is of order 5, G is evidently the direct product of the tetrahedral group and the group of order 5, and, when t is of order 2, G is the non-twelve group of order 24. This completes a proof of the theorem:

If two non-commutative operators s_1, s_2 satisfy the two conditions $s_1^3 = s_2^2$, $(s_1 s_2)^3 = 1$, they must generate one of the following four groups: the tetrahedral group, the non-twelve group of order 24, the direct products of these respective groups and the group of order 5.

If s_1, s_2 are commutative they must generate the group of order 15 or a subgroup of this group, and they may be so chosen as to generate any one of these subgroups.

60. Generalization of the Octahedron Group. The equations

$$s_1^2 = s_2^3, \quad (s_1 s_2)^4 = 1$$

evidently furnish a direct generalization of the octahedron group. To obtain an upper limit for the order of such a group we may consider the two operators s_1, $s_2^{-1} s_1 s_2$. They have a common square and this square is invariant under G. Hence it results that the commutator of s_1, s_2 is transformed into its inverse by each of the operators s_1, $s_2^{-1} s_1 s_2$. Squaring this commutator there results

$$\begin{aligned}
&s_1^{-1} s_2^{-1} s_1 s_2 \cdot s_1^{-1} s_2^{-1} s_1 s_2 = s_1^{-8} s_1 s_2^2 s_1 s_2 s_1 s_2^2 s_1 s_2 \\
&\quad = s_1^{-8} s_1 s_2^2 \cdot s_2^{-1} s_1^{-1} s_2^{-1} s_1^{-1} \cdot s_2 s_1 s_2 = s_1^{-14} s_1 s_2 s_1 s_2^2 s_1 s_2 s_1 s_2 \\
&\quad = s_1^{-14} s_1 s_2 s_1 s_2 s_1^{-1} s_2^{-1} s_1^{-1} = s_1^{-20} \cdot s_2^{-1} s_1^{-1} s_2 s_1 \\
&\quad = s_1^{-20} \cdot (s_1^{-1} s_2^{-1} s_1 s_2)^{-1}.
\end{aligned}$$

Hence it follows that $(s_1^{-1}s_2^{-1}s_1s_2)^3 = s_1^{-20}$. As s_1^{-20} is transformed into its inverse by s_1, the order of s_1 is a divisor of 40 and the order of G must therefore be a divisor of 480.

We begin with the case when s_1 is of order 8 and hence G is of order 96. To prove the existence of this G we may extend the non-twelve G_{24} by means of an operator of order 8 which transforms it according to an operator of order 2 corresponding to an outer isomorphism. Under the resulting group of order 96 the given G_{24} must therefore be transformed according to the octahedral group, which is the group of isomorphisms of this G_{24} as well as of its quaternion subgroup. If s_1' is the operator of order 2 in this octahedral group, which corresponds to the given operator s_1 of order 8 in the group of order 96, and if s_2' is an operator of order 3 in this octahedral group such that $s_1's_2'$ is of order 4, we can select an operator s_2 of order 12 corresponding to s_2' so that $s_1^2 = s_2^3$, $(s_1s_2)^4 = 1$; for, all the operators of this G_{96} which correspond to operators of order 4 in the octahedral group are of order 4, since the commutator subgroup of each of the three Sylow subgroups of order 32 is a subgroup of order 4 contained in the invariant quaternion subgroup. It is easy to verify that this group of order 96 is also generated by the following substitutions:

$$s_1 = aa'gg'ee'cc' \cdot bo'hm'fk'di' \cdot id'ob'mh'kf' \cdot jn'pl'nj'lp',$$
$$s_2 = amlgkjeipcon \cdot bdfh \cdot a'm'l'g'k'j'e'i'p'c'o'n' \cdot b'd'f'h'.$$

Having established the existence of a group of order 96 generated by two operators of orders 8 and 12 which satisfy the given conditions, it is easy to find the group of order 480 generated by two operators of orders 40 and 60 respectively which satisfy these conditions. In fact, it is obvious that such operators exist in the direct product of the given G_{96} and the cyclic group of order 5. For if s_1, s_2 generate the former group and satisfy the relations $s_1^2 = s_2^3$, $(s_1s_2)^4 = 1$, and if t is an operator of order 5 which is commutative with each of these operators, then s_1t, s_2t^{-1} will also satisfy these equations. Hence we have proved that the largest group which can be generated by two operators which satisfy the two conditions

$s_1^2 = s_2^3$, $(s_1 s_2)^4 = 1$, is the direct product of the group of order 5 and the group or order 96 obtained by extending the non-twelve group of order 24 by means of an operator of order 8 which transforms it according to an outer isomorphism of order 2.

It is evident that the group of order 48 obtained by establishing a (2, 12) isomorphism between the cyclic group of order 4 and the octahedron group is generated by two operators of orders 4 and 6 respectively which satisfy the given equations. Moreover, the direct product of this group of order 48 and the group of order 5, and the direct product of the octahedral group and this group of order 5 contain two generating operators which satisfy the conditions under consideration. Hence we have arrived at the theorem:

There are exactly six non-abelian groups which can be generated by two operators which fulfil the equations $s_1^2 = s_2^3$, $(s_1 s_2)^4 = 1$. *Three of these are of orders* 24, 48, *and* 96, *respectively, while the other three are the direct products of these respective groups and the group of order* 5.

A second generalization of the octahedron group is given by the equations

$$s_1^3 = s_2^4, \quad (s_1 s_2)^2 = 1.$$

Since the two operators $s_1 s_2$, $s_2 s_1$ are of order 2, they generate a dihedral group. To determine an upper limit of the order of this group we observe that

$$(s_2 s_1^2 s_2)^3 = (s_2^2 s_1 s_2^2)^3 \cdot s_1^9 = s_1^{21}.$$

As s_1^{21} is invariant under G, its order is a divisor of 42, and an upper limit of the order of this dihedral group is evidently 12, while the order of G is a divisor of 336. When s_1 is of order 6 the order of G is 48. Moreover, it is easy to see that the group of order 48, which may be obtained by extending the non-twelve group of order 24 by an operator of order 2 which transforms it according to an outer isomorphism, is generated by two operators of orders 6 and 8 respectively, which satisfy the given conditions. This group may be represented transitively on eight letters, and it involves 12 operators of each of the orders

2 and 8 in addition to the given subgroup of order 24. It is the group of isomorphisms of the non-cyclic group of order 9.

If we multiply the two given generators by an operator of order 7 and its inverse, the operator of order 7 being commutative with each of these generators, we obtain two operators of orders 42 and 56 respectively which satisfy the conditions in question, and hence we have the theorem:

If two operators satisfy the conditions $s_1^3 = s_2^4$, $(s_1 s_2)^2 = 1$, *the largest group which they can generate is the direct product of the group of order* 7 *and the group of isomorphisms of the non-cyclic group of order* 9. *The total number of the non-abelian groups which can be generated by two operators which satisfy these equations is six: viz., the dihedral group of order* 6, *the octahedral group, the group of isomorphisms of the non-cyclic group of order* 9, *and the direct products of these respective groups and the group of order* 7.

The third generalization of the octahedron group to be considered is given by the equation

$$s_1^2 = s_2^4, \quad (s_1 s_2)^3 = 1.$$

We may again consider the commutator of s_1, s_2 and observe that

$$(s_1^{-1} s_2^{-1} s_1 s_2)^3 = (s_2 s_1 s_2^2)^3 s_1^6 = s_1^6 s_2^{-2} (s_2^3 s_1)^3 s_2^2$$
$$= s_1^6 s_2^{-2} (s_1^4 s_2^{-1} s_1^{-1})^3 s_2^2 = s_1^{18}.$$

As s_1^{18} is transformed into its inverse by s_1, it results that the order of s_1 is a divisor of 36, and hence the order of G is a divisor of 432. It is easy to see that the group of order 48, which may be constructed by extending the non-twelve group of order 24 by means of an operator of order 4 which has its square in this non-twelve group and transforms it according to an outer isomorphism of order 2, can be generated by two operators of orders 4 and 8 respectively which satisfy the given conditions. If we multiply this s_1 and this s_2 by an operator of order 9 and by its fifth power respectively, this operator of order 9 being commutative with each of the operators s_1, s_2, and having only the identity in common with (s_1, s_2), we obtain two operators

of orders 36 and 72 respectively which satisfy the given condition and generate the group of order 432 in question. Hence it is easy to deduce the following theorem:

If two non-commutative operators satisfy the conditions $s_1^2 = s_2^4$, $(s_1 s_2)^3 = 1$, *they may generate the dihedral group of order* 6, *the octahedral group, the group of order* 48 *obtained by extending the non-twelve group of order* 24 *by means of an operator of order* 4 *which has its square in this group and transforms it according to an outer isomorphism of order* 2, *the direct products of these respective groups and a cyclic group of order* 3 *or* 9. *Hence there are exactly nine non-abelian groups which may be generated by two such operators.*

EXERCISES

1. There are exactly six non-abelian groups whose two generators s_1, s_2 satisfy the equations $s_1^2 = s_2^3$, $(s_1 s_2)^5 = 1$. They are the icosahedron group, a group of order 120, and the direct products of these respective groups and the cyclic groups of orders 5 and 25.

2. If two commutative operators satisfy the equations $s_1^2 = s_2^5$, $(s_1 s_2)^3 = 1$, they generate a cyclic group whose order is 3, 7, or 21; if they satisfy the equations $s_1^3 = s_2^5$, $(s_1 s_2)^2 = 1$, they generate a cyclic group whose order is 2, 4, 8, or 16; if they satisfy the equations $s_1^2 = s_2^3$, $(s_1 s_2)^5 = 1$, they generate a cyclic group whose order is either 5 or 25.

3. There are exactly six non-abelian groups whose generators satisfy the equations $s_1^3 = s_2^5$, $(s_1 s_2)^2 = 1$. They are a group of order 1920 and the direct products of the icosahedral group and the cyclic group of order 2^α, $\alpha = 0, 1, 2, 3, 4$.

4. If two commutative operators satisfy the equation $s_1^2 = s_2^4$, $(s_3 s_2)^3 = 1$, they generate a cyclic group whose order is 2 3, 6, 9, or 18; if they satisfy the equations $s_1^2 = s_2^3$, $(s_3 s_2)^4 = 1$, they generate a cyclic group whose order is 2, 4, 5, 10, or 20; if they satisfy the equations $s_1^3 = s_2^4$, $(s_1 s_2)^2 = 1$, they generate a cyclic group whose order is 2, 7, or 14.

CHAPTER VII

ISOMORPHISMS

61. Relative and Intrinsic Properties of the Operators of a Group. The operators or elements of a group have both relative and intrinsic properties. The latter relate to periodicity and are common to group operators and the roots of unity. Hence some of the earliest workers in abstract group theory associated this theory with the roots of unity. For instance, Cayley remarks that "a group may be considered as representing a system of roots of the symbolic binomial equation $\theta^n = 1$," * and Sir W. R. Hamilton regards the icosahedral group as "a system of non-commutative roots of unity which are entirely distinct from the i, j, k of the quaternion though having some analogy thereto." † He calls this group the *Icosian Calculus*.

In a non-abelian group the relative properties of the operators are of greatest interest, while they are of comparatively little interest as regards abelian groups. In fact, they reduce to the question of common subgroups generated by these operators in the latter case. In an automorphism of a group, the corresponding operators must evidently have the same intrinsic as well as the same relative properties. The great importance of the study of automorphisms rests on the fact that the properties of an operator are the same as those of the operators which correspond to it in some automorphism of the group, and hence these properties need to be studied for only one of these corresponding operators. Thus the concept of isomorphisms economizes thought, which is a fundamental object in mathematics.

* Cayley, *Philosophical Magazine*, vol. 7 (1854), p. 40.

† Hamilton, *Philosophical Magazine*, vol. 12 (1856) p. 446.

In its most elementary form the concept of isomorphisms is one of the oldest in mathematics, as it lies at the base of the development of abstract numbers. The concept of abstract number evidently rests on a kind of isomorphism between concrete units of various kinds, so that for many purposes we may fix our attention entirely on what is common, viz., the abstract concept of units. In the theory of groups the concept of isomorphisms assumes a new importance in view of the fact that the different automorphisms of a group may be represented by the corresponding substitutions on its operators, and, as was noted in § 19, the totality of these substitutions constitute a group known as the group of isomorphisms,* or the group of automorphisms, of the original group. We have thus associated with each group its group of isomorphisms, which is of fundamental importance in many applications of the group.

62. Group of Isomorphisms as a Substitution Group. If g distinct letters are placed in a (1, 1) correspondence with the operators of the group G of order g, the symmetric substitution group will correspond to the totality of the possible arrangements of the operators of G. Such an arrangement cannot correspond to an automorphism of G unless the identity corresponds to itself. Hence the group of isomorphisms I of G can always be represented as a substitution group on at most $g-1$ letters, and its order must therefore be a divisor of $(g-1)!$. This order cannot be equal to $(g-1)!$ except in case of three groups besides the identity, viz., the groups of orders 2 and 3, and the four-group. In fact, it is evident that I cannot be more than doubly transitive on $g-1$ letters, since the correspondence of two operators fixes the correspondence of their product. In particular, the order of the group of isomorphisms of any finite group is a finite number.

A necessary condition that I be transitive on $g-1$ letters is that all the operators of G besides the identity have the same

* Isomorphisms were first studied in an explicit manner by C. Jordan and A. Capelli. Their group properties were first studied by O. Hölder and by E. H. Moore.

order, and hence g must be of the form p^m, p being a prime number. Since the correspondence of two operators determines the correspondence of their powers, it is clear that I cannot be a primitive substitution group unless $p=2$. If all the operators of G besides the identity are of order 2, I is evidently doubly transitive. Hence it results that a necessary and sufficient condition that I be primitive on $g-1$ letters is that all the operators of G be of order 2.*

The group I is generally intransitive on $g-1$ letters, and the number of its systems of intransitivity is equal to the number of complete sets of conjugate operators of G under I. In particular, the number of characteristic operators of G is equal to g diminished by the degree of I. A sufficient condition that I is simply isomorphic with one of its transitive constituents, when it is represented as such a substitution group, is that G is generated by one of its complete sets of conjugates under I. When G is abelian it is generated by its operators of highest order, and these constitute a complete set of conjugates under I. As they constitute the only complete set of such conjugates that generate G, it results that *the group of isomorphisms of an abelian group can always be represented in one and in only one way as a transitive substitution group on letters corresponding to operators of this abelian group.* In other words, if the group of isomorphisms of an abelian group is represented on letters corresponding to the various operators of this abelian group, this group of isomorphisms has only one transitive constituent which is simply isomorphic with it, since every abelian group of order p^m, except the group of order 2, admits a non-identical isomorphism in which every operator which is not of highest order corresponds to itself. A like theorem does not apply in general to the non-abelian groups. In fact, if the I of a non-abelian group is represented on the $g-1$ letters corresponding to the operators of the group, excepting the identity, the number of its transitive constituents which are simply isomorphic with I may vary from zero to an indefinitely large number, as results from the alternating groups.

* E. H. Moore, *Bulletin of the American Mathematical Society*, vol. 2 (1896), p. 33.

Suppose that G is abelian and that I is represented as a transitive group on letters corresponding to operators of G. These operators may be composed of the operators of highest order (m) in G. As any operator of highest order may be regarded as an independent generator of G, it is evident that I cannot be regular unless G is cyclic and that I is always regular when G is a cyclic group. As an abelian group cannot be represented as a non-regular transitive substitution group, it results directly from this fact that

*A necessary and sufficient condition that the group of isomorphisms of an abelian group be abelian is that this abelian group be cyclic.**

The subgroup composed of all the substitutions of I which omit one letter must omit exactly $\phi(m)$ letters, $\phi(m)$ being the totient of m, since an operator of order m generates $\phi(m)$ operators of this order. As the number of substitutions which are commutative with every substitution of a transitive group of degree n is α, where α is the exact number of the letters omitted by the subgroup of this transitive group which is composed of all its substitutions which omit a particular letter, it results directly that I contains exactly $\phi(m)$ invariant substitutions, and that these substitutions transform every substitution of I into the same power. Hence the theorem:

If an abelian group involves operators of order m but none of higher order, its group of isomorphisms contains exactly $\phi(m)$ invariant operators.

63. Groups of Isomorphisms of Non-abelian Groups. Suppose that G is non-abelian and that I is represented on letters corresponding to a set of operators of G. If all of these operators were commutative they would generate a characteristic abelian subgroup of G. If this subgroup were in the central of G, I would involve operators corresponding to inner automorphisms, but which would not affect any of the operators of the given set. This would also be the case if this subgroup

* This theorem and the theorem of the following paragraph were proved abstractly in § 41. The fundamental importance of these theorems seems to justify the present alternative proofs.

were not in the central of G, since one of these operators would then transform into different operators some of the operators of G which are not contained in this set. Hence it has been proved that

The group of isomorphisms of a non-abelian group cannot be represented on letters corresponding to a set of relatively commutative operators of this non-abelian group.

It is now easy to see that if the group of isomorphisms I of any group G can be represented transitively on letters corresponding to a set of operators of G, then I cannot be more than doubly transitive. In fact, when G is non-abelian and we fix the correspondence of two non-commutative operators of the set in an automorphism, the correspondence of a third operator has also been fixed, since such an operator may be obtained by transforming one of the two given operators by the other. That is,

When the group of isomorphisms of any group G is represented on letters corresponding to operators of G, then this group of isomorphisms is at most doubly transitive.

It is very easy to find non-abelian groups in which the I is doubly transitive if it is constructed in a given manner. As such a group we may consider the metacyclic group of degree p and of order $p(p-1)$. The I of this group can evidently be represented on the p letters corresponding to its operator of order 2, and if it is represented in this way it coincides with the metacyclic group itself. Instead of representing I on the operators of a group we may frequently represent it more conveniently on a set of generating subgroups. If this is done I may be more than doubly transitive, as results from the fact that the group of isomorphisms of the tetrahedral group is the symmetric group of degree 4 if each letter corresponds to a subgroup of order 3.

If I is a primitive group on letters corresponding to a set of operators of a non-abelian group G, its invariant subgroup corresponding to the inner isomorphisms of G must be transitive, since a primitive group cannot involve an intransitive invariant subgroup. That is, if I is a primitive group on letters

corresponding to the operators of G, then G is either the abelian group of order 2^m and of type $(1, 1, 1, \ldots)$ or G transforms transitively the set of operators to which the letters of I correspond. As every multiply transitive group is primitive, this theorem applies to all multiply transitive groups as well as to the simply transitive primitive groups.

EXERCISES

1. If G is the symmetric group of degree 4 its I may be represented as an imprimitive group of degree 6 on letters corresponding either to its operators of order 4, or to its six conjugate operators of order 2. These two imprimitive groups are not conjugate as substitution groups, since the one is composed of positive substitutions, while the other contains negative substitutions.

2. The group of isomorphisms of the symmetric group of degree n, $n \neq 6$, can be represented as a transitive substitution group on the $n(n-1)/2$ letters corresponding to the transpositions of the symmetric group. When I is thus represented, it is a simply transitive primitive group whenever $n > 4$.

Suggestions: Use the theorem that the symmetric group of degree n, $n \neq 6$ and $n > 2$, is its own group of isomorphisms, and that it has no outer isomorphisms. See § 65.

3. Prove that if the I of the quaternion group is represented as a substitution group whose letters correspond to its operators of order 4, it will be conjugate with the group in the first of these exercises which involves negative substitutions.

64. Doubly Transitive Substitution Groups of Isomorphisms. If I is doubly transitive on letters corresponding to operators of G, each of these operators generates a cyclic subgroup (s) which is transformed into itself under the holomorph of G by a subgroup composed entirely of operators which are commutative with s; for, if a complete set of conjugate operators of G under I includes at least two powers of the same operator, the operators of this system must be transformed according to an imprimitive group. Suppose that s_1 and s_2 are two operators of G which correspond to letters of I. We may assume that s_1, s_2 are non-commutative; for, if all such operators were commutative, G would be abelian and hence the order of every operator of G would divide 2. Since this case is so elementary,

we shall exclude it in what follows and hence we shall assume that s_1, s_2 are non-commutative.

If s_1, s_2 correspond to themselves in a given automorphism of G, all the operators of the subgroup generated by s_1, s_2 must also correspond to themselves and this subgroup must include more than two operators which are conjugate to s_1, s_2 under I. Hence we have as a first result:

If the group of isomorphisms of a group G can be represented as a doubly transitive group on letters corresponding to operators of G, then the subgroup composed of all substitutions which omit one letter of this doubly transitive group is either imprimitive or it is a regular group of prime degree.

This theorem follows directly from the well-known theorem that the subgroup which is composed of all the substitutions which omit one letter of a non-regular primitive group of degree n is always of degree $n-1$. When G is abelian the given theorem evidently remains true and the imprimitive group in question involves systems of two letters each except when G is the four-group.

When the subgroup which is composed of all the substitutions of I which omit one letter is a regular primitive group, the order of I is $p(p+1)$, p being a prime, and I involves $p+1$ subgroups of order p. It must therefore involve an invariant subgroup of order $p+1$ which involves p conjugate operators under I. That is, the subgroup of order $p+1$ must be the abelian group of order 2^m and of type (1, 1, 1, . . .). Hence the following theorem:

If I is doubly transitive on letters corresponding to operators of G and if the subgroup composed of all the substitutions which omit one letter of I is primitive, then I is of order $p(p+1)$, p being a prime, and it involves an invariant subgroup of order $p+1$.

When I is a doubly transitive group on letters corresponding to a set of conjugate operators of G, either all the operators of this set are commutative or no two of them are commutative. This results immediately from the fact that when I is doubly transitive any two of its letters can be transformed into an

arbitrary pair, but a pair corresponding to two commutative operators could not be transformed into a pair corresponding to two non-commutative ones. Hence it results that when I is a doubly transitive group on letters corresponding to a set of operators of G, then G is either an abelian group of order 2^m and of type $(1, 1, 1, \ldots)$ or no two of the operators of the set under consideration are commutative.

65. Groups of Isomorphisms of the Alternating and the Symmetric Groups. In this section we propose to prove the theorems that the alternating and the symmetric group of degree n, $n \neq 3$, have the same group of isomorphisms, and that this group coincides with the symmetric group whenever $n > 3$, with the exception of the single case when $n = 6$. In this special case the group of isomorphisms of the symmetric and alternating group is a well-known group whose order is 1440; that is, this order is twice that of the corresponding symmetric group. The proof of these theorems entails the proof of several auxiliary theorems, which are also of considerable interest in themselves and of still greater historic interest in view of the fact that they relate to one of the oldest problems of group theory, viz., the determination of subgroups of small index under the symmetric and alternating groups. This is known as *Bertrand's problem.*

As it will be desirable to use the theorems that the alternating group of degree n, $n \neq 6$, involves only one subgroup of index n, viz., the alternating group of degree $n-1$, and that the symmetric group of degree n involves no subgroup of index n, $n \neq 6$, besides the symmetric group of degree $n-1$, we shall establish the somewhat more general theorem, sometimes called Bertrand's theorem,* that the symmetric group of degree n, $n > 4$, has no subgroup whose index lies between n and 2, and that its only subgroups of index n, $n \neq 6$, are of degree $n-1$; moreover, the alternating group contains no subgroup of index

* Serret, Algèbre superieure, 1849, p. 267. Bertrand proved this theorem in 1845, *Journal de l'Ecole Polytechnique*, p. 129, by assuming the theorem, afterwards proved by Čebyšëv, that there is always at least one prime number between $n/2$ (exclusive) and $n-2$ (inclusive) whenever the natural number n exceeds 6.

less than n, $n>4$, and its only subgroup of this index is the alternating group of degree $n-1$, when $n\neq 6$.

We begin with the proof of the latter part of this theorem, since the former part can be readily deduced from the latter. As the theorem of Čebyšëv, to which we have just referred, applies only to all numbers greater than 6, and the groups of degree seven are well known, we shall assume that $n>7$, and prove that the alternating group of degree n does not contain any subgroup whose index is less than $n+1$, with the exception of its alternating subgroups of degree $n-1$ and of index n. If such a subgroup existed it would be transitive on its letters, since the order of an intransitive subgroup could clearly not exceed $2\cdot(n-2)!$. As the order of an imprimitive subgroup is evidently less than this number, the subgroup in question would be primitive, and hence its order could not be divisible by the highest power of 3 which divides $n!$, since a primitive group of degree n does not involve a substitution of the form abc unless it is the alternating group of degree n.

Since the order of the subgroup in question would not be divisible by the highest power of 3 that divides $n!$, this order would have to be divisible by the prime p, where $n/2<p\leqq n-2$. Hence this subgroup would involve $1+kp$ conjugate cyclic subgroups of order p. If two such subgroups had less than $p-1$ common letters, we could transform one by an operator of the other so as to obtain two such subgroups having a larger number of common letters without having all letters in common. This process could be repeated until two subgroups of order p would be found having $p-1$ common letters, and hence the primitive subgroup in question would itself involve primitive subgroups of each of the degrees p, $p+1$, . . . , n. It would therefore be at least four-fold transitive.

As the transitive subgroup composed of all the substitutions involving a certain set of p letters would be invariant under a group of degree $p+3$, which would involve two transitive constituents of degrees p and 3 respectively, and as this transitive constituent of degree 3 would be the symmetric group of this degree, it results that each of the cyclic subgroups of order p

would be invariant under a group having the symmetric group of degree 3 as a transitive constituent. As the group of isomorphisms of the group of order p is cyclic, this would imply that the subgroup, composed of all the substitutions in the primitive group of degree n and index less than $n+1$, which transform a subgroup of order p into itself, would involve substitutions of the form ab or abc. As this is impossible, it has been proved that the alternating group of degree n, $n>7$, cannot involve a transitive subgroup of degree n and of index less than $n+1$. Hence *the symmetric group of degree* n, $n>7$, *cannot contain a subgroup of index less than* $n+1$ *and greater than* 2 *except the symmetric group of degree* $n-1$.

From what precedes, it results that the only subgroups of index n in the symmetric and the alternating groups are those of degree $n-1$, whenever $n>7$. This theorem is known to be true also as regards the groups of degree 7. From this fact and from the theorem in § 67, it follows directly that *the group of isomorphisms of the alternating and of the symmetric group of degree* n, $n>6$, *is the symmetric group of this degree.*

EXERCISES

1. Prove that in an automorphism of the symmetric group of degree 6 substitutions of the form abc may correspond to those of the form $abc\cdot def$, and that all the operators of order 3 in this symmetric group are conjugate under its holomorph.

2. Prove that the symmetric groups of degrees 4 and 5 are complete groups, and that the alternating groups of these degrees have the corresponding symmetric groups for their groups of isomorphisms.

3. Give an instance of a group which involves an invariant subgroup whose group of isomorphisms is larger than that of the entire group.

66. Several Useful Theorems Relating to the Groups of Isomorphisms.* Every abelian group can be extended so that we obtain a group of twice the order of the original group, by means of operators of order 2 which transform each operator of this abelian group into its inverse. These groups may be regarded as a direct generalization of the dihedral groups, and may therefore be called *generalized dihedral groups* as regards

* Cf. *Philosophical Magazine*, vol. 231 (1908), p. 223.

the given abelian groups. If the given abelian subgroup involves operators whose order exceeds 2, the corresponding general dihedral group is non-abelian and vice versa. Let G be any non-abelian generalized dihedral group of order g and let H be the abelian subgroup of order $g/2$ which was extended to obtain G. In any automorphism of G the $g/2$ non-invariant operators of order 2 must correspond to themselves, and hence the I of G can be represented as a substitution group of degree h, h being the order of H.

It is evident that the non-invariant operators of order 2 in G can be arranged in h different ways after the automorphism of H has been fixed. Hence the order of the I of G is the same as the order of the holomorph of H. We proceed to prove that the I of G is simply isomorphic with the holomorph of H. In fact, this I can be represented as a transitive substitution group of degree h which involves an invariant regular subgroup which is simply isomorphic with H, since G can be made simply isomorphic with itself in such a way that the operators of H correspond to themselves while the remaining operators of G correspond to themselves multiplied by an arbitrary operator of H. These isomorphisms therefore correspond to a regular subgroup of order h in I, I being represented on letters corresponding to the non-invariant operators of order 2 in G, and this regular subgroup is simply isomorphic with H by construction.

Moreover this regular subgroup is invariant under I, since H must correspond to itself in every automorphism of G, and this regular subgroup includes all the substitutions of I corresponding to the automorphisms of G in which all the operators of H correspond to themselves. From this fact it results that I must be a subgroup of the holomorph of H, and as the order of I is equal to the order of the holomorph of H it results that I is this holomorph. These results may be stated as follows:

The group of isomorphisms of the generalized dihedral group of an abelian group H, involving operators whose orders exceed 2, is the holomorph of H.

As a special case of this theorem we may observe that the group of isomorphisms of the dihedral group of order $2h$, $h>2$, is the holomorph of the cyclic group of order h.

If H is any abelian group of even order, it may be extended by means of h operators of order 4 such that they have a common square, and each operator of H is transformed into its inverse by each of these operators of order 4. The group G of order $2h$ which can be constructed in this way will be called the *generalized dicyclic group* as regards H, since it reduces to the dicyclic group whenever H is cyclic. With the single exception when H is of order 2^m and of type $(2, 1, 1, 1, \ldots)$, the I of G can always be represented as a transitive substitution group on the given h operators of order 4. By exactly the same reasoning as was employed in the preceding case we see that, when H does not satisfy the given special condition, the I of this G is also the holomorph of G whenever the common square of the given h operators of order 4 is a characteristic operator of H. This proves the following theorem:

The group of isomorphisms of the generalized dicyclic group as regards an abelian group H, which is not both of order 2^m and type $(2, 1, 1, 1, \ldots)$, is the holomorph of this abelian group whenever the common square of the h operators of order 4 which were added to H is a characteristic operator of H.

It should be observed that H is a characteristic subgroup of G also when it is both of order 2^m and of type $(2, 1, 1, 1, \ldots)$ provided the squares of the remaining operators of order 4 in G are not the same as those of the operators of order 4 in H. In this case, as well as in the more general case considered above, the group of isomorphisms of G is the subgroup of the holomorph of H composed of all the operators of this holomorph which are commutative with the square of the given h operators of order 4. The method of proof employed above may serve to establish a very elementary but useful theorem, which may be stated as follows:

If a group G containing a characteristic subgroup H is such that automorphisms of G may be obtained by multiplying successively an operator s of G which is not in H by all the operators

of H while the operators of H are left unchanged, then the group of isomorphisms of G involves an invariant subgroup which is simply isomorphic with H, whenever this group of isomorphisms can be represented as a transitive group of degree h, corresponding to the conjugates of s.

Suppose that G is a complete group which involves only one subgroup of index 2, and consider the direct product of G and the group of order 2. If a group contains only one subgroup of index 2, this subgroup is generated by the square of the operators of the group, and, conversely, if a subgroup of index 2 is generated by the squares of the operators of a group, it is the only subgroup of index 2 in the group. That is, a necessary and sufficient condition that a group contain one and only one subgroup of index 2 is that the squares of its operators generate such a subgroup. Hence the squares of the operators in the direct product of G and the group of order 2 generate a characteristic subgroup of index 4 under this direct product. The I of this product involves an invariant operator of order 2 corresponding to the automorphisms in which two of the three co-sets as to the given characteristic subgroup are multiplied by the invariant operator of order 2. As the order of this I is the double of the order of G and as I involves an invariant operator of order 2 which is not in the I of G there results the theorem:

If G is a complete group and contains only one subgroup of index 2, then the group of isomorphisms of the direct product of G and the group of order 2 is simply isomorphic with this direct product.

As special cases of this theorem we may observe that the I of the direct product of the symmetric group of degree n, $n>2$ and $n\neq 6$, and the group of order 2, is simply isomorphic with this direct product; and that the I of the direct product of the metacyclic group of order $p(p-1)$, p being an odd prime, and the group of order 2, is simply isomorphic with this direct product. If a group G is the direct product of characteristic subgroups, the I of G is evidently the direct product of the I's of these subgroups. As an abelian group is the direct prod-

uct of its Sylow subgroups, *the I of an abelian group is always the direct product of the I's of its Sylow subgroups.*

67. Group of Isomorphisms of a Transitive Substitution Group. Suppose that G is a transitive substitution group of degree n which involves no subgroups of index n and degree n, but involves subgroups of degree $n-1$. Its n subgroups of degree $n-1$ must therefore correspond among themselves in every automorphism of G, and these subgroups may be so lettered that they are transformed by every substitution in G in exactly the same manner as the letters of this substitution are transformed. From this it results that if each of the n subgroups corresponds to itself in any automorphism of G, each of the substitutions of G must also correspond to itself in this automorphism. That is, the I of G may be represented on letters corresponding to these subgroups.

As G involves subgroups of degree $n-1$, it is simply isomorphic with its group of inner isomorphisms. Hence the I of G may be represented as a transitive substitution group of degree n which contains G invariantly. This proves the following theorem:

If G is a transitive substitution group of degree n which involves subgroups of degree $n-1$ but no subgroups of both degree n and index n, then the group of isomorphisms of G can be represented as a transitive substitution group of degree n which contains G as an invariant subgroup.

As the symmetric group of degree n involves no subgroup of degree and index n when $n \neq 6$, and as it contains a subgroup of degree $n-1$ whenever $n \neq 2$, it results from the given theorem that the I of every symmetric group of degree n, except when n is either 2 or 6, can be represented as a substitution group on n letters, which contains this symmetric group. This substitution group must therefore be the corresponding symmetric group, as was proved above. In a similar way we may observe by means of this theorem that the metacyclic group of degree p and of order $p(p-1)$ is its own group of isomorphisms. These illustrations may suffice to point out the usefulness of this theorem in the study of the groups of isomorphisms of substitution groups.

When G is an intransitive group of degree n such that every subgroup which omits one letter is of degree exactly $n-1$, it is still true that these n subgroups of G are transformed by every substitution of G in exactly the same manner as the letters of this substitution are permuted. If G is such that these n subgroups of degree $n-1$ must correspond to themselves in every possible automorphism of G, the group of isomorphisms of G can again be represented as a substitution group on n letters. It is, however, not necessary that this substitution group should be transitive, as may be seen by letting G represent the intransitive group of degree 7 and of order 24 obtained by establishing a (1, 4) isomorphism between the symmetric groups of degrees 3 and 4.

EXERCISES

1. There is no group whose group of isomorphisms is a cyclic group of odd order greater than 1.*

2. The quaternion group and the cyclic group of order 8 are the only two groups of this order that cannot be the groups of isomorphisms of any group.†

3. There are two and only two groups which have the symmetric groups of order 6 for their group of isomorphisms.‡

4. Find the groups of isomorphisms of all the substitution groups whose degrees do not exceed 5.

5. The order of the group of isomorphisms of any abelian group is divisible by the number of its operators of highest order. A necessary and sufficient condition that the order be equal to this number is that the group be cyclic.

6. The number of distinct groups which have a given group of inner isomorphisms is either zero or infinity.

7. If a non-abelian group can be represented transitively only as a regular group, it cannot be the group of isomorphisms of an abelian group.

* *Annals of Mathematics*, second series, vol. 2 (1900), p. 79

† *Bulletin of the American Mathematical Society*, vol. 6 (1900), p. 339.

‡ *Transactions of the American Mathematical Society*, vol. 1 (1900), p. 399.

CHAPTER VIII

SOLVABLE GROUPS *

68. Introduction. A group is said to be *solvable* if, and only if, it contains a series of invariant subgroups such that the last of the series is the identity and the index of each of these subgroups under the next larger subgroup is a prime number. For instance, the symmetric group of order 24 contains an invariant subgroup of index 2, this subgroup contains an invariant subgroup of index 3, this subgroup is the four-group and contains an invariant subgroup of index 2, and the identity is of index 2 under this last subgroup. Hence the symmetric group of order 24 is solvable. The numbers 2, 3, 2, 2 are said to be its *factors of composition*. In general, the factors of composition of a group are the indices of the successive largest invariant subgroups. For example, the symmetric group of order 120 contains an invariant subgroup of index 2, but this subgroup involves no invariant subgroup besides the identity. Hence the symmetric group of order 120 is *insolvable* and has 2 and 60 for its factors of composition. Every abelian group is evidently solvable.

The terms solvable and insolvable as applied to groups of finite order are transferred from the theory of equations. An algebraic equation is solvable by rational processes in addition to root extractions whenever the group of the equation is solvable and only then (cf. Part III). It should be observed that an invariant subgroup of an invariant subgroup is not necessarily an invariant subgroup of the entire group. For instance, the invariant subgroup of order 2 used in connection with the

* In H. Weber's *Lehrbuch der Algebra*, solvable groups are called *metacyclic*. In the present work we use the term metacyclic with its older meaning to represent the holomorph of the group of order p. See p. 12.

symmetric group of order 24 in the preceding paragraph is not invariant under this symmetric group, but it is invariant under the four-group.

It may appear possible that one might obtain only prime factors of composition by one method of selecting the successive invariant subgroups while another method would lead to composite factors. If this were possible the determination of solvability or insolvability of a group would sometimes require an examination of different sets of subgroups such that each is a largest invariant subgroup of the one which precedes it, and the last is the identity. That the factors of composition of a group are entirely independent of the order in which the invariant subgroups in question are selected can easily be established by means of the theorem that two invariant subgroups which have only the identity in common must have the property that each operator of the one is commutative with every operator of the other (cf. § 29). We proceed to prove the invariance of the factors of composition of any group by means of this theorem.

Let G_0 be any solvable group, and let the following series of subgroups, with the exception of G_0, have the property that each is invariant and of prime index under the one which immediately precedes it:

$$G_0,\ G_1,\ G_2,\ \ldots,\ G_{p-1},\ G_p=1.$$

In selecting another such series, suppose that the first α groups coincide with the first α groups in given series, but that the $(\alpha+1)$th is different. We thus have the series:

$$G_0,\ G_1,\ \ldots,\ G_{\alpha-1},\ G'_\alpha,\ \ldots$$

As both G_α and G'_α are invariant under $G_{\alpha-1}$, their cross-cut is also invariant under $G_{\alpha-1}$. The quotient group of $G_{\alpha-1}$ with respect to this cross-cut must therefore involve two maximal invariant subgroups, corresponding to G_α and G'_α, which have only the identity in common. Hence this quotient group is the direct product of these invariant subgroups of prime orders. This proves that the given cross-cut could be

selected for $G_{\alpha+1}$ regardless of whether G_α or G'_α was selected, and hence it establishes the *invariance of the factors of composition* of any solvable group, since this invariance may be assumed for the groups G_α and G'_α, as they are of lower order than G_0 is.

It may be observed that the above proof is not dependent on the fact that G_0 was assumed to be solvable. The quotient group with respect to a given cross-cut is always the direct product of two simple groups, since the invariant subgroups are maximal, and hence the factors of composition are invariants as regards any group, even if this group be insolvable. Moreover, as the two factor groups of a direct product of two simple groups are evidently invariants of this direct product,* it results immediately that the following series of quotient groups

$$G_0/G_1,\ G_1/G_2,\ \ldots,\ G_{\rho-1}/G_\rho = G_{\rho-1}$$

is an invariant of G_0 irrespective of whether G_0 is solvable or not. That is, *the totality of these simple quotient groups is independent of the choice of the maximal invariant subgroups.* The important theorem as regards the invariance of the factors of composition of any group was first proved by C. Jordan in *Journal de Mathématiques*, volume 14 (1869), page 139. The fact that the given series of quotient groups is also an invariant of G_0 was observed by O. Hölder in the *Mathematische Annalen*, volume 34 (1889), page 37.

Instead of defining a solvable group as one having only prime factors of composition, we may also define it as a group which has the property that we arrive at the identity by forming the successive commutator subgroups. That is, if G_α is the commutator subgroup of $G_{\alpha-1}$, $\alpha=1, 2, \ldots$, and if we form the series of groups

$$G_0,\ G_1,\ G_2,\ \ldots,\ G_\lambda,$$

* This is a special case of the theorem that factor groups of any direct product are always completely determined by this direct product. Cf. Remak, *Crelle's Journal*, vol. 139 (1911), p. 293.

a necessary and sufficient condition that G_0 be solvable is that for a finite value of λ, $G_\lambda = 1$. It is evident that this implies that $G_{\lambda-1}$ is abelian and that the order of G_α is less than that of $G_{\alpha-1}$ whenever $\alpha \leqq \lambda$. The given condition for the solvability of G_0 is therefore equivalent to saying that a necessary and sufficient condition that a group be solvable is that none of its successive commutator subgroups besides the identity is a perfect group (cf. § 29).

That this second definition of a solvable group is equivalent to the first, follows immediately from the fact that if a group has an invariant subgroup of prime index, this subgroup must include the commutator subgroup of the group, and if the order of the commutator subgroup of a group is less than the order of the group, there must be an invariant subgroup of prime index in the group, since the commutator quotient group is always abelian.

While every simple group of composite order is evidently a perfect group, there are perfect groups which are composite.

EXERCISES

1. The smallest perfect group which is not also simple is of order 120.

2. The factors of composition of the symmetric group of degree n, $n \neq 4$, are 2 and $n!/2$.

3. Every perfect group besides the identity is insolvable, but an insolvable group is not necessarily perfect.

4. Every subgroup of a solvable group is solvable.

5. Each one of the series of successive commutator subgroups is invariant under the original group.

6. Every solvable group of composite order contains an invariant subgroup which is abelian and whose order exceeds unity.

69. Series of Composition. If each one of the series of groups

$$(A) \qquad G_0, G_1, G_2, \ldots, G_\rho = 1,$$

excluding the first, is a maximal invariant subgroup of the one which immediately precedes it, the series is said to be an *ordinary series of composition* of G_0. For brevity an ordinary series of composition is often called a *series of composition.* A necessary and sufficient condition that G_0 be a simple group

whose order exceeds unity is that this series consists of only two terms. We may form another series

$$(B) \qquad G_0,\ G'_1,\ G'_2,\ \ldots,\ G'_\lambda = 1$$

in which each subgroup is an invariant subgroup of G_0 and has the property that no larger invariant subgroup of G_0, containing this one, exists in the group which immediately precedes it. The series (B) is said to be a *chief series of composition* of G_0. It is sometimes possible to select a series of composition in such a manner that it is also a chief series. This can evidently always be done when the order of G_0 is a power of a prime number.

It is always possible to construct an ordinary series of composition by inserting some terms in a chief series of composition if the chief series is not already an ordinary series of composition. Suppose that it is necessary to insert some terms in the series (B) between G'_α and $G'_{\alpha+1}$ to obtain an ordinary series of composition and that H_1 is such a term, which corresponds to a maximal invariant subgroup in the quotient group $G'_\alpha/G'_{\alpha+1}$, while H_2 is a conjugate of H_1 under G_0. Since H_1 and H_2 are maximal invariant subgroups of G'_α their cross-cut is also invariant under G'_α, and the corresponding quotient group is the direct product of two conjugate simple groups. When G_0 is solvable these simple groups have the same prime order p, and hence this quotient group is of order p^2.

As every group of order p^2 is abelian, it results that the cross-cut of H_1 and any of its conjugates under G_0 involves the pth power of every operator in these conjugate subgroups as well as the commutators of all their operators. Hence it follows that if we find the complete set of conjugates of H_1 under the solvable group G_0, their common cross-cut, which is invariant under G_0 and hence coincides with $G'_{\alpha+1}$, involves all their commutators as well as the pth powers of all their operators. This proves the following theorem:

If G_0 is any solvable group and $G_0,\ G_1',\ G'_2,\ \ldots,\ G'_\lambda = 1$ is a chief series of composition, then the quotient group of any of the groups in this series with respect to the one immediately

following it is an abelian group which involves only operators of prime order besides the identity.

This abelian group is therefore of type (1, 1, 1, . . .). If the order of this quotient group is p^α, we must evidently insert $\alpha-1$ terms in order to obtain an ordinary series of composition from the given chief series. The first of these can be chosen in $(p^\alpha-1)/(p-1)$ different ways.

When G_0 is insolvable, the given method of proof leads directly to the results that the quotient group of any one of the groups, in the given chief series, with respect to the one immediately following it, is a direct product of simple groups of composite order which are simply isomorphic. If these simply isomorphic simple groups are of prime order, we have the result expressed in the preceding theorem. It is easy to prove that the totality of the quotient groups of each group of a chief series of composition with respect to the one following it is an invariant of the group. In fact this proof is practically the same as the proof of the fact that the factors of composition of any group is an invariant of the group.

The theorem that the quotient group of any group in a chief series of composition, with respect to the one which follows it, is a power of a simple group, results also directly from the fact that this quotient group cannot involve a characteristic subgroup. The given method of proof leads directly to the theorem that a necessary and sufficient condition that a group does not contain a characteristic subgroup is that this group is a power of a simple group. If this theorem had been assumed as known, the fact that each of the given quotient groups is a power of a simple group would not have required any proof.

If we form the successive commutator subgroups of a solvable group G_0 we obtain a third series

$$(C) \qquad G_0,\ G''_1,\ G''_2,\ \ldots,\ G''_\gamma = 1.$$

As the quotient group of each of these groups with respect to the one which immediately follows it is abelian and as each one of the successive commutator subgroups is invariant under G_0, it results that as regards the three series A, B, C we have

$\rho \geqq \lambda \geqq \gamma$. We may clearly pass from the successive commutator subgroups series to a chief series of composition by inserting additional terms wherever necessary. It should be observed that in the successive commutator subgroups series all the terms of the series are invariants of G_0, and hence the order of the quotient group of each term of the series with respect to the one just following it is also an invariant of G_0, while in series A and B we proved only that the totality of these quotient groups is an invariant of G_0, but the order in which these two quotient groups occur is not necessarily an invariant in these two series.

To illustrate the difference between the series A, B, C, we first use for G_0 any group of order p^m, $m>2$. It is clear in this special case that $\rho=\lambda=m$, while $\gamma \leqq m/2$ when m is even and $\gamma \leqq (m+1)/2$ when m is odd. This results directly from the fact that every group of order p^2 is abelian. If G_0 is the symmetric group of order 24 it results that $\rho=4$ while $\lambda=\gamma=3$. A necessary and sufficient condition that G_0 be abelian is that $\gamma=1$. Although it is always possible to pass from a successive commutator subgroups series to a chief series of composition by inserting (if necessary) terms into the former series, it is not always possible to obtain the commutator subgroups series by dropping terms out of a chief series of composition. Similar remarks apply to series A and B; that is, it is not always possible to obtain a chief series of composition by omitting terms of an ordinary series of composition, but it is always possible to obtain an ordinary series of composition by inserting terms, if necessary, between terms of a chief series of composition.

The fact that it is not always possible to obtain a chief series of composition by omitting some groups of an ordinary series which is not also a chief series, should be emphasized, since erroneous statements in regard to this matter are rather common. For instance, such erroneous statements appear in the *Encyclopédie des Sciences Mathématiques*, tome 1, volume 1, page 568. As a very simple illustration it may be observed that if G is the octic group, and if G_1 is a non-cyclic

group of order 4 contained in G, we may construct an ordinary series of composition of G by using for G_2 a subgroup of order 2 contained in G_1 but not invariant under G. By omitting G_2 from this series there results a series which is not a chief series of composition of G, since G_1 contains the commutator subgroup of G. The fact that a commutator subgroup series of composition cannot always be obtained by omitting subgroups from a chief series which is not also a commutator subgroup series can be illustrated by means of the direct product of the octic group and a group of order 2.

A solvable group of composite order must be composite, but not every composite group is solvable. Sometimes the proof that all the groups which belong to a certain system are composite is equivalent to the proof that they are solvable. This is clearly the case when the invariant subgroups and the corresponding quotient groups belong to the same system. For instance, the proof that every group whose order is the product of distinct prime numbers is composite is equivalent to the proof that all such groups are solvable. Similarly, the proof that every group whose order is a power of a prime is composite is equivalent to the proof that all such groups are solvable. On the contrary, the proof that every group whose order is divisible by 2 but not by 4 is composite does not establish the fact that such a group is solvable. If it could be proved that every group of odd order is composite, it would result from this that every group whose order is not divisible by 4 would be solvable.

70. Groups Involving no More than one Non-cyclic Sylow Subgroup. One of the most useful theorems as regards solvable groups is the one which affirms that a group is solvable if it involves either no non-cyclic Sylow subgroup or contains only cyclic Sylow subgroups besides those whose orders are divisible by the highest prime which divides the order of the group. To prove this theorem we assume that the order of such a group G is written in the form $g = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\lambda^{\alpha_\lambda}$, where $p_1, p_2, \ldots, p_\lambda$ are distinct prime numbers, arranged in ascending order of magnitude.

Since G involves operators of orders $p_1^{\alpha_1}$, the number of its operators whose orders divide g/p_1 is less than g. This number is known to be a multiple of g/p_1 (§ 32) and hence it can be written in the form kg/p_1, where k is an integer. The number of operators of G whose orders are divisible by $p_1^{\alpha_1}$ is therefore equal to

$$g-kg/p_1=l(p_1-1),$$

since this number is also a multiple of the number of the different possible generators of a cyclic subgroup of order $p_1^{\alpha_1}$. The first member of the given equation is divisible by g/p_1, and, as each of the prime factors of this divisor exceeds p_1-1, it results that l is also divisible by g/p_1. Hence $k=1$, and $l=g/p_1$.

If $\alpha_1>1$, it can be proved, in exactly the same way, that the number of the operators of G whose orders are divisible by $p_1^{\alpha_1-1}$ but not by $p_1^{\alpha_1}$ is

$$g/p_1-k_1g/p_1^2=l_1(p_1-1).$$

Hence $k_1=1$, and $l_1=g/p_1^2$. By continuing this process it results that the number of operators of G whose orders divide $p_\beta^{\alpha_\beta}\ldots p_\lambda^{\alpha_\lambda}$, $\beta<\lambda$, is exactly equal to this number. In particular, G contains only one Sylow subgroup of order $p_\lambda^{\alpha_\lambda}$, and the corresponding quotient group contains only one subgroup of order $p_{\lambda-1}^{\alpha_{\lambda-1}}$, etc. Hence G contains a cyclic quotient group of order $p_1^{\alpha_1}$, and the invariant subgroup of G which corresponds to the identity in this quotient group is such that each of its Sylow subgroups, with the possible exception of those of order $p_\lambda^{\alpha_\lambda}$, is cyclic. This completes a proof of the following theorem:

If all the Sylow subgroups whose orders are not divisible by the highest prime which divides the order of the group are cyclic, the group is solvable.

In particular, every group whose order is not divisible by the square of a prime number is solvable. Hence there is only one such group when none of these primes diminished by unity is divisible by another.

71. Groups whose nth Group of Inner Isomorphisms is the Identity. Let

$$I_1, I_2, \ldots, I_n$$

represent a series of successive groups of inner isomorphisms of a group G. A necessary and sufficient condition that I_1 be simply isomorphic with G is that the central of G be the identity. In this case, all of the successive groups of inner isomorphisms are simply isomorphic with G. If I_α has the same order as $I_{\alpha+1}$, $\alpha<n$, then I_α is simply isomorphic with all the groups of the given series which succeed I_α. It may happen that for a sufficiently large value of n, $I_n=1$. In this case G is clearly solvable.

Suppose that one of the prime numbers which divide the order of G does not divide the order of I_n. From the theorem that a group has exactly the same number of Sylow subgroups of any order as its group of inner isomorphisms has, where the identity is counted as a Sylow subgroup of order p^α if the order of the group of inner isomorphisms is not divisible by p, it results that G involves only one Sylow subgroup of order p^m whenever the order of I_n, for a sufficiently large value of n, is not divisible by p.

If G is a solvable group whose order is divisible by p, while the order of I_n is not divisible by p, then G is a direct product of its Sylow subgroups of order p^m and some other subgroup. On the other hand, it is evident that when G is such a direct product, then it is possible to find a number n such that the order of I_n is not divisible by p. Hence the theorem:

A necessary and sufficient condition that a solvable group G be the direct product of a Sylow subgroup of order p^m and some other subgroup is that the order of the nth group of inner isomorphisms of G should not be divisible by p when n is sufficiently large.

In particular, a necessary and sufficient condition that G be the direct product of its Sylow subgroups is that we can arrive at the identity by forming successive groups of inner isomorphisms of G.*

* Cf. Loewy, *Mathematische Annalen*, vol. 55 (1901), p. 69.

EXERCISES

1. If the nth successive group of inner isomorphisms of a group is the identity, the nth successive group of inner isomorphisms of each of its subgroups must also be the identity.

2. A group of order 455 is necessarily cyclic.

3. The direct product of any finite number of solvable groups is again a solvable group.

4. If n is the number of operators or subgroups in a complete set of conjugates of a simple group, the order of this group divides $n!$ and is a multiple of n.

72. Arbitrary Choice of Factors of Composition. If a group G is the direct product of its Sylow subgroups, then each subgroup of G is also such a direct product, since we must arrive at the identity by forming successive groups of inner isomorphisms. Hence it results directly that it is possible to find a series of composition of G such that the factors of composition occur in an arbitrary order, whenever G is the direct product of its Sylow subgroups.

On the other hand, suppose that G is a solvable group such that it is possible to select a series of composition in such a manner that all the factors of composition which are equal to a given prime number p appear at the end of the series, while all the other factors of composition are prime to this number. Hence G contains one and only one Sylow subgroup of order p^m. In particular, there results the theorem:

A necessary and sufficient condition that a series of composition of a solvable group G can be found which corresponds to an arbitrary arrangement of the factors of composition is that G is the direct product of its Sylow subgroups.

By combining the theorem of the present section with those of the preceding one, it results that a necessary and sufficient condition that a series of composition of a solvable group can be found such that the corresponding factors of composition occur in an arbitrary order, is that we can arrive at the identity by forming successive groups of inner isomorphisms. These results can readily be extended so as to apply to groups which have composite factors of composition. Such a group is also the direct product of groups whose orders are powers of given

factors of composition whenever there is a series of composition corresponding to every possible order of the factors of composition.

73. Groups of Order $p^\alpha q^\beta$, p and q being Prime Numbers. In § 138 it will be proved that every group of order $p^\alpha q^\beta$ is solvable. Two very simple special cases will be considered here. The case when $\beta = 1$ is especially simple and will be considered first. If G is of order $p^\alpha q$ and $q < p$, then G contains only one subgroup of order p^α and it must therefore be solvable. When $q > p$ and G contains more than one subgroup of order p^α, it must contain just q such subgroups. We proceed to prove that no two of these subgroups can have a cross-cut which is non-invariant.

Let K represent the largest possible cross-cut of a pair of these subgroups. Since K is invariant under operators of each of these subgroups which are not contained in K, it must be invariant under a subgroup of G whose order is divisible by some prime number besides p. Hence K is invariant under an operator of order q, and it is therefore contained in each one of the q subgroups of order p^α. Since K is composed of all the operators which are common to a complete set of conjugates, it is invariant under G, and the corresponding quotient group has an order which is of the same form as the order of G. It remains therefore only to consider the case when the q subgroups of order p^α are such that no two of them have two operators in common.

In this case these q subgroups are transformed according to a transitive substitution group of degree q which involves no substitution whose degree is less than $q-1$. It can therefore not contain more than $q-1$ substitutions of degree q, since the average number of letters in all its substitutions is $q-1$. Hence it contains only one subgroup of order q, and it must therefore be composite. As no group of order $p^\alpha q$ can be simple, every group whose order is of this form must be solvable.

The case when all the Sylow subgroups of a group of order $p^\alpha q^\beta$ are abelian is almost equally elementary. Let G be such a group and suppose that G is simple. If s represents any

operator of order p contained in G and if J is any Sylow subgroup of order q^β, it is evident that s can be transformed into all its conjugates under G by means of the operators of J. If each operator of G is represented by a substitution according to which this operator transforms the conjugates of s, there results a substitution group S which is simply isomorphic with G, since G is simple.

To the subgroup J in G there corresponds a transitive substitution group in S, since J transforms s into all its conjugates. As a transitive abelian group is regular, s has exactly q^β conjugates under G. Hence the identity is the cross-cut of any two of the q^β Sylow subgroups of order p^α contained in G. That is, if G were simple it would contain $(p^\alpha-1)q^\beta$ operators whose orders are powers of p, and hence it could contain only q^β operators whose orders are powers of q. As such a group could contain only one subgroup of order q^β, it could not be simple. This proves that every group of order $p^\alpha q^\beta$ is solvable whenever the Sylow subgroups of orders p^α and q^β are abelian.

74. Insolvable Groups of Low Composite Orders. From the theorems which have been established it follows directly that every group whose order is less than 60 is solvable. That there is an insolvable group of order 60 and that this is the lowest order of a simple group of composite order was observed by E. Galois. We proceed to prove that there is only one insolvable group of this order. If a group of order 60 contains only one subgroup of order 5, the corresponding quotient group is of order 12 and hence the group is solvable. Hence an insolvable group of order 60 must involve 6 conjugate subgroups of order 5 and must transform them according to a transitive substitution group of degree 6 and order 60. As there is only one such substitution group,* there is only one insolvable group of order 60.

* The fact that there could not be more than one such substitution group may be seen as follows: Such a group contains the group of degree 5 and of order 10, and hence it involves exactly 15 substitutions of order 2. As none of these can occur in two subgroups of order 4 the group must contain five subgroups of this order.

The first order beyond 60 which is not included in the given theorems is 72. As this is of the form $8p^m$, p being an odd prime number, we shall prove that no group whose order is of this form is insolvable. If such a group were insolvable it would contain 4 or 8 subgroups of order p^m, and hence p would be 3 or 7. In the former case the 4 subgroups of order p^m would be permuted either according to the symmetric or according to the alternating group of degree 4. In either case there would be a solvable invariant subgroup and the corresponding quotient group would also be solvable. Hence the entire group would be solvable.

If there were 8 subgroups of order p^m, then p would be 7, and the 8 subgroups of order p^m would be permuted according to the group of degree 8 and of order 56. As this group is solvable, it results that no group whose order is of the form $8p^m$ can be insolvable.

Similarly it may be observed that no group whose order is of form $4p^m$ can be insolvable. The only remaining number less than 100 which requires consideration is 84. Every group of order 84 involves an invariant subgroup of order 7. Hence such a group is solvable, and *there is one and only one insolvable group whose order is less than* 100. As there is no number between 99 and 120 which could be the order of an insolvable group we proceed to consider the insolvable groups of order 120.

Since a group of order 120 involves either one or six subgroups of order 5, every insolvable group of this order contains 6 subgroups of order 5, which it transforms according to a transitive group of degree 6. Every group of order 120 which contains six subgroups of order 5 is insolvable, since the order of the group according to which these six subgroups are transformed is either 60 or 120. If this order is 120 the group in question must be simply isomorphic with it, and hence it must be simply isomorphic with the symmetric group of degree 5. If the order of this group of degree 6 is 60, the groups in question must have a (2, 1) isomorphism with the icosahedral group and must

involve two substitutions (s_1, s_2) which satisfy one of the following two sets of conditions:

$$s_1^3 = s_2^5 = (s_1 s_2)^2 = 1; \quad s_1^3 = s_2^5 = (s_1 s_2)^2, \ s_1^6 = 1.$$

In the former case s_1, s_2 generate the icosahedral group, and the group in question is the direct product of this group and the group of order 2. In the latter case s_1, s_2 generate the group of order 120, which has no subgroup of order 60, but has the icosahedral group for a quotient group. This proves that there cannot be more than three insolvable groups of order 120. As it is well known that three such groups exist, it has been proved that *there are only three insolvable groups of order* 120; *viz., the symmetric group of this order, the direct product of the icosahedral group and the group of order* 2, *and the group of order* 120 *which involves operators of order* 4 *and has the icosahedral group for a quotient group.*

Between 120 and 168 are four numbers which are not included in the general theorems which were established above. These numbers are 132, 140, 144, and 156. If a group of any of these orders were insolvable it would have to be simple. Hence we may confine ourselves to a proof of the theorem that every group of these orders must be composite. If a group of order 132 were simple, it would permute its twelve subgroups of order 11 according to a simply isomorphic transitive substitution group of degree 12. As this would be of class 11 it would contain an invariant subgroup of order 12.

A group of order $140 = 2^2 \cdot 5 \cdot 7$ contains a characteristic subgroup of order 5, a group of order 144 contains 1, 3, or 9 subgroups of order 16, and hence cannot be simple, and a group of order $156 = 2^2 \cdot 3 \cdot 13$ contains a characteristic subgroup of order 13. Hence 168 is the lowest order, beyond 120, of an insolvable group. We proceed to prove that there is only one simple group, and hence only one insolvable group, of this order. That there is at least one such group results from the theory of the transitive substitution groups of degree 7, and

from the group of isomorphisms of the abelian group of order 8 and of type (1, 1, 1).

A simple group of order 168 contains 8 subgroups of order 7, and can therefore be represented as a transitive substitution group G of degree 8. A maximal subgroup of G is of degree 7 and of order 21, and it therefore involves seven subgroups of the form $(abc\cdot def)$. Each of these subgroups is transformed into itself by six substitutions under G. Hence it may be assumed that all the possible simple groups of order 168 contain a particular subgroup of degree 7 and order 21, and are generated by this subgroup and a substitution of the form $ab\cdot cd\cdot ef\cdot gh$, which transforms into itself a particular subgroup of the form $(abc\cdot def)$ contained in the given subgroup of order 21.

If the given subgroup of order 6 is the symmetric group of this order, the three possible substitutions of the form $ab\cdot cd\cdot ef\cdot gh$ are completely determined by the subgroup of the form $(abc\cdot def)$. That is, there is not more than one transitive group of degree 8 which contains a particular subgroup of degree 7 and of order 21, and which is such that its six substitutions which transform into itself a particular subgroup of the form $(abc\cdot def)$ constitute the symmetric group of order 6. It is clear that there is one such group, since the simple group of degree 7 and of order 168 transforms its eight subgroups of order 7 according to a transitive group of degree 8.

To prove that there is only one simple group of order 168 it remains only to prove that a transitive group of degree 8 and of order 168 cannot be simple if the subgroup of order 6 which transforms a subgroup of the form $(abc\cdot def)$ into itself is cyclic. In fact, such a transitive group contains 28 cyclic subgroups of order 6, and hence it contains $48+56+56$ substitutions of orders 7, 3, and 6 respectively. It can therefore contain only one subgroup of order 8. Hence we have completed a proof of the theorem that *there is only one simple group of order* 168, *and hence there is also only one insolvable group of this order.*

The only order between 168 and 200 which is not included in the general theorems which have been established is 180, and it is known that there is at least one insolvable group of this order, viz., the direct product of the icosahedral group and the group of order 3. We proceed to prove that this is the only insolvable group of order 180. A group of this order must have one, six, or thirty-six subgroups of order 5. If it has only one such subgroup it is evidently solvable. It could not contain thirty-six such subgroups, since these subgroups would form a single set of conjugates. As an operator of order 2 could not have 45 conjugates, the group would contain operators of order 6. As the number of its operators of each of the orders 3 and 6 would be even and a multiple of 5, and as it would contain just 36 operators whose orders are prime to 5, it results that such a group would involve not more than 5 subgroups of order 3. Hence there is no group of order 180 which contains 36 subgroups of order 5.

It remains to consider the possible groups of order 180 which contain exactly six subgroups of order 5. In this case the groups must be isomorphic with the icosahedral group on six letters and they must therefore involve an invariant subgroup of order 3. If we can prove that such a group G must also contain the icosahedral group invariantly, it must be the direct product of the icosahedral group and the group of order 3, and hence there is only one such group. If the subgroups of order 9 in G are non-cyclic, it is evident from the given isomorphism that G contains two operators, s_1, s_2, which satisfy the conditions $s_1^3 = s_2^5 = (s_1 s_2)^2 = 1$, and hence G contains the icosahedral group invariantly. It remains therefore only to prove that the subgroups of order 9 in G cannot be cyclic.

If these subgroups were cyclic, G would clearly contain two operators t_1, t_2 which would satisfy the conditions $t_1^3 = t_2^5 = (t_1 t_2)^2$, $t_1^9 = 1$. Hence the equations

$$t_1^2 = t_2 t_1 t_2, \quad t_2^4 = t_1 t_2 t_1.$$

If we consider the powers of the commutator

$$t_1t_2t_1^{-1}t_2^{-1}=t_1^{-3}\cdot t_1t_2t_1^2t_2^{-1}=t_1^{-3}\cdot t_1t_2^2t_1,$$

we have

$$(t_1t_2t_1^{-1}t_2^{-1})^2=t_1^{-6}t_1t_2^2t_1^2t_2^2t_1=t_1^{-6}t_1t_2^3t_1t_2^3t_1$$

$$(t_1t_2t_1^{-1}t_2^{-1})^3=t_1^{-9}t_1t_2^3t_1t_2^3t_1^2t_2^2t_1=t_1^{-9}t_1t_2^3t_1t_2^4t_1t_2^3t_1$$

$$=t_1^{-9}t_1t_2^3t_1^2t_2t_1^2t_2^3t_1=t_1^{-9}t_1t_2^4t_1t_2^3t_1t_2^4t_1$$

$$=t_1^{-9}t_1^2t_2t_1^2t_2^3t_1^2t_2t_1^2=t_1^{-6}t_1^2t_2^2t_1^2t_2^2t_1^2$$

$$(t_1t_2t_1^{-1}t_2^{-1})^5=t_1^{-12}t_1^2t_2^2t_1^2t_2^2t_1^2\cdot t_1t_2^3t_1t_2^3t_1=t_1^3$$

As $t_1t_2t_1^{-1}t_2^{-1}$ is the product of t_1t_2 and $t_1^{-1}t_2^{-1}$, and as t_1t_2 and t_2t_1 have a common square, it results that t_1^3 is transformed into its inverse by t_1t_2. Since it is also invariant under t_1t_2, the order of t_1 cannot exceed 6; but this order divides 9 and hence it must be 3. That is, G involves the icosahedral group, and hence *there is only one insolvable group of order* 180, *viz., the direct product of the group of order* 3 *and the icosahedral group.*

We have now considered all the possible insolvable groups whose orders are not greater than 200 and found that there are six such groups, viz., one of each of the orders 60, 168, 180, and three of order 120. From the simplicity of the above considerations it appears probable that these enumerations could readily be carried much further, but enough may have been done to exhibit the general nature of the problems involved. Several years ago Hölder carried this investigation through all groups whose orders are less than 480 with the results exhibited in the following table:

INSOLVABLE GROUPS *

Order	60	120	168	180	240	300	336	360	420
Number of groups	1	3	1	1	8	1	3	6	1

* Hölder, *Mathematische Annalen*, vol. 46 (1895), p. 420.

EXERCISES

1. A group whose Sylow subgroups of order 2^m are cyclic contains an invariant subgroup of index 2.

Suggestion: Represent the group as a regular group.

2. If a primitive substitution group of degree n is solvable, n must be a power of a prime and the primitive group must be contained in the holomorph of the abelian group of order n and of type (1, 1, 1, . . .).

Suggestion: Consider a chief series of composition of the primitive substitution group.

3. If a transitive group of the prime degree p is solvable, its order is a divisor of $p(p-1)$.

PART II*

FINITE GROUPS OF LINEAR HOMOGENEOUS TRANSFORMATIONS

CHAPTER IX

PRELIMINARY THEOREMS

LINEAR TRANSFORMATIONS, §§ 75–82

75. Introduction and Definition. It is often of importance in analysis to exchange one set of variables for another, the variables of either set being linear homogeneous functions of the variables of the other set (cf. Ch. XVIII), as in coördinate geometry:

$$x = x' \cos\theta - y' \sin\theta,$$
$$y = x' \sin\theta + y' \cos\theta. \tag{1}$$

We assume that a function $f(x, y)$ is given, in which the new variables (x', y') are to be put in place of the old (x, y) by means of (1); this is called *operating upon* f by the *linear transformation* (1).

A capital letter is in general used to denote a linear transformation; thus, we shall here denote (1) by S. The result of operating upon $f(x, y)$ by S may then be indicated symbolically as follows:

$$(f)S = f(x' \cos\theta - y' \sin\theta, \quad x' \sin\theta + y' \cos\theta). \tag{2}$$

* This part was written by H. F. Blichfeldt.

However, since f is generally subjected to several transformations successively, we find it convenient after each operation to drop the accents. In the future we shall therefore write, instead of (2),

$$(f)S = f(x\cos\theta - y\sin\theta,\quad x\sin\theta + y\cos\theta).$$

FORMAL DEFINITION. *A linear transformation in n variables $x_1, x_2, \ldots, x_n$ is a set of linear homogeneous equations*

$$A: \qquad \begin{aligned} x_1 &= a_{11}x'_1 + a_{12}x'_2 + \ldots + a_{1n}x'_n, \\ &\cdots\cdots\cdots\cdots \\ x_n &= a_{n1}x'_1 + a_{n2}x'_2 + \ldots + a_{nn}x'_n, \end{aligned}$$

expressing the original variables $x_1, \ldots, x_n$ in terms of new variables $x'_1, \ldots, x'_n$, under the condition that the equations can be solved for the latter.

76. Matrix and Determinant. It is customary to represent the transformation A above by the matrix of the coefficients (called the *matrix of* A):

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix},$$

or simply

$$A = [a_{st}].$$

The determinant of this matrix is called the *determinant of* A.

77. Inverse of a Linear Transformation. The solutions of the equations A (§ 75) for $x'_1, \ldots, x'_n$, say

$$x'_1 = b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n, \quad x'_2 = \text{etc.}, \quad \text{etc.},$$

will constitute a new linear transformation which will take the conventional form adopted for A after the accented and unaccented variables have been interchanged:

$$B: \qquad \begin{aligned} x_1 &= b_{11}x'_1 + b_{12}x'_2 + \ldots + b_{1n}x'_n, \\ &\cdots\cdots\cdots\cdots \\ x_n &= b_{n1}x'_1 + b_{n2}x'_2 + \ldots + b_{nn}x'_n. \end{aligned}$$

This is called the *inverse of* A, and is denoted by A^{-1} (cf. § 22).

78. Product of Linear Transformations. If a function f be subjected to two linear transformations successively, A and B, the result is equivalent to operating upon f by a single linear transformation C, called the *product of A and B*. We shall prove

THEOREM 1. *The product of two linear transformations in the same variables,*

$$A=[a_{st}], \qquad B=[b_{st}],$$

is a linear transformation $C=[c_{st}]$, where

$$c_{st}=a_{s1}b_{1t}+a_{s2}b_{2t}+\ \ldots\ +a_{sn}b_{nt}=\sum_{v=1}^{n}a_{sv}b_{vt};$$

symbolically, $AB=C$.

Proof. Consider a function $f(x_1, \ldots, x_n)$ operated upon by A:

$$(f)A=f(y_1, \ldots, y_n),$$

where (§ 75)

$$y_s=\sum_{v=1}^{n}a_{sv}x_v.$$

The result of operating upon $(f)A$ by B, namely $((f)A)B$, which we shall write $(f)AB$, is then $f(z_1, \ldots, z_n)$, where

$$z_s=\sum_{r=1}^{n}a_{sv}\sum_{t=1}^{n}(b_{vt}x_t)=\sum_{t=1}^{n}x_t\left(\sum_{r=1}^{n}a_{sv}b_{vt}\right)=\sum_{t=1}^{n}x_tc_{st}.$$

Accordingly, if C be the linear transformation defined above, we have

$$(f)C=f(z_1, \ldots, z_n)=(f)AB.$$

Note that the element c_{st} in the product $AB=C$ is obtained by multiplying the elements of the sth row of A into the corresponding elements of the tth column of B and adding the results.

79. The Commutative and Associative Laws. The commutative law does not hold in general; that is, $C=AB$ and $C'=BA$ do not represent the same linear transformation. On the other hand, the associative law holds always: $A(BC)=(AB)C$ whatever be the transformations A, B and C; that is, if we write S for the product BC and T for AB, then $AS=TC$.

This we prove by comparing the matrices of these products, as obtained by the application of Theorem 1.

80. Canonical Form of a Linear Transformation. Identical and Similarity-transformations. A transformation whose matrix has zero elements everywhere except in the principal diagonal is said to have the *canonical form* (or to be *written in the canonical form*):

$$S: \qquad x_1 = \alpha_1 x'_1, \quad x_2 = \alpha_2 x'_2, \quad \ldots, \quad x_n = \alpha_n x'_n.$$

In such a case we employ the notation $S = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

If the coefficients $\alpha_1, \alpha_2, \ldots, \alpha_n$, which are called the *multipliers* of S, are all equal, we say that S is a *similarity-transformation*; if they are all equal to unity, S is the *identical transformation* or *the identity*. Denoting the latter by E and any transformation by A, we have $EA = AE = A$.

81. Power and Order of a Linear Transformation. Since the associative law holds for a product, it follows that we may write A^2 for AA, A^3 for $(AA)A$, etc., and call these products the *second, third, etc., powers of* A. Moreover, denoting the inverse of A^n by A^{-n}, we have $A^n A^{-n} = A^{-n} A^n = E$, and $A^{-n} = (A^{-1})^n$. The index laws hold for positive and negative integral powers if we interpret A^0 as E.

Usually no power of a linear transformation A taken at random will be the identity. If, however, such a power exists, we say that A is of *finite order*, and the lowest power of A which equals the identity is called the *order* of A.

EXERCISES

1. Prove that the determinant of the product of two transformations A and B is equal to the product of the determinants of A and B. Hence prove that the determinant of A is the reciprocal of that of A^{-1}.

2. Find the inverse of S, § 75.

3. Prove that if

$$A = \begin{bmatrix} p & q \\ r & s \end{bmatrix}, \quad B = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}, \quad ps - qr = 1,$$

then B is the inverse of A.

4. Construct AB and BA, where

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}.$$

5. Find the general form of a linear transformation in three variables which is commutative with

$$S=\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix}, \quad a \neq b.$$

6. Prove that a similarity-transformation is commutative with any linear transformation in the same variables.

7. Prove that the multipliers of a transformation of finite order are roots of unity (cf. § 116).

82. Remarks. For the purpose of avoiding a possible confusion on the part of the student of the terms "literal substitution" and "linear substitution," the term "linear transformation" has here been adopted throughout.

A different value for c_{st} from that given in § 78 is obtained by interpreting the linear transformations A and B in a different manner or by writing last in the product that transformation which operates first, as is the custom with functional operators. Thus, Klein, Jordan and Burnside regard the variables in the left-hand members of A, § 75, as the new, and those in the right-hand members as the old variables (the accents being placed accordingly or entirely absent), and therefore get $c_{st}=\sum_{v=1}^{n} a_{vs}b_{tv}$ instead of the value given in § 78; while Weber, attaching the same meaning to the linear transformations, inverts the order in the product, writing BA where the authors mentioned write AB. On the other hand, Frobenius and Schur, though writing y_s for x'_s in the equations A, § 75, interpret linear transformations in the same way and arrive at the same results as the author of this Part II. The latter has deviated from his customary notation in papers published on the subject to the extent of dropping accents of variables that were formerly supplied with them and vice versa.

Groups of Linear Transformations, §§ 83–87

83. Linear Group. If ω is an imaginary cube root of unity, the six transformations

$$A_1=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_3=\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},$$

$$A_4=\begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, \quad A_5=\begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}, \quad A_6=\begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}$$

form a group of order 6 which is isomorphic with the symmetric group in 3 letters (cf. § 1). Here A_1 is the identical transformation; the inverse of A_3 is A_5, while A_2, A_4 and A_6 are their own inverses. The transformations A_3 and A_5 are both of order 3; and A_2, A_4, A_6 all of order 2.

A set of g distinct linear transformations $s_1, \ldots, s_g$ will form a group of order g if the conditions of § 22 are all fulfilled. Such a group we shall simply call a *linear group*.

84. Collineations and Collineation-groups. It is often convenient not to regard as essentially different two transformations whose matrices can be obtained one from the other by multiplying all the elements of one by a constant factor, as, for instance, in the case of

$$S=\begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix}, \quad T=\begin{bmatrix} 4 & 6 \\ 0 & 2 \end{bmatrix}.$$

The two transformations are then said to represent the same *collineation*. In other words, a collineation is specified by the mutual ratios of the elements of the corresponding matrix, not by the actual values of these elements. In practice it is customary to affix a factor of proportionality to either the old or the new variables to distinguish a collineation from a linear transformation; the collineation represented by S or T above would thus be written

$$\rho x_1 = 2x'_1 + 3x'_2, \quad \rho x_2 = x'_2.$$

If A and B are two distinct linear transformations which represent the same collineation, then $BA^{-1}=A^{-1}B$ is a similarity-transformation. For, let the common ratio of the elements of the matrix of B to the corresponding elements of the matrix of A be θ, then we immediately verify that $B=AS=SA$, where $S=(\theta, \theta, \ldots, \theta)$.

If now a linear group G of order g be given, two cases may arise. Either no two distinct transformations of G will represent the same collineation, or there will be some one set of, say f, transformations which all represent the same collineation. In the former case G contains g distinct collineations;

in the latter, the g transformations of G can be arranged into g/f sets, of f transformations each, furnishing g/f distinct collineations. For, let $A_1, \ldots, A_f$ be any set of transformations representing the same collineation, then

$$A_1A_1^{-1}=S_1, \quad A_2A_1^{-1}=S_2, \quad \ldots, \quad A_fA_1^{-1}=S_f$$

are similarity-transformations and are all distinct. Hence, if the group F of similarity-transformations $S_1, S_2, \ldots, S_f$ contained in G (cf. Ex. 1, § 87) is of order f, we have $f \geqq f'$. On the other hand, if A is an arbitrary transformation in G, then the f distinct transformations $AS_1, \ldots, AS_f$ all represent the same collineation, so that $f' \geqq f$. Hence $f'=f$.

The sets of G can therefore be exhibited as follows:

$$\begin{array}{llll} S_1, & S_2, & \ldots, & S_f; \\ AS_1, & AS_2, & \ldots, & AS_f; \\ BS_1, & BS_2, & \ldots, & BS_f; \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

To each line will correspond a single collineation. Moreover, if the product of a transformation from a set (α) and a transformation from a set (β) fall in the set (γ), then the product of any transformation from (α) and any transformation from (β) will fall in (γ), since the two products merely differ by a similarity-transformation. Accordingly, the group G is $(f, 1)$-isomorphic with an abstract group H of order $h=g/f$, namely the quotient-group G/F (§ 13). Since a collineation in n variables can be interpreted as a projective transformation in space of $n-1$ dimensions by using homogeneous coördinates, the abstract group H becomes a group of operators of order h, called the *collineation-group* corresponding to G.

85. An Example. Take the linear group G of order 8:

$$A_1=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad A_3=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A_4=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$B_1=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B_2=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B_3=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B_4=\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

The group F of similarity-transformations is here of order 2: A_1 and A_3. The table of § 84 will therefore consist of four lines as follows:

$$\left.\begin{array}{ll} A_1, & A_3; \\ A_2A_1, & A_2A_3; \\ B_1A_1, & B_1A_3; \\ B_2A_1, & B_2A_3; \end{array}\right\} = \left\{\begin{array}{ll} A_1, & A_3; \\ A_2, & A_4; \\ B_1, & B_3; \\ B_2, & B_4. \end{array}\right.$$

The corresponding collineation-group, of order 4, can be written by selecting a representative from each of the four lines, as A_1, A_2, B_1, B_2.

Remark. It will be noticed that in this example neither the set A_1, A_2, B_1, B_2, nor any other set that may be selected from the four lines will form a linear group of order 4.

86. Groups of Linear Transformations of Determinant Unity. It follows from the manner in which the product AB of two linear transformations A, B is formed (§ 78) that the determinant D_{AB} of AB is the product of the determinants of A and B:

$$D_{AB} = D_A D_B.$$

Now let S be a transformation belonging to a collineation-group G of order g in n variables:

$$A, B, \ldots, S, \ldots,$$

and D_S the determinant of S. A linear group isomorphic with G and whose transformations have unity for the value of their determinants may then be constructed in the following manner. Let θ be a solution of the equation

$$\theta^n = D_S{}^{-1}, \tag{3}$$

and let S_1 be the similarity-transformation $(\theta, \theta, \ldots, \theta)$, the value of whose determinant is θ^n. Then $S_2 = SS_1$ is of determinant unity. Since (3) has n solutions, there are n different transformations associated with S in this manner, say $S_2^{(1)}, \ldots, S_2^{(n)}$. Hence the following correspondence:

G: $\quad A, \quad \ldots \quad S, \ldots$

G_2: $\quad A_2^{(1)}, \ldots, A_2^{(n)}; \ldots S_2^{(1)}, \ldots, S_2^{(n)}; \ldots$

It is easy to verify that the set of transformations in the last line form a linear group (G_2) which is (n, 1)-isomorphic with the collineation-group G; in fact, if $AB=C$, and α, β arbitrary accents, then

$$A_2^{(\alpha)}B_2^{(\beta)}=C_2^{(\gamma)},$$

where γ is fully determined.

As an illustration, let G be the collineation-group

$$A=(1,\ 1),\quad B=\begin{bmatrix}0 & -2\\ 2 & 0\end{bmatrix}.$$

We find

$$A_1^{(1)}=(1,\ 1),\ A_1^{(2)}=(-1,\ -1);\ B_1^{(1)}=(\tfrac{1}{2},\ \tfrac{1}{2}),\ B_1^{(2)}=(-\tfrac{1}{2},\ -\tfrac{1}{2}),$$

and therefore

$$G_2:\qquad A_2^{(1)}=(1,\ 1),\qquad A_2^{(2)}=(-1,\ -1);$$

$$B_2^{(1)}=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\qquad B_2^{(2)}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}.$$

It may, however, be possible to find a subgroup of G_2 of lower order whose corresponding collineation-group is likewise G, and whose transformations also have unity for the value of their determinants (cf. § 110). This will be the case if G is a group of odd order in two variables (§ 97). When in the future we mention a group of linear transformations of determinant unity corresponding to a given collineation-group or linear group, we shall mean such a group G_3 of lowest possible order, having the same collineation-group as that given or as that corresponding to the given linear group.

87. Linear Fractional Group. When only the mutual ratios of the elements of the matrices are of importance and not their actual values, we may adopt another mode of representing the operators, namely by writing them in linear fractional form. Let a given linear transformation be

$$A:\qquad x_s=a_{s1}x'_1+\ \ldots\ +a_{sn}x'_n\qquad (s=1,\ 2,\ \ldots,\ n),$$

and let the ratios $x_1/x_n, \ldots, x_{n-1}/x_n$ be denoted by $y_1, \ldots, y_{n-1}$ respectively. Then from A we get

$$y_s = \frac{a_{s1}y'_1 + \ldots + a_{s\,n-1}y'_{n-1} + a_{sn}}{a_{n1}y'_1 + \ldots + a_{n\,n-1}y'_{n-1} + a_{nn}} \qquad (s=1, 2, \ldots, n-1).$$

To a similarity-transformation here corresponds the identity

$$y_s = y'_s \qquad (s=1, 2, \ldots, n-1),$$

and we see that the linear fractional group is simply isomorphic with the corresponding collineation-group and may be regarded as its equivalent.

EXERCISES

1. Prove that the similarity-transformations contained in a linear group G form a subgroup which is invariant in G.

2. Prove that the determinant of a linear transformation belonging to a finite group is a root of unity (cf. § 116).

3. Among the determinants of the transformations of a group G of order g let there be one which is a root of unity whose index is the power of a prime p (§ 116). Prove that if all those transformations be eliminated whose determinants contain as a factor a root whose index is the highest power of p occurring among such indices, then will the remaining transformations form an invariant subgroup of G of order g/p.

In particular, prove that the transformations of determinant unity form an invariant subgroup of G.

4. Let T be one of the transformations of the group in the last exercise whose determinant contains a factor ϵ of index p^a, and assume that p is relatively prime to the number of variables n. Then we can always find a root of unity, say ψ, of index p^a, whose nth power is ϵ^{-1}. If now all the elements of the matrix of T be multiplied by ψ, the determinant of the new transformation T' will no longer contain as a factor a root whose index is a power of p.

(For instance, let $T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}$, $D_T = \omega$. Here $\psi = \omega$, and $T' = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$.)

Now prove that if all the transformations be modified in this manner we shall obtain a group G' which is isomorphic with G.

Evidently, to a possible similarity-transformation $(\alpha, \alpha, \ldots, \alpha)$ of G whose multipliers α are roots of unity of index a power of p will correspond the identity $(1, 1, \ldots, 1)$ of G'. In such a case therefore the order of G' will be that of G divided by a power of p.

5. Construct the group G_8 corresponding to the linear group of order 8 given in § 85.

6. The group listed in § 83 is of order 6. Show that the corresponding collineation-group and group G_3 are of orders 6 and 12 respectively.

7. Construct the collineation-group and group G_3 corresponding to the linear fractional group of order 6:

$$y=y',\quad 1/y',\quad 1-y',\quad 1/(1-y'),\quad (y'-1)/y',\quad y'/(y'-1).$$

88. Change of Variables. Before subjecting a given function $f(x, y)$ to a linear transformation or a group of linear transformations, we may introduce a different set of variables in the function and in the transformations. We shall examine in detail the important case where the new variables are linear homogeneous functions of the old; in other words, where the new value of f is obtained from the old by subjecting the latter to a linear transformation T which expresses the change of variables considered.

To illustrate, let S be the transformation

$$S:\quad x=x'\cos\theta-y'\sin\theta,\quad y=x'\sin\theta+y'\cos\theta.$$

We now suppose that new variables X, Y are introduced, where

$$T:\qquad x=\frac{1}{2}(X+Y),\qquad\qquad y=\frac{1}{2i}(X-Y),$$

and correspondingly

$$T':\qquad x'=\frac{1}{2}(X'+Y'),\qquad\qquad y'=\frac{1}{2i}(X'-Y'),$$

where $i^2=-1$. The function f becomes

$$(f)T=f\left(\frac{1}{2}(X+Y),\quad\frac{1}{2i}(X-Y)\right)\equiv F(X,\ Y),\quad\text{say,}$$

and the transformation S expressed in the new variables (S_1) is found by solving for X, Y from the equations

$$\frac{1}{2}(X+Y)=\frac{1}{2}(X'+Y')\cos\theta-\frac{1}{2i}(X'-Y')\sin\theta,$$

$$\frac{1}{2i}(X-Y)=\frac{1}{2}(X'+Y')\sin\theta+\frac{1}{2i}(X'-Y')\cos\theta.$$

We obtain

$$S_1: \qquad X = X'e^{i\theta}, \quad Y = Y'e^{-i\theta}.$$

The function F may now be subjected to the transformation S_1, producing

$$(F)S_1 = ((f)T)S_1 = (f)TS_1. \tag{4}$$

Obviously, the final result could equally well have been obtained by operating first upon f by S before introducing the new variables; that is, the final expression in (4) is also obtained by introducing X', Y' in

$$(f)S = f(x' \cos\theta - y' \sin\theta, \quad x' \sin\theta + y' \cos\theta)$$

by means of T', giving

$$((f)S)T' = (f)ST'.$$

Hence we have

$$(f)TS_1 = (f)ST',$$

so that, since f is an arbitrary function,

$$TS_1 = ST',$$

or

$$S_1 = T^{-1}ST'.$$

As remarked in § 75, we drop accents after operating by a linear transformation. Accordingly, our final formula is

$$S_1 = T^{-1}ST. \tag{5}$$

In the general case, the same symbolic result is obtained. Hence the

THEOREM 2. *Let there be given a linear group*

$$G: \qquad A, B, \ldots,$$

and a change of variables in the form of a linear transformation T; then we obtain in the new variables a linear group

$$G_1: \qquad T^{-1}AT, \quad T^{-1}BT, \ldots.$$

These two groups are simply isomorphic (§§ 13, 24), *and we shall write the latter symbolically $T^{-1}GT$.*

89. Characteristic Equation. If we add $-\theta$ to each of the elements in the principal diagonal of the matrix of a linear transformation $A=[a_{st}]$ and equate the resulting determinant to zero, we have an equation in θ which is called the *characteristic equation of A:*

$$\begin{vmatrix} a_{11}-\theta & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\theta & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\theta \end{vmatrix} = 0. \tag{6}$$

THEOREM 3. *If T and A be linear transformations, the roots of the characteristic equation of A are the same as those of $T^{-1}AT$.*

To prove this theorem, let us put $T^{-1}AT=B=[b_{st}]$, whose characteristic equation is

$$\begin{vmatrix} b_{11}-\theta & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn}-\theta \end{vmatrix} = 0. \tag{7}$$

Regarding θ as a variable temporarily, we denote the transformations whose matrices are the left-hand members of (6) and (7) by $\overline{A-\theta}$ and $\overline{B-\theta}$. Then, since $T^{-1}AT=B$, and $T^{-1}ST=S$, where S is the similarity-transformation $(\theta, \theta, \ldots, \theta)$, we may readily prove that $T^{-1}(\overline{A-\theta})T=\overline{B-\theta}$. Hence, if the determinants of T, $\overline{A-\theta}$ and $\overline{B-\theta}$ be denoted by p, q, r, we have (cf. Ex. 1, § 81) $p^{-1}qp=r$, so that $q=r$. Accordingly, the coefficients of the various powers of θ in q and r are equal, and the theorem follows.

The sum of the characteristic roots of A is called the *characteristic* of A. It is equal to the sum of the elements in the principal diagonal of A, namely $a_{11}+a_{22}+\cdots+a_{nn}$.

EXERCISES

1. Prove that if S, § 88, is a similarity-transformation, then $S_1=S$. Prove also that if S and T both have the canonical form, then $S_1=S$.

2. Prove (5) in the case of two variables directly by multiplying out the right-hand member (cf. §§ 77, 78).

3. Find the characteristic roots and characteristic of a transformation written in canonical form; also of the transformation (1), § 75.

90. Transitive and Intransitive Groups. Consider a group G in four variables whose transformations all have the typical form

$$A = \begin{pmatrix} a & b & e & f \\ b & a & f & e \\ h & g & c & d \\ g & h & d & c \end{pmatrix}.$$

If in this group we introduce new invariables y_1, y_2, z_1, z_2 such that $y_1 = x_1 + x_2$, $y_2 = x_3 + x_4$; $z_1 = x_1 - x_2$, $z_2 = x_3 - x_4$, the transformations take the simpler form

$$A_1 = \begin{pmatrix} p & q & 0 & 0 \\ r & s & 0 & 0 \\ 0 & 0 & t & u \\ 0 & 0 & v & w \end{pmatrix}.$$

It seems natural to adopt the notation

$$A_1 = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix},$$

A' representing a matrix in y_1, y_2 only, and A'' one in z_1, z_2 only. Correspondingly we write

$$G_1 = \begin{pmatrix} G' & 0 \\ 0 & G'' \end{pmatrix}.$$

We say that the group G (or G_1) is *intransitive*, and that (y_1, y_2) and (z_1, z_2) form its *sets of intransitivity*.

Similarly, if in a group in four variables, these fall into two sets of 3 and 1 variables respectively, by a suitable change to new variables, the group is intransitive.

In general, *a group G in which the variables fall into two or more sets of intransitivity*

$$G = \begin{pmatrix} G' & 0 \\ 0 & G'' \end{pmatrix},$$

either directly or after a suitable choice of new variables, shall be said to be intransitive. If such a division is not possible, we say that G is transitive.

EXERCISES

1. The group of order 6 listed in § 83 is transitive. It contains an intransitive subgroup of order 3 and three intransitive subgroups of order 2 each.

2. Find the largest intransitive subgroup contained in the group of order 8 listed in § 85.

3. Prove that if a group in four variables appears as intransitive by two different changes of variables, $S^{-1}GS$ and $T^{-1}GT$, such that the sets of intransitivity in $S^{-1}GS$ contain (2, 2) variables, and in $T^{-1}GT$ contain (3, 1) variables, then a change of variables $V^{-1}GV$ can be found such that there will appear at least three sets of intransitivity (2, 1, 1).

Note. Maschke introduced the term transitive as applied to linear groups (*Mathematische Annalen*, Bd. 52 (1899), p. 363). Jordan denoted both intransitive and imprimitive groups (§ 106) by decomposable groups (*Atti della Reale Accademia della Scienze fisiche e matematiche*, Napoli, t. 8 (1879), p. 6).

HERMITIAN INVARIANT, §§ 91–93

91. Hermitian Form. If the conjugate-imaginary of a quantity w be written $\bar{w}$, a *positive-definite Hermitian form* (or simply *Hermitian form*) is an expression such as

$$J=\sum_{k=1}^{n}\sum_{l=1}^{n}q_{kl}x_k\bar{x}_l \qquad (q_{lk}=\bar{q}_{kl}),$$

subject to the conditions that it vanishes only if $x_1=x_2=\ \ldots\ =x_n=0$, and is real and positive for all other sets of values assigned to these variables.

THEOREM 4. *A positive-definite Hermitian form J in n variables may be reduced to the form*

$$y_1\bar{y}_1+y_2\bar{y}_2+\ \ldots\ +y_n\bar{y}_n$$

by a change of variables of the following type:

$$y_1 = \rho_{11}x_1,$$

$$y_2 = \rho_{21}x_1 + \rho_{22}x_2,$$

. . . . . .

$$y_s = \rho_{s1}x_1 + \rho_{s2}x_2 + \ldots + \rho_{ss}x_s,$$

. . . . . .

$$y_n = \rho_{n1}x_1 + \rho_{n2}x_2 + \ldots + \rho_{ns}x_s + \ldots + \rho_{nn}x_n.$$

Proof. Arranging J according to x_n and $\bar{x}_n$ we have

$$J = J_n = q_{nn}x_n\bar{x}_n + x_n\overline{X}_{n-1} + \bar{x}_nX_{n-1} + X,$$

where X_{n-1} represents a linear function of $x_1, \ldots, x_{n-1}$.

The coefficient q_{nn} is real and positive, since it is the value of J obtained by putting $x_n = 1$, $x_{n-1} = x_{n-2} = \ldots = x_1 = 0$.

Accordingly,

$$+\sqrt{q_{nn}} = +\overline{\sqrt{q_{nn}}},$$

and we may write

$$J = \left(\sqrt{q_{nn}}x_n + \frac{X_{n-1}}{\sqrt{q_{nn}}}\right)\left(\sqrt{q_{nn}}\bar{x}_n + \frac{\overline{X}_{n-1}}{\sqrt{q_{nn}}}\right) + X - \frac{X_{n-1}\overline{X}_{n-1}}{q_{nn}}$$

$$= y_n\bar{y}_n + J_{n-1}, \quad \text{say,}$$

where

$$y_n = \sqrt{q_{nn}}x_n + \frac{X_{n-1}}{\sqrt{q_{nn}}},$$

and is therefore a linear function of $x_n, \ldots, x_1$.

The function J_{n-1} fulfils the conditions of an Hermitian form in $n-1$ variables $x_{n-1}, \ldots, x_1$, as it is of the required type and is real and positive for any set of values allotted to these $n-1$ variables except $0, \ldots, 0$. For, it is the value of J_n obtained by putting $x_n = -X_{n-1}/q_{nn}$. Hence, we may arrange J_{n-1} according to x_{n-1} and $\bar{x}_{n-1}$ and proceed as above. We find

$$J_{n-1} = y_{n-1}\bar{y}_{n-1} + J_{n-2},$$

where y_{n-1} is a linear function of $x_{n-1}, x_{n-2}, \ldots, x_1$. Continuing thus, we finally prove the theorem.

92. Conjugate-imaginary Groups and Invariant Hermitian Form. If in a group G we replace the variables $x_1, \ldots, x_n$ and the elements a_{st} of the matrices by their conjugate-imaginary values $\bar{x}_1, \ldots, \bar{x}_n, \bar{a}_{st}$, we evidently obtain a group $\bar{G}$ simply isomorphic with G. We shall say that either group is the *conjugate-imaginary* of the other.

We say that an Hermitian form J is *invariant* under a group G, or that J is an *Hermitian invariant* of G, when J is transformed into itself by the (intransitive) group in $2n$ variables $x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n$ made up of G and $\bar{G}$.

THEOREM 5. *There is always an invariant Hermitian form of a given linear group G in n variables.**

Proof. Let the transformations of the group made up of G and $\bar{G}$ be denoted by $T_1, T_2, \ldots, T_g$, and let I represent the Hermitian form $x_1\bar{x}_1+x_2\bar{x}_2+\ldots+x_n\bar{x}_n$. Then the sum

$$J=(I)T_1+(I)T_2+\ldots+(I)T_g$$

is an invariant Hermitian form of G.

First, J is an Hermitian form. For, each of the terms $(I)T_\alpha$ is the sum of n expressions $(x_s\bar{x}_s)T_\alpha=X_s\bar{X}_s$ which are real and non-negative. The function J is therefore real and non-negative, and cannot vanish unless every term $(I)T_\alpha$ vanishes. But, if T_1 represents the identity, $(I)T_1=I$ and does not vanish unless every variable $x_1, \ldots, x_n$ vanishes. This is therefore also the case with J.

Second, J is transformed into itself by $T_1, T_2, \ldots, T_g$. For, evidently

$$(J)T_\alpha=((I)T_1)T_\alpha+\ldots+((I)T_g)T_\alpha=(I)T'_1+\ldots+(I)T'_g,$$

where

$$T'_\beta=T_\beta T_\alpha.$$

* This theorem was proved for $n=3$ by Picard and Valentiner (1887, 1889), and for any n by Fuchs, Moore and Loewy (1896). See *Encyklopädie der Mathematischen Wissenschaften*, Leipzig, 1898–1904, Bd. I, 1; p. 532.

But, $T_1T_\alpha, \ldots, T_\theta T_\alpha$ are the transformations $T_1, \ldots, T_\theta$ over again in some order. It follows that

$$(J)T_\alpha=(I)T_1+\ \ldots\ +(I)T_\theta=J.$$

From Theorems 4 and 5 we get the

COROLLARY. *Such variables* $x_1, \ldots, x_n$ *may be selected for a group* G *that the function*

$$I=x_1\bar{x}_1+x_2\bar{x}_2+\ \ldots\ +x_n\bar{x}_n$$

is an Hermitian invariant of G.

93. Linear Transformations in Unitary Form. The variables of G being chosen as specified in the previous corollary, let

$$A=[a_{st}],\quad \overline{A}=[\bar{a}_{st}]$$

represent corresponding transformations of G and $\overline{G}$. Operating upon I by A and $\overline{A}$, we find the following conditions that I may be reproduced:

$$(8)\quad \begin{aligned} &a_{1k}\bar{a}_{1k}+a_{2k}\bar{a}_{2k}+\ \ldots\ +a_{nk}\bar{a}_{nk}=1 \qquad (k=1, 2, \ldots, n),\\ &a_{1k}\bar{a}_{1l}+a_{2k}\bar{a}_{2l}+\ \ldots\ +a_{nk}\bar{a}_{nl}=0 \ (k, l=1, 2, \ldots, n; k\neq l). \end{aligned}$$

The transformation A fulfilling these conditions is said to have the *unitary form*, or to be a *unitary transformation*.

The inverse of A can here be written down at once:

$$A^{-1}=[a'_{st}] \qquad (a'_{st}=\bar{a}_{ts}).$$

For, the condition $A^{-1}A=$ the identity leads to the equations (8).

Now, since $AA^{-1}=$ the identity also, we obtain the following set of equations as consequences of (8):

$$(9)\quad \begin{aligned} &a_{k1}\bar{a}_{k1}+a_{k2}\bar{a}_{k2}+\ \ldots\ +a_{kn}\bar{a}_{kn}=1 \qquad (k=1, 2, \ldots, n),\\ &a_{k1}\bar{a}_{l1}+a_{k2}\bar{a}_{l2}+\ \ldots\ +a_{kn}\bar{a}_{ln}=0 \ (k, l=1, 2, \ldots, n; k\neq l). \end{aligned}$$

94. Reducible and Irreducible Groups. A group G is said to be *reducible* if, by a suitable choice of variables, it can be written in the symbolic form (cf. § 90):

$$G=\begin{bmatrix} G' & 0 \\ G'' & G''' \end{bmatrix},$$

that is, if a certain number of the n variables, say $x_1, \ldots, x_m$, where $m<n$, are transformed into linear functions of themselves by every transformation of G.

For instance, a group in two variables is reducible if (either directly or after a proper change of variables) all the matrices are of type

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}.$$

If this is not the case, the group is said to be *irreducible*. We shall say that the m variables $x_1, \ldots, x_m$ form a *reduced set* for G.

THEOREM 6. *A reducible group G is intransitive, and a reduced set constitutes one of the sets of intransitivity of G.*

Applied to the illustration above, the theorem asserts that the group there given can be written in the form

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$$

by a suitable choice of variables.

Proof. The group G has an Hermitian invariant, which by the change of variables specified in § 91 may be written:

$$y_1\bar{y}_1+y_2\bar{y}_2+ \ldots +y_n\bar{y}_n.$$

Making the corresponding changes in G, this group is still seen to be of the form

$$\begin{pmatrix} G' & 0 \\ G'' & G''' \end{pmatrix},$$

namely,

$$(10)\qquad \begin{aligned} y_s &= a_{s1}y'_1+ \ldots +a_{sm}y'_m && (s=1, 2, \ldots, m),\\ y_t &= a_{t1}y'_1+ \ldots +a_{tm}y'_m+ \ldots +a_{tn}y'_n && \\ & && (t=m+1, m+2, \ldots, n). \end{aligned}$$

Applying the conditions (8)' and (9), § 93, and writing c_{st} for the product $a_{sv}\bar{a}_{st}$, we obtain, among others, the following $2(n-m)$ equations:

$$\begin{aligned} c_{m+1\,v}+ \ldots +c_{nv} &= 1 && (v=m+1, m+2, \ldots, n);\\ c_{w1} + \ldots +c_{wm} &= 1 && (w=m+1, m+2, \ldots, n). \end{aligned}$$

If we now subtract from the sum of the last $n-m$ equations the sum of the first $n-m$, we get

$$\sum_{s=m+1}^{n}\sum_{t=1}^{m} c_{st}=0.$$

The quantities c_{st} being real and non-negative, it follows that those which enter into this sum all vanish. Moreover, since $a_{st}=0$ follows from $c_{st}=0$, the equations (10) now take the form

$$y_s=a_{s1}y'_1+\ \ldots\ +a_{sm}y'_m \qquad (s=1,\ 2,\ \ldots\ ,m),$$

$$y_t=a_{t\,m+1}y'_{m+1}+\ \ldots\ +a_{tn}y'_n \qquad (t=m+1,\ m+2,\ \ldots\ ,\ n),$$

and the theorem is proved

EXERCISES

1. Prove that if

$$A=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

is a unitary transformation of determinant unity, then $\underline{r}=-\overline{q}$ and $\underline{s}=\overline{p}$.

2. Prove that if all the elements of the matrices of the transformations of G are real, then there is a quadratic function of the variables which is invariant under G.

95. Theorem 7. *A linear transformation of finite order will assume the canonical form* (§ 80) *by a suitable choice of variables.*

Proof. Let the transformation be

$$A: \qquad x_s=\sum_{t=1}^{n} a_{st}x'_t \qquad (s=1,\ 2,\ \ldots\ ,\ n).$$

Then we can always find a linear function $y_1=b_1x_1+\ \ldots\ +b_nx_n$ which is transformed into a constant (θ) times itself by A (i.e., y_1 is a *relative invariant* of A). For, we get

$$(y_1)A=\sum_{s=1}^{n} b_s\sum_{t=1}^{n} a_{st}x_t=\sum_{t=1}^{n} x_t\sum_{s=1}^{n} b_sa_{st},$$

and this expression is θy_1 provided the following equations are true:

$$\theta b_t=\sum_{s=1}^{n} b_sa_{st} \qquad (t=1,\ 2,\ \ldots\ ,\ n).$$

By the theory of linear homogeneous equations, a solution $b_1, \ldots, b_n$, not all zero, of these equations, can always be found if θ is a root of the characteristic equation of A (§ 89).

If we now introduce new variables such that y_1 is one of these, the group generated by A is reducible, since

$$(y_1)A = \theta y_1, \quad (y_1)A^2 = \theta^2 y_1, \quad \text{etc.},$$

and therefore

$$y_1 = \theta y'_1$$

is one of the equations specifying A in its new form. By Theorem 6, the group generated by A is intransitive, one of the sets of intransitivity being y_1. Let $(y_2, \ldots, y_n)$ form the other (temporary) set of intransitivity.

The above process may now be repeated for the set $(y_2, \ldots, y_n)$ We determine the linear function $c_2y_2 + \ldots + c_ny_n$ which is a relative invariant of A, and introduce this function as one of $n-1$ new variables to take the place of $y_2, \ldots, y_n$. Continuing thus, the transformation A will finally appear in the canonical form.

96. Theorem 8. *In any given abelian group K (§ 26) of linear transformations, such new variables may be introduced that all the transformations of K will simultaneously have the canonical form.*

Proof. If the group contains only similarity-transformations, the theorem is self-evident. Hence we assume in K a transformation S which is not a similarity-transformation. Let the variables of the group be chosen such that S appears in the canonical form

$$S = (\alpha_1, \ldots, \alpha_1; \quad \alpha_2, \ldots, \alpha_2; \quad \ldots; \quad \alpha_n, \ldots, \alpha_n),$$

the variables being arranged so that those having the same multipliers are grouped together. Let there be a variables $x_1, \ldots, x_a$ having the multiplier α_1; b variables $x_{a+1}, \ldots, x_{a+b}$ having the multiplier α_2, etc.

Now let T be any transformation in K. Since $TS = ST$,

we find by applying the rule for forming products that T has the form

$$x_s = a_{s1}x'_1 + \ldots + a_{sa}x'_a \qquad (s = 1, 2, \ldots, a),$$

$$x_t = a_{t\,a+1}x'_{a+1} + \ldots + a_{t\,a+b}x'_{a+b} \quad (t = a+1, a+2, \ldots, a+b),$$

. . . . . .

Hence we infer that K is intransitive, and if we now confine our attention to one of the sets of intransitivity, we may apply the above process to that set. This will, therefore, break up into further sets of intransitivity. Continuing thus, the ultimate sets of intransitivity contain one variable each, and the theorem is proved.

Instead of the phrase "let the variables be so chosen that a (given) transformation (or group) will appear in the canonical form" we shall often say simply: "let the (given) transformation (or group) be written in canonical form."

EXERCISES

1. Can the transformation

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

be reduced to the canonical form? Find the condition that the transformation

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix},$$

which is not necessarily of finite order, can be written in canonical form.

2. Prove that an abelian group in two variables can be written in canonical form and that at the same time the Hermitian invariant becomes $x_1\bar{x}_1 + x_2\bar{x}_2$.

CHAPTER X

THE LINEAR GROUPS IN TWO VARIABLES

97. Introduction. We shall limit ourselves to the determination of the groups whose transformations have unity for the value of their determinants. From these all other forms of groups may readily be constructed (cf. §§ 83–87). We shall say that a given group is a *type* of all groups which may be obtained from it by a mere change of variables.

All the types we encounter (with one exception) contain a group of similarity-transformations of order 2, $E=(1,\ 1)$, $E_1=(-1,\ -1)$, due to the fact that a linear transformation of determinant unity and of order 2 does not exist unless it be the similarity-transformation E_1. A transformation whose corresponding collineation is of order 2, if written in canonical form, must necessarily be $(i,\ -i)$, where $i^2=-1$. The exception mentioned is the type of an abelian group of odd order.

Following Jordan, it shall be our practice to call the order of a linear group $g\phi$, if g is the order of the corresponding collineation-group, and ϕ the order of the subgroup of similarity-transformations contained in the given group.

There are several processes available for the determination of the types of groups sought.* We shall here employ a modified form of Klein's original process, which depends largely on geometrical intuition.

* Klein, *Mathematische Annalen*, Bd. 9 (1876), p. 183 ff.; *Vorlesungen über das Ikosaeder*, Leipzig, 1884, pp. 116–120. Gordan, *Mathematische Annalen*, Bd. 12 (1877), p. 23 ff. Jordan, *Journal für die reine und angewandte Mathematik*, Bd. 84 (1878), pp. 93–112; *Atti della Reale Academia di Napoli*, t. 8 (1879). Fuchs, *Journal für die reine und angewandte Mathematik*, Bd. 81, 85 (1876, 1878), pp. 97, 1 ff. Valentiner, *De endelige Transformations-gruppers Theori*, Copenhagen, 1889, p. 100 ff.

98. Outline of the Process. 1°. Let G be a group in two variables x_1, x_2. Then by the introduction of the conjugate-imaginary group $\overline{G}$ (cf. § 92) and by the selection of new variables X, Y, Z which are bilinear in x_1, x_2 and their conjugate-imaginary values $\overline{x}_1$, $\overline{x}_2$, we obtain a group G' of real rotations in space, leaving the origin fixed (§ 99).

2°. Consider now a sphere Σ of radius 1 whose center is the origin. With each rotation of G' belongs an axis of rotation. One of the points where such an axis pierces Σ together with all those points into which this point is moved by G' form the vertices of a regular polyhedron, including the limiting cases where there is a single axis of rotation or where the polyhedron becomes a flat polygon (§ 100).

3°. The determination of G' is therefore made to depend upon the construction of the analytical expressions representing the rotations of the regular solids. We find five different types for G' and correspondingly five different types for the linear groups G (§§ 101–103).

99. The Group of Rotations G'. Let

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be any transformation of G, whose variables x_1, x_2 are chosen such that the Hermitian invariant is $I = x_1\overline{x}_1 + x_2\overline{x}_2$ (Cor., § 92). Then the following equations are true (§§ 93, 97):

$$ad - bc = 1 = \overline{a}\overline{d} - \overline{b}\overline{c},$$

$$a\overline{a} + b\overline{b} = 1, \quad a\overline{c} + b\overline{d} = 0, \quad c\overline{c} + d\overline{d} = 1.$$

From these we obtain

$$c = -\overline{b}, \quad d = \overline{a}.$$

Moreover, if we let p, q represent the positive square roots of $a\overline{a}$ and $b\overline{b}$ respectively, and put $a = p\alpha$, $b = q\beta$, we get, since $\overline{p} = p$, $\overline{q} = q$:

$$c = -q\overline{\beta}, \quad d = p\overline{\alpha};$$

$$\alpha\overline{\alpha} = \beta\overline{\beta} = 1, \quad p^2 + q^2 = 1.$$

Furthermore, if we put $\gamma=\sqrt{\alpha\beta}$ and $\delta=\sqrt{\alpha/\beta}$, we have

$$\gamma\bar{\gamma}=\delta\bar{\delta}=1.$$

Then it follows by direct multiplication (§ 78) that

$$S=S_1S_2S_3,$$

where

$$S_1=\begin{pmatrix}\gamma & 0\\ 0 & \bar{\gamma}\end{pmatrix},\quad S_2=\begin{pmatrix}p & q\\ -q & p\end{pmatrix},\quad S_3=\begin{pmatrix}\delta & 0\\ 0 & \bar{\delta}\end{pmatrix}.$$

The corresponding transformation $\bar{S}$ of the conjugate-imaginary group $\bar{G}$ can similarly be written as a product $\bar{S}_1\bar{S}_2\bar{S}_3$, where

$$\bar{S}_1=\begin{pmatrix}\bar{\gamma} & 0\\ 0 & \gamma\end{pmatrix},\quad \bar{S}_2=\begin{pmatrix}p & q\\ -q & p\end{pmatrix},\quad \bar{S}_3=\begin{pmatrix}\bar{\delta} & 0\\ 0 & \delta\end{pmatrix}.$$

In these expressions we shall finally put

$$\gamma=\cos u-i\sin u,\quad \delta=\cos w-i\sin w,\quad p=\cos v,\quad q=\sin v,$$

u, v, w being real angles.

We now introduce the new variables

$$X=x_1\bar{x}_1-x_2\bar{x}_2,\quad Y=x_1\bar{x}_2+x_2\bar{x}_1,\quad Z=i(x_1\bar{x}_2-x_2\bar{x}_1)$$

These are transformed into linear functions of themselves by S_1, S_2, S_3, operating simultaneously with $\bar{S}_1$, $\bar{S}_2$, $\bar{S}_3$. In fact, we find

$$(X)S_1\bar{S}_1=X,\quad (Y)S_1\bar{S}_1=Y\cos 2u-Z\sin 2u,$$

$$(Z)S_1\bar{S}_1=Y\sin 2u+Z\cos 2u;$$

or, to follow our previous practice,

$$S_1\bar{S}_1=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos 2u & -\sin 2u\\ 0 & \sin 2u & \cos 2u\end{pmatrix}$$

Similarly we find

$$S_2\overline{S}_2 = \begin{pmatrix} \cos 2v & \sin 2v & 0 \\ -\sin 2v & \cos 2v & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad S_3\overline{S}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos 2w & -\sin 2w \\ 0 & \sin 2w & \cos 2w \end{pmatrix}$$

If we interpret X, Y, Z as rectangular coördinates in ordinary space, we recognize here three real rotations around the X-, Z-, X-axes respectively, the origin remaining fixed. The rotations performed successively will, as is well known, be equivalent to a single rotation. With the transformations of the group G are therefore associated rotations which evidently form a group G' isomorphic with G. The isomorphism is (1, 2) in the case where G contains $E_1 = (-1, -1)$; otherwise it is (1, 1), since we may readily prove that to identity of G' will correspond only $E = (1, 1)$ or E_1 of G_4. In other words, G' is simply isomorphic with the collineation-group corresponding to G.

100. The Regular Polyhedron. Consider an axis of rotation (L) of G', and let the various angles of rotations around L be the different multiples of $(360/m)°$; we shall say that L is of *index* m. Let P_1 be one of the points where L cuts the sphere Σ. This point will be transformed into (say) k distinct points upon Σ by G': $P_1, P_2, \ldots, P_k$, all of which will be extremities of axes of rotation of index m. The distribution of these points about any one of them is similar to the distribution about any other.

Now let arcs of great circles be drawn connecting P_1 with all the other points $P_2, \ldots, P_k$, and let the shortest arc be of length A. The number of arcs of this length radiating from P_1 is m or a multiple of m, since always m of the arcs are interchanged by rotations about L through the different multiples of $(360/m)°$. However, there cannot be more than 5 arcs A; an exception occurring where we have just one or two points P_1, P_2, one or both extremities of L, in which case $A = 360°$ or $180°$. For, if there were 6 or more, a pair of them (say C_s, C_t) would make an angle $\beta \leqq 60°$ with each other at P_1;

and, this being the case, the arc B connecting P_s and P_t (the points of $P_1, \ldots, P_k$ located on C_s and C_t) would have a length $<A$. For, by trigonometry,

$$\cos B = \cos^2 A + \sin^2 A \cos \beta \geqq \cos^2 A + \tfrac{1}{2} \sin^2 A > \cos A;$$

and, since $0 < B < 90°$, it follows that $B < A$. But this is contrary to hypotheses, since the lengths of the arcs radiating from P_s are equal to the lengths of the arcs radiating from P_1.

Let $m > 2$. Then it follows that there are just m arcs of length A radiating from P_1, each making an angle of $(360/m)°$ with its adjacent arcs. The same will be true for each of the points $P_2, \ldots, P_k$, and we see readily that the sphere will be divided by all the arcs of length A, joining the various points $P_1, \ldots, P_k$ which can be reached from one of them by passing along such arcs, into a number of equal and regular polygons. Accordingly, these points, say $P_1, \ldots, P_l$, are the vertices of a regular polyhedron inscribed in Σ.

Consider next the case where there are no axes of index greater than 2. Proceeding as above, we let L denote an axis of index 2, and we obtain the points $P_1, \ldots, P_k$ by G'. There are at least two arcs of length A radiating from P_1 making an angle of 180° with each other. Taken together they form a single arc C upon which (when extended round the sphere) P_1 and some other points $P_2, \ldots, P_l$ lie, equally distributed over the entire circle. If $l > 2$, a rotation of 180° around P_1 followed by a rotation of 180° around one of the points next to P_1 is equivalent to a rotation of $(720/l)°$ around an axis perpendicular to the plane of the circle C.

Every axis is of index 2 by assumption. It follows that $2/l = 1$ or $1/2$; i.e., $l = 4$. In this case we have three mutually perpendicular axes of index 2.

The distance A is therefore either 180° or 90°. In the former case we have a single axis of index 2 in G'. In the latter case there are four arcs of length A radiating from P_1, lying on two circles which are at right angles to each other at P_1. Their extremities lie in the diametral plane which is perpendicular to the axis L, and must be 90° or 180° apart. Con-

sequently, G' contains just one axis of index 2, or just three such which are mutually perpendicular.

THE GROUPS OF THE REGULAR POLYHEDRA, §§ 101–103

101. Limiting Cases. We notice first that the most general linear homogeneous change of variables (x_1, x_2) in G is indicated by a linear transformation T (§ 88) to which again corresponds the most general rotation of Σ about its center. It follows that any given configuration arrived at in § 100 may at the outset be placed in any required position relative to the axes of coördinates X, Y, Z.

Beginning then with the simplest case where there is a single axis L of rotation, we let this be the X-axis. Then $\sin 2v = 0$ and $\cos 2v = 1$ (cf. § 99). Hence S has the form $(\pm\alpha, \pm\alpha^{-1})$. If S is of order g we have $(\pm\alpha)^g = 1$.

(A) G': a single axis of index g;
G: an abelian group (intransitive) of order g:

$$S_\lambda = (\epsilon^\lambda, \epsilon^{-\lambda}); \quad \lambda = 1, 2, \ldots, g; \quad \epsilon^g = 1.$$

The next case to be considered is where there is an axis L of index g, assumed to be the X-axis as above, in addition to g axes of index 2 lying in a plane perpendicular to L. Let one of the latter be the Z-axis; we then have $\cos 2v = -1$, $\cos 2(u-w) = 1$, and the corresponding transformation of G is found to be

$$T = \begin{bmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{bmatrix}.$$

(B) *Dihedral Group.*
G': one axis L of index g and g axes of index 2;
G: an imprimitive group of order $2g\phi$ consisting of the transformations

$$S_\lambda = (\pm\epsilon^\lambda, \pm\epsilon^{-\lambda}), \; T_\lambda = \begin{bmatrix} 0 & \pm\epsilon^\lambda \\ \mp\epsilon^{-\lambda} & 0 \end{bmatrix}; \quad \lambda = 1, 2, \ldots, g; \quad \epsilon^g = 1.$$

102. The Tetrahedron and Octahedron. We now examine the five ordinary regular solids. Of these, the hexahedron and octahedron furnish the same set of axes of rotation, as do also the dodecahedron and icosahedron. We therefore have only three cases to consider: the tetrahedron, octahedron and icosahedron.

In the case of the tetrahedron we have four vertices and correspondingly four axes of rotation of index 3; besides, three axes of index 2, each passing through the middle points of a pair of opposite edges. The latter axes are mutually perpendicular and may be taken as the X-, Y-, and Z-axes. The corresponding transformations of G are then as follows:

$$T_1=(i,\ -i),\quad T_2=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix},\quad T_3=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},$$

either directly or after multiplication by $E_1=(-1,\ -1)$. If the vertices are named a, b, c, d, the three rotations permute them among themselves according to the substitutions

$$(ab)(cd),\quad (ad)(bc),\quad (ac)(bd).$$

The remaining rotations permute the vertices three at a time cyclically, as (abc), . . . The corresponding transformations of G may be determined analytically from the conditions that they are each of order 3 and transform the *collineations* corresponding to T_1, T_2, T_3 cyclically. Certain ambiguities arise from the fact that the similarity-transformation $E_1=(-1,\ -1)$ is present in the group. Thus, $S=(abc)$ may transform T_1 into T_2 or into T_2E_1, etc. For (abc) we find four forms possible, all of which are present in G if one of them is. We shall choose the following form:

$$S=\begin{bmatrix}\dfrac{-1+i}{2} & \dfrac{-1+i}{2}\\ \dfrac{1+i}{2} & \dfrac{-1-i}{2}\end{bmatrix}$$

(C) *Tetrahedral Group.*

G': generated by $S=(abc)$ and $T_1=(ab)(cd)$;

G: a primitive group (§ 106) of order 12ϕ generated by the transformations S and T_1 above.

The rotations of the octahedron include those of the tetrahedron $S=(abc)$, $T_1=(ab)(cd)$ if here a, b, c, d represent each a pair of opposite faces. To the list of generating rotations we now add one, U say, of order 4, having the same axis as T_1, and $U^2=T_1$, or $U=(acbd)$. The corresponding transformation of G is readily found to be

$$U=\begin{pmatrix}\frac{1+i}{\sqrt{2}}, & \frac{1-i}{\sqrt{2}}\end{pmatrix}.$$

(D) *Octahedral Group.*

G': generated by $S=(abc)$ and $U=(acbd)$;

G: a primitive group of order 24ϕ, generated by S and U above.

103. The Icosahedron. An icosahedron contains 10 axes of rotation of index 3. These (counted twice) may be grouped in 5 sets of 4 axes each, such that the axes of each set are arranged in the same way as the axes of index 3 in (C). In this manner we obtain 5 regular tetrahedrons, each corresponding to a subgroup of order 12. The group is accordingly isomorphic with the alternating group of order 60 and is generated by the substitutions S, T_1 of (C) and a substitution $V=(ab)(de)$, whose corresponding transformation may be determined from the relations

$$V^2=E \text{ or } E_1, \quad (T_1V)^3=E \text{ or } E_1, \quad (SV)^2=E \text{ or } E_1.$$

The first and last ambiguities fall away, as of necessity $V^2=(SV)^2=E_1$ (cf. § 97); and by using VE_1 if necessary in place of V we may take $(T_1V)^3=E$. We then find

$$V=\begin{pmatrix}\frac{i}{2} & \beta-i\gamma \\ -\beta-i\gamma & \frac{-i}{2}\end{pmatrix},$$

where

$$\beta=\frac{1-\sqrt{5}}{4}, \quad \gamma=\frac{1+\sqrt{5}}{4}.$$

(E) *Icosahedral Group.*

G': generated by $S=(abc)$, $T_1=(ab)(cd)$ and $V=(ab)(de)$;

G: a primitive group of order 60ϕ generated by S, T_1 and V above.

EXERCISES

1. Construct the analytical forms of the rotations of G' corresponding to the generating transformations T_1, T_2, T_3, S, U and V. Prove that the X-, Y-, Z-axes are permuted among themselves by all of these rotations except V, and hence that the group G' in the cases (C), (D), as a group in three variables, is imprimitive (cf. § 106).

2. Determine a set of generators of (E) corresponding to the substitutions $S'=(abcde)$, $U'=(ad)(bc)$, $T'=(ab)(cd)$ of the alternating group in five letters; under the condition that S' is written in canonical form: $S'=(\epsilon^3, \epsilon^2)$; $\epsilon^5=1$.

Hints: We first determine U' from the condition $U'^{-1}S'U'=S'^{-1}$:

$$U'=\begin{bmatrix} 0 & p \\ q & 0 \end{bmatrix}, \quad pq=-1.$$

The change of variables $x=pX$, $y=Y$ will leave S' unaltered and will reduce U' to the form above, except that now $p=1$, $q=-1$. We finally assume

$$T'=\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad \alpha\delta-\beta\gamma=1.$$

The condition $T'^2=E_1$ (§ 97) gives us $\alpha+\delta=(i)+(-i)=0$ (§ 89), which, combined with $U'^{-1}T'U'=T'$ or $T'E_1$ (only $T'E_1$ will be compatible with the previous results) is equivalent to $\delta=-\alpha$, $\gamma=\beta$; $\alpha^2+\beta^2=-1$. Finally, we have the relation $(abcde)\cdot(ab)(cd)=(bde)$; that is, the transformation $S'T'$ is of order 3 and its characteristic roots are consequently ω, ω^2 or $-\omega$, $-\omega^2$. The latter possibility can be avoided by taking $T'E_1$ instead of T'. Applying this condition we finally have

$$\alpha=\frac{\epsilon^4-\epsilon}{\sqrt{5}}, \quad \beta=\frac{\epsilon^2-\epsilon^3}{\sqrt{5}}.$$

INVARIANTS OF THE LINEAR GROUPS IN TWO VARIABLES, §§ 104–105

104. General Theory. A homogeneous function of the variables x_1, x_2 of a group

$$G: \qquad S_1,\ S_2,\ \ldots,\ S_{g\phi}$$

is called an *invariant* of G (or we say that G *leaves* f *invariant*) when f is transformed into a constant multiple of itself by G:

$$(f)S_j = c_j f.$$

Let f be resolved into linear factors. These are permuted among themselves by G, and the product of a set of them which are permuted transitively will evidently furnish an invariant by itself. This invariant, say $F = f_1 f_2 \ldots f_h$, can readily be constructed by operating upon one of the factors f_1 by the transformations of G, and we shall call it a *fundamental invariant.* Any invariant is accordingly a product of fundamental invariants.

If f_1 be selected at random, the corresponding fundamental invariant is evidently of degree g. To obtain fundamental invariants of lower degree we make use of a theorem of transitive substitution groups, namely that the ratio $g\phi/h$ is the order of that subgroup of G which leaves f_1 invariant.

Now this subgroup, G_1, must be abelian. For we may change the variables, introducing f_1 as one of the new variables, say x_1. Then G_1 must appear in the form of a reducible group:

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$$

and can accordingly be written as an intransitive group

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$$

But this is the canonical form of an abelian group. It follows furthermore that two subgroups, G_1 and G_2, having in common a linear invariant f_1, generate an abelian group.

The other factors $f_2, \ldots, f_h$ of F are linear invariants of subgroups $G_2, \ldots, G_h$ of G, conjugate to G_1. For, if $S_\alpha^{-1} G_1 S_\alpha = G_2$, then $(f_1)S_\alpha = f_2$ belongs to F and is an invariant of G_2. Hence our problem becomes one of determining the different conjugate sets in G of abelian subgroups which are not subgroups in larger abelian subgroups. The fundamental invariant F will be made up of one factor for each of the subgroups of the set if there is no transformation in G which transforms one of the linear invariants of G_1 into the other. In other words, if G_1 be written in the canonical form (a, c), and if there is no transformation in G of type

$$\begin{pmatrix} 0 & p \\ q & 0 \end{pmatrix},$$

we get two fundamental invariants by starting with $f_1 = x_1$ and $f_1 = x_2$; otherwise we get just one invariant, containing both x_1 and x_2 as factors.

105. List of the Fundamental Invariants. We shall, of course, limit ourselves to the invariants of degree $< g$.

(A) Case (A), § 101. Two invariants, x_1 and x_2.

(B) *Dihedral Group.* One invariant, $x_1 x_2$.

(C) *Tetrahedral Group.* There are two conjugate sets of subgroups, of orders 2ϕ and 3ϕ. The first set consists of groups conjugate to that generated by T_1, and the invariant is *

$$t = x_1 x_2 (x_1^4 - x_2^4).$$

The second set contains the groups conjugate to that generated by S. Here we have two invariants, each containing just one of the linear invariants of S:

$$\Phi = x_1^4 + 2\sqrt{-3} x_1^2 x_2^2 + x_2^4, \qquad \Psi = x_1^4 - 2\sqrt{-3} x_1^2 x_2^2 + x_2^4.$$

These invariants satisfy the relation

$$12\sqrt{-3} t^2 - \Phi^3 + \Psi^3 = 0.$$

(D) *Octahedral Group.* Here we have three conjugate sets of subgroups, of orders 4ϕ, 3ϕ and 2ϕ. In the first set

* The notation is that given by Klein, *Vorlesungen, etc.*, pp. 51–58.

there is a group generated by U, and the corresponding invariant is t above. The second set contains the group generated by S, and the corresponding invariant is the product of Φ and Ψ above:

$$W = \Phi\Psi = x_1^8 + 14x_1^4x_2^4 + x_2^8.$$

The third set contains the group generated by UT_2, and we get the invariant

$$\chi = x_1^{12} - 33x_1^8x_2^4 - 33x_1^4x_2^8 + x_2^{12}.$$

These invariants satisfy the relation

$$108t^4 - W^3 + \chi^2 = 0.$$

(E) *Icosahedral Group.* We shall take the group as represented in Exercise 2, § 103. There are three sets of subgroups of orders 2ϕ, 3ϕ and 5ϕ, containing the groups generated by U', $S'T'$ and S' respectively. We get, correspondingly, the three invariants

$$T = x_1^{30} + x_2^{30} + 522(x_1^{25}x_2^5 - x_1^5x_2^{25}) - 10005(x_1^{20}x_2^{10} + x_1^{10}x_2^{20}),$$

$$H = -x_1^{20} - x_2^{20} + 228(x_1^{15}x_2^5 - x_1^5x_2^{15}) - 494x_1^{10}x_2^{10},$$

$$f = x_1x_2(x_1^{10} + 11x_1^5x_2^5 - x_2^{10}),$$

which satisfy the relation

$$T^2 + H^3 - 1728f^5 = 0.$$

EXERCISES

1. The invariant Ψ of the tetrahedral group is the Hessian covariant (cf. § 174) of the function Φ:

$$48\sqrt{-3}\Psi = \begin{vmatrix} \Phi_{11} & \Phi_{12} \\ \Phi_{21} & \Phi_{22} \end{vmatrix},$$

and the invariant t is the Jacobian of the functions Φ and Ψ:

$$-32\sqrt{-3}t = \begin{vmatrix} \Phi_1 & \Phi_2 \\ \Psi_1 & \Psi_2 \end{vmatrix}.$$

Obtain similar relations for the octahedral and icosahedral groups.

2. From the fact that no two abelian subgroups of G can have a transformation in common (except similarity-transformations) unless they generate a larger abelian group, it follows that G is made up of a number of distinct abelian groups H_1, H_2, . . . , having no transformations in

common except E and E_1. Hence, if the orders of these groups be respectively $h_1, \ldots$, we must have

$$g\phi = 2^* + (h_1\phi - 2^*) + (h_2\phi - 2) + \ldots \tag{1}$$

Now, $h_1, \ldots$ are factors of g, say $h_1 = g/g_1, \ldots$, and there are either $g_1/2$ or g_1 subgroups conjugate to H_1, according as there is or is not a transformation in G which permutes the linear invariants of H_1. Hence, adding the corresponding terms in the right-hand member of (1), we obtain

$$g\phi = 2 + \sum \tfrac{1}{2} g_1 (h_1\phi - 2) + \sum g'_1 (h'_1\phi - 2)$$

$$= 2 + \sum \tfrac{1}{2}(g\phi - 2g_1) + \sum (g\phi - 2g'_1),$$

or

$$1 = \frac{1}{g} + \sum \frac{1}{2}\left(1 - \frac{1}{h_1}\right) + \sum \left(1 - \frac{1}{h'_1}\right).$$

Verify this (Diophantine) equation for the groups (A) to (E).

3. Prove that, in the case of (D) or (E), any invariant of degree g, say J, is an *absolute invariant;* that is, it is transformed into *itself* by every transformation of G.

Prove also that J is a rational integral function of two of the three fundamental invariants listed above for the respective group.

* Counting the transformations E and E_1 once each.

CHAPTER XI

SOME SPECIAL TYPES OF GROUPS

106. Primitive and Imprimitive Groups. Let us suppose that the group G, § 90, contains not only transformations of type A, but also some of type

$$B=\begin{pmatrix} p & q & t & v \\ -q & -p & -v & -t \\ u & w & r & s \\ -w & -u & -s & -r \end{pmatrix},$$

which upon the change of variables there employed becomes

$$B=\begin{pmatrix} 0 & 0 & p-q & t-v \\ 0 & 0 & u-w & r-s \\ p+q & t+v & 0 & 0 \\ u+w & r+s & 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & B' \\ B'' & 0 \end{pmatrix};$$

then we say that G is imprimitive, under the assumption that it is transitive.

In general, *a transitive group G, in which the variables (either directly or after a suitable choice of new variables) can be separated into two or more sets $Y_1, \ldots, Y_k$, such that the variables of each set are transformed into linear functions of the variables of the same set or into linear functions of the variables of a different set, is said to be imprimitive.* If such a division is not possible, the group is *primitive.* The sets $Y_1, \ldots, Y_k$ are called *sets of imprimitivity.*

107. Theorem 9. *Let G be an imprimitive linear group in n variables. These may be chosen in such a manner that they break up into a certain number of sets of imprimitivity $Y_1, \ldots, Y_k$ of m variables each ($n=km$), permuted according to a transitive substitution group K on k letters, isomorphic with G. That subgroup of G which corresponds to the subgroup of K leaving one letter unaltered, say Y_1, is primitive as far as the m variables of the set Y_1 are concerned.*

If $m=1$, $k=n$, then G is said to have the *monomial form* or to be a *monomial group.*

Proof. Let the variables of G break up into say k' sets $Y_1, \ldots, Y_{k'}$, permuted among themselves according to a substitution group K' on k' letters. This group K' is transitive (as a substitution group, § 12); otherwise G would not be a transitive linear group. Hence K' contains $k'-1$ substitutions $S_2, S_3, \ldots, S_{k'}$ which replace Y_1 by $Y_2, Y_3, \ldots, Y_{k'}$ respectively. We shall select $k'-1$ corresponding transformations of G and denote them by $A_2, A_3, \ldots, A_{k'}$. The condition that the determinants of these transformations do not vanish, implies that the sets contain the same number of variables n/k'.

There is in K' a subgroup K'_1 whose substitutions leave Y_1 unaltered (§ 12). This subgroup, together with the substitutions $S_2, \ldots, S_{k'}$ will generate K'. Correspondingly, G is generated by $A_2, \ldots, A_{k'}$ and that subgroup G_1 of G corresponding to K'_1, and which therefore replaces the variables of Y_1 (say $y_1, y_2, \ldots, y_m$) by linear functions of the same variables. If we now fix our attention upon just that portion of each transformation of G which affects only these m variables and which plainly forms the transformations of a linear group $[G_1]$ in m variables, we shall prove that *if* $[G_1]$ *is not primitive, then new variables may be introduced into G such that the number of new sets of imprimitivity is greater than k'.*

Accordingly, let the variables of $[G_1]$ break up into at least two subsets of intransitivity or imprimitivity, say $Y_1^{(1)}, \ldots, Y_1^{(0)}$. New variables will now be introduced into the sets $Y_2, \ldots, Y_{k'}$ such that A_t will replace $Y_1^{(1)}, \ldots, Y_1^{(0)}$ by dis-

tinct subsets $Y_i^{(1)}, \ldots, Y_i^{(l)}$. In this manner the variables of G will be divided into lk' subsets, and it remains for us to prove that any transformation S of G will permute these subsets among themselves; that is, S will transform the variables from any one subset into linear functions of the variables of one of these subsets.

Let S replace Y_α by Y_β. Then $A_\alpha S A_\beta^{-1} = T$ transforms Y_1 into itself; that is, T is a transformation of G_1 and will therefore permute among themselves the subsets $Y_1^{(1)}, \ldots, Y_1^{(l)}$. It follows that the transformation $A_\alpha^{-1} T A_\beta = S$ will transform any subset of Y_α into some subset of Y_β, and the proposition is proved.

We can therefore keep on changing the variables so as to increase the number of sets of imprimitivity, until the sets contain just one variable each, or until the group $[G_1]$ is primitive. The theorem is therefore proved.

108. Lemma. *A linear group G having an invariant abelian subgroup H whose transformations are not all similarity-transformations is either intransitive or imprimitive.*

Proof. Write H in canonical form. The variables can then be arranged into sets having the property that a transformation of H affects all the variables of any one set by the same constant factor.

To illustrate, let H be generated by the transformations

$$T_1 = (\alpha_1, \alpha_1, \alpha_1, \alpha_1, \alpha_2) \qquad (\alpha_1 \neq \alpha_2),$$

$$T_2 = (\beta_1, \beta_1, \beta_2, \beta_2, \beta_2) \qquad (\beta_1 \neq \beta_2).$$

Here we have three sets: $X = (x_1, x_2)$, $Y = (x_3, x_4)$, $Z = (x_5)$.

Then it is readily proved that G permutes these sets among themselves. Thus, in the illustration given, let S be a transformation of G and T_i, T_j of H, and let $S^{-1} T_i S = T_j$. Now suppose that the variables of X are transformed by S into two variables y_1, y_2 forming a set X'; we must then prove that X' is either X or Y. We have

$$(x_1, x_2) T_i S = (x_1, x_2) S T_j,$$

or

$$\alpha_i (y_1, y_2) = (y_1, y_2) T_j.$$

Hence, the variables y_1, y_2 are transformed by T_j into the same multiple of themselves. Since T_j may be taken to represent any transformation of H, it follows that y_1, y_2 are linear functions of x_1, x_2, or linear functions of x_3, x_4.

THEOREM 10. *A linear group whose order is the power of a prime number can be written as a monomial group by a suitable choice of variables* $x_1, \ldots, x_n$; *that is, its transformations have the form:* *

$$x_s = a_s x'_t \qquad (s=1, 2, \ldots, n; \quad t=1, 2, \ldots, n).$$

Proof. 1°. A group P whose order is the power of a prime number p is either abelian or it contains an invariant abelian subgroup Q whose transformations are not separately invariant in P (§ 48). In the first case the theorem follows from Theorem 8, § 96. In the second case, Q can be written in canonical form, and P is intransitive or imprimitive by the above lemma. If the theorem is true for a transitive group, it is evidently true for an intransitive group; hence we need merely discuss the case where P is imprimitive.

2°. By Theorem 9, P is monomial unless there is a group $[P_1]$ which is primitive in the m variables of a set Y_1. But the order of $[P_1]$ is again a power of p, and this group cannot therefore be primitive, by 1°.

COROLLARY. *A linear group in n variables whose order is the power of a prime greater than n is abelian.*

109. Theorem 11. *A linear group G in n variables and of order* $g = g' p^a q^b r^c \ldots$, *where p, q, r, . . . are different primes all greater than* $n+1$, *contains an abelian subgroup of order* $p^a q^b r^c \ldots$

To prove this theorem by the process of complete induction, we assume it true for any group whose order is a factor of $p^a q^b r^c \ldots$, smaller than this number. We shall also assume the theorem true for a transitive group in fewer than n variables; it will then immediately be true for an intransitive group in n variables.

* Proofs of this theorem were given by the author in *Transactions of the American Mathematical Society*, vol. 5 (1904), pp. 313–314; vol. 6 (1905), p. 232.

We therefore assume that G is transitive. At the outset we anticipate a theorem given below (Cor. 3, § 135), from which it follows that G contains a transformation of order pqr. . . . Now, among all abelian subgroups of G whose orders are of the form $p^\alpha q^\beta r^\gamma$. . . . , where $a \geqq \alpha \geqq 1$, $b \geqq \beta \geqq 1$, etc., let H be one whose order is the highest possible. We shall then prove that here

$$\alpha = a, \quad \beta = b, \quad \gamma = c, \ldots \tag{1}$$

For this purpose, let us assume that these equations are not all true; say $\alpha < a$. Then H contains a Sylow subgroup P_1 of order p^α which is contained in a Sylow subgroup P of G of order p^a (§ 11). The groups H and P being abelian (Cor., § 108), all the transformations of P_1 are invariant in both, and will therefore also be invariant in the group K generated by H and P. But, if such an invariant transformation is not a similarity-transformation, K will be intransitive (cf. proof of Theorem 8, § 96) and will (by assumption) in this case contain an abelian subgroup of order $p^\alpha q^\beta r^\gamma$ . . . , contrary to the supposition made in regard to H. Again, if the transformations belonging to P and invariant in K, say p^s in number, are all similarity-transformations, the group K contains an invariant subgroup (Theorem 12, Ex. 2), the order of which is divisible by p^{a-s}. Hence, by assumption, it contains an abelian subgroup of order $p^{a-s} q^\beta r^\gamma$ . . . The corresponding subgroup of K is evidently also abelian and has for its order $p^s \cdot p^{a-s} q^\beta r^\gamma$ . . . $= p^a q^\beta r^\gamma$ . . . Hence finally, if $\alpha < a$, H cannot be that abelian subgroup of highest order $p^\alpha q^\beta r^\gamma$ . . . contained in G. The equations (1) follow.

EXERCISES

1. Prove that if $n+1$ is a prime, and if the order of G is $g = g'(n+1)^t p^a q^b$ . . . , where $t > 1$, and $p, q, \ldots$ are primes greater than $n+1$, then there is in G an abelian subgroup of order $(n+1)^t p^a q^b$ . . .

2. It follows from Theorem 11 that a group in n variables whose order contains no prime factors smaller than $n+2$ is abelian. Prove that if the order contains no prime factors smaller than $n+1$, the group is abelian.

3. Construct all the types of collineation groups of order 2^4 in three variables, and show that such groups contain either a collineation of order 8 or one of order 4 having two distinct multipliers.

4. Construct all the types of groups of order $3^4\phi(\phi=1$ or 3; cf. § 111) and show that such groups contain a transformation of order 9ϕ.

110. On the Group of Similarity-transformations. The necessity for the presence of similarity-transformations in a given linear group can be determined from the following

Theorem 12. *If a Sylow subgroup P of order p^λ in a linear group G of order g can be generated by a group P' of order $p^{\lambda-1}$ and a similarity-transformation T of order p^α, then there is in G an invariant subgroup G' of order g/p which does not contain T.*

Proof. Let H represent the regular substitution group on g letters simply isomorphic with G (§ 27). Then, if among the letters of H, $y_1, y_2, \ldots, y_k$ form a transitive set for P', the sum

$$J=y_1+y_2+\ldots+y_k$$

will be transformed into itself by every substitution of P'.

Let furthermore θ be a primitive root of the equation $\theta^p-1=0$ (§ 116); then the function

$$I=J+\theta^{-1}(J)T+\theta^{-2}(J)T^2+\ldots+\theta^{-p+1}(J)T^{p-1}$$

is transformed into a constant (θ) times itself by T:

$$\begin{aligned}(I)T&=(J)T+\theta^{-1}(J)T^2+\ldots+\theta^{-p+1}(J)T^p\\&=\theta I+\theta[(J)T^p-J]=\theta I,\end{aligned}$$

since T^p belongs to P' and therefore transforms J into itself. Moreover, any substitution of P' transforms I into itself. For,

$$(I)S=\sum_{r=0}^{p-1}\theta^{-r}(J)T^rS=\sum_{r=0}^{p-1}\theta^{-r}(J)ST^r=\sum_{r=0}^{p-1}\theta^{-r}(J)T^r,$$

since T is commutative with S. It follows that I is an invariant of P (the function I cannot vanish identically, since no two of the terms J, $(J)T$, $(J)T^2$, . . . can have a letter in common).

Again, I is not an invariant of any substitution in G other than those in P. For, if R be a substitution such that $(I)R=cI$, the letters occurring in I must be permuted among themselves by R. Let us suppose that R changes y_1 into y_2. But, the

letters of I form a transitive set for P; accordingly, there is a substitution in P, say S_1, which also changes y_1 into y_2. Then RS_1^{-1} leaves y_1 fixed and must therefore be the identity; that is, $R=S_1$.

It follows that the substitutions of G transform I into just g/p^λ functions I, I_1, I_2, . . . , no one of which is a constant multiple of another. The product $K=II_1I_2$ . . . of these functions is therefore an invariant of G.

Now, all the substitutions of G for which K is an *absolute invariant*, that is, for which $(K)R=K$, must form an invariant subgroup G' of G, as is easily seen. To this group the substitution T does not belong, since

$$(K)T=\theta^k K,$$

where $k=g/p^\lambda$. For, let $I_r=(I)R$, then

$$(I_r)T=(I)RT=(I)TR=\theta(I)R=\theta I_r.$$

But, $\theta^k\neq 1$ since k is prime to p.

This subgroup G' is of index p. For, the constant multipliers of K that result by operating upon K by the various substitutions of G are integral functions of θ and must be roots of unity. Such roots can therefore, by § 116, 6°, be no others than powers of θ. Moreover, it is readily seen that each power must occur equally often, so that the power 1 occurs g/p times. Hence the theorem.

EXERCISES

1. Prove that a linear group in 3 variables of order $9g$ in which there is no transformation of order 9ϕ must contain similarity-transformations.

2. Prove that a linear group in n variables which contains a subgroup F of similarity-transformations of order p^k (p a prime $>n$), contains an invariant subgroup of index p^k, to which F does not belong.

CHAPTER XII

THE LINEAR GROUPS IN THREE VARIABLES

111. Introduction. As in the case of the binary groups we shall limit ourselves to the discussion of groups of transformations of determinant unity, and shall generally write $g\phi$ for the order of a linear group whose corresponding collineation group is of order g. Moreover, the order of a transformation S will often be written in the form $g\phi$, when the order of the group generated by S is $g\phi$. For instance, the order of the transformation

$$S=(\alpha,\ \alpha,\ \alpha\omega^2) \qquad (\alpha^3=\omega;\ \omega^3=1)$$

may be written either 9 or 3ϕ.

Though the orders as written may thus virtually refer to collineation groups, it must be kept in mind that all purely descriptive terms refer to linear groups. For instance, the group of order 9ϕ generated by

$$S_1=(1,\ \omega,\ \omega^2),\quad S_2=\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}$$

would be described as a non-abelian group, though the corresponding collineation-group is abelian.

The determination of the linear groups in three variables is based upon the following classification:

1. Intransitive and imprimitive groups.
2. Primitive groups having invariant imprimitive subgroups.
3. Primitive groups whose corresponding collineation groups are simple.
4. Primitive groups having invariant primitive subgroups.

The method for the first two and last classes is more or less evident. In the discussion below on the groups in class 3 some theorems are developed that with slight modifications can be extended to groups in n variables, and such generalizations are given in § 126, together with a résumé of results on the order of the primitive groups in n variables. An introduction to the theory of the invariants of the ternary linear groups is given in § 125.

112. Intransitive and Imprimitive Groups. We have two types of *intransitive groups*:

(A) $x_1=\alpha x'_1, \quad x_2=\beta x'_2, \quad x_3=\gamma x'_3$ (abelian type).

(B) $x_1=\alpha x'_1, \quad x_2=ax'_2+bx'_3, \quad x_3=cx'_2+dx'_3.$

In (B) the variables x_2, x_3 are transformed by a linear group in two variables (cf. Chapter X).

The *imprimitive groups* are all monomial. There are two types:

(C) A group generated by an abelian group

$$H: \qquad x_1=\alpha x'_1, \quad x_2=\beta x'_2, \quad x_3=\gamma x'_3$$

and a transformation which permutes the variables in the order $(x_1x_2x_3)$. By a suitable choice of variables this transformation can be thrown into the form

$$T: \qquad x_1=x'_2, \quad x_2=x'_3, \quad x_3=x'_1.$$

(D) A group generated by H, T of (C) and the transformation

$$R: \qquad x_1=ax'_1, \quad x_2=bx'_3. \quad x_3=cx'_2.$$

113. Remarks on the Invariants of the Groups (C) **and** (D). Interpreting x_1, x_2, x_3 as homogeneous coördinates of the plane, the triangle whose sides are $x_1=0$, $x_2=0$, $x_3=0$ is transformed into itself by the operators of (C) and (D); in other words, $x_1x_2x_3$ is an invariant of these groups.

It will later be imperative for us to know under what conditions there are other invariant triangles. Assuming the existence of one such, say

(1) $(a_1x_1+a_2x_2+a_3x_3)(b_1x_1+b_2x_2+b_3x_3)(c_1x_1+c_2x_2+c_3x_3)=0,$

we operate successively by the transformations of H and by T. Examining the various possibilities we find that (1) could not be distinct from $x_1x_2x_3=0$ unless H is the particular group generated by the transformations

$$S_1=(1,\ \omega,\ \omega^2),\quad S_2=(\omega,\ \omega,\ \omega)\qquad(\omega^3=1).$$

There are then four invariant triangles for (C), namely:

$$(2)\qquad \begin{gathered} x_1x_2x_3=0; \\ (x_1+x_2+\theta x_3)(x_1+\omega x_2+\omega^2\theta x_3)(x_1+\omega^2x_2+\omega\theta x_3)=0 \\ (\theta=1,\ \omega \text{ or } \omega^2). \end{gathered}$$

The same triangles are invariants of (D) if this is generated by (C) in the form just given and the following special form of R:

$$x_1=-x'_1,\quad x_2=-x'_3,\quad x_3=-x'_2.$$

114. Groups Having Invariant Intransitive Subgroups. All such groups are intransitive or imprimitive. This follows from the fact that the type (B) has a single linear invariant x_1, which is therefore also an invariant of a group containing (B) invariantly; * and the fact that a group containing (A) invariantly cannot be primitive by the lemma, § 108.

115. Primitive Groups Having Invariant Imprimitive Subgroups. It was shown above that the types (C) and (D) possess either one or a set of four invariant triangles. If they possess only one such triangle, a group containing one of these types invariantly would of necessity also leave invariant that triangle, as may be easily proved. That such a group may be primitive, it is therefore necessary that (C) and (D) possess the four invariants (2).

Let us therefore assume a group G permuting among themselves the triangles (2), which we shall for brevity denote respectively by t_1, t_2, t_3, t_4 in the order as they are listed in (2).

* Let V be any transformations of a group containing (B) invariantly, and T any transformation of (B). Then $VTV^{-1}=T_1$ belongs to (B), and if we put $(x_1)T_1=\alpha x_1$, $(x_1)V=y$, we have

$$(y)T=(y)V^{-1}T_1V=\alpha y,$$

so that y is an invariant of T. But, x_1 being the only linear invariant for (B), it follows that $y=cx_1$.

We now associate with each transformation of G a substitution on the letters t_1, t_2, t_3, t_4, indicating the manner in which the transformation permutes the corresponding triangles. We thus obtain a substitution group K on four letters to which G is multiply isomorphic, and the invariant subgroup (C) or (D) corresponds to identity of K. No one of the four letters could be left unchanged by every substitution of K; for, the corresponding triangle would be an invariant of G, and this group would not be primitive. Moreover, no transformation can interchange two of the triangles and leave the other two fixed, as may be verified directly.

Under these conditions the following possible forms for K are found:

(E′) $1,\ (t_1t_2)(t_3t_4)$; *

(F′) $1,\ (t_1t_2)(t_3t_4),\quad (t_1t_4)(t_2t_3),\quad (t_1t_3)(t_2t_4)$;

(G′) the alternating group on four letters, generated by $(t_1t_2)(t_3t_4)$ and $(t_2t_3t_4)$.

Now, to construct the corresponding transformations we observe that the group (D) as given in § 113 contains all the transformations which leave invariant each of the four triangles. Furthermore, we note that if a given transformation V permutes the triangles in a certain manner, then any transformation which permutes them in the same manner can be written in the form $V' = XV$, X being a transformation of (D). For, $V'V^{-1}$ must leave fixed each triangle, and is therefore a transformation X as defined.

We are now in a position to construct the required groups. By direct application we verify that the transformations U, V, UVU^{-1}:

$$
\begin{aligned}
&U: \quad x_1 = \epsilon x'_1, \quad x_2 = \epsilon x'_2, \quad x_3 = \epsilon\omega x'_3 \qquad (\epsilon^3 = \omega^2);\\
(3)\quad &V: \quad x_1 = \rho(x'_1 + x'_2 + x'_3), \quad x_2 = \rho(x'_1 + \omega x'_2 + \omega^2 x'_3),\\
&\qquad x_3 = \rho(x'_1 + \omega^2 x'_2 + \omega x'_3) \qquad \left(\rho = \frac{1}{\omega - \omega^2}\right);\\
&UVU^{-1}: x_1 = \rho(x'_1 + x'_2 + \omega^2 x'_3), \quad x_2 = \rho(x'_1 + \omega x'_2 + \omega x'_3),\\
&\qquad x_3 = \rho(\omega x'_1 + x'_2 + \omega x'_3)
\end{aligned}
$$

* The three different subgroups of order 2 of K would furnish only one type for G, since the three different groups obtained are transformable one into the other by a change of variables.

permute the triangles in the following manner:

$$(t_2t_3t_4), \quad (t_1t_2)(t_3t_4), \quad (t_1t_4)(t_2t_3).$$

Accordingly, since all the required groups contain a transformation corresponding to $(t_1t_2)(t_3t_4)$, every such group must contain a transformation XV, X belonging to (D). Hence, if G contains (D) as a subgroup, it also contains V. If, however, (C) were a subgroup of G, but not (D), then either V is contained in G, or else XV, where X belongs to (D) but not to (C). In this event X may be written X_1R, where X_1 belongs to (C). Hence finally, either V or RV belongs to G. However, $V^2=(RV)^2=R$. Thus R, and therefore also V, are contained in G in any case.

Again, if G contains a transformation corresponding to $(t_2t_3t_4)$ or $(t_1t_4(t_2t_3)$, such a transformation can be written XU or $XUVU^{-1}$, X belonging to (D). Hence, since G contains (D) as we have just seen, it will contain either U or UVU^{-1} in the cases considered. We therefore have the following types:

(E) Group of order 36ϕ generated by (C) as given in § 113:

$$S_1=(1, \omega, \omega^2), \quad T: \quad x_1=x'_2, \quad x_2=x'_3, \quad x_3=x'_1,$$

and the transformation V of (3).

(F) Group of order 72ϕ generated by S_1, T, V and UVU^{-1}.

(G) Group of order 216ϕ generated by S_1, T, V and U.

These groups are all primitive, and they all contain (D) as an invariant subgroup. The group (G) is called the Hessian group (cf. Jordan, *Journal für die reine und angewandte Mathematik*, Bd. 84 (1878), p. 209).

116. On Roots of Unity. A solution of the equation

$$x^n=1,$$

n being a positive integer, is called a *root of unity*. A solution α is in particular called a *primitive* nth *root of unity*, if n is the least integer for which $\alpha^n=1$. In such a case n is called the *index* of the root.

THEOREMS. 1°. The product or ratio of two roots of unity is again a root of unity.

2°. Any positive or negative rational power of a root of unity is again a root of unity.

3°. If n is the index of a root α, and m a positive integer, the index of α^m is n/d, where d is the highest common factor of n and m.

4°. If the index of a root θ is $n=ab$, where a and b are two integers which are prime to each other, then it is possible to find a root of index a, say α, and one of index b, say β, such that $\theta=\alpha\beta$.

As is customary, we write ω, ω^2 for the roots of index 3; i, $-i$ for the roots of index 4; $-\omega$, $-\omega^2$ for the roots of index 6, etc.

5°. If α is a primitive nth root, then the n roots of $x^n-1=0$ are α, α^2, . . . , α^{n-1}, α^n, and we have

$$1+\alpha+\alpha^2+\ \ldots\ +\alpha^{n-1}=0.$$

6°. *Theorem of Kronecker.* For the proper handling of a certain class of equations we use a very effective theorem of Kronecker.* Instead of making a formal statement of the theorem we shall explain its meaning by implication.

The class of equations referred to are all of the form $\sum_{i=1}^{i=k}\alpha_i=0$; α_1, . . . , α_k being roots of unity, and the question involved is this: if these roots are not known originally, but their number k is known. what can be inferred about their values? The theorem implies that the roots of this equation can be arranged into sets (either directly or after the addition of certain pairs of mutually cancelling roots), such that each set contains a prime number $p \leqq k$ of roots the sum of which vanishes, being of the form $\epsilon+\epsilon\alpha+\ldots+\epsilon\alpha^{p-1}$ where α is a root of index p, while ϵ may have any index. We shall discuss in full the cases $k=3, 4, 5$.

$k=3$: $\alpha_1+\alpha_2+\alpha_3=0$. Here we have $\alpha_2=\alpha_1\omega$, $\alpha_3=\alpha_1\omega^2$.

$k=4$: $\alpha_1+\alpha_2+\alpha_3+\alpha_4=0$. We have two sets of two roots each, say $\alpha_1+\alpha_2=0$, $\alpha_3+\alpha_4=0$.

$k=5$: $\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5=0$. There are two possibilities: one set only, or two sets containing 3 and 2 roots respectively.

* Mémoires sur les facteurs irréductibles de l'expression x^n-1, *Journal de Mathématiques pures et appliquées*, ser. 1, t. 19 (1854), p. 178.

If β represents a primitive 5th root, and γ, δ roots of unknown indices, the two cases are respectively given by

$$\gamma+\gamma\beta+\gamma\beta^2+\gamma\beta^3+\gamma\beta^4=0;$$

$$(\gamma-\gamma)+(\delta+\delta\omega+\delta\omega^2)=0.$$

By means of Kronecker's theorem the following can be proved:

7°. If N represents the sum of a finite number of roots of unity and k an integer, and if it be known that N/k is an *algebraic integer* (that is, a solution of an equation $x^m+a_1x^{m-1}+\ldots+a_m=0$, where $a_1, \ldots, a_m$ are positive or negative integers or zero), then N/k equals the sum of a finite number of roots of unity.

If the indices of the roots in N are all powers of a single prime number p, then these roots can be separated directly into two sets such that the sum of those in one set vanishes, and those in the other set are each repeated k or a multiple of k times.

PRIMITIVE GROUPS WHOSE CORRESPONDING COLLINEATION GROUPS ARE SIMPLE,* §§ 117–123

117. Theorem 13. *No prime $p>7$ can divide the order of a primitive linear group G in three variables.*

Proof. The process consists in showing that, if the order g contains a prime factor $p>7$, then G is not primitive. We subdivide this process into four parts as follows: 1° proving the existence of an equation $F=0$, where F is a certain sum of roots of unity; 2° giving a method for transforming such an equation into a congruence (mod p); 3° applying this method to the equation $F=0$; 4° deriving an abelian self-conjugate subgroup P of order p^k.

1°. The order g being divisible by p, G contains a Sylow subgroup of order p^λ and therefore a transformation S of order p. We choose such variables that S has the canonical form

$$S=(\alpha_1, \alpha_2, \alpha_3); \quad \alpha_1^p=\alpha_2^p=\alpha_3^p=1, \quad \alpha_1\alpha_2\alpha_3=1.$$

Two cases arise: two of the multipliers are equal, say $\alpha_1=\alpha_2$, or they are all distinct. They cannot all be equal, since $\alpha_1^p=1$

* We shall briefly call such groups *primitive simple groups*.

and $\alpha_1^3 = 1$ imply $\alpha_1 = 1$, whereas S is not the identity. Of the two cases we shall treat the latter only: the method would be the same in the former case,* and the result as stated in Theorem 13 would be the same.

Selecting now from G any transformation V of order p:

$$V = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix},$$

we form the products VS, VS^2, VS^μ. Their characteristics (§ 89) and that of V will be denoted by $[VS]$, . . . , $[V]$, and we have

$$\begin{aligned} [V] &= a_1 + b_2 + c_3, \\ [VS] &= a_1\alpha_1 + b_2\alpha_2 + c_3\alpha_3, \\ [VS^2] &= a_1\alpha_1^2 + b_2\alpha_2^2 + c_3\alpha_3^2, \\ [VS^\mu] &= a_1\alpha_1^\mu + b_2\alpha_2^\mu + c_3\alpha_3^\mu. \end{aligned} \tag{4}$$

We now eliminate a_1, b_2, c_3 from these equations, obtaining

$$\begin{vmatrix} [V] & 1 & 1 & 1 \\ [VS] & \alpha_1 & \alpha_2 & \alpha_3 \\ [VS^2] & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \\ [VS^\mu] & \alpha_1^\mu & \alpha_2^\mu & \alpha_3^\mu \end{vmatrix} = 0. \tag{5}$$

Expansion and division by $(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ gives us

$$[VS^\mu] + K[V] + L[VS] + M[VS^2] = 0, \tag{6}$$

K, L, M being certain polynomials in $\alpha_1, \alpha_2, \alpha_3$, with the general term of the type $\alpha_1^a\alpha_2^b\alpha_3^c$. Since α_1, α_2, α_3 are powers of a primitive pth root of unity α (§ 116, 5°), the quantities K, . . . are certain sums of powers of α. Moreover, the characteristics $[V]$ . . . are each the sum of three roots of unity (§ 81, Ex. 7). If, therefore, the products in (6) were multiplied out, there would result an equation of the kind discussed in § 116, 6°. We

* The congruence (10) would here be of the first degree in μ.

could therefore carry out the process as explained in that paragraph, which gives us an equation of the form

$$(7)\qquad A(1+\alpha+\alpha^2+\ \ldots\ +\alpha^{p-1})+B(1+\beta+\beta^2\ \ldots\ +\beta^{q-1})$$
$$+C(1+\gamma+\gamma^2+\ \ldots\ +\gamma^{r-1})+\ \ldots\ =0,$$

A, B, C, . . . being certain sums of roots of unity; α, β, γ, . . . primitive roots of the equations $x^p=1$, $x^q=1$, $x^r=1$, . . . respectively; and p, q, r, . . . different prime numbers.

The coefficients A, B, C, . . . may be put into certain standard forms. Thus, any root $\epsilon\neq 1$ occurring in any of these sums will be assumed to be resolved into factors of prime-power indices (§ 116, 4°): $\epsilon=\epsilon_p\epsilon_q\epsilon_r\ \ldots$, the root ϵ_p being of index p^m, ϵ_q of index q^n, etc. Furthermore, within A any root ϵ_p will be assumed to be either unity or a root whose index is divisible by p^2. For, if it were of index p, say $\epsilon_p=\alpha^k$, we could put 1 in its place, since

$$\alpha^k(1+\alpha+\alpha^2+\ \ldots\ +\alpha^{p-1})\equiv\alpha^k+\alpha^{k+1}+\alpha^{k+2}+\ \ldots\ +\alpha^{k+p-1}$$
$$=1+\alpha+\alpha^2+\ \ldots\ +\alpha^{p-1}$$

by means of the relation $\alpha^p=1$. Likewise we assume that any root ϵ_q within B is either equal to unity or is a root whose index is divisible by q^2; and so on.

To illustrate, let i be a root of index 4 and τ a root of index 9 (namely $\tau^3=\omega$), and let $p=2$, $q=3$. Then the standard form for the expression

$$(8)\qquad (-i\omega-1)(1-1)+(\tau^2\omega-\omega^2+i)(1+\omega+\omega^2)$$

would be

$$(i^3\omega+1)(1-1)+(\tau^5-1+i)(1+\omega+\omega^2).$$

2°. We shall now make certain changes in the values of the roots in the equation (7). First we put 0 for every root ϵ_q, ϵ_r, . . . whose index is divisible by the square of a prime other than p^2 (as τ^5 in the example above), leaving undisturbed the roots whose indices are not divisible by such a square, as α, α^2, . . . , β, . . . The quantities A, B, . . . are thereby changed into certain sums A', B', . . . The equation (7) is still true, the vanishing sums $1+\alpha+\alpha^2+\ \ldots\ +\alpha^{p-1}$, etc., not having been affected.

Next we put 0 in place of $q-2$ of the roots $\beta, \beta^2, \ldots, \beta^{q-1}$, and -1 for the remaining root, thus changing $B'(1+\beta+\beta^2+\ldots+\beta^{q-1})$ into $B'(1+0+0+\ldots+(-1))$, so that this product still remains equal to zero. Similarly, we put 0 in place of $r-2$ of the roots $\gamma, \gamma^2, \ldots, \gamma^{r-1}$, and -1 for the remaining root, and so on. Proceeding thus, we shall ultimately change (7) into an equation of the form

$$A''(1+\alpha+\alpha^2+\ldots+\alpha^{p-1})=0,$$

where A'' contains roots of the form $\pm\epsilon_p$ only.

Finally, we put 1 in the place of every root $\alpha, \alpha^2, \ldots, \alpha^{p-1}$, as well as every root ϵ_p. The left-hand member may then no longer vanish, but will in any event become a multiple of p.

The final value of the expression (8) would be $(\omega+1)(1+1)=2$ or 0, according as ω is replaced by 0 or -1.

Notation 1. Any expression N which is a sum of roots of unity, changed in the manner described above, shall be denoted by N'_p.

3°. We shall now study the effect of these changes upon the left-hand member of (6). Each of the characteristics $[VS], \ldots, [VS^\mu]$, being the sum of three (unknown) roots of unity, will finally become one of the seven numbers $0, \pm1, \pm2, \pm3$, whereas $[V]$, being the sum of three roots of index 1 or p (cf. 1°), will become 3. The left-hand member of (6) will thus take the form

$$[VS^\mu]'_p+3K'_p+L'_p[VS]'_p+M'_p[VS^2]'_p, \tag{9}$$

and this number is a multiple of p (by 2°).

The values K'_p, L'_p, M'_p may be obtained by treating them as indeterminates 0/0. Thus,

$$K=\frac{-1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)}\begin{vmatrix}\alpha_1 & \alpha_2 & \alpha_3\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2\\ \alpha_1^\mu & \alpha_2^\mu & \alpha_3^\mu\end{vmatrix}, \quad K'_p=\frac{0}{0}.$$

We find

$$K'_p=-\tfrac{1}{2}(\mu-1)(\mu-2), \quad L'_p=\mu(\mu-2), \quad M'_p=-\tfrac{1}{2}\mu(\mu-1),$$

and if we substitute in (9) and multiply by $p-1$ we obtain the congruence:

$$[VS^\mu]'_p \equiv s\mu^2+t\mu+v \pmod{p}, \tag{10}$$

s, t, v being certain integers, the same for all values of μ.

We finally substitute in succession $\mu=0, 1, 2, \ldots, p-1$ in the right-hand member of (10). The remainders (mod p) should all lie between -3 and $+3$ inclusive, the interval of the values of $[VS^\mu]'_p$. Now, each of these seven remainders can correspond to at most two different values of μ less than p, if s and t are not both $\equiv 0 \pmod{p}$, by the theory of such congruences. Hence, there will correspond to the seven remainders at most 14 different values of μ, so that p is not greater than 14 unless $s\equiv t\equiv 0$. Trying $p=13$ and $p=11$, choosing for s, t, v the different possible sets of numbers $<p$ (the problem can be simplified by special devices)* we find that in no case can the remainders all be contained in the set $0, \pm 1, \pm 2, \pm 3$, unless $s\equiv t\equiv 0$ Choosing therefore this alternative we get, if $p>7$,

$$[VS^\mu]'_p \equiv v \pmod{p}.$$

In particular,

$$[VS]'_p \equiv v \equiv [V]'_p = 3 \pmod{p},$$

from which it follows that $[VS]'_p=3$. Again, from this equation we deduce that the roots of $[VS]$ are of index 1 or p. For, if the index of one of these roots were divisible by the square of a prime, or by a prime different from p, then the changes indicated in 2° could be made at the outset in such a way that 0 or -1 would take the place of this root. But then $[VS]'_p$ would be one of the numbers $0, \pm 1, \pm 2, -3$.

4°. Accordingly, the product VS of any two transformations both of order p is a transformation of order p or 1. The totality of such transformations in G, together with E, will

* Since $a\mu+b$ runs through the p values $0, 1, 2, \ldots, p-1 \pmod{p}$ when μ does, we may substitute this expression for μ in the right-hand member of (10) and select constants a, b so that this member takes a simpler form. For instance, if $p=11$, the right-hand member of (10) may be reduced by this substitution to one of the forms $\pm\mu^2+c$; μ; or c; according as $s\not\equiv 0$; $s\equiv 0$, $t\not\equiv 0$; $s\equiv t\equiv 0 \pmod{p}$. When $p=13$ we get the forms $\pm\mu^2+c$; $\pm 2\mu^2+c$; μ; c.

therefore form a group P. The order of this group must be a power of p, since it contains no transformations whose order differs from p or 1. Moreover, P is invariant in G, since an operator of order p is transformed into one of order p. Hence, G has an invariant subgroup P of order p^k. But this subgroup is abelian (§ 108, Corollary) and therefore G is intransitive or imprimitive (§ 108, Lemma).

Notation 2. A quantity N, which is the sum of a certain number of roots of unity, in which every root ϵ_p is replaced by 1, but in which none of the other changes indicated in 2° are carried out, will be denoted by N_p. If $N=0$, then $N_p \equiv 0 \pmod{p}$.

118. Theorem 14. *If a group G contains a transformation S of order $p^2\phi$, p being a prime >2, then there is an invariant subgroup H_p in G (not excluding the possibility $G=H_p$) which contains S^p. Any transformation in H_p, say T, has the property expressed by the following congruence:*

$$[V]_p \equiv [VT]_p \pmod{p}, \tag{11}$$

V being any transformation of G.

In the case $p=2$ the group G contains an invariant subgroup H_p if the order of S is p^3, and S^{p^2} will belong to H_p; also if $S=(-1, i, i)$, in which case S^2 will belong to H_p.

The proof follows the plan of that of the previous theorem. If $p>2$, we write S in canonical form, and construct the products VS, VS^2, VR, where R denotes S^p. Assuming that the three multipliers of S are all distinct, we obtain an equation corresponding to (6) in 1°:

$$[VR]+K[V]+L[VS]+M[VS^2]=0.$$

However, the changes indicated in 2° are not carried out except that 1 is put for every root ϵ_p whose index is a power of p (cf. Notation 2 above). The coefficients L, M become multiples of p by this change, and we find $K \equiv -1 \pmod{p}$. Hence finally,

$$[VR]_p - [V]_p \equiv 0 \pmod{p}.$$

Now consider all the conjugates $R_1, \ldots, R_k$ to R within G. They generate an invariant subgroup H_p (§ 14, Ex. 6), and

they all have the property of T as expressed by (11), since they fulfil the conditions of the theorem. Moreover, any transformation T in H_p satisfies the congruence (11), since such a transformation can be written as a product of powers of $R_1, \ldots, R_h$. For instance, let $T=R_1R_2$, and we have

$$[VR_1]_p \equiv [V]_p, \quad [(VR_1)R_2]_p \equiv [(VR_1)]_p \pmod{p}.$$

Hence,

$$[VT]_p = [VR_1R_2]_p \equiv [VR_1]_p \equiv [V]_p.$$

119. The Invariant Group H_p. The order of this group is a power of p. For, if its order contained a prime factor q, $q \neq p$, there would be a transformation of order q in H_p, say T. Then, if E represents the identical transformation, we have by (11),

$$[T^j]_p = [ET^j]_p \equiv [E]_p = 3 \pmod{p}.$$

Hence, the multipliers of T being α, β, γ, we have

$$\alpha^j + \beta^j + \gamma^j \equiv 3 \pmod{p},$$

and therefore

$$\sum_{j=1}^{q} \alpha^{-j}(\alpha^j + \beta^j + \gamma^j) \equiv 3 \sum_{j=1}^{q} \alpha^{-j}. \tag{12}$$

Unless T is a similarity-transformation (which we may assume it is not), the roots α, β, γ are not all equal. Hence, the left-hand sum is $2q$ or q according as α is or is not equal to one of the roots β, γ. The right-hand sum is, however, $3q$ or zero, according as α is or is not unity. It follows that the congruence is impossible except when $p=2$, and α is one of the roots β, γ, or unity. Substituting β^{-j} and γ^{-j} for α^{-j} in (12) we get similar results. Collecting these, we finally discover that in no case can $q \neq p$.

The order of H_p is accordingly a power of p, and the group is monomial (Theorem 10). The possibility $G=H_p$ is accordingly untenable if G is primitive.

COROLLARY. *No primitive simple group can contain a transformation of order $p^2\phi$ if $p>2$; or p^3 if $p=2$.*

120. Theorem 15. *No primitive simple group can contain a transformation S of prime order p, $p>3$, which has at most two distinct multipliers.*

Let $S=(\alpha_1, \alpha_1, \alpha_2)$ * and assume first that $p=7$. This transformation leaves invariant a point $(x_1=x_2=0)$ and every straight line through it. This will also be the case with any other transformation S' conjugate to S (Theorem 3). Therefore, the line joining the two invariant points is invariant for both S and S'. If now the variables be changed so that the common invariant line is $y_1=0$, the group generated by S and S' will be reducible and therefore intransitive, breaking up into a group in one variable (y_1) and one in two variables (y_2, y_3). But, there being no primitive or imprimitive finite linear groups in two variables generated by two transformations of order $p=7$ (cf. Chapter X), it follows that S and S' are commutative.

Accordingly, all the conjugates to S are mutually commutative and generate an abelian group, which must be invariant in G (§ 14, Ex. 6), and the latter cannot be primitive (§ 108, Lemma).

Next, let $p=5$. If S and S' are not commutative, they generate the icosahedral group (E), § 103, in the variables y_2, y_3. This contains a transformation of order 3 whose multipliers are ω, ω^2, and a similarity-transformation whose multipliers are $-1, -1$ (cf. § 97). The product of these two transformations, as a transformation in the variables y_1, y_2, y_3, can be written in the canonical form $T=(1, -\omega, -\omega^2)$. But such a transformation is excluded by the next theorem [put $S_1=T^2=(1, \omega^2, \omega)$ and $S_2=T^3=(1, -1, -1)$].

121. Theorem 16. *No primitive simple group can contain a transformation S of order pq, where p and q are different prime numbers, and $S_1=S^p$ has three distinct multipliers, while $S_2=S^q$ has at least two.*

Let S be written in canonical form and assume $S_1=(\alpha_1, \alpha_2, \alpha_3)$. We then construct the transformations V, VS_2, VS_1, VS_1^2 and proceed as in § 117, 1°, obtaining an equation corre-

* Such a transformation is called a ***homology***.

sponding to (5). After putting unity for every root of index p^k, the equation becomes the congruence:

$$\{[VS_2]_p - [V]_p\}(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1) \equiv 0 \pmod{p},$$

which can be changed into the following:

$$\{[VS_2]_p - [V]_p\}q^3 \equiv 0$$

after multiplying by a suitable factor, since

$$(1-\epsilon)(1-\epsilon^2) \ldots (1-\epsilon^{q-1}) = \lim_{x=1} \frac{x^q-1}{x-1} = q$$

when ϵ is a primitive qth root of unity.

Hence finally,

$$[VS_2]_p \equiv [V]_p \pmod{p},$$

and the argument of § 118 is now valid.

COROLLARY. *No primitive simple group can contain a transformation of order* 35, 15ϕ, or 21ϕ. (If S_1, representing respectively S^7, $S^{3\phi}$, or $S^{3\phi}$, has not three distinct multipliers, Theorem 15 applies.)

122. The Sylow Subgroups. Consider now a primitive group G of order $g\phi$. A possible subgroup of order 5^2 or 7^2 would be abelian (§ 108, Cor.). By trial we find readily that no such group can be constructed without violating Theorem 15 or the Corollary to Theorem 14. Again, if g is divisible by 35, we have a transformation of this order (§ 135, Cor. 3). But this is impossible in a primitive simple group (§ 121, Cor.).

A subgroup of order $3^k\phi$ is monomial, and contains an abelian subgroup of order $3^{k-1}\phi$ at least. Assume $k \geqq 3$; we then have an abelian subgroup P' of order $3^2\phi$.. When we construct such a group, avoiding the invariant subgroup H_p resulting from Theorem 14, we discover that it must contain a transformation of type $T=(\epsilon, \epsilon, \epsilon\omega^2)$, where $\epsilon^3=\omega$. Then if g is divisible by 5 or 7 at the same time, we would have a transformation of order 15ϕ or 21ϕ (§ 135, Cor. 3), violating the Corollary, § 121. In any event, we can have no abelian subgroup of order $3^{k-1}\phi$ if $k>3$ (cf. Ex. 4, § 109).

Finally, a subgroup of order 2^k is monomial and contains an abelian subgroup of order 2^{k-1} at least. By trial we find that $k-1 \leqq 2$ (cf. Ex. 3, § 109).

Collecting our results, we find that g is a factor of one of the numbers

$$2^3 \cdot 3^3, \quad 2^3 \cdot 3^2 \cdot 5, \quad 2^3 \cdot 3^2 \cdot 7,$$

and the question arises what simple groups can have such orders.

Now, all simple groups whose orders do not exceed the largest of these numbers have been listed. There are four possibilities:

$$g = 60, \quad 360, \quad 168, \quad 504.$$

123. The Three Types of Primitive Simple Groups. The first two of the numbers just given are the orders of the alternating groups on 5 and 6 letters, and the last two the orders of certain transitive substitution groups on 7 and 8 letters (§ 20). The last case may be excluded from consideration for the reason that we should here have a Sylow subgroup of order 8 which is abelian and generated by three operators each of order 2 (§ 20, Ex. 3). But no such group can be constructed in three variables, as may be found by trial.

In the other cases the corresponding types may be constructed after a set of generators and their generational relations are given (cf. § 103, and Ex. 2, ibid.). The variables are selected so that the generators appear in as simple a form as possible; for instance, some one of them is always written in canonical form at the outset. We shall omit the details here; it would afford excellent practice for the student to carry out this work.

(H) Group of order 60 generated by E_1, E_2, E_3, satisfying the relations:*

$$E_1^3 = E_2^2 = E_3^2 = 1, \quad (E_1E_2)^3 = (E_2E_3)^3 = 1, \quad (E_1E_3)^2 = 1;$$

namely:

$$E_1\colon\ x_1 = x'_2, \quad x_2 = x'_3, \quad x_3 = x'_1;$$

$$E_2 = (1, \quad -1, \quad -1);$$

$$E_3\colon\ x_1 = \tfrac{1}{2}(-x'_1 + \mu_2 x'_2 + \mu_1 x'_3), \quad x_2 = \tfrac{1}{2}(\mu_2 x'_1 + \mu_1 x'_2 - x'_3),$$
$$x_3 = \tfrac{1}{2}(\mu_1 x'_1 - x'_2 + \mu_2 x'_3);$$

* E. H. Moore, *Proceedings of the London Mathematical Society*, vol. 28, p. 357.

where

$$\mu_1 = \tfrac{1}{2}(-1+\sqrt{5}), \quad \mu_2 = \tfrac{1}{2}(-1-\sqrt{5}).$$

(I) Group of order 360ϕ, generated by E_1, E_2, E_3 of (H) and E_4, where

$$E_4^2 = 1, \quad (E_1E_4)^2 = (E_2E_4)^2 = (E_3E_4)^3 = 1;$$

E_4: $\quad x_1 = -x'_1, \quad x_2 = -\omega x'_3, \quad x_3 = -\omega^2 x'_2.$

(J) Group of order 168 generated by S, T, R with the relations (cf. § 20, Ex. 2)

$$S^7 = T^3 = R^2 = 1, \quad T^{-1}ST = S^4, \quad R^{-1}TR = T^2, \quad (RS)^4 = 1;$$

namely:

$$S = (\beta, \beta^2, \beta^4);$$

$$T: \quad x_1 = x'_2, \quad x_2 = x'_3, \quad x_3 = x'_1;$$

$$R: \quad x_1 = h(ax'_1 + bx'_2 + cx'_3), \quad x_2 = h(bx'_1 + cx'_2 + ax'_3),$$
$$x_3 = h(cx'_1 + ax'_2 + bx'_3);$$

where

$$\beta^7 = 1, \quad a = \beta^4 - \beta^3, \quad b = \beta^2 - \beta^5, \quad c = \beta - \beta^6,$$

$$h = \tfrac{1}{7}(\beta + \beta^2 + \beta^4 - \beta^6 - \beta^5 - \beta^3) = -\frac{1}{\sqrt{-7}}.$$

124. Primitive Groups Having Invariant Primitive Subgroups. We have already determined the primitive groups containing an invariant subgroup of order 2^λ or 3^λ (§§ 114–115). The possibility of a subgroup H_p shall therefore be excluded from consideration (cf. § 119).

Let us assume that the group (H) is contained invariantly in a larger group (H′) of order $60h\phi$. In (H) we have 6 subgroups of order 5, which must be permuted among themselves by (H′). One of them must therefore be invariant in a subgroup of (H′) of order $60h\phi/6 = 10h\phi$. But no such group can be constructed if $h > 1$ without introducing the group H_p.

In this manner the cases (I) and (J) may be disposed of. There are left the cases (E), (F), (G). Now, these groups all permute among themselves a single set of four triangles. This set is therefore also permuted among themselves by a larger group including either (E), (F) or (G) invariantly. But the groups having this property were found in § 115 to be just these three.

EXERCISES

1. Determine the linear groups in two variables by the method of this chapter. (To determine the primitive simple groups, show first that the order of such a group is a factor of 60ϕ).

2. Prove by the method of § 120 that a primitive group in four variables cannot contain a transformation whose order is greater than 5, if its characteristic equation has only two distinct roots.

3. Why is it necessary to add the statement "while $S_2=S^q$ has at least two" (distinct multipliers) at the end of Theorem 16?

4. Obtain the group (H) by the method of Ex. 2, § 103, in the following form:

$$S=(abcde)=(1,\ \epsilon^4,\ \epsilon);$$

$$U=(ad)(bc):\quad x_1=-x'_1,\quad x_2=-x'_3,\quad x_3=-x'_2;$$

$$T=(ab)(cd):\quad x_1=\frac{1}{\sqrt{5}}(x'_1+x'_2+x'_3),$$

$$x_2=\frac{1}{\sqrt{5}}(2x'_1+sx'_2+tx'_3),\quad x_3=\frac{1}{\sqrt{5}}(2x'_1+tx'_2+sx'_3);$$

where

$$\epsilon^5=1,\qquad s=\epsilon^2+\epsilon^3,\qquad t=\epsilon+\epsilon^4,\qquad \sqrt{5}=t-s.$$

Show also that (E) as given in Ex. 2, § 103, transforms the variables $y_0=-x_1x_2$, $y_1=x_2^2$, $y_2=-x_1^2$ into linear functions of themselves and hence appears as a linear group in three variables, which is precisely the group (H) as just exhibited if we write y_0, y_1, y_2 for x_1, x_2, x_3 respectively in (H).

5. Obtain the group (I) by adding a transformation $W=(ad)(ef)$ to the list S, U, T of (H), Ex. 4, and show that

$$W:\quad x_1=\frac{1}{\sqrt{5}}(x'_1+\lambda_1x'_2+\lambda_1x'_3),\quad x_2=\frac{1}{\sqrt{5}}(2\lambda_2x'_1+sx'_2+tx'_3),$$

$$x_3=\frac{1}{\sqrt{5}}(2\lambda_2x'_1+tx'_2+sx'_3);$$

where

$$\lambda_1=\tfrac{1}{4}(-1\pm\sqrt{-15}),\quad \lambda_2=\tfrac{1}{4}(-1\mp\sqrt{-15}).$$

In this and the previous example we need not verify that the transformations obtained actually generate the respective groups as soon as they have been fully determined from a number of arbitrarily chosen relations, since just one type of each group (H) and (I) has been shown to exist by the generational relations given in § 123. (In determining W, account has to be taken of the fact that (I) contains similarity-transformations; cf. the determination of (E), § 103.)

125. Invariants of the Linear Groups in Three Variables. The theory of these invariants is by no means so simple as the theory of the invariants for the groups in two variables, and it is beyond the scope of this book to enter into a general discussion, except as to indicate the principal results.

In all cases we have a set of fundamental invariants such that all others are rational integral functions of these.* We shall here give such sets for the groups (G), (H), (I) and (J). That they are invariants may be verified directly by the student.

(G) If we introduce the abbreviations

$$x_1x_2x_3=\phi, \quad x_1^3+x_2^3+x_3^3=\psi, \quad x_1^3x_2^3+x_2^3x_3^3+x_3^3x_1^3=\chi,$$

the fundamental set consists of the functions †

$$\begin{aligned} C_6&=\psi^2-12\chi;\\ C_9&=(x_1^3-x_2^3)(x_2^3-x_3^3)(x_3^3-x_1^3);\\ C_{12}&=\psi(\psi^3+216\phi^3);\\ D_{12}&=\phi(27\phi^3-\psi^3); \end{aligned}$$

which satisfy the relation

$$(432C_9^2-C_6^3+3C_6C_{12})^2=4(1728D_{12}^3+C_{12}^3).$$

(H) Here we have four fundamental forms. One of them is

$$A=x_1^2+x_2x_3,$$

if we take the group as given in § 124, Ex. 4.

The other three can be obtained in a manner similar to that which we employed in the case of the group (E), § 105. We select a linear invariant f_1 for each of a set of subgroups of (H) of orders 10, 6, 4, respectively, and form the products of the 6, 10, 15 different linear expressions into which f_1 is transformed by (H). Selecting, for instance, the group generated by S and U, Ex. 4, § 124, for the subgroup of order 10, we get $f_1=x_1$ and a corresponding invariant

$$\begin{aligned} B_1=&x_1(x_1+x_2+x_3)(x_1+\epsilon^4x_2+\epsilon x_3)(x_1+\epsilon x_2+\epsilon^4x_3)\\ &\cdot(x_1+\epsilon^3x_2+\epsilon^2x_3)(x_1+\epsilon^2x_2+\epsilon^3x_3)\\ =&x_1(x_2^5+x_3^5+5x_1x_2^2x_3^2-5x_1^3x_2x_3+x_1^5). \end{aligned}$$

* Cf. Dickson, *Algebraic Invariants* (Wiley & Sons), New York, 1914, p. 70 ff.

† Maschke, *Mathematische Annalen*, Bd. 33 (1889), pp. 325–326.

These invariants must evidently be transformed into the functions f, H, T of the group (E), § 105, by the substitution of $-x_2x_1$, x_2^2, $-x_1^2$ for x_1, x_2, x_3 respectively (cf. Ex. 4, § 124). The relation among the invariants A, B_1, . . . corresponding to that connecting f, H, T is of degree 30 in the variables x_1, x_2, x_3, and its determination may be left as an exercise for the student.*

(I) The fundamental invariants are four in number.† One is the function

$$F=A^3+\lambda B_1,$$

where (taking for (I) the group given in Ex. 5, § 124) A and B_1 are the functions listed above under (H), and

$$\lambda=\frac{-9\pm 3\sqrt{-15}}{20}.$$

The three other invariants are obtained by evaluating the Hessian of F:

$$X=\begin{vmatrix} F_{11} & F_{12} & F_{13} \\ F_{21} & F_{22} & F_{23} \\ F_{31} & F_{32} & F_{33} \end{vmatrix};$$

then the bordered Hessian:

$$Y=\begin{vmatrix} F_{11} & F_{12} & F_{13} & X_1 \\ F_{21} & F_{22} & F_{23} & X_2 \\ F_{31} & F_{32} & F_{33} & X_3 \\ X_1 & X_2 & X_3 & 0 \end{vmatrix};$$

and finally the Jacobian of F, X, and Y.

(J) As in the previous case, the fundamental invariants are four in number; ‡ a function

$$f=x_1^3x_3+x_2^3x_1+x_3^3x_2;$$

the Hessian of f (say X); the Hessian of f bordered by the first derivatives of X (as Y above); finally, the Jacobian of the three functions already determined.

* Cf. Klein, *Vorlesungen über das Ikosaeder*, Leipzig, 1884, p. 219.

† Wiman, *Mathematische Annalen*, Bd. 47 (1896), pp. 548–556.

‡ Klein, *Mathematische Annalen*, Bd. 14 (1879), pp. 446–448.

EXERCISES

1. Construct a fundamental set of invariants for the groups (E) and (F).

2. The invariant D_{12} under (G) is the product of the four functions t_1, t_2, t_3, t_4, § 113. Are there other relations among the invariants C_8, C_9, C_{12}, D_{12} and the functions t_1, t_2, t_3, t_4?

126. Order of a Primitive Group in n Variables. In conclusion we shall state some general results bearing on the order of a primitive group G in n variables.

The Theorem 13 admits of generalization to n variables as follows. The number of the equations (4) would now be $n+1$, the left-hand members being $[V], \ldots, [VS^{n-1}]$ and $[VS^{\mu}]$. Eliminating $a_1, b_2, \ldots$, we obtain the corresponding equation (5), from which a congruence similar to (10) is derived:

$$[VS^{\mu}]'_p \equiv s\mu^{n-1} + t\mu^{n-2} + v\mu^{n-3} + \ldots \pmod{p}.$$

In this we substitute in succession $\mu = 0, 1, \ldots, p-1$. The left-hand members are integers having the $2n+1$ values ranging from $-n$ to $+n$ inclusive, and for each such value we can have at most $n-1$ values of μ by the theory of congruences, unless the right-hand member is merely a constant. Hence, excluding this possibility, there are at most $(n-1)(2n+1)$ values of μ corresponding to the values assumed by the right-hand members; accordingly, if $p > (n-1)(2n+1)$, the right-hand member is a constant merely, or

$$[VS^{\mu}]'_p \equiv [V]'_p = 3 \pmod{p}.$$

From this it follows as in § 117, 4°, that the group has an invariant abelian subgroup of order p^k and cannot be primitive. Hence, *the order of a primitive linear group in n variables cannot be divisible by a prime greater than* $(n-1)(2n+1)$.

The Theorem 14 may similarly be generalized to read: *if a group G contains a transformation S of order $p^k\phi \geq pn\phi$, then there is an invariant subgroup H_p in G whose transformations have the property*

$$[V]_p \equiv [VT]_p \pmod{p},$$

where V and T represent any transformations of G and H_p respectively.

By a different principle it can be proved that a primitive group G in n variables cannot contain an abelian subgroup of order $h\phi > k^{n-1}\phi$, where k is a number ranging from 3.7 to 5, depending upon the nature of the prime factors of h. By means of this theorem and some of those given above it is possible to set a fairly low limit to the order $g\phi$ of G, as we shall proceed to do.

A Sylow subgroup of G of order p^a is monomial and must accordingly contain an abelian subgroup of order p^{a-b} at least, where p^b denotes the highest power of p which divides $n!$ (cf. §9, Ex. 2). Hence, by the theorem mentioned above, we must have

$$p^a \leqq p^b 5^{n-1}\phi,$$

so that finally that portion of g which is made up of prime factors not greater than n is not greater than $n!5^{(n-1)\theta(n)}$, where $\theta(n)$ denotes the number of primes smaller than $n+1$. Again, if $n+1$ is a prime and is a factor of g, the corresponding Sylow subgroup is abelian (§ 108, Cor.) and its order is $\leqq 5^{n-1}$. Finally, by Theorem 11, § 109, the remaining factor of g is the order of an abelian group and is also $\leqq 5^{n-1}$. It follows that the order of a primitive group in n variables is

$$g\phi \leqq n!5^{(n-1)\theta(n)+2}\phi.$$

HISTORICAL NOTE. In 1878 Jordan proved the classical theorem that the order of a finite linear group in n variables is of the form λf, where f is the order of an abelian self-conjugate subgroup, and where λ is inferior to a fixed number which depends only upon n (*Journal für die reine und angewandte Mathematik*, Bd. 84, p. 91). Definite limits to λ have been given by Schur for the case where the characteristics belong to a given algebraic domain (*Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften*, 1905, p. 77 ff.); by Bieberbach and Frobenius (*Sitzungsberichte, etc.*, 1911, p. 231 ff and p. 241 ff); and by the author (*Transactions of the American Mathematical Society*, vol. 5 (1904), pp. 320–321 for primitive groups; vol. 6 (1905), p. 232 for imprimitive groups). The derivation of the limit given above has not been published.

Concerning the linear groups in three variables, the following papers may be consulted: Jordan, *l.c.*, p. 125 ff; Valentiner, *De endelige Transformations-Gruppers Theori*, Copenhagen, 1889; Mitchell, *Transactions of the American Mathematical Society*, vol. 12 (1911), pp. 207–242; and the author, *Mathematische Annalen*, Bd. 63 (1907), pp. 552–572.

CHAPTER XIII

THE THEORY OF GROUP CHARACTERISTICS

127. Introduction and Definitions. This theory was initiated by Frobenius and is largely due to him,* though Schur† and Burnside ‡ simplified the theory and added important applications. We shall devote this chapter to an exposition of the main points of the theory by a process differing somewhat from the methods employed by the authors cited.

We consider a linear group in n variables $x_1, x_2, \ldots, x_n$,

$$G: \qquad S_1, S_2, \ldots, S_g,$$

whose transformations are not now necessarily of determinant unity. As noted in § 89, the sum of the multipliers of S_t, which is equal to the sum of the elements in the principal diagonal of the matrix of S_t, is called the *characteristic* of S_t and is denoted by χ_t or $\chi(S_t)$.§ Since χ_t is the sum of n roots of unity (§ 81, Ex. 7, and § 95), and since the conjugate-imaginary of a root of unity is its reciprocal, it follows that $\overline{\chi}_t$, the conjugate-imaginary of χ_t, is the characteristic of S_t^{-1}. That is,

$$\overline{\chi}(S_t) = \chi(S_t^{-1}), \quad \chi(S_t) = \overline{\chi}(S_t^{-1}).$$

* *Sitzungsberichte der Kgl. Preussischen Akademie der Wissenschaften*, 1896, p. 985, 1343; 1897, p. 994; 1899, p. 482.

† *Sitzungsberichte*, etc., 1905, p. 406; *Journal für die reine und angewandte Mathematik*, Bd. 127 (1904), pp. 20–50; Bd. 132 (1907), pp. 85–137; Bd. 139 (1910), pp. 155–250.

‡ *Acta Mathematica*, vol. 28 (1904), pp. 369–387; *Proceedings of the London Mathematical Society*, 1904, pp. 117–123; *Theory of Groups of Finite Order*, second edition, Cambridge, 1911, p. 243 ff.

See also a paper by Molien in *Sitzungsberichte*, etc., for 1897, pp. 1152–1156.

§ Frobenius and Schur call the set of quantities $\chi_1, \ldots, \chi_g$ a *character* of G. In their terminology, an abstract group G would possess as many *simple* characters as there are non-equivalent linear groups to which G is simply or multiply isomorphic (cf. § 131).

A function $f(x_1, \ldots, x_n)$ which is transformed into a constant multiple of itself by every transformation of G is called an *invariant* of G. It is an *absolute invariant* if the constant multiplier is unity for every transformation of G; otherwise it is a *relative invariant.*

A series of invariants $f_1, \ldots, f_k$ are said to be *independent* of each other if the variables $x_1, \ldots, x_n$ cannot be eliminated from the equations

$$f_1 = a_1, \ldots, f_k = a_k,$$

where $a_1, \ldots, a_k$ are arbitrary constants. They are said to be *linearly independent* if no identity exists of the form

$$b_1 f_1 + \ldots + b_k f_k = 0,$$

where $b_1, \ldots, b_k$ are constants, not all zero.

We shall as hitherto denote by $(f)S$ the result of operating upon a function f by a transformation S.

128. Theorem 17. *The number of linearly independent absolute invariants of G of the first degree in $x_1, \ldots, x_n$ is*

$$\frac{1}{g}\sum_{t=1}^{g} \chi_t.$$

Proof. 1°. If $\Sigma\chi_t \neq 0$, then G will have an absolute invariant of the first degree. For, let $y_1, \ldots, y_n$ be arbitrary constants, and let $f = y_1x_1 + \ldots + y_nx_n$. Then the function

$$(f)S_1 + \ldots + (f)S_g \equiv F$$

will be an absolute invariant of G provided that it does not vanish identically. This is seen as follows. We have

$$(F)S_t = (f)S_1S_t + \ldots + (f)S_gS_t = (f)S_1 + \ldots + (f)S_g = F.$$

Thus, F is an absolute invariant unless it vanishes. If it does, then $\Sigma\chi_t = 0$. For, the sum of the coefficients of y_1x_1, $y_2x_2, \ldots, y_nx_n$ in $(f)S_t$ is readily found to be χ_t. Hence, at least one of these terms will be present in F if $\Sigma\chi_t \neq 0$; say y_1x_1. If therefore we put $y_1 = 1$, $y_2 = \ldots = y_n = 0$, the function F will contain a term involving x_1 and hence it does not vanish.

2°. Let us now suppose that G has just k linearly independent absolute invariants of the first degree. We may assume that the n variables were chosen originally such that $x_1, x_2, \ldots, x_k$ are the invariants in question. Then G is intransitive, breaking up into $k+1$ sets of intransitivity, containing respectively 1, 1, . . . , 1; $n-k$, variables: x_1, $x_2, \ldots, x_k$; $(x_{k+1}, \ldots, x_n)$, by Theorem 6.

Thus, if $n=2$, $k=1$, and if x_1 is the absolute invariant, the matrix of any transformation of G will be of the form

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}.$$

The reducible group may now be transformed into an intransitive group of the following special form

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

The characteristic $\chi(S_t)$ is accordingly equal to $k+\chi(S'_t)$, where S'_t is the transformation corresponding to S_t in that component of G which involves the set $(x_{k+1}, \ldots, x_n)$. Now, $\Sigma\chi(S'_t)=0$, or we would have a new invariant by 1°. Hence,

$$\sum_{t=1}^{g} \chi(S_t) = kg,$$

which completes the proof.

COROLLARY 1. *The number of linearly independent absolute invariants of degree m in $x_1, \ldots, x_n$ is*

$$\frac{1}{g}\sum_{t=1}^{g} \chi(S_t^{(m)}),$$

where $\chi(S_t^{(m)})$ represents the sum of the homogeneous products of degree m in the multipliers of S_t, namely

$$\alpha_1^m+\alpha_2^m+ \ldots +\alpha_1^{m-1}\alpha_2+ \ldots +\alpha_1^{m-2}\alpha_2\alpha_3+\ldots$$

Proof. For brevity we take $n=m=2$. When the variables x_1, x_2 are subjected to a linear transformation

$$S=\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

the products of x_1, x_2 of the second degree, namely x_1^2, x_1x_2, x_2^2, are correspondingly subjected to a linear transformation

$$S^{(2)} = \begin{vmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{vmatrix};$$

and to a group G of transformations S, . . . will correspond an isomorphic group $G^{(2)}$ of transformations $S^{(2)}$, ... If S is written in canonical form (α, β), so is $S^{(2)}$, namely $(\alpha^2, \alpha\beta, \beta^2)$. Hence $\chi(S^{(2)}) = \alpha^2+\alpha\beta+\beta^2$.

We now apply Theorem 17 to the group $G^{(2)}$ and obtain the Corollary 1 for the case $n=m=2$.

COROLLARY 2. *In the case of a transitive group,* $\sum_{t=1}^{t=g}\chi_t = 0$. For, in this case there are no invariants of the first degree.

By an elaboration of this principle we obtain the important result that if Φ_t represents any given integral symmetric function with integral coefficients of the multipliers of S_t, then $\sum_{t=1}^{t=g}\Phi_t = lg$, where l is a positive or negative integer or zero.*

EXERCISES

1. Write a given substitution group as a linear group so that the letters of the former are the variables of the latter, and determine the characteristics.

2. Prove that the average number of letters which remain unchanged by a substitution of a transitive substitution group G is equal to unity. (Prove first that G contains a single absolute invariant of the first degree.)

129. Lemma. Let there be given a function

$$f = X_1Y_1 + \ldots + X_kY_k,$$

where $X_1, \ldots, X_k$ are linear functions of $x_1, \ldots, x_n$, the variables of a group G', and $Y_1, \ldots, Y_k$ linear functions of $y_1, \ldots, y_m$, the variables of a group G'' simply isomorphic with G'. We may assume that $X_1, \ldots, X_k$ (as well as $Y_1, \ldots, Y_k$) are linearly independent of each other; if it were possible to

* See *Transactions of the American Mathematical Society*, vol. 5 (1904), p. 464 ff.

write, say, $X_k = a_1X_1 + \ldots + a_{k-1}X_{k-1}$, the function f could be expressed in fewer than k terms:

$$X_1(Y_1 + a_1Y_k) + X_2(Y_2 + a_2Y_k) + \ldots + X_{k-1}(Y_{k-1} + a_{k-1}Y_k) = X_1Y'_1 + X_2Y'_2 + \ldots + X_{k-1}Y'_{k-1}.$$

Now if f be unaltered when operated upon simultaneously by corresponding transformations of G' and G'' (in other words, if f is a bilinear invariant), and if $k<n$, G' is intransitive.

Proof. For the sake of simplicity take $k=3$. The variables of G' and G'' may be so chosen that $f = x_1y_1 + x_2y_2 + x_3y_3$.

A transformation of G' will change x_1, x_2, x_3 into three linearly independent functions of $x_1, \ldots, x_n$, and the corresponding transformation of G'' will change y_1, y_2, y_3 into three linearly independent functions of $y_1, \ldots, y_m$. Let the resulting expression be $f' = X'_1Y'_1 + X'_2Y'_2 + X'_3Y'_3$, and we should have $f \equiv f'$. But this implies that X'_1, X'_2, X'_3 are linear functions of x_1, x_2, x_3. Hence, if $n>3$, G' is reducible and accordingly intransitive.

130. Theorem 18. *Representing by $\bar{\chi}_t$ the conjugate-imaginary of χ_t we have, for a transitive group G,*

$$\sum_{t=1}^{\rho} \chi_t\bar{\chi}_t = g.$$

Proof. Let $\bar{G}$ be the conjugate-imaginary group of G (§ 92). Then, if S and $\bar{S}$ are corresponding transformations of G and $\bar{G}$:

$$S = \begin{pmatrix} a & b & \ldots \\ c & d & \ldots \\ . & . & \ldots \end{pmatrix}, \quad \bar{S} = \begin{pmatrix} \bar{a} & \bar{b} & \ldots \\ c & \bar{d} & \ldots \\ . & . & \ldots \end{pmatrix},$$

the n^2 products $x_1\bar{x}_1$, $x_1\bar{x}_2$, $\ldots$, $x_n\bar{x}_n$ are subjected to a corresponding linear transformation S' belonging to a group K isomorphic with G and $\bar{G}$:

$$S' = \begin{pmatrix} aa & a\bar{b} & \ldots \\ a\bar{c} & a\bar{d} & \ldots \\ . & . & \ldots \end{pmatrix}.$$

The characteristic of S' is the product of the characteristics of S and $\bar{S}$: $\chi(S')=\chi(S)\chi(\bar{S})$ (this is seen readily when S (and therefore $\bar{S}$ and S') is written in canonical form). Hence, by Theorem 17, the number of linearly independent absolute invariants of the first degree in the variables of K is $\sum\chi_t\bar{\chi}_t/g$. Any such invariant can be thrown into the form

$$f=X_1\bar{x}_1+X_2\bar{x}_2+\ \ldots\ +X_n\bar{x}_n,$$

where $X_1, \ldots, X_n$ are linear functions of $x_1, \ldots, x_n$.

We know one such invariant already, namely the Hermitian invariant (§ 92), and we may assume the variables originally so chosen in G and $\bar{G}$ that this invariant is

$$I=x_1\bar{x}_1+x_2\bar{x}_2+\ \ldots\ +x_n\bar{x}_n.$$

Then, if λ be any constant, the expression

$$f+\lambda I=(X_1+\lambda x_1)\bar{x}_1+(X_2+\lambda x_2)\bar{x}_2+\ \ldots\ +(X_n+\lambda x_n)\bar{x}_n$$

is also an invariant.

Now, the constant λ may always be determined such that $X_1+\lambda x_1, X_2+\lambda x_2, \ldots, X_n+\lambda x_n$ are not linearly independent. Therefore either G is intransitive by the lemma above, or $f+\lambda I$ vanishes identically. Hence, since the first alternative violates the assumption of the theorem, any invariant f of K is merely a constant multiple of I (viz., $f=-\lambda I$); in other words, the number $\sum\chi_t\bar{\chi}_t/g$ of linearly independent invariants f is unity. The theorem follows.

EXERCISE

Prove that if G is intransitive, $\sum\chi_t\bar{\chi}_t=lg$, where l is a positive integer greater than 1.

131. Equivalence. Two simply isomorphic groups are *equivalent* if a suitable change of variables in one will make the matrices of their corresponding transformations identical. If no such choice of variables is possible, the groups are *non-equivalent.*

For example, the groups generated by the transformations

$$S=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\quad T=(1,\ -1)$$

are equivalent. If we put $y_1=x_1+x_2$, $y_2=x_1-x_2$ in S, then this transformation takes the form $(1, -1)$ in the variables y_1, y_2.

THEOREM 19. *Let* $G'=(S'_1, S'_2, \ldots, S'_g)$ *and* $G''=(S''_1, S''_2, \ldots, S''_g)$ *be simply isomorphic linear groups in* n *and* m *variables respectively, and let* G' *be transitive. Then if* $\overline{S''_t}$ *represents the conjugate-imaginary of the transformation* S''_t,

$$\sum_{t=1}^{g} \chi(S'_t)\,\chi(\overline{S''_t}) = kg,$$

where $k=0$ *or a positive integer. If* $k=1$, G'' *is equivalent to* G'; *if* $k>1$, G'' *is intransitive, and in this case* k *of its sets of intransitivity are transformed according to* k *groups each equivalent to* G'.

Proof. Let $x_1, \ldots, x_n$ be the variables of G' and $y_1, \ldots, y_m$ those of G''. We construct the group K in the nm variables $x_1\bar{y}_1, \ldots, x_n\bar{y}_m$, where $\bar{y}_1, \ldots, \bar{y}_m$ are the conjugate-imaginaries of the variables of G''. Applying Theorem 17 we find k linearly independent absolute invariants of K all of the form $a_{11}x_1\bar{y}_1+\ldots+a_{nm}x_n\bar{y}_m$. By a suitable change of variables in G'' we now cause one of these invariants to become $x_1\bar{y}_1+x_2\bar{y}_2+\ldots+x_n\bar{y}_n$, and comparing this with the Hermitian invariant $x_1\bar{x}_1+\ldots+x_n\bar{x}_n$ of G' we may readily prove that G'' transforms the variables $y_1, \ldots, y_n$ among themselves according to a group equivalent to G'. Hence, if $k=1$ and $m=n$, G' and G'' are equivalent; if $k\geq 1$ and $m>n$, G'' is reducible and therefore intransitive.

Conversely, if G'' is known to break up into sets of intransitivity, k of which are transformed according to groups which are equivalent to G', then the conjugate-imaginaries of the variables $y_1, \ldots, y_n$ of any one of these sets will combine with $x_1, \ldots, x_n$ to form one invariant $x_1\bar{y}_1+\ldots+x_n\bar{y}_n$ for K, making k such invariants in all.

COROLLARY 1. *If* G' *and* G'' *are equivalent, their corresponding characteristics are equal, and*

$$\chi(S'_1)\cdot\chi(\overline{S''_1})+\ldots+\chi(S'_g)\cdot\chi(\overline{S''_g})=g,$$

if they are non-equivalent and are both transitive, this sum vanishes.

COROLLARY 2. *Let G be a transitive linear group of order g in n variables, and let H be a regular substitution group* (§ 27) *on g letters simply-isomorphic with G. Then if H be looked upon as a linear group in g variables, it is intransitive, breaking up into a number of component groups among which are found just n which are equivalent to G.*

Proof. When a substitution T_t of H other than the identity is written in matrix form as a linear transformation, every element in the principal diagonal is zero, since otherwise the corresponding letter would be replaced by itself in T_t. Accordingly, $\chi(T_t)=0$ unless T_t is the identity; if T_1 is the identity: $(1, 1, \ldots, 1)$, then $\chi(T_1)=g$. The transformations of G being correspondingly S_t and $S_1=(1, 1, \ldots, 1)$, we have therefore

$$\sum_{t=1}^{g} \chi(S_t)\cdot\chi(\overline{T_t})=ng.$$

The corollary now follows by applying Theorem 19.

132. Remark. The propositions of § 131 become wider in scope by an obvious extension of the concept "group." A group G' of order g' to which another group G of order $g=hg'$ is multiply isomorphic may be exhibited in such a way as if it were a group simply isomorphic with G, namely by repeating each of its transformations h times. For instance, the substitution group of order 6: 1, (ab), (ac), (bc), (abc), (acb) is multiply isomorphic with two of its subgroups: 1; and 1, (ab). With the concept of "group" extended as indicated above, we may exhibit the three groups as simply isomorphic in the following manner:

1,	(ab),	(ac),	(bc),	(abc),	(acb);
1,	1,	1,	1,	1,	1;
1,	(ab),	(ab),	(ab),	1,	1.

EXERCISES

1. Prove that if the regular substitution group H is broken up into its ultimate sets of intransitivity with their corresponding component groups, and if H be multiply isomorphic with a transitive linear group G

in n variables, then n of the component groups into which H breaks up are equivalent to G.

2. The group H of order g is always multiply isomorphic with the group consisting of *the identity* alone, which is a transitive linear group in one variable: $x=x'$. Hence, one of the sets of intransitivity of H will contain one variable, and the component group will consist of the identity repeated g times. Prove this in another way by showing that H possesses a single absolute invariant of the first degree.

Prove also that if an additional set of intransitivity of H contains one variable, then H possesses a *relative* invariant (§ 127) of the first degree. In such a case H is not a simple group; all those of its transformations for which this invariant is *absolute* form a self-conjugate subgroup.

3. Among all the component transitive linear groups into which H breaks up, let there be k which are non-equivalent: $G_1, G_2, \ldots, G_k$ in $n_1, n_2, \ldots, n_k$ variables respectively. Prove that $g=n_1^2+n_2^2+\ldots+n_k^2$.

133. The Sum of Matrices. The *sum* of a series of square matrices of the same order is the matrix whose elements are the algebraic sums of the corresponding elements of the given matrices. Thus,

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$$

If $S_1, S_2, \ldots$ are linear transformations in the same variables, we shall write $S_1+S_2+\ldots$ to denote the matrix which is the sum of the matrices of $S_1, S_2, \ldots$

Multiplication of matrices is carried out according to the rule given in § 78, irrespective of whether the matrices represent linear transformations or not.

We find

$$S_1+S_2=S_2+S_1,$$

$$T(S_1+S_2+\ldots)=TS_1+TS_2+\ldots,$$

$$T^{-1}(S_1+S_2+\ldots)T=T^{-1}S_1T+T^{-1}S_2T+\ldots,$$

$$(S_1+S_2+\ldots)(T_1+T_2+\ldots)=$$

$$S_1T_1+S_1T_2+S_2T_1+S_2T_2+\ldots$$

If M represents a matrix, and c a constant or a variable, the symbol cM shall represent the matrix obtained by multiplying every element of M by c.

134. Lemma 1. *If $S_1, \ldots, S_m$ are the different transformations of a conjugate set of a transitive linear group G in n variables, then the matrix*

$$M = S_1 + \ldots + S_m$$

is commutative with every transformation of G and has the form of a similarity-transformation $(\alpha, \alpha, \ldots, \alpha)$, where $\alpha = m\chi(S_1)/n$.

Proof. That M is commutative with any given transformation T of G is seen as follows. We have

$$T^{-1}MT = T^{-1}S_1T + T^{-1}S_2T + \ldots = S_1 + S_2 + \ldots = M,$$

since $T^{-1}S_1T, \ldots, T^{-1}S_mT$ are the transformations $S_1, \ldots, S_m$ over again in some order. Hence $MT = TM$. Again, that M has the form of a similarity-transformation can be proved in several ways. We shall here give a very simple proof based upon the proposition, following from Theorem 21: the n^2 elements of each of the matrices of the transformations of G do not satisfy a linear homogeneous equation whose coefficients are the same for every transformation. Now, the condition $MT = TM$ is readily found to imply just such an equation, unless M is in the form of a similarity-transformation $(\alpha, \alpha, \ldots, \alpha)$.

Finally, to find the value of α we observe from the formation of M that the sum of the elements of its principal diagonal, $n\alpha$, equals the sum of the characteristics of $S_1, \ldots, S_m$. But these are all equal (§ 89); hence $n\alpha = m\chi(S_1)$.

LEMMA 2. *If $M_1, \ldots, M_h$ are the matrices representing each the sum of the matrices of a conjugate set of G, there being h such sets, then*

$$M_sM_t = c_{st1}M_1 + c_{st2}M_2 + \ldots + c_{sth}M_h \quad (s, t = 1, 2, \ldots, h),$$

where the coefficients $c_{st1}, \ldots$ are positive integers or zero.

Proof. Let

$$M_s = S_1 + S_2 \ldots + S_{g_s}, \quad M_t = R_1 + R_2 + \ldots + R_{g_t},$$

then the g_sg_t matrices in the product $M_sM_t = \sum S_\lambda R_\mu$ must make up one or more conjugate sets, since

$$T^{-1}(M_sM_t)T = (T^{-1}M_sT)(T^{-1}M_tT) = M_sM_t.$$

Accordingly, this product is the sum of one or more of the matrices $M_1, \ldots, M_h$, possibly repeated a certain number of times. Hence the lemma.

135. Theorem 20. *Let the number of transformations in the different conjugate sets of a transitive group G in n variables be $g_1, g_2, \ldots, g_h$, and let the corresponding characteristics be denoted by $\chi_1, \chi_2, \ldots, \chi_h$* (cf. § 89). *Then*

$$(1) \quad \left(\frac{g_s\chi_s}{n}\right)\left(\frac{g_t\chi}{n}\right) = \sum_{v=1}^{h} c_{stv}\left(\frac{g_v\chi_v}{n}\right) \qquad (s,\ t=1,\ 2,\ \ldots,\ h),$$

where $c_{st1}, \ldots$ represent certain positive integers or zero.

Proof. We substitute in the equation of Lemma 2 the canonical forms of the matrices $M_1, \ldots, M_h$ as given by Lemma 1, and obtain the equation $(\beta, \ldots, \beta) = (\gamma, \ldots \gamma)$, where β has for value the left-hand member of (1), and γ the right-hand member.

EXERCISES

1. Selecting the h equations (1) obtained by keeping s fixed while taking $t=1, 2, \ldots, h$, prove that $g_s\chi_s/n$ is an algebraic integer (cf. § 116, 7°).

2. Prove that if S_s and S_t^{-1} are conjugate, then

$$\sum_{j=1}^{k} \chi_s^{(j)}\chi_t^{(j)} = \sum_{j=1}^{k} \chi_s^{(j)}\overline{\chi_s}^{(j)} = \frac{g}{g_s},$$

where the summation extends over a set of non-equivalent groups into which the regular substitution group H breaks up; if S_s and S_t^{-1} are not conjugate, the first sum vanishes.

(Prove that $\sum_{j=1}^{j=k} n_j\chi_v^{(j)} = 0$ if S_v is not the identity; and that if it is, the sum equals g. Prove also that if S_s and S_t^{-1} are conjugate, $g_s = g_t$, and in the right-hand member of (1) we shall then have $c_{st1} = g_s$. We assume $n_j = \chi_1^{(j)}$ to be the characteristic of the identity.)

COROLLARY 1. *The quantity $g_s\chi_s$ equals the product of n by the sum of a finite number of roots of unity.*

This follows from the statement of Exercise (1) and § 116, 7°

COROLLARY 2. *The number of variables n of a transitive linear group G is a factor of the order g.*

Proof. The equation from Theorem 18 may be written

$$(2) \qquad g = g_1\chi_1\overline{\chi_1} + g_2\chi_2\overline{\chi_2} + \ldots + g_h\chi_h\overline{\chi_h}.$$

Now, since the sums and products of algebraic integers are again algebraic integers, the quantity

$$\frac{g}{n}=\frac{g_1\chi_1}{n}\overline{\chi_1}+\frac{g_2\chi_2}{n}\overline{\chi_2}+\ \cdots\ +\frac{g_h\chi_h}{n}\overline{\chi_h},$$

is an algebraic integer. It follows that g/n, being a rational number, must be an ordinary integer.

EXERCISE

3. Prove that if a transitive linear group G of order g in n variables contains a subgroup of order f composed of similarity-transformations. then g is divisible by fn (Schur).

(Prove first that if χ_s does not vanish, there will be f distinct conjugate sets for which the products $g_s\chi_s\overline{\chi_s}$ in (2) have the same value.)

COROLLARY 3. *If a transitive linear group G in n variables contains two characteristics χ_s, χ_t such that the sum of the n^2 roots in the product $\chi_s\chi_t$ cannot be written as a sum in which primitive roots of index k are absent, then there is in G a characteristic containing roots of index k and therefore a transformation whose order is k or a multiple of k.**

This follows from the equation (1). By the conditions of the corollary, at least one of the characteristics χ_v of the right-hand member must contain roots of index k. There is, therefore, a transformation whose order is divisible by k. For, the order m of a transformation $S=(\alpha,\ \beta,\ \ldots)$ is the least common multiple of the indices of the roots $\alpha,\ \beta,\ \ldots$, since $S^m=(1,\ 1,\ \ldots)=(\alpha^m,\ \beta^m,\ \ldots)$.

To illustrate, let $\chi_s=-1+i+i$ and $\chi_t=\alpha+\alpha+\alpha^3$, where $i=\sqrt{-1}$ and α is a primitive fifth root. Here $\chi_s\chi_t$, or $4i\alpha+2i\alpha^3-2\alpha-\alpha^3$, cannot be written as a sum which is free from roots of index 20 ($i\alpha$, etc.) by Kronecker's theorem (§ 110)

EXERCISE

4. Prove that if a group in n variables contains transformations of orders p and q, two different prime numbers both greater than $n+1$, then the group contains a transformation of order pq.

136. Theorem 21. *Let $G=(S_1,\ S_2,\ \ldots,\ S_g)$ be a transitive linear group in n variables. Then the n^2 elements in the*

* Burnside, *Theory of Groups*, second edition, p. 347.

matrix $y_1S_1+y_2S_2+\ \ldots\ +y_gS_g$ (§ 133), *considered as functions of the* g *independent variables* $y_1, \ldots, y_g$, *are linearly independent.*

Proof. 1°. When a square matrix M of n^2 elements is transformed into a similar matrix M' by means of a linear transformation T in n variables:

$$T^{-1}MT=M', \quad M=TM'T^{-1},$$

then the elements of M' are linear functions of the elements of M, and vice versa; the coefficients being functions of the elements of T. Hence, if the elements of M are linear functions of certain independent variables, the elements of M' will likewise be linear functions of these variables; and, if among the former just l are found to be linearly independent, the same will be the case with the elements of M'.

2°. Now consider a regular substitution group H of order g written in the form of a linear group. As an example we take the symmetric group on 3 letters, which may be written as a regular group on 6 letters $x_1, \ldots, x_6$ as follows:

$$S_1=\text{the identity}, \qquad S_2=(x_1x_2x_3)(x_4x_5x_6),$$
$$S_3=(x_1x_3x_2)(x_4x_6x_5), \qquad S_4=(x_1x_4)(x_2x_6)(x_3x_5),$$
$$S_5=(x_1x_5)(x_2x_4)(x_3x_6), \qquad S_6=(x_1x_6)(x_2x_5)(x_3x_4).$$

The matrix $y_1S_1+y_2S_2+\ \ldots\ +y_6S_6$ is here

$$M=\begin{pmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ y_3 & y_1 & y_2 & y_5 & y_6 & y_4 \\ y_2 & y_3 & y_1 & y_6 & y_4 & y_5 \\ y_4 & y_5 & y_6 & y_1 & y_2 & y_3 \\ y_5 & y_6 & y_4 & y_3 & y_1 & y_2 \\ y_6 & y_4 & y_5 & y_2 & y_3 & y_1 \end{pmatrix}$$

New variables may be introduced in H so that this group takes the intransitive form, namely

$$z_1=x_1+x_2+x_3+x_4+x_5+x_6, \qquad z_2=x_1+x_2+x_3-x_4-x_5-x_6,$$
$$z_3=x_1+\omega x_2+\omega^2x_3, \qquad z_4=x_4+\omega^2x_5+\omega x_6,$$
$$z_5=x_4+\omega x_5+\omega^2x_6, \qquad z_6=x_1+\omega^2x_2+\omega x_3,$$

where ω is a primitive cube root of unity. When H is written in the new form (we shall denote this by H', and its transformations by $S'_1, \ldots, S'_6$), the matrix M will become

$$M' = \begin{vmatrix} A & 0 & 0 & 0 & 0 & 0 \\ 0 & B & 0 & 0 & 0 & 0 \\ 0 & 0 & C & D & 0 & 0 \\ 0 & 0 & E & F & 0 & 0 \\ 0 & 0 & 0 & 0 & C & D \\ 0 & 0 & 0 & 0 & E & F \end{vmatrix}$$

where

$$A = y_1+y_2+y_3+y_4+y_5+y_6,$$
$$B = y_1+y_2+y_3-y_4-y_5-y_6,$$
$$C = y_1+\omega^2 y_2+\omega y_3, \qquad D = y_4+\omega y_5+\omega^2 y_6,$$
$$E = y_4+\omega^2 y_5+\omega y_6, \qquad F = y_1+\omega y_2+\omega^2 y_3.$$

Now, there is a transformation, T say, which transforms H into H' (§ 88): $T^{-1}S_1T = S'_1$, etc. Therefore, since

$$T^{-1}(y_1S_1+ \ldots +y_\varphi S_\varphi)T = y_1S'_1+ \ldots +y_\varphi S'_\varphi,$$

we have $T^{-1}MT = M'$. Hence, by 1°, there are as many linearly independent functions of $y_1, \ldots, y_\varphi$ among the elements A, B, C, D, E, F of M' as among the elements of M, namely 6. It follows that $A, \ldots, F$ are all linearly independent.

In the general case, H' breaks up into k non-equivalent groups $G_1, \ldots, G_k$, with G_s repeated as an equivalent group n_s times, namely the number of its variables (§ 131, Cor. 2). Correspondingly, the n_s component matrices involved in M' will have the same elements. Hence, there will be at most as many independent elements in M' as are found in a set of non-equivalent groups, namely $n_1^2+n_2^2+ \ldots +n_\varphi^2$. But this number is equal to g (§ 132, Ex. 3), the number of independent elements $(y_1, \ldots, y_\varphi)$ in M*. Hence, by 1°, all

* Each element of M will contain a single variable y_j. This is proved easily from the facts that H is a transitive substitution group and every one of its substitutions (except the identity) displaces all of the g letters.

these $n_1^2 + \ldots + n_k^2$ elements are linearly independent, and the theorem is proved.

EXERCISES

1. Prove that the n^2 elements of each of the matrices of the transformations of G do not satisfy a linear homogeneous equation whose coefficients are the same for every transformation (Burnside).

2. Prove that if a certain element a_{st} vanishes in every transformation $S=[a_{\alpha\beta}]$ of a group G, the subscripts s, t being given, then G is not transitive (Maschke).

137. Theorem 22. *The number (k) of non-equivalent transitive linear groups into which the regular substitution group H breaks up (cf. § 131) is equal to the total number of sets of conjugate substitutions of H*

The proof follows that of Theorem 21 closely, after we have first made equal to each other those of the variables $y_1, \ldots, y_g$ which are factors of conjugate transformations in the matrix M. If, therefore, H contains h conjugate sets of respectively $g_1, \ldots, g_h$ transformations, we shall have h independent variables, say $v_1, \ldots, v_h$.

The matrix M' now has the form of a transformation in canonical form. Thus, the matrix M' in the example given in § 136, 2°, becomes $M'=(A, B, C, C, C, C)$, where

$$A=v_1+2v_2+3v_3, \quad B=v_1+2v_2-3v_3, \quad C=v_1-v_2.$$

In general, let G_j be any one of the groups into which H breaks up, and $\chi_1, \ldots, \chi_h$ the characteristics of the various conjugate sets of G_j. Then it follows by Lemma 1, § 134, that, as far as the variables of G_j are concerned, M' will appear in the form of a similarity-transformation $(\beta_j, \beta_j, \ldots, \beta_j)$, where

$$\beta_j=(g_1v_1\chi_1+g_2v_2\chi_2+\ldots+g_hv_h\chi_h)/n.$$

If G_j and G'_j are equivalent groups, $\beta_j=\beta'_j$; and conversely (§ 131). Hence, if G_j and G'_j are non-equivalent, $\beta_j \neq \beta'_j$.

Accordingly, among the g multipliers of M' in its new form, there will be just k that are distinct, and these can certainly not furnish more than k expressions linearly independent in $v_1, \ldots, v_h$. On the other hand, the matrix M will contain

just h linearly independent elements, namely $v_1, \ldots, v_h$. Hence by 1°, § 136, $k \geqq h$, and h of the multipliers, $\beta_1, \ldots, \beta_k$ are linearly independent, say $\beta_1, \beta_2, \ldots, \beta_h$. These h expressions can therefore not all vanish unless $v_1 = v_2 = \ldots = v_h = 0$.

However, if $k > h$, the expressions $\beta_1, \ldots, \beta_h$ must all vanish if for $v_1, \ldots, v_h$ we put, respectively, the conjugate-imaginaries of the characteristics $\chi_1, \ldots, \chi_h$ of the group G_{h+1} (§ 131, Cor. 1). But these quantities, $\overline{\chi_1}, \ldots, \overline{\chi_h}$, are not all zero (one of them represents the number of variables of G_{h+1}). We conclude that $k \not> h$. Hence, finally, $k = h$.

EXERCISE

Prove that if $S_1, \ldots, S_g$ are the substitutions of the regular substitution group H, and $\chi_t^{(1)}, \chi_t^{(2)}, \ldots, \chi_t^{(k)}$ the characteristics of the transformations corresponding to S_t in a set of non-equivalent groups into which H breaks up, then these characteristics do not satisfy an equation

$$a_1\chi_t^{(1)} + a_2\chi_t^{(2)} + \ldots + a_k\chi_t^{(k)} = 0$$

where the coefficients $a_1, \ldots, a_k$ are the same for all the g subscripts t.

138. Theorem 23. *No simple group can be of order $p^a q^b$, p and q being different prime numbers.**

The proof is divided into two parts: 1°. If H is the regular substitution group simply isomorphic with a group of order $g = p^a q^b$, assumed simple, then one of the non-equivalent transitive linear groups $G_1, \ldots, G_k$ into which H breaks up (§ 131) contains q^α variables, and one of the conjugate sets of H contains p^β transformations. 2°. Under these conditions an impossible equation is obtained.

1°. The relation $g = p^a q^b = n_1^2 + n_2^2 + \ldots + n_k^2$ (§ 132, Ex. 3) with the condition that the numbers $n_1, \ldots, n_k$ are all factors of g (§ 135, Cor. 2) and that only one of them is unity (§ 132, Ex. 2) implies that at least one of them is greater than unity and prime to p; say $n_i = q^\alpha > 1$.

Again, the relation $g = p^a q^b = g_1 + g_2 + \ldots + g_h$ with the condition that the numbers $g_1, \ldots, g_h$ are factors of g and

* Burnside, *Proceedings of the London Mathematical Society*, 1904, p. 388.

that only one of them is unity (as otherwise H would not be simple; cf. § 24) implies in the same manner that one of them is a power of p; say $g_s = p^\beta > 1$.

2°. We now have a transitive group G_t in $n_t = q^\alpha$ variables, and a conjugate set of $g_s = p^\beta$ transformations. Let $S^{(t)}$ denote one of the transformations of this set, $\chi^{(t)}$ its characteristic, and T the corresponding transformation (substitution) of H. We have (§ 135, Cor. 1)

$$p^\beta \chi^{(t)} = q^\alpha N,$$

where N represents the sum of a finite number of roots of unity. It follows that $\chi^{(t)} = q^\alpha N'$, N' being such a sum also (§ 116, 7°). But, $\chi^{(t)}$ is already the sum of q^α roots of unity. Hence, either all these roots are alike, or $\chi^{(t)} = 0$. The first supposition makes $S^{(t)}$ a similarity-transformation, which would be self-conjugate in G_t. This being impossible for a simple group, we infer that $\chi^{(t)} = 0$; and this not only for the group G_t, but also for every one among the groups $G_1, \ldots, G_k$ (and their equivalent groups), the number of whose variables, like n_t, does not contain p as a factor. Hence, the sum of the characteristics of the transformations corresponding to T, from all these groups, is of the form

$$n_1\chi^{(1)} + \ldots + n_k\chi^{(k)} = 1 + pN'' + q^\alpha\chi^{(t)} + \ldots = 1 + PN'',$$

when account is taken of the fact that one of the numbers $n_1, \ldots, n_k$, say n_1, is unity, and that the corresponding characteristic $\chi^{(1)} = 1$.

However, this sum is equal to the characteristic $\chi(T)$ in H, being equal to the sum of the elements of the principal diagonal of the matrix of T. Hence, since $\chi(T) = 0$,

$$1 + pN'' = 0.$$

But such an equation is impossible by Kronecker's theorem (§ 116, 7°).

EXERCISE

Prove that a group in which the number of operators in a conjugate set is the power of a prime number is not simple (Burnside).

139. Theorem 24. *A transitive substitution group of degree n and class $n-1$ contains an invariant subgroup of degree and class n.**

Proof. 1°. Let g be the order of G, and $g'=g/n$ the order of that subgroup G' of G whose substitutions leave fixed a given letter. Again, let H represent the regular substitution group simply isomorphic with G, and H' the regular substitution group simply isomorphic with G'. The groups H and H' are of degrees g and g' respectively.

Now let H be resolved into its component linear groups, from which we select a set of non-equivalent groups H_1, H_2, . . . , H_k, the number of whose variables are respectively $n_1=1$, n_2, . . . , n_k. Similarly, let H' be resolved into its different linear groups, from which we select a set of non-equivalent groups H'_1, H'_2, . . . , H'_i, in respectively $n'_1=1$, n'_2, . . . , n'_i variables. The latter set and their equivalent groups are all irreducible components of that subgroup of H which corresponds to H'; they are, in fact, contained as irreducible components in the subgroups of H_1, . . . , H_k (and their equivalent groups) which correspond to G' of G. Let us suppose, for any subscript $s \leqq k$, that the subgroup of H_s which corresponds to G' of G breaks up into f_{s1} groups equivalent to H'_1, f_{s2} groups equivalent to H'_2, etc. This division may be exhibited clearly by the following equation:

$$|H_s|=f_{s1}H'_1+f_{s2}H'_2+ \ldots +f_{si}H'_i.$$

Evidently, $|H_1|=H'_1$, so that

$$f_{11}=1, \quad f_{12}=0, \ldots, f_{1i}=0.$$

Moreover, (§ 132, Ex. 3),

$$n_1^2+n_2^2+ \ldots +n_k^2=g, \quad n'^2_1+n'^2_2+ \ldots +n'^2_i=g'.$$

Again, if T_1(=the identity), T_2, . . . , $T_{g'}$ are the transformations of $|H_s|$, and $\chi_{1s}(=n_s)$, χ_{2s}, . . . , $\chi_{g's}$ their char-

* Frobenius, *Sitzungsberichte, etc.*, 1901, pp. 1223–1225.

acteristics, while $\theta_{1\sigma}(=n'_\sigma)$, $\theta_{2\sigma}$, . . . , $\theta_{g'\sigma}$ are the corresponding characteristics of H'_σ, we have $(\theta_{t1}=1)$:

$$\chi_{ts}=f_{s1}+f_{s2}\theta_{t2}+\ldots+f_{st}\theta_{tt}. \tag{3}$$

2°. Assuming for the present that $f_{s1}=0$ for a certain subscript s, the theorem is easily proved. If we denote by $\sum\chi$ the sum of the n characteristics of H_s corresponding to the identity and to the substitutions of G of class n,* we have, applying Cor. 2, § 128,

$$\begin{aligned}0&=\sum\chi+n\dagger\sum_{t=2}^{g'}\chi_{ts}=\sum\chi+n\Big(-n_s+\sum_{t=1}^{g'}\chi_{ts}\Big)\\&=\sum\chi+n\Big(-n_s+f_{s2}\sum_{t=1}^{g'}\theta_{t2}+\ldots+f_{st}\sum_{t=1}^{g'}\theta_{tt}\Big)\\&=\sum\chi-nn_s,\end{aligned}$$

or

$$\sum\chi=nn_s. \tag{4}$$

Hence, there being n characteristics in $\sum\chi$, and each being the sum of n_s roots of unity, the equation (4) can be true only if each characteristic χ is n_s. But then the corresponding transformation of H_s must be the identity (1, 1, . . . , 1); and all such transformations correspond to an invariant subgroup of G (cf. § 132). This subgroup includes all the substitutions of class n and possibly some more (though not all of G, by virtue of the condition $f_{s1}=0$). If it includes more, then this new group, of order $<g$, may be chosen instead of G, and thus we would, by a proof by induction, ultimately show the existence in G of a subgroup of degree and class n, which would obviously be an invariant subgroup of the original group G.

* There are $n-1$ substitutions in G which permute all the letters; $n(g'-1)$ which permute all but one; and one (identity) which leaves them all fixed.

† No two different subgroups of G of class $n-1$ can have a substitution in common.

3°. Going back to 1°, it remains for us to prove that at least one of the numbers $f_{21}, f_{31}, \ldots, f_{k1}$ is zero. To accomplish this we start with the following equations (which we shall establish in 4°):

$$f_{21}^2+f_{31}^2+\ldots+f_{k1}^2=\frac{g-g'}{g'^2},$$

$$(5)\qquad f_{21}f_{22}+f_{31}f_{32}+\ldots+f_{k1}f_{k2}=\frac{g-g'}{g'^2}n'_2,$$

$$f_{22}^2+f_{32}^2+\ldots+f_{k2}^2=\frac{g-g'}{g'^2}n'^2_2+1,$$

from which we derive

$$(f_{22}-n'_2f_{21})^2+(f_{32}-n'_2f_{31})^2+\ldots+(f_{k2}-n'_2f_{k1})^2=1.$$

Now, since the terms in the left-hand member are positive integers or zero, it follows that one of them is unity and the rest zero; say

$$f_{22}=n'_2f_{21}\pm1,\quad f_{32}=n'_2f_{31},\ \ldots,\ f_{k2}=n'_2f_{k1}.$$

Substituting in the second of the equations (5) and subtracting n'_2 times the first gives us $\pm f_{21}=0$, what we set out to prove.

4°. To prove (5), consider the sum

$$\begin{aligned}M=&\chi_{v1}\bar{\chi}_{11}\theta_{1t}+\chi_{v1}\bar{\chi}_{21}\theta_{2t}+\ldots+\chi_{v1}\bar{\chi}_{g'1}\theta_{g't}\\&+\chi_{v2}\bar{\chi}_{12}\theta_{1t}+\chi_{v2}\bar{\chi}_{22}\theta_{2t}+\ldots+\chi_{v2}\bar{\chi}_{g'2}\theta_{g't}\\&\cdots\cdots\cdots\cdots\\&+\chi_{vk}\bar{\chi}_{1k}\theta_{1t}+\chi_{vk}\bar{\chi}_{2k}\theta_{2t}+\ldots+\chi_{vk}\bar{\chi}_{g'k}\theta_{g't}\qquad(1<v\leqq g').\end{aligned}$$

Let there be h' operators conjugate to T_v in G', and there will be $h'g/g'$ conjugates to T_v in G. Then, adding by columns, we get (§ 135, Ex. 2)

$$M=h'(\chi_{v1}\bar{\chi}_{v1}+\chi_{v2}\bar{\chi}_{v2}+\ldots+\chi_{vk}\bar{\chi}_{vk})\theta_{vt}=g'\theta_{vt}.$$

Again, substituting for $\overline{\chi}_{tt}$ from (3) and adding by lines we have (§ 131, Cor. 1):

$$M=(\chi_{v1}f_{1t}+\chi_{v2}f_{2t}+\ \dots\ +\chi_{vk}f_{kt})(\bar{\theta}_{1t}\theta_{1t}+\bar{\theta}_{2t}\theta_{2t}+\ \dots\ +\bar{\theta}_{g't}\theta_{g't})$$
$$=\sum_{r=1}^{k}(f_{r1}f_{rt}+\theta_{v2}f_{r2}f_{rt}+\ \dots\ +\theta_{vt}f_{rt}f_{rt})g'.$$

Hence, equating the two values of M obtained we get

$$(6)\quad 0=\sum f_{r1}f_{rt}+\theta_{v2}\sum f_{r2}f_{rt}+\ \dots\ +\theta_{vt}(-1+\sum f_{rt}^2)\cdot$$
$$+\ \dots\ +\theta_{vt}\sum f_{rt}f_{rt}=A_1+\theta_{v2}A_2+\ \dots\ +\theta_{vt}A_t,$$

say, where the summation extends from $r=1$ to $r=k$, and $1<v\leqq g'$.

We can now prove the following equation:

$$(7)\quad 0=A_1-q+\theta_{v2}(A_2-qn'_2)+\ \dots\ +\theta_{vt}(A_t-qn'_t)\quad(1\leqq v\leqq g'),$$

where

$$q=\frac{g-g'}{g'^2}n'_t.$$

When $v>1$ the equation reduces to the following by means of (6):

$$0=-q(1+n'_2\theta_{v2}+\ \dots\ +n'_t\theta_{vt}),$$

which is true, since the quantity in the parenthesis is the characteristic corresponding to T_v in the regular group H' and is therefore zero. If $v=1$, the right-hand member of (7) becomes (cf. 1°)

$$A_1-q+n'_2(A_2-qn'_2)+\ \dots\ +n'_t(A_t-qn'_t)$$
$$=A_1+n'_2A_2+\ \dots\ +n'_tA_t-q(1+n'^2_2+\ \dots\ +n'^2_t)$$
$$=\sum_{r=1}^{k}f_{rt}(f_{r1}+n'_2f_{r2}+\ \dots\ +n'_tf_{rt})-n'_t-qg'$$
$$(8)\quad=\sum_{r=1}^{k}f_{rt}n_r-\frac{g}{g'}n'_t.$$

Now, $\sum_{r=1}^{r=k}f_{rt}n_r$ is the number of times the group H'_t (or equivalent groups) enters as a component of the subgroup $|H|$ of H. In this group, G' will evidently be represented as an

intransitive substitution group made up of g/g' sets of intransitivity, of g' letters each. For each such set there are n'_t groups H'_t. Accordingly, $\sum_{r=1}^{r=k} f_r n_r = n'_t g/g'$. Substituting in (8), the quantity vanishes.

Having thus proved (7) for $v=1, 2, \ldots, g'$, we may apply the proposition stated in the exercise, § 137, from which it follows that every coefficient $A_p - qn'_p$ must vanish. Equating to zero the coefficients for $p=1$ and $p=2$, $t=1$ and $t=2$, the equations (5) are finally obtained.

PART III*

APPLICATIONS OF FINITE GROUPS

CHAPTER XIV

THE GROUP OF AN ALGEBRAIC EQUATION FOR A GIVEN DOMAIN

140. Introduction. The theory of substitutions and groups of substitutions grew out of the investigations by Lagrange, Ruffini and Abel of the question of the solvability by radicals of the general algebraic equation of degree n. We shall answer this question by means of the theory of Galois, which is applicable to any algebraic equation, whether its coefficients are constants or depend upon one or more variables. In the latter case we must first give a definition of the roots of the equation and the concept equality of two functions of the roots. Consequently, we shall begin with the more concrete, and yet typical, case of numerical equations.

With a given equation we shall associate a certain group of substitutions on its roots and shall prove that the equation is solvable by radicals if and only if the group is solvable, i.e., if each of the factors of composition of the group is a prime number. If we regard as known not merely the coefficients of the given equation, but also certain constants, such as roots of unity, the solution of our equation may be thereby simplified and the group altered. In fact, most of our concepts, such as the irreducibility of the equation, its group, etc., depend upon the constants regarded as known. In order to specify

* This part was written by L. E. Dickson.

these constants briefly and clearly, we shall define and employ the concept " domain."

After developing the essential principles of Galois' theory of algebraic equations, we shall apply the theory to various problems in geometry; first to constructions by ruler and compasses, including the proof of the impossibility of certain constructions of intrinsic and historic interest; then to the inflexion points on a plane cubic curve, the 27 straight lines on a cubic surface, and the 28 bitangents to a quartic curve; finally, to a general series of problems on contacts of curves.

141. Number Domains. The set of all rational functions with rational coefficients of the complex (real or imaginary) numbers $k_1, k_2, \ldots, k_m$ is called a *domain* and denoted by $R(k_1, \ldots, k_m)$. Hence if we perform any one of the four rational operations (addition, subtraction, multiplication, divison by a number not zero) upon any two equal or distinct numbers of the domain, we obtain a number of the domain.

We assume that each k_i is not zero. The domain contains every rational number r, since it contains rk_1/k_1. The domain $R(1)$ is the set of all rational numbers.

EXERCISES

1. Every number of $R(i)$, where $i^2=-1$, can be given the form $a+bi$, where a and b are rational. Every number of $R(\sqrt{3})$ is of the form $a+b\sqrt{3}$.

2. If $\omega=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$, then $R(\omega)=R(\sqrt{-3})$.

3. If $\xi=i+\sqrt{2}$, $R(i, \sqrt{2})=R(\xi)$. Hint: $i-\sqrt{2}=-3/\xi$.

4. If k is the real cube root of 2, every number of $R(k)$ can be given the form $a+bk+ck^2$, where a, b, c are rational.

142. Reducibility and Irreducibility. An integral rational function $f(x)$ of degree n of a variable x whose coefficients belong to the domain R is said to be *reducible in R* if it can be expressed as a product of integral rational functions of x each of degree $<n$ with coefficients in R; *irreducible in R* if no such factorization is possible.

EXAMPLE 1. The function x^2+1 is reducible in $R(i)$ since it has the factors $x\pm i$, but is irreducible in $R(1)$ and in $R(\sqrt{2})$.

EXAMPLE 2. x^4+1 is reducible in any domain which contains either $\sqrt{2}$, or $\sqrt{-2}$, or $i=\sqrt{-1}$, or $\epsilon=(1+i)/\sqrt{2}$, but is irreducible in all other

domains. Indeed, its linear factors are $x\pm\epsilon$, $x\pm\epsilon^{-1}$; while every quadratic factor is of one of the forms $x^2\pm i$, $x^2+ax\pm 1$ $(a^2=\pm 2)$.

EXAMPLE 3. x^3-2 is irreducible in $R(1)$. For, if it were reducible, it would have a linear factor $x-a/b$, where a and b are relatively prime integers, of which b may be taken to be positive. Then $a^3-2b^3=0$. If b has a prime factor $\beta(\beta>1)$, then β divides a^3 and hence divides a, whereas a and b have no common factor β. Thus $b=1$, $a^3=2$. Hence the positive integer a divides 2, so that $a=1$ or 2, and $a^3=1$ or 8, whereas $a^3=2$. Hence x^3-2 is irreducible in $R(1)$.

If $f(x)$ is reducible in R, $f(x)=0$ is called a reducible equation in R; in the contrary case, an irreducible equation in R.

143. Irreducible Binomials. *If p is a prime number and if A is a number of a domain R, but A is not the pth power of a number of R, then x^p-A is irreducible in R.*

The roots of $x^p=A$ may be denoted by

$$r,\ \omega r,\ \omega^2 r,\ \ldots,\ \omega^{p-1}r,$$

where ω is an imaginary pth root of unity. Let there be a factor with coefficients in R of x^p-A. It has a constant term of the form $\pm\omega^s r^t$, where $0<t<p$. By the theory of numbers, there exist integers b, c such that $bt-cp=1$. Hence R contains

$$(\omega^s r^t)^b=\omega^{sb}r^{cp+1}=\omega^{sb}rA^c=r'A^c,$$

where r' is one of the above roots. Thus r' is in R, so that A is the pth power of a number r' in R, contrary to hypothesis.

144. Theorem. *Let the coefficients of the polynomials $f(x)$ and $g(x)$ be numbers of a domain R and let $f(x)$ be irreducible in R. If one root α of $f(x)=0$ satisfies $g(x)=0$, every root of $f(x)=0$ satisfies $g(x)=0$ and $f(x)$ is a divisor of $g(x)$ in R.*

The greatest common divisor $h(x)$ of $f(x)$ and $g(x)$ is not a constant, since it has the factor $x-\alpha$. The usual process for finding $h(x)$ involves only rational operations; hence its coefficients are numbers of the domain R. Since $f(x)$ is irreducible in R, its divisor $h(x)$, with coefficients in R, is of the same degree as $f(x)$, and hence equals $cf(x)$, where c is a number in R. But $h(x)$ divides $g(x)$. Hence $f(x)$ divides $g(x)$ in R.

EXERCISES

1. If $x^3+cx^2+dx+e=0$, where c, d and e are integers, has a rational root, that root is an integer. Hint: Let $x=a/b$, where a and b are relatively prime integers, and multiply the equation obtained from the cubic equation by b^2.

2. An integral root of the equation in Ex. 1 is a divisor of e. Hint: It divides x^3, cx^2 and dx.

3. x^3-3x+1 is irreducible in $R(1)$.

4. x^3-7x+7 is irreducible in $R(1)$.

5. State and prove for equations of degree n the theorems corresponding to those of Exs. 1, 2 for $n=3$.

6. $x^4+x^3+x^2+x+1=0$ is irreducible in $R(1)$. Hints: It has no rational root (Ex. 5). If it has the factors x^2+ax+r, x^2+bx+r^{-1}, where a, b, r are rational, then

$$a+b=1, \quad ab+r+r^{-1}=1, \quad ar^{-1}+br=1.$$

Either $$a=\tfrac{1}{2}(1\pm\sqrt{5}), \quad b=\tfrac{1}{2}(1\mp\sqrt{5}), \quad r=1;$$

or $$a=\frac{r}{r+1}, \quad b=\frac{1}{r+1}, \quad r^4+r^3+r^2+r+1=0.$$

145. Functions with $n!$ values. Let R be a given domain which contains all of the coefficients of a given numerical equation

$$(1) \qquad f(x)\equiv x^n-c_1x^{n-1}+c_2x^{n-2}- \ \ldots \ +(-1)^nc_n=0,$$

which, without * real loss of generality, will be assumed to have the *distinct* roots $x_1, \ldots, x_n$. There exist integers $m_1, \ldots, m_n$ such that

$$V_1=m_1x_1+m_2x_2+ \ \ldots \ +m_nx_n$$

gives rise to $n!$ numerically distinct functions V_s when the $n!$ substitutions s on $x_1, \ldots, x_n$ are applied to it. For, if s and s' are different substitutions, V_s and $V_{s'}$ are not equal identically as to $m_1, \ldots, m_n$. We can, however, choose integers $m_1, \ldots, m_n$ which satisfy no one of the $n!(n!-1)/2$ equations of the form $V_s=V_{s'}$. In fact, $m_1=m_2$ is the only one of these equations involving only m_1 and m_2. Give to m_1 any integral value (say 0) and to m_2 any integral value

* For, if it has a multiple root, $f(x)$ and its derivative $f'(x)$ have a greatest common divisor $g(x)$ with coefficients in R. Then $f(x)/g(x)$ has its coefficients in R, has no multiple root, and vanishes for each root of $f(x)=0$.

$\neq m_1$ (say 1). Consider the equations involving m_3, but not m_i $(i>3)$; they determine certain values of m_3; give to m_3 any integral value distinct from the latter. Next we give to m_4 an integral value distinct from the values of m_4 determined by the equations involving m_4, but not $m_i (i>4)$; etc.

For $m_1=0$, $m_2=1$, the values of m_3 to be avoided are *

$$0,\ 1,\ \lambda,\ 1-\lambda,\ \frac{1}{\lambda},\ \frac{1}{1-\lambda},\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1},$$

where

$$\lambda=\frac{x_1-x_2}{x_1-x_3}.$$

Thus x_2+mx_3 has six distinct values under the six substitutions

$$1,\ a=(x_1x_2),\quad b=(x_1x_3),\quad c=(x_2x_3),\quad d=(x_1x_2x_3),\quad e=(x_1x_3x_2),$$

if m is an integer distinct from the above eight numbers.

We shall often employ as an example the equation

$$x^3+x^2+x+1=0, \tag{2}$$

with the roots $x_1=-1$, $x_2=i=\sqrt{-1}$, $x_3=-i$. Here $\lambda=i$, so that x_2+mx_3 is six-valued if $m\neq 0,\ 1,\ \pm i,\ 1\pm i,\ \frac{1}{2}(1\pm i)$, and hence if $m=-1$. The six distinct values of x_2-x_1 are

$$V_1=x_2-x_1=1+i,\quad V_b=x_2-x_3=2i,\quad V_c=x_3-x_1=1-i,$$
$$V_a=-V_1,\qquad V_d=-V_b,\qquad V_e=-V_c.$$

146. Galoisian Resolvents. The substitutions on $x_1, \ldots, x_n$ will be denoted by $s_1, \ldots, s_{n!}$, where s_1 is the identity. If $s_js_k=s_l$, and we apply s_j to V_1 and then s_k to the resulting function V_{s_j}, we get V_{s_l}. When k is fixed, but j takes the values $1, 2, \ldots, n!$, then l takes the same values in some new order. Hence s_k merely permutes

$$V_1,\ V_{s_2},\ \ldots,\ V_{s_{n!}}$$

amongst themselves. Thus the elementary symmetric functions of these V's are symmetric functions of $x_1, \ldots, x_n$,

* If one of the cross-ratios of four points is λ, the others are $1-\lambda$, etc. The six transformations $\lambda'=\lambda$, $\lambda'=1-\lambda$, $\ldots$, $\lambda'=\lambda/(\lambda-1)$ form a group. Cf. Ex. 3, § 6 and Ex. 7, § 87.

and hence * are integral rational functions of $m_1, \ldots, m_n$, $c_1, \ldots, c_n$ with integral coefficients, and therefore are numbers of the domain R. Thus the coefficients of the polynomial in V, given by the expansion of

$$F(V) \equiv (V-V_1)(V-V_{s_2}) \ldots (V-V_{s_{n!}}), \tag{3}$$

are numbers of the domain R.

If $F(V)$ is reducible in R, let $G(V)$ be that irreducible factor in R for which $G(V_1)=0$. If $F(V)$ is irreducible in R, take $G(V)$ to be $F(V)$ itself. In either case, $G(V)=0$ is an irreducible equation in R, having the root V_1; it is called a *Galoisian resolvent* of equation (1) for the domain R.

The corresponding resolvent for equation (2) in $R(1)$ is

$$G(V) \equiv (V-V_1)(V-V_c) \equiv V^2-2V+2=0.$$

For the domain $R(i)$, the resolvent is $V-V_1=0$.

147. Theorem. *Let $\phi(x_1, \ldots, x_n)$ be any rational integral function, with coefficients in a domain R, of the roots of an equation with coefficients in R. Let s be any substitution on the roots and let it replace ϕ by ϕ_s, and an $n!$-valued linear function V_1, with coefficients in R, by V_s. Then*

$$\phi_s = \frac{\lambda(V_s)}{F'(V_s)}, \tag{4}$$

where λ is a polynomial with coefficients in R, while F' is the derivative of the polynomial (3) with coefficients in R, so that $F'(V_s) \neq 0$. Thus ϕ_s is the same rational function $\rho(V_s)$ of V_s that $\phi \equiv \phi_1$ is of V_1.

If $s_j s_k = s_l$, then s_k replaces ϕ_{s_j} by ϕ_{s_l}. Thus s_k permutes $\phi_1, \ldots, \phi_{s_{n!}}$ in the same manner that it permutes $V_1, \ldots, V_{s_{n!}}$ (§ 146). Hence the terms of

$$\lambda(V) \equiv \phi_1 \frac{F(V)}{V-V_1} + \phi_{s_2} \frac{F(V)}{V-V_{s_2}} + \ldots + \phi_{s_{n!}} \frac{F(V)}{V-V_{s_{n!}}} \tag{5}$$

* Several detailed proofs of this fundamental theorem on symmetric functions, which is frequently applied below, are given in Dickson's *Elementary Theory of Equations*.

are merely permuted amongst themselves by any substitution on $x_1, \ldots, x_n$. Thus the coefficients of the polynomial $\lambda(V)$ are rational integral symmetric functions of $x_1, \ldots, x_n$ with coefficients in the domain R, and hence equal numbers of R. Taking $V=V_s$, we obtain $\lambda(V_s)=\phi_s F'(V_s)$. Since $F'(V_s)\neq 0$, we get (4).

EXAMPLE. Recurring to the special equation (2), we shall obtain the explicit expressions (4) for the case $\phi=x_2$, $V_1=x_2-x_1$. Then

$$F(V)=V^6+4V^4+4V^2+16, \tag{3'}$$

$$\lambda(V)=F(V)\left\{\frac{x_i}{V-V_1}+\frac{x_1}{V+V_1}+\frac{x_2}{V-V_b}+\frac{x_3}{V-V_c}+\frac{x_3}{V+V_b}+\frac{x_1}{V+V_c}\right\} \tag{5'}$$

$$=-2V^5-4V^4-12V^3-8V^2-16V-48,$$

as shown by inserting the values of $x_1, \ldots, V_c$ given at the end of § 145. Hence

$$x_2=\rho(V_1)\equiv\frac{-2V_1^5-4V_1^4-12V_1^3-8V_1^2-16V_1-48}{6V_1^5+16V_1^3+8V_1}.$$

In view of the theorem, we have

$$x_1=\rho(V_a),\quad x_2=\rho(V_b),\quad x_3=\rho(V_c),\quad x_3=\rho(V_d),\quad x_1=\rho(V_e).$$

These results may be verified by evaluating the expressions.

The numerator and denominator of the above fraction for x_2 may be expressed as linear functions of V_1 by means of the relation $V_1^2-2V_1+2=0$ of § 146. We get

$$\frac{-48V_1+32}{16V_1-64}=\frac{(-3V_1+2)(V_1+2)}{(V_1-4)(V_1+2)}=\frac{-3V_1^2-4V_1+4}{V_1^2-2V_1-8}=\frac{-10V_1+10}{-10}=V_1-1.$$

While therefore x_2 is numerically equal to V_1-1 (each being i), it is not admissible to take this *reduced* function $r(V_1)\equiv V_1-1$ as the function $\rho(V_1)$ of the theorem, since it would no longer be true that, by applying the substitution $a=(x_1x_2)$, we would have $x_1=r(V_a)$. Indeed, if we apply a to $V_1-1\equiv x_2-x_1-1$, we obtain $x_1-x_2-1\neq x_1$. The explanation is that we should reduce the second member of the true relation $x_1=\rho(V_a)$ by means of $V^2_a+2V_a+2=0$; we thus obtain

$$\rho(V_a)=\frac{-16V_a-64}{16V_a+64}=-1,$$

which is the correct value of x_1. Since V_c satisfies the same quadratic equation as V_1, our first reduction yields also the true relation $x_3=V_c-1$.

We therefore see why we obtain a true relation if we apply the substitution c to the members of the reduced relation $x_2 = V_1 - 1$, and why it would be accidental if we obtained a true relation when we apply to $x_2 = V_1 - 1$ any substitution other than c and the identity substitution. This example brings us to the core of our subject and indicates the care which must be taken in its development.

148. The Group of an Equation for a Domain R. Let the roots of a Galoisian resolvent $G(V) = 0$ of the given equation be

$$V_1, \ V_a, \ V_b, \ \ldots, \ V_l, \tag{6}$$

in which the subscripts denote the substitutions on $x_1, \ldots, x_n$ by which these V's are derived from V_1. We shall prove the

THEOREM. *The g substitutions*

$$1, \ a, \ b, \ \ldots, \ l \tag{7}$$

form a group G, called the **group of the given equation (1) for the domain R.**

We are to prove that the product rs of any two of the substitutions (7) is one of those substitutions. Take V_r as the function ϕ in § 147. Then

$$V_r = \frac{\lambda(V_1)}{F'(V_1)}, \quad V_{rs} \equiv (V_r)_s = \frac{\lambda(V_s)}{F'(V_s)},$$

where λ is a polynomial with coefficients in R. Since V_r is a root of $G(V) = 0$,

$$G\left(\frac{\lambda(V)}{F'(V)}\right) = 0$$

is satisfied when $V = V_1$. Multiplying the left member by the gth power of $F'(V)$, we obtain an integral function $I(V)$ of V which vanishes for $V = V_1$ and has numbers of R as coefficients. Hence the root V_s of the irreducible equation $G(V) = 0$ in R is a root of $I(V) = 0$ (§ 144). Since $F'(V_s) \neq 0$, we may divide $I(V_s)$ by the gth power of $F'(V_s)$ and get

$$0 = G\left(\frac{\lambda(V_s)}{F'(V_s)}\right) = G(V_{rs}).$$

Hence V_{rs} is one of the functions (6) and rs one of the substitutions (7).

EXAMPLE. For the domain of rational numbers, a Galoisian resolvent of the cubic equation (2) was seen in § 146 to have the roots V_1 and V_6. Hence the group of (2) for $R(1)$ is $\{1, (x_2x_3)\}$. But for the domain $R(i)$, a resolvent is $V-V_1=0$ and the group is the identity.

149. Characteristic Properties of the Group G of a Given Equation for a Domain R. Let ϕ/ψ be the quotient of two rational integral functions of the roots with coefficients in R, such that $\psi\neq 0$. We have (4) and

$$\psi_s=\frac{\mu(V_s)}{F'(V_s)},$$

where μ is a polynomial with coefficients in R, and $\mu(V_1)\neq 0$. If s is a substitution of G, then $\psi_s\neq 0$. For, if $\mu(V)=0$ has the root V_s, it has also the root V_1 in common with the irreducible Galoisian resolvent $G(V)=0$ (§ 144). Hence the functions

$$\frac{\phi_s}{\psi_s}=\frac{\lambda(V_s)}{\mu(V_s)} \qquad (s=1, a, \ldots, l)$$

are defined for each substitution s of the group G.

Suppose that these g functions are equal numerically, in other words, that ϕ/ψ is unaltered in value by all of the substitutions of G. Then

$$\frac{\phi}{\psi}=\frac{1}{g}\left\{\frac{\lambda(V_1)}{\mu(V_1)}+\frac{\lambda(V_a)}{\mu(V_a)}+\ \ldots\ +\frac{\lambda(V_l)}{\mu(V_l)}\right\}$$

The second member is a rational symmetric function, with coefficients in R, of the roots (6) of $G(V)=0$ and hence equals a rational function of its coefficients, which belong to R. Hence ϕ/ψ equals a number in R.

A. *If a rational function with coefficients in R of the roots of an equation with coefficients in R remains unaltered in value by all of the substitutions of the group G of the equation for R. it equals a number in R.*

B. *Conversely, if a rational function of the roots with coefficients in R equals a number in R, it remains unaltered in value by all of the substitutions of G.*

It remains to prove B. Let ϕ/ψ equal the number r in R. Then $\lambda(V)/\mu(V)-r$ vanishes for $V=V_1$. Hence the equation

$\lambda(V)-r\mu(V)=0$ with coefficients in R is satisfied by every root V_s of the irreducible equation $G(V)=0$ (§ 144). Hence

$$r=\frac{\lambda(V_s)}{\mu(V_s)}=\frac{\phi_s}{\psi_s} \qquad (s=1,\ a,\ \ldots,\ l),$$

so that ϕ/ψ is unaltered in value by the substitutions of G.

EXAMPLE. Consider a cubic equation, like (2), with a rational root x_1 and no multiple root. By property B with x_1 as the rational function, its group for any domain containing the coefficients has no substitution other than 1 and (x_2x_3). If the domain contains x_2 and hence also x_3, the group is the identity; this is the case with equation (2) for $R(i)$. In the contrary case, there must, by property A, be a substitution altering x_2, so that the group is $\{1,\ (x_2x_3)\}$.

Since an $n!$-valued function V_1 with coefficients in a given domain R can be chosen in an infinitude of ways, there are infinitely many Galois resolvents $G(V)=0$. Our definition of the group G of the given equation for the domain was based upon a single such resolvent, i.e., upon a particular V_1. It is a fundamental proposition that different functions V_1 always lead to the same group G. This follows from the

THEOREM. *The group of a given equation for a given domain R is uniquely defined by properties* A *and* B.

First, suppose that $G'=\{1,\ a',\ b',\ \ldots,\ m'\}$ is a group for which property A holds. Then the coefficients of

$$\phi(V)\equiv(V-V_1)(V-V_{a'})(V-V_{b'})\ \ldots\ (V-V_{m'}),$$

being symmetric functions of $V_1, \ldots, V_{m'}$, are unaltered numerically by the substitutions of G' and hence equal numbers in R. Since the equation $\phi(V)=0$, with coefficients in R, admits one root V_1 of the irreducible Galoisian resolvent $G(V)=0$, it admits all of the roots (6) of the latter (§ 144). Hence $1, a, \ldots, l$ occur among the substitutions of G', so that G is a subgroup * of G'.

Second, suppose that $\Gamma=\{1,\ \alpha,\ \beta,\ \ldots,\ \chi\}$ is a group for which property B holds. Then the Galoisian function

* In Part III, a group is included among its subgroups.

$G(V_1)$, being equal to the number zero in R, remains unaltered in value by the substitutions $\alpha, \beta, \ldots, \chi$, so that

$$0=G(V_1)=G(V_\alpha)= \ \ldots \ =G(V_\chi).$$

Hence $V_\alpha, \ldots, V_\chi$ occur among the roots (6) of $G(V)=0$. Thus Γ is a subgroup of G.

If $G'=\Gamma$, then $G'=G$.

In view of its repeated application below, we state our second result as the

COROLLARY. *If every rational function of the roots with coefficients in R which equals a quantity in R is unaltered in value by every substitution of a group Γ, then Γ is a subgroup of the group G for R of the equation.*

150. Transitive Group. We shall make much use of the

THEOREM. *If an equation is irreducible in a domain R, its group for R is transitive, and conversely.*

Consider an equation $f(x)=0$ irreducible in R. Contrary to the theorem, suppose that its group G for R is intransitive and contains substitutions replacing x_1 by $x_1, x_2, \ldots, x_m$, but none replacing x_1 by one of $x_{m+1}, \ldots, x_n$. Hence every substitution of G permutes $x_1, \ldots, x_m$ amongst themselves and thus leaves unaltered any symmetric function of them. Hence

$$g(x)\equiv(x-x_1)(x-x_2) \ \ldots \ (x-x_m)$$

has its coefficients in R, in view of property A. Thus $f(x)$ has the factor $g(x)$ in R, contrary to its irreducibility in R.

To prove the converse, let G be transitive and the equation $f(x)=0$ be reducible in R. Let the preceding function $g(x)$ be a factor of $f(x)$, the coefficients of $g(x)$ being in R and its degree m being less than n. Since $g(x_1)$ equals the number zero of R, it is unaltered by every substitution of G (property B). Since G is transitive, $g(x_i)=0$ for $i=1, \ldots, n$. This contradicts $m<n$.

EXAMPLE 1. Find the group G of $x^3-7x+7=0$ for $R(1)$.

The equation is irreducible (Ex. 4, § 144), so that G is transitive. It

will therefore be the alternating group $G_3=\{1, (x_1x_2x_3), (x_1x_3x_2)\}$ if shown not to be the symmetric group. The square of the function

$$\psi=(x_1-x_2)(x_2-x_3)(x_3-x_1) \tag{8}$$

is the discriminant * 49 of our cubic, so that ψ equals a number ± 7 of the domain $R(1)$. A transposition changes ψ to $-\psi$ and hence is not in G (property B). Hence $G=G_3$.

EXAMPLE 2. Find the group G of $x^4+1=0$ for $R(1)$.

If $x_1, \ldots, x_4$ are the roots of $x^4+ax^3+bx^2+cx+d=0$, then

$$y_1=x_1x_2+x_3x_4, \quad y_2=x_1x_3+x_2x_4, \quad y_3=x_1x_4+x_2x_3$$

are the roots of the resolvent cubic equation

$$y^3-by^2+(ac-4d)y-a^2d+4bd-c^3=0, \tag{9}$$

as shown † by finding $y_1+y_2+y_3, \ldots, y_1y_2y_3$, or by Ferrari's method of solving the quartic equation. For $x^4+1=0$, (9) is $y^3-4y=0$ and has three distinct rational roots. Hence (by B), each substitution of G leaves y_1, y_2 and y_3 formally unaltered. Now y_1 is unaltered only by the substitutions of the group

$$G_8=\{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}, \tag{10}$$

while y_2 is unaltered only by the substitutions of

$$G'_8=\{1, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\}. \tag{11}$$

The substitutions common to these groups form the group

$$G_4=\{1, (12)(34), (13)(24), (14)(23)\}. \tag{12}$$

By Ex. 2 of § 142, x^4+1 is irreducible in $R(1)$. Hence $G=G_4$.

EXAMPLE 3. Find the group G of $x^4+x^3+x^2+x+1=0$ for $R(1)$.

The roots may be denoted by $x_1=\epsilon$, $x_2=\epsilon^2$, $x_3=\epsilon^4$, $x_4=\epsilon^3$, where ϵ is an imaginary fifth root of unity. Then $y_3=2$, while $y_1=\epsilon^3+\epsilon^2$ and $y_2=\epsilon^4+\epsilon$ are the roots $\frac{1}{2}(-1\pm\sqrt{5})$ of $y^2+y-1=0$, as may also be shown by use of (9). Thus G is a subgroup of G'_8, which leaves y_2 formally unaltered. But the substitutions (13), (24), (12)(34) and (14)(23) replace $x_2-x_1^2$, whose value is zero, by functions which are not zero. Hence G is a subgroup of the cyclic group generated by (1234). Since the equation is irreducible in $R(1)$, by Ex. 6, § 144, G is this cyclic group.

* For $x^3+px+q=0$, $\psi^2=-4p^3-27q^2$.

† Cf. Dickson's *Elementary Theory of Equations*, p. 39, § 3.

EXERCISES.

For the domain of rational numbers, find the group of

1. $x^3-1=0$. 2. $(x-1)(x+1)(x-2)=0$.

3. $x^3-9x+9=0$ [compute (8)]. 4. $x^3-2=0$.

5. For the domain $R(\omega)$, where ω is an imaginary cube root of unity, the group of $x^3-2=0$ is of order 3. [Compute (8)].

6. For the domain $R(i)$, the group of $x^4+1=0$ is of order 2.

7. Find the group G of a reciprocal quartic equation

$$x^4+ax^3+bx^2+ax+1=0$$

for the domain $R=R(a, b)$, when it is irreducible in R.

Hints: Choose the notation for the roots so that $x_1x_2=x_3x_4=1$. Then one root of the cubic (9) is $y_1=2$; thus y_2 and y_3 are the roots $\frac{1}{2}b-1\pm\sqrt{A}$ of $y^2+(2-b)y+a^2-2b=0$, where $A\equiv(\frac{1}{2}b+1)^2-a^2$. The three y's are distinct; for example, $y_2-y_1=(x_1-x_4)(x_3-x_2)$. Hence G is a subgroup of G_8, given by (10). Further, G is G_4, given by (12), if and only if $\sqrt{A}$ is in R.

By the usual substitution $v=x+1/x$, our quartic becomes $v^2+av+b-2=0$, whose roots are therefore x_1+x_2 and x_3+x_4. Its discriminant $B\equiv a^2-4(b-2)$ is thus the square of $t=x_1+x_2-x_3-x_4$. Why is $t\neq0$? Now (1324), (14)(23) and (13)(24) replace t by $-t$, while the first four substitutions in (10) leave t unaltered. Again, y_2-y_3 is unaltered only by the subgroup G_4 of G_8, being changed in sign by the remaining four substitutions of G_8. Hence $t(y_2-y_3)$ is unaltered only by the subgroup C_4 generated by (1324). Hence $G=C_4$ if and only if $\sqrt{AB}$ is in R.

If a transitive subgroup of G_8 does not contain (1324) or its inverse (1423), it contains (13)(24) and (14)(23), the only remaining substitutions replacing x_1 by x_3 and x_4, respectively, and hence is G_4. Thus if G is not C_4 or G_4, it is G_8. It follows by formal logic that $G=G_8$ if and only if neither $\sqrt{A}$ nor $\sqrt{AB}$ is in R.

8. If the quartic in Ex. 7 is reducible in R, it is the product of two factors x^2+px+r and x^2+qx+1/r, where p, q, r are in R, and

$$p+q=a, \quad \frac{p}{r}+rq=a, \quad r+\frac{1}{r}+pq=b.$$

If $r=1$, p and q are in R only when $\sqrt{B}$ is in R. If $r=-1$, then $a=0$ and $\sqrt{-b-2}$ must be in R. If $r^2\neq1$, we may eliminate p and q and obtain for $y=r+1/r$ the quadratic * in Ex. 7 with the roots y_2, y_3; thus R must contain $\sqrt{A}$ and the square roots of $(\frac{1}{2}b-1\pm\sqrt{A})^2-4$, the latter being the values of $(r-1/r)^2=y^2-4$ for $y=y_2$, y_3. By Ex. 7, $AB\neq0$ if the four roots are distinct.

9. If $a=b=0$, then $A=1$, $B=8$, and x^4+1 is irreducible in $R(1)$, and

* Except for $a=0$; then $p=q=0$, $y=b$.

has the group G_4. If $a=b=1$, then $A=5/4$, $B=5$, and $x^4+x^3+x^2+x+1=0$ is irreducible in $R(1)$ and has the group C_4.

Let $f(x)=a_0x^n+a_1x^{n-1}+\ldots=0$ be an equation with rational coefficients, irreducible in the domain of rational numbers. Prove * Exs. 10–14:

10. If there is a complex root of absolute value unity, the equation is a reciprocal equation of even degree.

11. If there is a root $r+si$, where r is rational, then n is even and the n roots may be paired so that the sum of the two of any pair is $2r$, whence $r=-a_1/(na_0)$. In particular, if $r=0$, the equation involves only even powers of x.

12. If there is an imaginary root $a+bi$ whose norm a^2+b^2 is rational, then n is even and the n roots can be paired so that the product of any two of a pair is a^2+b^2.

13. If there is a root whose absolute value ρ is rational, ρ can be expressed in terms of the coefficients. $(\rho^n=a_n/a_0.)$

14. If we set $x=\rho y$ in the equation in Ex. 13, we obtain a reciprocal equation in y.

EQUATIONS WHOSE COEFFICIENTS INVOLVE VARIABLES, §§ 151–6

151. Definition of the Roots. We begin with the so-called *general equation* (1) whose coefficients $c_1, \ldots, c_n$ are independent complex variables. Let $\Delta(c_1, \ldots, c_n)$ be its discriminant. Let $a_1, \ldots, a_n$ and $A_1, \ldots, A_n$ be any two sets of constant values of $c_1, \ldots, c_n$ for which $\Delta\neq 0$. We shall prove that the A's can be derived from the a's by continuous variation such that, for each intermediate set of values, $\Delta\neq 0$; expressed in geometrical language, there is a continuous path from the point (a) to the point (A) not passing through a point of the locus $\Delta=0$.

We shall prove this by induction from $n-1$ to n, assuming that, if $P(c_1, \ldots, c_{n-1})$ is any polynomial in $c_1, \ldots, c_{n-1}$, zero neither at $(l_1, \ldots, l_{n-1})$ nor at $(L_1, \ldots, L_{n-1})$, there is a continuous path from (l) to (L) not passing through a point of the locus $P=0$. Neither of the polynomials

$$\Delta(c_1, \ldots, c_{n-1}, a_n) \quad \Delta(c_1, \ldots, c_{n-1}, A_n)$$

is identically zero, since the first is not zero when each $c_i=a_i$, and the second is not zero when each $c_i=A_i$. Hence there are constants α_i for which

$$\Delta(\alpha_1, \ldots, \alpha_{n-1}, a_n)\neq 0, \quad \Delta(\alpha_1, \ldots, \alpha_{n-1}, A_n)\neq 0.$$

Thus there is, by hypothesis, a continuous path from $(a_1, \ldots, a_{n-1}, a_n)$ to $(\alpha_1, \ldots, \alpha_{n-1}, a_n)$, not passing through a point of $P\equiv\Delta(c_1, \ldots, c_{n-1}, a_n)=0$ and composed only of points with $c_n=a_n$, and hence not passing

* Exs. 10, 11, 13 are due to Dr. A. J. Kempner.

through a point of $\Delta(c_1, \ldots, c_n)=0$. The equation $\Delta(\alpha_1, \ldots, \alpha_{n-1}, v)=0$ in v has only a finite number of roots. Hence v can be varied continuously from a_n to A_n so that $\Delta(\alpha_1, \ldots, \alpha_{n-1}, v)\neq 0$ at each intermediate point. The combination of our two paths gives a continuous path from (a) to $(\alpha_1, \ldots, \alpha_{n-1}, A_n)$ not passing through a point of $\Delta=0$.

Similarly, there exist constants β_i for which

$$\Delta(\beta_1, \ldots, \beta_{n-2}, \alpha_{n-1}, A_n)\neq 0, \quad \Delta(\beta_1, \ldots, \beta_{n-2}, A_{n-1}, A_n)\neq 0.$$

By hypothesis, there is a continuous path from $(\alpha_1, \ldots, \alpha_{n-1}, A_n)$ to $(\beta_1, \ldots, \beta_{n-2}, \alpha_{n-1}, A_n)$, not passing through a point of $\Delta(c_1, \ldots, c_{n-2}, \alpha_{n-1}, A_n)=0$ and composed of points with $c_{n-1}=\alpha_{n-1}$, $c_n=A_n$, and hence not passing through a point of $\Delta(c_1, \ldots, c_n)=0$. Evidently there is a continuous path from our final point to $E=(\beta_1, \ldots, \beta_{n-2}, A_{n-1}, A_n)$ not passing through a point of $\Delta=0$. We now have a continuous path from (a) to E not passing through a point of $\Delta=0$. Proceeding in this manner, we finally get such a path from (a) to (A).

Let $x_1^0, \ldots, x_n^0$ be the n distinct roots of the equation with the coefficients $a_1, \ldots, a_n$. These roots receive increments as small in absolute value as we please when $a_1, \ldots, a_n$ are given increments sufficiently small in absolute value.* Hence if we proceed along our path from (a) to (A), we obtain a definite coördination of the roots $x'_1, \ldots, x'_n$ of the equation having the coefficients $A_1, \ldots, A_n$ with the initial values $x_1^0, \ldots, x_n^0$. Thus the latter and definite paths radiating from (a) lead to n functions $x_1, \ldots, x_n$ of $c_1, \ldots, c_n$ uniquely defined for every set of c's for which $\Delta\neq 0$, and called the roots of the general equation (1). In fact, for a particular set of c's, the roots of the equation are the values of the functions $x_1, \ldots, x_n$ for those c's. Our main investigation is the comparison of a rational function of the roots with that derived by a substitution on the roots; hence we shall not be interested in values of the c's for which $\Delta=0$, i.e., for which two or more roots become equal.

The same scheme defines *a fortiori* the roots of any equation whose coefficients are functions of one or more variables. We retain only those sets (A) which are sets of values of our present coefficients. The fact that certain of the sets intermediate to (a) and (A) are not now values of our coefficients does not disturb the coördination of the roots at (A) with those at (a). The scheme therefore assembles the root values into root functions.

152. Function Domains, Equality, Group of an Equation. Instead of a domain composed of constants, we now employ a domain $R(k_1, \ldots, k_m)$ composed of all rational functions

* The roots are continuous functions of the coefficients. For a proof, see Weber's *Algebra*, vol. 1, 1895, p. 132.

with rational coefficients of $k_1, \ldots, k_m$, either all of which are given functions, or certain of which are functions and the others are constants. For example, $R(\sqrt{3}, k)$ is composed of all rational functions of the variable k with coefficients of the form $a+b\sqrt{3}$, where a and b are rational numbers.

Two polynomials ϕ and ψ in the variables $v_1, \ldots, v_i$ with coefficients in R are called equal if they have the same numerical value for every set of numerical values which $v_1, \ldots, v_i, k_1, \ldots, k_m$ can assume. For example, if v_1 and v_2 are the roots of $x^2+kx+1=0$, then $v_1+v_2=-kv_1v_2$.

The equality of two rational functions of $v_1, \ldots, v_i$ is defined similarly, but with restriction to those sets of values of the v's and k's for which each denominator is not zero.

If ψ is derived from ϕ by a substitution s on $v_1, \ldots, v_i$ and if $\psi=\phi$ in the present sense of equality, we shall say that ϕ is unaltered by s.

The definitions and theorems in §§ 142–4 concerning irreducibility evidently hold for the present generalized domain R. Each element (function) in R is conveniently called a *quantity* in R.

Proceeding as in §§ 145–9, we see that an equation whose coefficients $c_1, \ldots, c_n$ are any given functions or constants has a definite group G for any given domain containing $c_1, \ldots, c_n$.

153. Group of the General Equation. Let the coefficients $c_1, \ldots, c_n$ be independent complex variables. Let $x_1, \ldots, x_n$ be the roots in the sense of § 151.

LEMMA. *If a rational integral function $\psi(x_1, \ldots, x_n)$ of the roots with constant coefficients is zero for every set of values of $c_1, \ldots, c_n$, each coefficient of ψ is zero.*

We consider those sets of values of $c_1, c_2, \ldots, c_n$ which are the values of the elementary symmetric functions Σv_1, $\Sigma v_1v_2, \ldots, v_1 \ldots v_n$ of the independent variables $v_1, \ldots, v_n$. For each set of values of the v's we therefore obtain a set of values of $x_1, \ldots, x_n$ forming a permutation of the v's. Consider the product P of $\psi(v_1, \ldots, v_n)$ by the functions obtained from it by applying the various substitutions,

other than identity, on $v_1, \ldots, v_n$. For every set of v's, one factor of P is a value of $\psi(x_1, \ldots, x_n)$ and hence is zero. Thus P is zero identically in the v's. Hence some factor ψ of it is zero identically.

THEOREM. *The group of the general equation for the domain R defined by its coefficients and any chosen constants is the symmetric group.*

The coefficients of its Galoisian resolvent $G(V)=0$ are rational integral functions of $c_1, \ldots, c_n$ with constant coefficients. Replace $c_1, \ldots, c_n$ by the elementary symmetric functions of $x_1, \ldots, x_n$. Then $G(V)$ becomes a polynomial $P(V)$ whose coefficients are rational integral functions of the x's with constant coefficients. Let $V_1=\Sigma m_i x_i$, where $m_1, \ldots, m_n$ are distinct integers, be the function used in constructing $G(V)$. Then $P(V_1)$ is a rational integral function of the x's with constant coefficients which is zero for every set of values of the c's. By the Lemma, $P(V_1)$ is zero identically in the x's. The function derived from it by applying any substitution s on the x's is therefore zero identically in the x's. Since the coefficients of $G(V)$ are unaltered by this substitution, we get $G(V_s)=0$. Hence every substitution s occurs in the group of the equation.

EXERCISES

1. Prove the last theorem by showing that properties A and B in § 149 hold when G is the symmetric group. Note that if $\phi=\phi_s$ for all values of the c's, then, by the Lemma, $\phi\equiv\phi_s$ identically in the x's; if this is true for every substitution s, ϕ is symmetric and hence is a rational function with rational coefficients of $c_1, \ldots, c_n$ and the coefficients of ϕ. Next, if $\phi(x_1, \ldots, x_n)$ equals a rational function of the c's and hence a rational symmetric function ψ of the x's, for every set of c's, then $\phi\equiv\psi$ identically in the x's (Lemma), so that ϕ is symmetric, and property B holds.

2. If G is the group of $f(x, c)\equiv x^n-c_1x^{n-1}+\ldots\pm c_n=0$ for the domain $R=R(c_1, \ldots, c_n, k_1, \ldots, k_l)$, where $k_1, \ldots, k_l$ are constants, and if $c'_1, \ldots, c'_n$ are values which $c_1, \ldots, c_n$ can take, then the group G' of $f(x, c')=0$ for $R'=R(c'_1, \ldots, c'_n, k_1, \ldots, k_l)$ is G or a subgroup of G.

Hint: If $G(V, c)=0$ is the Galoisian resolvent of $f(x, c)=0$ for R, the group of $f(x, c')=0$ for R' is G or a subgroup according as $G(V, c')$ is irreducible or reducible in R'.

3. Hence the group of the general cubic $x^3-c_1x^2+c_2x-c_3=0$ for $R(c_1, c_2, c_3)$ is G_6, since that of $x^3-2=0$ for $R(1)$ is G_6.

4. For a and b independent variables, the group of $x^4+ax^3+bx^2+ax+1=0$ is G_8.

5. The group of an irreducible quartic equation for a domain R is the symmetric group if no one of the roots y_1, y_2, y_3 of the resolvent cubic equation (9) is in R, and if the product P of the differences of the y's is not in R.

Hints: Its group G is not (10) or (11), and not the group G''_3 leaving y_3 unaltered, nor their common subgroup (12), nor a cyclic group of order four, necessarily contained in one of these groups of order eight. The only remaining transitive groups are the alternating and symmetric groups, § 16. But G is not the former in view of P.

6. The group of an irreducible quartic for R is G_{24} if that of the resolvent cubic (9) is G_6.

154. Rational Functions belonging to a Group. Let $1, a, b, \ldots, k$ be all of the substitutions of the group G of a given equation for a given domain R which leave unaltered (in the sense of § 152) a given rational function $\psi(x_1, \ldots, x_n)$ of the roots with coefficients in R. Since $\psi-\psi_a$ has tne value zero, we have $\psi_b-\psi_{ab}=0$ by property B. Hence $\psi_{ab}=\psi$ and ab is in the set $1, a, \ldots, k$, which therefore forms a group H. We shall say that *ψ belongs to the subgroup H of G.*

EXAMPLE. Let x_1 and $x_2=-x_1$ be two roots of $x^4+1=0$. The only substitutions of its group (12) for $R(1)$ which leave x_1^2 unaltered are 1, (12)(34). Hence they form the subgroup to which x_1^2 belongs.

Conversely, let H be any given subgroup of G. Let V_1 be any $n!$-valued function of the roots with coefficients in R, and let $V_1, V_a, \ldots, V_k$ be the functions obtained from V_1 by applying the substitutions of H. If ρ is a suitably chosen number in R,

$$\psi\equiv(\rho-V_1)(\rho-V_a)\ \ldots\ (\rho-V_k)$$

is a rational function of the roots x_i with coefficients in R which belongs to H. For, if s be any substitution of H, then $s, as, \ldots, ks$ are distinct and are in H, and hence form a permutation of $1, a, \ldots, k$. Thus ψ equals

$$\psi_s\equiv(\rho-V_s)(\rho-V_{as})\ \ldots\ (\rho-V_{ks}).$$

But, if s is a substitution of G not in H, then ψ_s is not identical with ψ as to the variable ρ, since V_s is different from V_1, V_a, . . . , V_k. We may therefore choose an integer ρ such that ψ belongs to H. This proves

THEOREM 1. *Every rational function ψ with coefficients in R of the roots of an equation with the group G for the domain R belongs to a definite subgroup of G. There exist such functions ψ belonging to any assigned subgroup of G.*

We next prove the important supplementary

THEOREM 2. *If a rational function ψ, with coefficients in a domain R, of the roots of an equation with the group G for R, belongs to a subgroup H of index ν under G, then the substitutions of G replace ψ by exactly ν distinct functions; they are the roots of an equation*

$$g(y) \equiv (y-\psi_1)(y-\psi_2) \ . \ . \ . \ (y-\psi_\nu) \tag{13}$$

with coefficients in R and irreducible in R.

As in § 10, let

$$G = H + Hg_2 + Hg_3 + \ . \ . \ . \ + Hg_\nu. \tag{14}$$

Let h be any substitution of H. Then

$$\psi_{hg_i} = (\psi_h)_{g_i} = (\psi)_{g_i} = \psi_{g_i}.$$

Thus ψ takes at most ν values under G. But, if

$$\psi_{g_i} = \psi_{g_j} \qquad (j<i),$$

then $\psi_{g_i g_j^{-1}} = \psi$, so that $g_i g_j^{-1}$ is a substitution h of G leaving ψ unaltered and hence is in H. Then $g_i = hg_j$, contrary to (14). Thus $\psi_1, \psi_2, \ . \ . \ . \ , \psi_\nu$ are distinct, where ψ_i has been written for ψ_{g_i}. They are called the *conjugates to* $\psi \equiv \psi_1$ under G.

Any substitution s of G merely permutes $\psi_1, \ . \ . \ . \ , \psi_\nu$ amongst themselves. For, any product $g_i s$ may be written in the form hg_j where h is in H; then

$$(\psi_i)_s = \psi_{g_i s} = \psi_{hg_j} = \psi_{g_j} = \psi_j.$$

Hence the coefficients of (13) are unaltered by every substitution of G and therefore equal quantities in R.

If $g(y)$ has a factor with coefficients in R, it has a factor

$\gamma(y)$ which is zero for $y=\psi_1$ and hence (by B of § 149) for $y=\psi_2, \ldots, y=\psi_\nu$. Thus $\gamma \equiv g$, so that $g(y)$ is irreducible in R.

EXAMPLE 1. The group G of $x^3+x^2+x+1=0$ for $R(1)$ is $\{1, (x_2x_3)\}$, if $x_1=-1$ denotes the real root. The conjugates to $\psi_1=x_2-x_1$ under G are ψ_1 and $\psi_2=x_3-x_1$; they are the roots of $y^2-2y+2=0$.

EXAMPLE 2. The group G of $x^4+1=0$ for $R(i)$ is $\{1, (x_1x_3)(x_2x_4)\}$ if $x_1=\epsilon$, $x_2=i\epsilon$, $x_3=-\epsilon$, $x_4=-i\epsilon$, where $\epsilon=(1+i)/\sqrt{2}$, so that $\epsilon^2=i$. The conjugates x_1 and x_3 to x_1 under G are the roots of $y^2-i=0$, which is irreducible in $R(i)$, to which ϵ does not belong.

155. Galois' Generalization of Lagrange's Theorem. *If a rational function ϕ, with coefficients in a domain R, of the roots of an equation $f(x)=0$, with the group G for R, remains unaltered by all those substitutions of G which leave unaltered another rational function ψ of the roots with coefficients in R, then ϕ equals a rational function of ψ with coefficients in R.*

In case ψ is an $n!$-valued function V_1, the only substitution leaving ψ unaltered is the identity, and this leaves any ϕ unaltered. For this case, the theorem states that any rational function ϕ with coefficients in R equals a rational function of V_1 with coefficients in R. This follows from the like result in § 147 for the rational integral numerator and denominator of ϕ.

Let H be the subgroup of G of index ν to which ψ belongs. By means of (14), we obtain the ν distinct conjugates $\psi_1, \ldots, \psi_\nu$ to $\psi \equiv \psi_1$ under G. Since every substitution h of H leaves ϕ unaltered, each product hg_i replaces ϕ by $\phi_i \equiv \phi_{\theta_i}$. Any substitution s of G replaces ψ_i by a certain ψ_j (end of § 154) and likewise ϕ_i by ϕ_j. Thus, for $g(y)$ defined by (13),

$$\lambda(y) \equiv g(y)\left(\frac{\phi_1}{y-\psi_1}+\frac{\phi_2}{y-\psi_2}+\ \cdots\ +\frac{\phi_\nu}{y-\psi_\nu}\right)$$

is an integral function of y each of whose coefficients is unaltered by every substitution of G and hence is in R. Taking $\psi_1 \equiv \psi$ as y, we get $\phi=\lambda(\psi) \div g'(\psi)$.

The theorem will be shown to be a generalization of

LAGRANGE'S THEOREM. *If a rational function ϕ of the independent variables $x_1, \ldots, x_n$ remains unaltered by all those substitutions on $x_1, \ldots, x_n$ which leave unaltered another*

rational function ψ of $x_1, \ldots, x_n$, then ϕ equals a rational function of ψ and the elementary symmetric functions

$$c_1 = \Sigma x_1, \ \ldots, \ c_n = x_1 x_2 \ \ldots \ x_n.$$

The group of the equation with the coefficients $c_1, \ldots, c_n$ for the domain R, defined by $c_1, \ldots, c_n$ and given constants k_i, is the symmetric group. For, property A then states that any symmetric function of $x_1, \ldots, x_n$ with coefficients rational in the k's is in R, and is the well-known theorem on symmetric functions. Conversely, a function equal to a quantity in R is symmetric.

EXAMPLE. $y_2 = x_1x_3 + x_2x_4$ is unaltered by all of the substitutions 1, (13), (24), (13)(24), which leave $\psi = x_1 + x_3 - x_2 - x_4$ unaltered. We see that

$$y_2 = \tfrac{1}{4}(\psi^2 - c_1^2 + 4c_2), \quad c_1 = \Sigma x_1, \quad c_2 = \Sigma x_1 x_2.$$

When a rational function of independent variables $x_1, \ldots, x_n$ is unaltered by each substitution of a group H on the x's, but is altered by every substitution not in H, it is said to *belong* to the group H. We need not specify as in § 154 that H is a subgroup of the group G of the equation with the x's as roots, since G is now the total symmetric group.

156. Effect on the Group by an Adjunction to the Domain. Let G be the group of $f(x) = 0$ for a domain $R = R(k_1, \ldots, k_m)$ containing the coefficients. Let $R' = R(\psi, k_1, \ldots, k_m)$ be the domain composed of the rational functions of $\psi, k_1, \ldots, k_m$ with rational coefficients. This enlarged domain R' is said to be derived from R by *adjoining* the quantity ψ. If the irreducible Galoisian resolvent $G(V) = 0$ for the initial domain R remains irreducible in R', the group of $f(x) = 0$ for R' is evidently G. But if it reduces in R', let $G'(V)$ be that factor of $G(V)$ which has its coefficients in R', is irreducible in R', and vanishes for $V = V_1$. Then if $V_1, V_a, \ldots, V_k$ are the roots of $G'(V) = 0$, the group of $f(x) = 0$ for R' is $G' = \{1, a, \ \ldots, k\}$, a subgroup of G. As a group is included among its subgroups, we have

THEOREM 1. *By an adjunction to the domain, the group of an equation is reduced to a subgroup.*

EXAMPLE 1. The group ot $x^3+x^2+x+1=0$ for $R(1)$ is $\{1, (x_2x_3)\}$ if $x_1=-1$ is the rational root. By adjoining i, we obtain the enlarged domain $R(i)$, for which the group is the identity, since now also $x_2=i$ and $x_3=-i$ are in the enlarged domain. The Galoisian resolvent V^2-2V+2 for $R(1)$ has the factors $V\pm i-1$ in $R(i)$.

EXAMPLE 2. The group of $x^4+1=0$ for $R(1)$ is G_4, given by (12). By Ex. 2 of § 154, the group for $R(i)$ is $G_2=\{1, (x_1x_3)(x_2x_4)\}$, which is the subgroup of G_4 to which $i=x_1^2=x_3^2=-x_2^2=-x_4^2$ belongs.

These examples illustrate also the important

THEOREM 2. *By the adjunction of a rational function $\psi(x_1, \ldots, x_n)$ of the roots with coefficients in the initial domain R, the group of the equation is reduced from G to the subgroup H to which ψ belongs.*

It is to be shown that H has the characteristic properties A and B (§ 149) of the group of the equation for the enlarged domain R'. Any rational function ϕ of the roots with coefficients in R' equals a rational function ϕ_1 of the roots with coefficients in R.

First, let ϕ be unaltered by all the substitutions of H. By § 155, ϕ_1 (which is unaltered by H) is a rational function of ψ with coefficients in R. Hence $\phi_1=\phi$ is in R'. Hence property A holds for H and R'.

Second, let ϕ equal a quantity ρ in R', namely, a rational function $\rho(\psi)$ with coefficients in R. Then $\phi_1-\rho(\psi)$ is a rational function of $x_1, \ldots, x_n$ with coefficients in R having the value zero, and hence is unaltered by every substitution of G and, in particular, by the substitutions of H. The latter leave $\rho(\psi)$ unaltered and therefore also $\phi_1=\phi$. Hence property B holds for H and R'.

EXERCISES

1. By the adjunction of $\sqrt{2}$, the group G_2 of $x^4+1=0$ for $R(i)$ is reduced to the identity G_1.

2. By the adjunction of an imaginary cube root ω of unity, the group G_6 of $x^3-2=0$ for $R(1)$ is reduced to the cyclic group C_3. Verify that $\omega=x_2/x_1$ belongs to the group C_3. By the further adjunction of $\sqrt[3]{2}$, the group is reduced to the identity G_1.

3. Find the group of $x^4+x^3+x^2+x+1=0$ for $R(\sqrt{5})$.

CHAPTER XV

SUFFICIENT CONDITION THAT AN ALGEBRAIC EQUATION BE SOLVABLE BY RADICALS

157. Solvability by Radicals. An algebraic equation is said to be solvable by radicals if all of its roots can be derived by addition, subtraction, multiplication, division, and extraction of a pth root (where p has a finite number of positive integral values), these operations being performed a finite number of times upon the coefficients of the equation or upon quantities obtained from them by those operations.

For example, Cardan's formulas (deduced in § 158) for the roots of $x^3+c_2x-c_3=0$ are $A+B$, $\omega A+\omega^2 B$, $\omega^2 A+\omega B$, where ω is an imaginary cube root of unity and

$$A=\sqrt[3]{\frac{1}{2}c_3+\sqrt{r}}, \quad B=\sqrt[3]{\frac{1}{2}c_3-\sqrt{r}}, \quad r=\frac{c_2^3}{27}+\frac{c_3^2}{4},$$

A being any definite cube root of $\frac{1}{2}c_3+\sqrt{r}$, and B being chosen so that $AB=-c_2/3$. The radical in $\omega=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$ is a square root of the number -3 which can be derived from the coefficient of x^3 by rational operations.

In the above definition we permitted the use of the operation of finding one of the pth roots of a quantity previously determined, but not the use of the operations of finding all of the pth roots. The use of the latter operations would imply a knowledge of all of the pth roots of unity, whereas we shall prove that the pth roots of unity are expressible in terms of $\sqrt{-1}$ and real radicals.

The solution of an equation solvable by radicals is often accomplished by the use of a series of auxiliary equations, the roots of any one of which can be found by rational operations

and root extractions performed upon its coefficients as well as upon the coefficients and roots of the preceding equations of the series. In order to focus our attention upon a particular equation of a series, and to have a general and hence simpler phraseology, it is convenient to have the following generalization of the above definition of solvability by radicals.

An equation with coefficients in a domain $R(k_1, \ldots, k_m)$ shall be said to be solvable by radicals relatively to R if all of its roots can be derived by rational operations and root extractions performed upon $k_1, \ldots, k_m$ or upon quantities obtained from them by those operations.

For example, $x^{13}=2^{13}$ is evidently solvable relatively to $R(\epsilon)$, where ϵ is a particular imaginary 13th root of unity.

While a quintic equation whose coefficients $c_1, \ldots, c_5$ are independent variables will be shown to be not solvable by radicals, i.e., relatively to $R(c_1, \ldots, c_5)$, it is solvable relatively to $R'=R(x_1, c_1, \ldots, c_5)$, where x_1 is one root of the quintic (since its group for R' is a solvable group of order 24). We have merely shifted the difficulty to the determination of the new domain R'. The benefit that may be gained by the use of R' is merely one of phraseology.

158. Solution of a Cubic Equation. In

$$x^3-c_1x^2+c_2x-c_3=0,$$

let c_1, c_2, c_3 be independent variables. This general cubic equation will be discussed from the group standpoint with the aim of providing a concrete illustration of the general theory which is to follow.

Let ω be an imaginary cube root of unity. For the domain $R=R(\omega, c_1, c_2, c_3)$, the group of the cubic equation is the symmetric group G_6 on the roots x_1, x_2, x_3 (§ 153). To the cyclic subgroup C_3 belongs the function

$$\delta=(x_1-x_2)(x_2-x_3)(x_3-x_1).$$

By Theorem 2 of § 154, δ is a root of a quadratic equation with coefficients in R. In fact, the discriminant of the cubic equation is

$$\delta^2=c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2.$$

For the domain $R'=(R,\ \delta)$, the group of the cubic equation is the cyclic group C_3 (§ 156). The substitution $(x_1x_2x_3)$ of C_3 replaces the functions

$$\psi=x_1+\omega x_2+\omega^2x_3,\quad \chi=x_1+\omega^2x_2+\omega x_3,$$

with coefficients in R, by $\omega^2\psi$ and $\omega\chi$, respectively. Thus the substitutions of C_3 leave ψ^3 and χ^3 unaltered. Hence (§ 155) the latter are rational functions, with coefficients in R, of δ. We have

$$\psi^3+\chi^3=a\equiv 2c_1{}^3-9c_1c_2+27c_3,\quad \psi^3-\chi^3=-3\sqrt{-3}\,\delta,$$

$$\psi^3=\tfrac{1}{2}(a-3\sqrt{-3}\,\delta).$$

A cube root ψ of the last quantity is adjoined to R'; the group is thereby reduced to the identity group G_1 to which ψ belongs. The roots x_i are now in the enlarged domain $(R',\ \psi)$. From the expressions for c_1, ψ, χ, we find by multiplications

$$x_1=\tfrac{1}{3}(c_1+\psi+\chi),\quad x_2=\tfrac{1}{3}(c_1+\omega^2\psi+\omega\chi),\quad x_3=\tfrac{1}{3}(c_1+\omega\psi+\omega^2\chi).$$

Here $\chi=(c_1{}^2-3c_2)/\psi$. In brief, the above solution consists in finding, by means of a quadratic equation, a function ψ^3 which belongs to C_3, and then finding, by means of a binomial cubic equation, the function ψ which belongs to G_1.

Taking $c_1=0$, we obtain Cardan's formulas (§ 157).

159. Resolvent Equations and their Groups. The auxiliary quadratic and binomial cubic equations employed in the solution * of the general cubic equation are called *resolvent* equations of the latter. In general, let $f(x)=0$ be any given equation with coefficients in a given domain R, and let ψ be a rational function of its roots with coefficients in R. If ψ belongs to a subgroup H of index ν under the group G of $f(x)=0$ for R, we have seen (§ 154) that ψ is a root of a resolvent equation of degree ν with coefficients in R. Suppose that we can solve this resolvent equation relatively to R. By adjoining its root ψ to the domain R, we obtain a domain $R_1=(R,\ \psi)$ for which the group of $f(x)=0$ is H. If repeated adjunctions lead to a domain R_t for which the group is the identity G_1,

* For brevity, we omit the words " by radicals " after " solution " or "solve."

the roots of $f(x)=0$ will be in R_k (property A of § 149). Hence if such a series of resolvent equations can be constructed and solved relatively to their domains, the given equation can be solved relatively to R. Consequently, we shall discuss the question of the solvability of a resolvent equation; to this end we must find its group.

By use of (14) in § 154, we proved that ψ is one of ν conjugate functions under the group G:

$$\psi, \quad \psi_{\theta_2}, \quad \psi_{\theta_3}, \quad \dots, \quad \psi_{\theta_\nu}, \tag{1}$$

and that any substitution s of G replaces these by

$$\psi_s, \quad \psi_{\theta_2 s}, \quad \psi_{\theta_3 s}, \quad \dots, \quad \psi_{\theta_\nu s}, \tag{2}$$

which are merely the distinct functions (1) rearranged. Hence to any substitution s of G on the letters $x_1, \dots, x_n$ there corresponds one definite substitution

$$\sigma=\begin{pmatrix} \psi & \psi_{\theta_2} & \dots & \psi_{\theta_\nu} \\ \psi_s & \psi_{\theta_2 s} & \dots & \psi_{\theta_\nu s} \end{pmatrix} \equiv \begin{pmatrix} \psi_{\theta_i} \\ \psi_{\theta_i s} \end{pmatrix} \tag{3}$$

on the ν letters (1). Similarly, to t corresponds

$$\tau=\begin{pmatrix} \psi_{\theta_i} \\ \psi_{\theta_i t} \end{pmatrix} \equiv \begin{pmatrix} \psi_{\theta_i s} \\ \psi_{\theta_i st} \end{pmatrix},$$

since we may rearrange at will the letters in the upper line in the two-rowed notation of a substitution. The product $\sigma\tau$ replaces ψ_{θ_i} by $\psi_{\theta_i st}$ and hence corresponds to st.

THEOREM 1. *The substitutions of G correspond to substitutions* (3) *forming a group* Γ.

The group Γ is transitive and isomorphic to G.

EXAMPLE. Let G be the alternating group on the independent variables $x_1, \dots, x_4$. Now $\psi=(x_1-x_2)(x_3-x_4)$ belongs formally to the group G_4 given by (12) of § 150. We have

$$G=G_4+G_4(x_2x_3x_4)+G_4(x_2x_4x_3).$$

The indicated substitutions of period 3 replace ψ by

$$\psi_2=(x_1-x_3)(x_4-x_2), \quad \psi_3=(x_1-x_4)(x_2-x_3).$$

Since every substitution of G_4 leaves also ψ_2 and ψ_3 unaltered,

$$\Gamma=\{1, \quad (\psi\psi_2\psi_3), \quad (\psi\psi_3\psi_2)\}.$$

The importance of the group Γ is due to

THEOREM 2. *Γ is the group for R of the resolvent equation*

$$g(y) \equiv (y-\psi_1)(y-\psi_2) \ \ldots \ (y-\psi_\nu) = 0. \tag{4}$$

To prove that Γ has the characteristic properties A and B of the group of (4) for R, note that any rational function $\rho(\psi_1, \ldots, \psi_\nu)$ with coefficients in R equals a rational function $r(x_1, \ldots, x_n)$ with coefficients in R:

$$\rho(\psi_1, \ldots, \psi_\nu) - r(x_1, \ldots, x_n) = 0. \tag{5}$$

Since this difference equals a quantity in R, it is unaltered by any substitution s of G on $x_1, \ldots, x_n$. Since s gives rise to a substitution σ of Γ on $\psi_1, \ldots, \psi_\nu$, we have

$$\rho_\sigma(\psi_1, \ldots, \psi_\nu) - r_s(x_1, \ldots, x_n) = 0. \tag{6}$$

First, let ρ be unaltered by every substitution of Γ, so that $\rho = \rho_\sigma$, for every σ in Γ. Then, by (5) and (6), $r_s = r$ for every s in G. Hence, by property A for the group G, r is in the domain R. This proves property A for the group Γ.

Next, let ρ be in R. Then, by (5), r is in R. Hence, by property B for the group G, $r = r_s$ for every s in G. Then, by (5) and (6), $\rho = \rho_\sigma$ for every σ in Γ. This proves property B for the group Γ.

EXERCISES

1. Since Γ is transitive, (4) is irreducible in R.

2. If G is the symmetric group on $x_1, \ldots, x_4$, the group Γ on the three y's of Example 2, § 150, is the symmetric group of order 6.

3. If G is the symmetric group on x_1, x_2, x_3, and ψ is the alternating function, Γ is of order 2.

The function ψ_θ belongs to the subgroup $g^{-1}Hg$ of G (§ 9). Hence the ν conjugate functions (1) belong to a complete set of conjugate subgroups of G:

$$H, \quad g_2^{-1}Hg_2, \quad g_3^{-1}Hg_3, \ \ldots, \ g_\nu^{-1}Hg_\nu.$$

In case these groups are all identical, H is an invariant subgroup of G. In this case, the substitution (3) is the identity if s is in H, since s then leaves unaltered each ψ_{θ_i}; while any substitution s of G and any product hs in which h is in H corre-

spond to the same substitution (3) of Γ. Hence, by (14) in § 154, we obtain the ν distinct substitutions of Γ by taking those which correspond to $s = 1, g_2, \ldots, g_\nu$. We thus have

THEOREM 3. *If H is an invariant subgroup of G of index ν, the group Γ is a transitive group of order ν on ν letters and hence is regular.*

COROLLARY. *If H is an invariant subgroup of G of prime index ν, then Γ is a regular cyclic group of order ν.*

This is illustrated by the above example.

Beginning with the group G of the given equation for the given domain R, we can find a series of groups $G, H, K, \ldots, G_1$, terminating with the identity group G_1 and such that each is a maximal invariant subgroup of the preceding. If ν is the index of H under G, ρ the index of K under H, etc., the factors of composition of G are $\nu, \rho, \ldots$.

Construct a rational function ψ of the roots with coefficients in R such that ψ belongs to the subgroup H of G. Then ψ is a root of an equation of degree ν whose group Γ for R is simply isomorphic with the simple quotient group G/H. After the adjunction of the root ψ to R, the group of the given equation becomes H for the domain (R, ψ).

Construct a rational function χ of the roots with coefficients in (R, ψ) such that χ belongs to the subgroup K of H. Then χ is a root of an equation of degree ρ whose group for (R, ψ) is simply isomorphic with the simple group H/K. After the adjunction of χ, the group of the given equation is K. Finally, we adjoin a function belonging to G_1 and obtain a domain containing $x_1, \ldots, x_n$. We therefore have

THEOREM 4. *The solution of an equation with the group G for the domain R can be reduced to the solution of a series of equations each with a simple regular group for the domain obtained by adjoining to R a root of each of the earlier equations of the series. If, in particular, G is a solvable group, each auxiliary equation has a regular cyclic group of prime order.*

160. Equations with a Regular Cyclic Group. To supplement the last theorem we need the result that any equation with a regular cyclic group of prime order p is solvable by radicals.

We shall now prove this with the restriction that the domain contains an imaginary pth root ϵ of unity. This restriction will be removed in § 164 by proving that ϵ can be found by root extractions.

THEOREM. *An equation, whose group G for a domain R containing an imaginary pth root ϵ of unity is a regular cyclic group of prime order p, is solvable by radicals relatively to R.*

Let $x_0, x_1, \ldots, x_{p-1}$ be the roots of the equation and let G be generated by the substitution $s=(x_0x_1 \ldots x_{p-1})$. Then s replaces the function

$$\theta_i \equiv x_0+\epsilon^i x_1+\epsilon^{2i}x_2+ \ldots +\epsilon^{(p-1)i}x_{p-1},$$

with coefficients in R, by $\epsilon^{-i}\theta_i$. Let $\Theta_i=\theta_i^p$. Then Θ_i is unaltered by s and is therefore in R. Thus θ_i is one of the pth roots $\sqrt[p]{\Theta_i}$ of a quantity in R. Also the sum of the roots is given by a coefficient of our equation. Thus

$$\begin{aligned}
&x_0+x_1+x_2 &&+ \ldots +x_{p-1}=c,\\
&x_0+\epsilon x_1+\epsilon^2x_2 &&+ \ldots +\epsilon^{p-1}x_{p-1}=\sqrt[p]{\Theta_1},\\
&x_0+\epsilon^2x_1+\epsilon^4x_2 &&+ \ldots +\epsilon^{2(p-1)}x_{p-1}=\sqrt[p]{\Theta_2},\\
&\cdots\cdots\cdots

be chosen as any one of the pth roots of Θ_1, the remaining radicals are then fully determined. We have

$$\sqrt[p]{\Theta_j} = (\sqrt[p]{\Theta_1})^j \cdot \theta_j / \theta_1^j,$$

where the final factor is in R, being unaltered by s.

This proof is illustrated by the final work on the cubic equation (§ 158).

161. Cyclotomic Equations. It remains to treat the equation

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0 \tag{7}$$

for the imaginary pth roots of unity, where p is an odd prime.

For $p = 5$, the roots of (7) may be arranged in the order

$$\epsilon, \quad \epsilon^2, \quad \epsilon^{2^2} = \epsilon^4, \quad \epsilon^{2^3} = \epsilon^3.$$

For any prime p, it is shown in the theory of numbers that there exists a *primitive root* g of p such that

$$1, \quad g, \quad g^2, \ \ldots, \ g^{p-2},$$

when divided by p, give in some order the remainders

$$1, \ 2, \ 3, \ \ldots, \ p-1.$$

Thus the roots of (7) may be written in the order

$$x_1 = \epsilon, \quad x_2 = \epsilon^g, \quad x_3 = \epsilon^{g^2}, \ \ldots, \quad x_{p-1} = \epsilon^{g^{p-2}}$$

Hence

$$x_2 = x_1^g, \quad x_3 = x_2^g, \ \ldots, \quad x_{p-1} = x^g{}_{p-2}, \quad x_1 = x^g{}_{p-1}, \tag{8}$$

the last relation following from Fermat's theorem that g^{p-1} is of the form $1 + kp$, where k is an integer.

Consider any substitution s of the group G of (7) for $R(1)$:

$$s = \begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_{p-1} \\ x_a & x_b & x_c & \ldots & x_l \end{pmatrix}.$$

By (8) and property B of § 149, it follows that

$$x_b = x_a^g, \quad x_c = x_b^g, \ \ldots, \quad x_a = x_l^g.$$

But

$$x_{a+1} = x_a^g, \text{ etc.},$$

by (8). Hence

$$x_b = x_{a+1}, \quad x_c = x_{b+1}, \ \ldots, \ x_a = x_{l+1},$$

provided the symbol x_p be replaced by x_1. Thus

$$b \equiv a+1, \quad c \equiv b+1 \equiv a+2, \ \ldots \pmod{p-1},$$

$$s = \begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_{p-1} \\ x_a & x_{a+1} & x_{a+2} & \ldots & x_{a+p-2} \end{pmatrix},$$

in which x_{k+p-1} is to be replaced by x_k. Hence s is the power $a-1$ of $(x_1 x_2 x_3 \ldots x_{p-1})$, so that G is a subgroup of the cyclic group generated by that substitution.

After proving in § 163 by means of Gauss' lemma that equation (7) is irreducible in $R(1)$, we shall know that G is transitive (§ 150) and hence have the important

THEOREM. *If p is an odd prime, the group for the domain of rational numbers of the cyclotomic equation for the imaginary pth roots of unity is a regular cyclic group of order $p-1$.*

162. Gauss' Lemma. *If a polynomial $f(x)$ with integral coefficients, that of the highest power of x being unity, is the product of two polynomials with rational coefficients,*

$$\phi(x) = x^m + b_1 x^{m-1} + \ldots + b_m, \quad \psi(x) = x^n + c_1 x^{n-1} + \ldots + c_n,$$

then these coefficients are integers.

Let the fractions $b_1, \ldots, b_m$ be brought to the least positive common denominator β_0 and set $b_i = \beta_i/\beta_0$. Then $\beta_0, \ldots, \beta_m$ have no common divisor exceeding unity. Similarly, let $c_i = \gamma_i/\gamma_0$, where $\gamma_0, \ldots, \gamma_n$ are integers with no common divisor >1. Multiplying $f = \phi\psi$ by $\beta_0\gamma_0$, we get

$$\beta_0\gamma_0 f(x) = \phi_1(x) \cdot \psi_1(x), \tag{9}$$

where

$$\phi_1 = \beta_0 x^m + \beta_1 x^{m-1} + \ldots + \beta_m, \quad \psi_1 = \gamma_0 x^n + \gamma_1 x^{n-1} + \ldots + \gamma_n.$$

We shall assume that $\beta_0\gamma_0 > 1$ and prove that a contradiction results from this assumption. Let p be a prime divisor of $\beta_0\gamma_0$. Since p divides each coefficient of the left member of (9), it divides each coefficient of the product $\phi_1\psi_1$. Let β_i be the first coefficient in $\phi_1(x)$ which is not divisible by p; let γ_k be the first γ not divisible by p. The total coefficient of $x^{m+n-i-k}$ in $\phi_1\psi_1$ is

$$\ldots + \beta_{i+2}\gamma_{k-2} + \beta_{i+1}\gamma_{k-1} + \beta_i\gamma_k + \beta_{i-1}\gamma_{k+1} + \beta_{i-2}\gamma_{k+2} + \ldots$$

Since $\beta_{t-1}, \beta_{t-2}, \ldots$ and $\gamma_{t-1}, \gamma_{t-2}, \ldots$ are divisible by p and $\beta_t\gamma_t$ is not, and yet the preceding sum must be divisible by p, we have a contradiction. Hence $\beta_0 = \gamma_0 = 1$.

163. Irreducibility of the Cyclotomic Equation. To prove that the function $f(x)$, defined by the left member of (7), is irreducible in the domain of rational numbers, it is sufficient in view of Gauss' lemma to show that $f(x)$ is not the product of two polynomials $\phi(x)$ and $\psi(x)$ with integral coefficients, each having unity as the coefficient of the highest power of x. Kronecker's first proof of this fact is essentially as follows: Suppose that such a factorization $f(x) = \phi(x) \cdot \psi(x)$ is possible. Taking $x = 1$, we get $p = \phi(1) \cdot \psi(1)$. Since p is a prime, one of these integers, say $\phi(1)$, has the value ± 1. Since the factor $\phi(x)$ vanishes for at least one of the roots $\epsilon, \epsilon^2, \ldots, \epsilon^{p-1}$ of $f(x) = 0$, where ϵ is any one of the roots, we have

$$\phi(\epsilon) \cdot \phi(\epsilon^2) \ldots \phi(\epsilon^{p-1}) = 0.$$

In other words, the function

$$P(x) \equiv \phi(x) \cdot \phi(x^2) \ldots \phi(x^{p-1})$$

vanishes when x is replaced by any one of the roots of $f(x) = 0$, and hence has the factor $f(x)$. Thus

$$P(x) = f(x) \cdot q(x),$$

where $q(x)$ is a polynomial with integral coefficients (§ 162, or from the fact that the leading coefficient of the divisor $f(x)$ is unity).

Taking $x = 1$, and noting that $f(1) = p$, we get

$$[\phi(1)]^{p-1} = (\pm 1)^{p-1} = p \cdot q(1).$$

Since this is impossible, $f(x)$ is irreducible in $R(1)$.

164. Sufficient Condition for Solvability by Radicals. An equation having a solvable group for the domain defined by the coefficients is solvable by radicals. We shall prove the more general

THEOREM. *An algebraic equation having a solvable group for any domain R containing the coefficients is solvable by radicals relatively to R.*

This will follow if proved for the case of a regular cyclic group of prime order. Assuming the theorem for this case, let $f(x)=0$ be an equation whose group for R has the prime factors of composition ν, ρ, . . . As in the proof of Theorem 4 of § 159, there is a series of equations $n(\psi)=0$, $r(\chi)=0$, . . . of prime degrees ν, ρ, . . . , the solution of which is equivalent to the solution of $f(x)=0$. The group for R of $n(\psi)=0$ is a regular cyclic group of prime order ν so that this auxiliary equation is solvable by radicals relatively to R. The coefficients of $r(\chi)=0$ are in the domain $R'=(R, \psi)$ and its group for R' is a regular cyclic group of prime order ρ, hence it is solvable by radicals relatively to R'. In view of the earlier result, this second auxiliary equation is solvable by radicals relatively to R. A repetition of this argument shows that $f(x)=0$ is solvable by radicals relatively to R.

It remains only to prove that an equation $C(x)=0$ having a regular cyclic group G of prime order p for a domain R is solvable by radicals relatively to R. This is true for $p=2$. To proceed by induction, suppose that every equation having a regular cyclic group of prime order $<p$ for any domain D is solvable by radicals relatively to D. As in the proof above, this implies that the equation for the imaginary pth roots of unity is solvable by radicals (i.e., relatively to the domain of rational numbers). In fact, its group for that domain is a regular cyclic group of order $p-1$ (§ 161), each of whose factors of composition is a prime $<p$.

Adjoin to R an imaginary pth root ϵ of unity. The group of $C(x)=0$ for (R, ϵ) is either the initial cyclic group G or the identity group. In the latter case, the roots are in (R, ϵ) and can be found from the quantities in R by rational operations and root extractions, since ϵ was shown to be derivable from the rational number by those operations. In the former case, $C(x)=0$ is solvable (§ 160) by radicals relatively to (R, ϵ) and hence, as before, relatively to R. Hence the induction is complete.

COROLLARY. *If p is an odd prime, the equation for the $p-1$ imaginary pth roots of unity is solvable by radicals.*

The theorem implies that any cubic equation is solvable by radicals, since its group for any domain containing the coefficients is solvable.

165. Solution of a Quartic Equation. Let the coefficients in

$$x^4+ax^3+bx^2+cx+d=0$$

be independent variables, so that we have the general quartic equation. Its group for the domain $R=R(\omega, a, b, c, d)$, where $\omega^2+\omega+1=0$, is the symmetric group G_{24} on the roots $x_1, \ldots, x_4$ (§ 153). It is a solvable group, having the factors of composition 2, 3, 2, 2. In view of the last theorem, the equation is solvable by radicals. We shall give a solution which will illustrate the developments of the general theory as presented in the next chapter. In fact, we shall employ only binomial resolvents.

To the invariant subgroup G_{12} composed of the even substitutions belongs the function

$$\delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4),$$

whose square equals * the discriminant of the quartic:

$$\delta^2=256(I^3-27J^2),$$

$$I=d-\frac{ac}{4}+\frac{b^2}{12}, \quad J=\frac{bd}{6}-\frac{c^2}{16}-\frac{a^2d}{16}+\frac{abc}{48}-\frac{b^3}{216}.$$

The group of the quartic equation is G_{12} for (R, δ). Employ the notations of Example 2, § 150. To the invariant subgroup G_4 of G_{12} belongs

$$\phi=y_1+\omega y_2+\omega^2 y_3,$$

whose conjugates under G_{12} are $\omega\phi$ and $\omega^2\phi$. Thus ϕ is a root of the resolvent cubic $z^3-\phi^3=0$. To find ϕ^3, set

$$\psi=y_1+\omega^2 y_2+\omega y_3.$$

Then

$$\psi^3-\phi^3=3(\omega-\omega^2)(y_1-y_2)(y_2-y_3)(y_3-y_1)=-3(\omega-\omega^2)\delta,$$

$$\psi^3+\phi^3=2(y_1^3+y_2^3+y_3^3)+12y_1y_2y_3+3(\omega+\omega^2)v,$$

* Dickson, *Elementary Theory of Equations*, p. 42, Ex. 7.

where

$$v = y_1^2y_2 + y_1y_2^2 + y_1^2y_3 + y_1y_3^2 + y_2^2y_3 + y_2y_3^2.$$

But

$$\left(\sum y_1\right)^3 = 3v + 6y_1y_2y_3 + \sum y_1^3,$$

$$\left(\sum y_1\right)\left(\sum y_1y_2\right) = v + 3y_1y_2y_3.$$

Thus

$$\psi^3 + \phi^3 = 2\left(\sum y_1\right)^3 - 9\left(\sum y_1\right)\left(\sum y_1y_2\right) + 27y_1y_2y_3$$

$$= 2b^3 - 9b(ac - 4d) + 27(c^2 + a^2d - 4bd) = -432J,$$

as seen from the y-cubic in the example referred to. Hence

$$\phi^3 = \tfrac{3}{2}(\omega - \omega^2)\,\delta - 216\,J.$$

After the adjunction of ϕ, the group is G_4. Since y_1, y_2 and y_3 are unaltered by G_4, they are in the new domain (R, δ, ϕ). To find them, note that

$$\phi\psi = \sum y_1^2 + (\omega + \omega^2)\sum y_1y_2 = \left(\sum y_1\right)^2 - 3\sum y_1y_2 = 12I,$$

$$y_1 + y_2 + y_3 = b, \quad y_1 + \omega y_2 + \omega^2 y_3 = \phi, \quad y_1 + \omega^2 y_2 + \omega y_3 = \frac{12I}{\phi}.$$

Hence

$$y_1 = \tfrac{1}{3}\left(b + \phi + \frac{12I}{\phi}\right), \quad y_2 = \tfrac{1}{3}\left(b + \omega^2\phi + \frac{12\omega I}{\phi}\right),$$

$$y_3 = \tfrac{1}{3}\left(b + \omega\phi + \frac{12\omega^2 I}{\phi}\right)$$

The square of $t_1 \equiv x_1 + x_2 - x_3 - x_4$ is

$$\left(\sum x_1\right)^2 - 4\sum x_1x_2 + 4y_1 = a^2 - 4b + 4y_1.$$

Adjoining a root of

$$t_1^2 = a^2 - 4b + 4y_1,$$

we obtain a domain (R, δ, ϕ, t_1) for which the group of the quartic equation is $G_2 = \{1, (x_1x_2)(x_3x_4)\}$. Adjoining also a root $t_2 \equiv x_1 + x_3 - x_2 - x_4$ of

$$t_2^2 = a^2 - 4b + 4y_2,$$

we have a domain for which the group is the identity G_1, to which therefore $x_1, \ldots, x_4$ belong. To find them, note that

$$t_3^2 = a^2 - 4b + 4y_3, \quad t_3 \equiv x_1 + x_4 - x_2 - x_3,$$

$$t_1^2 t_2^2 t_3^2 = -4^3 \prod_{i=1}^{3} \left(b - \frac{a^2}{4} - y_i \right) = 4^3 \left(c - \frac{ab}{2} + \frac{a^3}{8} \right)^2,$$

as shown by setting $y = b - a^2/4$ in the cubic function in the example referred to, which equals $\Pi(y - y_i)$. To determine the sign of the square root, take $x_1 = 1$, $x_g = 0 (g > 1)$; thus

$$t_1 t_2 t_3 = -8c + 4ab - a^3.$$

Subject to this condition, the roots are given by

$$4x_1 = -a + t_1 + t_2 + t_3, \quad 4x_2 = -a + t_1 - t_2 - t_3,$$

$$4x_3 = -a - t_1 + t_2 - t_3, \quad 4x_4 = -a - t_1 - t_2 + t_3.$$

The above solution can be modified indefinitely, since there are infinitely many functions belonging to a given subgroup of the equation. Moreover, we might employ other subgroups of order 2 of G_4 instead of G_2.

EXERCISES

1. After reducing the group to G_2, adjoin $i = \sqrt{-1}$ and find the quadratic equation for $V = x_1 - x_2 + ix_3 - ix_4$:

$$V^2 = (x_1 - x_2)^2 - (x_3 - x_4)^2 + 2i(x_1 - x_2)(x_3 - x_4)$$

$$= t_2 t_3 + 2i(y_2 - y_3) = \frac{4ab - 8c - a^3}{t_1} + \frac{2}{3}\sqrt{3}\left(\phi - \frac{12I}{\phi} \right)$$

For $W = x_1 - x_2 - ix_3 + ix_4$, we have

$$VW = (x_1 - x_2)^2 + (x_3 - x_4)^2 = \sum x_1^2 - 2y_1 = a^2 - 2b - 2y_1,$$

$$x_1, \; x_2 = \tfrac{1}{4}[-a + t_1 \pm (V + W)], \quad x_4, \; x_3 = \tfrac{1}{4}[-a - t_1 + i(V - W)].$$

The theoretical interest of this solution is that it leads to a 24-valued function V by means of a chain of binominal resolvents.

2. After reducing the group to G_2, we may find x_1 and x_2 by solving a quadratic equation with coefficients in (R, δ, ϕ, t_1):

$$x^2 + \tfrac{1}{2}(a - t_1)x + \tfrac{1}{2}y_1 - (\tfrac{1}{2}ay_1 - c)/t_1 = 0.$$

In terms of x_1, x_2 and the quantities known, we may find x_3, x_4:

$$x_3 + x_4 = x_1 + x_2 - t_1, \quad x_3 - x_4 = \frac{y_2 - y_3}{x_1 - x_2}.$$

CHAPTER XVI

NECESSARY CONDITION THAT AN ALGEBRAIC EQUATION BE SOLVABLE BY RADICALS

166. Galois' Criterion. *An algebraic equation is solvable by radicals if and only if its group for the domain defined by the coefficients is a solvable group*

It is occasionally useful to employ the generalization:

An equation is solvable by radicals relatively to a domain R containing the coefficients if and only if its group for R is solvable.

That the solvability of the group is a sufficient condition for the solvability of the equation was proved in § 164. We shall now prove that it is a necessary condition. By hypothesis the roots $x_1, \ldots, x_n$ of the equation can be derived by rational operations and root extractions from quantities in the domain $R = R(k_1, \ldots, k_m)$ or from quantities obtained from them by those operations. The index of each root extraction may be assumed to be prime, since $z^{pq} = a$ is equivalent to the pair of equations $z^p = w$, $w^q = a$. If $\xi, \eta, \ldots, \psi$ denote the radicals which enter the expressions for $x_1, \ldots, x_n$, the solution may be exhibited by a series of binomial equations

$$\xi^\lambda = L(k_1, \ldots, k_m),\ \eta^\mu = M(\xi, k_1, \ldots, k_m), \ldots, \quad \psi^\sigma = S(\ldots, \eta, \xi, k_1, \ldots, k_m) \tag{1}$$

of prime degrees $\lambda, \mu, \ldots, \sigma$, together with equations which express $x_1, \ldots, x_n$ rationally in terms of $\xi, \ldots, \psi, k_1, \ldots, k_m$. Here $L, \ldots, S$ are rational functions with rational coefficients of their arguments.

Consider, therefore, a binomial equation of prime degree

$$x^p - A = 0, \tag{2}$$

where A is in the domain R. Let ϵ be an imaginary pth root of unity. If one root r of (2) belongs to the domain $R'=(R, \epsilon)$, all of the remaining roots $\epsilon r, \epsilon^2 r, \ldots, \epsilon^{p-1} r$ belong to R' and the group of (2) for R' is the identity. In the contrary case, A is not the pth power of a quantity in R', and (2) is irreducible in R' (§ 143). The notation of the roots can be chosen so that

$$x_2=\epsilon x_1, \quad x_3=\epsilon x_2, \ \ldots, \ x_p=\epsilon x_{p-1}, \quad x_1=\epsilon x_p.$$

By an argument like that of § 161 with $p-1$ replaced by p, we see that the group of (2) for R' is a subgroup of the cyclic group generated by $(x_1 x_2 x_3 \ldots x_p)$. Since (2) is now irreducible in R', its group is transitive and hence of order $\geqq p$.

For a domain containing A and an imaginary pth root of unity, the group of the binomial equation (2) of prime degree p is the identity group if any root is in the domain, but is a regular cyclic group of order p if no root is in the domain. For examples, see § 150.

Any one of the binomial equations (1) of prime degree p is equivalent to a series of equations each having a regular cyclic group of prime order for a certain domain. We include in the series the equations having regular cyclic groups of prime orders dividing $p-1$, which together serve to determine an imaginary pth root ϵ of unity (§ 161, Theorem 4 of § 159). After the adjunction of ϵ, the group of the binomial equation was just proved to be either the identity group or a regular cyclic group of order p. In the former case, the desired series of equations is the one previously defined; in the latter case, that series together with the given binomial equation. Thus the set of binomial equations (1) is equivalent to a series of equations of prime degrees, each having a regular cyclic group for the domain symbolized in the same line:

$$\begin{aligned}
&\phi(y;\ k_1, \ldots, k_m)=0, && R=R(k_1, \ldots, k_m);\\
&\psi(z;\ y, k_1, \ldots)=0, && (y, R);\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\theta(w;\ \ldots z, y, k_1, \ldots)=0, && (\ldots z, y, R).
\end{aligned}$$

Each of these equations is solvable by radicals relatively to the corresponding domain (§ 164). Adjoin one root y of $\phi=0$ to R; the group is now a subgroup H of the initial group G, including the possibility that $H=G$ (§ 156). Solve $\psi=0$ and adjoin one root z to the domain (y, R); the group is now a subgroup of H. Proceeding in this manner, we finally reach the domain $(w, \ldots, z, y, R)$ containing each root x_i of the proposed equation, whose group is therefore now the identity group G_1.

The theorem of Galois states that, by each of these adjunctions, the group of the proposed equation is either not reduced at all or else is reduced to an invariant subgroup of prime index. This theorem will be derived as a corollary in the next section from a theorem of which other important applications will be made later on. Hence the distinct groups $G, H, \ldots, G_1$, obtained by the successive adjunctions, form a series of composition of G with only prime factors of composition. Thus G is a solvable group. We therefore have Galois' criterion for the solvability of an equation.

For $n>4$, the factors of composition of the symmetric group on n letters (§ 17) are 2 and $\frac{1}{2}n!$, the latter of which is not prime. By § 153 the group of the general equation of degree n, i.e., one whose coefficients $c_1, \ldots, c_n$ are independent complex variables, is the symmetric group when the domain is that defined by $c_1, \ldots, c_n$ and a finite number of constants. We therefore have the

THEOREM. *The general equation of degree $n>4$ is not solvable by radicals.* Moreover, its roots cannot be found by rational operations and root extractions performed upon the coefficients and any constants, finite in number, or upon quantities obtained from them by those operations.*

167. Theorems of Galois, Jordan and Hölder. Of prime importance is

JORDAN'S THEOREM.† *Let the group G_1 for a domain R of*

* Ruffini, *Teoria generale delle equazioni. . .*, Bologna, 1799. N. H. Abel, *Œuvres*, vol. 1, 1881, pp. 66–94.

† Jordan, *Traité des substitutions*, p. 268–9.

*an algebraic equation $F_1(x)=0$ be reduced to G'_1 by the adjunction of all of the roots of a second equation $F_2(x)=0$, and let the group G_2 for R of the second equation be reduced to G'_2 by the adjunction of all of the roots of the first equation. Then G'_1 and G'_2 are invariant subgroups of G_1 and G_2, respectively, of equal indices, and * the quotient-groups G_1/G'_1 and G_2/G'_2 are simply isomorphic.*

By § 154 there exists a rational function ψ_1 with coefficients in R of the roots $\xi_1, \ldots, \xi_n$ of the first equation, such that ψ_1 belongs to the subgroup G'_1 of G_1. Since the adjunction of the roots $\eta_1, \ldots, \eta_m$ of the second equation reduces G_1 to G'_1, property A of G'_1 (§ 149) shows that ψ_1 lies in the enlarged domain:

$$\psi_1(\xi_1, \ldots, \xi_n) = \phi_1(\eta_1, \ldots, \eta_m), \tag{3}$$

where ϕ_1 is a rational function with coefficients in R.

Let $\psi_1, \psi_2, \ldots, \psi_k$ denote all of the numerically distinct values which ψ_1 can take under the substitutions (on $\xi_1, \ldots, \xi_n$) of G_1. Then G'_1 is of index k under G_1 (§ 154, Theorem 2). Let $\phi_1, \ldots, \phi_l$ denote all of the numerically distinct values which ϕ_1 can take under the substitutions (on $\eta_1, \ldots, \eta_m$) of G_2. The k quantities ψ are the roots of an equation irreducible in R; likewise for the l quantities ϕ. Since these two irreducible equations have a common root $\psi_1=\phi_1$, they are identical (§ 144). Hence the ψ's coincide in some order with the ϕ's; in particular $k=l$.

If s_i is a substitution of G_1 which replaces ψ_1 by ψ_i, then s_i transforms the group G'_1 of ψ_1 into the group of ψ_i of the same order as G'_1. Since ψ_i equals a ϕ, it is in the domain $R'=(R, \eta_1, \ldots, \eta_m)$ and hence is unaltered by the substitutions of the group G'_1 of $F_1(x)=0$ for that domain R' (§ 149, property B). Hence the group of ψ_i contains all of the substitutions of G'_1 and, being of the same order, is identical with G'_1. Thus G'_1 *is invariant in* G_1. The group for R of the irreducible equation satisfied by ψ_1 is therefore the quotient group G_1/G'_1 (§ 159).

* This supplement and the proof here employed are due to Hölder, *Mathematische Annalen*, vol. 34, (1889), p. 47.

Let H_2 be the subgroup of G_2 to which $\phi_1(\eta_1, \ldots, \eta_m)$ belongs. Since ϕ_1 is a root of an equation of degree $l=k$ irreducible in R, the group H_2 is of index k under G_2. By the adjunction of ϕ_1, i.e., of ψ_1 by (3), the group G_2 of $F_2(x)=0$ for R is reduced to H_2 (§ 156, Theorem 2). If not merely $\psi_1(\xi_1, \ldots, \xi_n)$, but all of the ξ's themselves be adjoined, the group G_2 reduces perhaps further to a subgroup of H_2. Hence G'_2 is contained in H_2. We thus have the preliminary result: If the group of $F_1(x)=0$ reduces to a subgroup of index k on adjoining all of the roots of $F_2(x)=0$, then the group of $F_2(x)=0$ reduces to a subgroup of index k_1, $k_1 \geqq k$, on adjoining all of the roots of $F_1(x)=0$.

Interchanging F_1 and F_2 in the preceding statement, we obtain the result: If the group of $F_2(x)=0$ reduces to a subgroup of index k_1 on adjoining all the roots of $F_1(x)=0$, then the group of $F_1(x)=0$ reduces to a subgroup of index k_2, $k_2 \geqq k_1$, on adjoining all the roots of $F_2(x)=0$. Since the hypothesis for the second statement is identical with the conclusion for the first statement, it follows that

$$k_2=k, \quad k_1 \geqq k, \quad k_2 \geqq k_1,$$

so that $k_1=k$. Hence the group G'_2 of the theorem is identical with the group H_2 of all of the substitutions in G_2 which leave ϕ_1 unaltered. For the same reason that G'_1 is invariant in G_1, it now follows that G'_2 *is invariant in* G_2. The equation irreducible in R and satisfied by ϕ_1 has as its group the quotient-group G_2/G'_2.

Since the two irreducible equations in R satisfied by ϕ_1 and ψ_1, respectively, were shown to be identical, their groups G_1/G'_1 and G_2/G'_2 differ only in the notations employed for the letters on which they operate, and hence are simply isomorphic.

We shall derive as a corollary

GALOIS' THEOREM. *By the adjunction of any one root of an equation $F_2(x)=0$ whose group for R is a regular cyclic group of prime order p, the group for R of the equation $F_1(x)=0$ either is not reduced at all or else is reduced to an invariant subgroup of index p.*

In fact, by adjoining one root x_1 of $F_2(x)=0$, we adjoin all of its roots, since each is a rational function of x_1 with coefficients in R (§ 155). For, the identity is the only substitution of the group for R of $F_2(x)=0$ which leaves x_1 numerically unaltered.

We shall state certain results not presupposed in what follows. A brief argument (cf. Dickson's *Theory of Algebraic Equations*, 1903, p. 83) now leads to Abel's theorem: The roots of an equation solvable by radicals can be given such a form that each of the radicals occurring in the expressions for the roots are expressible rationally in terms of the roots of the equation and certain roots of unity. This was proved by Abel by a long algebraic discussion without the aid of groups and employed in his proof of the impossibility * of solving by radicals the general equation of degree $n \geqq 5$.

For a domain R an irreducible equation of prime degree whose roots are all rational functions of two of the roots with coefficients in R is called a Galoisian equation. Galois proved that it is solvable by radicals and that every irreducible equation of prime degree which is solvable by radicals is a Galoisian equation. For a detailed exposition with illustrative examples, see Dickson's *Theory of Algebraic Equations*, 1903, pp. 87–93.

A cubic equation having three real roots cannot † be solved by real radicals (the " irreducible case ").

* Cited in § 166. Cf. Serret, *Cours d'Algèbre supérieure*, ed. 4, vol. 2, pp. 497–517.

† H. Weber, *Algebra*, ed. 2, 1898, vol. 1, 657; *Kleines Lehrbuch der Algebra*, 1912, p. 381.

CHAPTER XVII

CONSTRUCTIONS WITH RULER AND COMPASSES

168. Some Celebrated Problems of Greek Origin. In the Delian problem of the duplication of a cube, we are given the length s of an edge of a cube and seek to construct by ruler and compasses the edge x of a cube whose volume is double that of the first cube. For this problem, as well as for the problem of the trisection of an arbitrary angle, and for the problem of the construction of a regular polygon of 7 or 9 sides, the ancients sought in vain for constructions by ruler and compasses. The impossibility of these constructions was proved only in recent times. To the analytic methods employed in the proof of this impossibility is due also the discovery of new constructions, such as that for the regular polygon of 17 sides, the constructibility of which was not suspected during the twenty centuries from Euclid to Gauss.

169. Analytic Criterion for Constructibility by Ruler and Compasses. The first step in our treatment of the problems mentioned in § 168 is their analytic formulation. In the Delian problem, we are led at once to the equation $x^3 = 2s^3$. Next, if angle 120° could be trisected or if a regular polygon of 9 sides could be constructed by ruler and compasses, angle 40° could be constructed and hence cos 40°. In the identity

$$\cos 3A = 4\cos^3 A - 3\cos A,$$

take $A = 40°$. Since $\cos 120° = -\frac{1}{2}$, we get

$$4\cos^3 40° - 3\cos 40° + \tfrac{1}{2} = 0.$$

Multiply by 2 and set $x = 2\cos 40°$; thus

$$x^3 - 3x + 1 = 0. \tag{1}$$

In this problem and the Delian problem, we are given the coefficients of a cubic equation and ask whether or not a line whose length is a root x can be constructed by ruler and compasses. We shall first prove that an affirmative or negative answer is to be given according as x can or cannot be derived from the coefficients by rational operations and extractions of real square roots.

For any proposed construction we are concerned with certain numbers, some expressing lengths, areas, etc., others being the coördinates of points, and still others being the coefficients of equations of straight lines or circles referred to rectangular axes. We shall establish the

CRITERION. *A proposed construction by ruler and compasses is possible if and only if the numbers which define analytically the desired geometrical elements can be derived from those defining the given elements by rational operations and extractions of real square roots performed a finite number of times.*

First, let the construction be possible. The straight lines and circles drawn in making the construction can be located by means of points either initially given or obtained as the intersections of straight lines and circles. The coördinates of the intersection of two intersecting lines are evidently rational functions of the coefficients of the equations of the lines. If the straight line $y=mx+b$ intersects the circle

$$(x-p)^2+(y-q)^2=r^2,$$

the coördinates of the points of intersection are found by eliminating y, solving the resulting quadratic for x, and inserting the roots x into $y=mx+b$. Hence the coördinates are found from m, b, p, q, r by rational operations and the extraction of a single real square root. Finally, two intersecting circles cross at the intersections of one of them with their common chord, so that this case reduces to the preceding.

That the criterion gives also a sufficient condition for constructibility is shown by the facts that the sum or difference of two segments of straight lines can be found by use of compasses, that $p=ab$ can be found by constructing p in $1 : a=b : p$

by use of parallels, and similarly $q=a/b$ in $1 : b=q : a$. Finally, if n is a positive number, $\sqrt{n}$ can be constructed by the use of a semicircle of diameter $1+n$ and a perpendicular at the point separating the segments of lengths 1, n.

170. Trisection of an Angle. To prove that it is impossible to trisect an arbitrary angle by ruler and compasses, it suffices to prove that angle $120°$ cannot be trisected. We saw that $2\cos 40°$ is a root of (1). In the domain of rational numbers, Eq. (1) is irreducible (§ 144, Ex. 3) and has the discriminant 81; hence its group is of order 3. By the adjunction of a square root, the group is either not reduced at all or is reduced to a invariant subgroup of index 2 (§ 167, Galois' Theorem). Hence no such reduction is possible in the present case. If therefore the cubic had a constructible root, its adjunction would cause no reduction of the group, whereas the adjunction of any root reduces the group to the identity.

171. Duplication of a Cube. If an edge of the cube be taken as the unit of length, the edge of the desired cube is a root of

$$x^3=2.$$

For the domain of rational numbers this irreducible equation has as its group the symmetric group G_6. The adjunction of any root reduces it to a group of index 3. Hence no root can be found by extractions of square roots.

172. Regular Polygons. The construction of a regular polygon of n sides by ruler and compasses is equivalent to that of angle $2\pi/n$ and hence of a line of length $\cos 2\pi/n$. The irreducible equation with rational coefficients satisfied by the latter number is much more difficult to form and treat than that with the root

$$r=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}, \tag{2}$$

where $i=\sqrt{-1}$. In view De Moivre's theorem, r is an nth root of unity. Moreover,

$$\frac{1}{r}=\cos\frac{2\pi}{n}-i\sin\frac{2\pi}{n}, \quad r+\frac{1}{r}=2\cos\frac{2\pi}{n}.$$

Hence if r can be expressed in terms of i and real square roots, $\cos 2\pi/n$ can be expressed in terms of real square roots. The converse is seen to be true by an inspection of (2), since the sine can be found from the cosine by a real square root. Hence a regular n-gon can be constructed by ruler and compasses if and only if the nth root (2) of unity can be found by the extraction of square roots, all except the last one of which is real.

If n is an odd prime p, r is a root of an equation of degree $p-1$ irreducible in the domain R of all rational numbers and having as its group for R a regular cyclic group C of order $p-1$ (§§ 161–3). The adjunction of any root reduces C to the identity. If a regular p-gon can be constructed, the adjunction of the root r is equivalent to that of several square roots, the adjunction of each of which causes either no reduction in the group or a reduction to a subgroup of index 2. Hence a regular p-gon can be constructed by ruler and compasses if and only if $p-1$ is a power 2^h of 2. But if $h=fq$, where f is odd, then 2^h+1 has the factor 2^q+1. Hence a prime of the form 2^h+1 is of the form

$$2^{2^t}+1. \tag{3}$$

For $t=0, 1, 2, 3, 4$, the corresponding numbers are 3, 5, 17, 257, 65537, and are all primes. But for $t=5, 6, 7, 8, 9, 11, 12$, etc., the number is known to be not prime.

Next, let $n=ab$, where a and b are relatively prime integers >1. If a regular a-gon and a regular b-gon can be constructed by ruler and compasses, the same is true of a regular n-gon. For, multiples of the angles $2\pi/a$ and $2\pi/b$ can then be constructed and hence also the sum of these multiples. Since there exist integers c and d such that $ca+db=1$, the angle

$$d\cdot\frac{2\pi}{a}+c\cdot\frac{2\pi}{b}=\frac{2\pi}{ab}(db+ca)=\frac{2\pi}{ab},$$

and therefore also the ab-gon, can be constructed. Conversely, from the latter we obtain a regular a-gon by using the 1st, $(b+1)$th, $(2b+1)$th, . . . , $[(a-1)b+1]$th vertices. Hence if $n=p^iq^j\ldots$, where p, q, . . . are distinct primes, a regular

n-gon can be constructed if and only if a regular p^s-gon, q^t-gon, . . . can be constructed. A 2^s-gon can be constructed by repeated bisections of 180°.

It therefore remains only to discuss the regular p^s-gon, where p is an odd prime. By De Moivre's theorem,

$$\rho = \cos\frac{2\pi}{p^s} + i\sin\frac{2\pi}{p^s},$$

is a root of $x^{p^s}=1$, but not of $x^{p^{s-1}}=1$, and hence is a root of

$$\frac{x^{tp}-1}{x^t-1} \equiv x^{t(p-1)} + x^{t(p-2)} + \ldots + x^t + 1 = 0 \qquad (t = p^{s-1}). \tag{4}$$

Since ρ^p, ρ^{2p}, . . . , ρ^{tp} give the t roots of $x^t=1$, the remaining $tp-t$ powers of ρ, with positive exponents less than tp and not divisible by p, are roots of (4) and give all of the roots of (4). They are called the *primitive* p^sth roots of unity.

For $p^s=9$, the six primitive ninth roots of unity are ρ, ρ^2, ρ^4, ρ^5, ρ^7, ρ^8 and are the roots of $x^6+x^3+1=0$.

The proof that (4) is irreducible in the domain R of all rational numbers differs from that in § 163 for the special case $s=1$ only in the detail of having, instead of ϵ, ϵ^2, . . . , ϵ^{p-1} in the former case, the roots ρ, ρ^a, ρ^b, . . . , ρ^l of (4), where 1, a, b, . . . , l denote the positive integers less than p^s and not divisible by p, and ρ is an arbitrary primitive p^sth root of unity.

As shown in the theory of numbers, there exists a *primitive root g of p^s*, where p is an odd prime, i.e., an integer g such that

$$1,\ g,\ g^2,\ \ldots,\ g^{k-1} \qquad (k = p^s - p^{s-1}),$$

when divided by p^s, give as remainders in some order the positive integers less than p^s and not divisible by p. Thus the roots of (4) are

$$\rho,\ \rho^g,\ \rho^{g^2},\ \ldots,\ \rho^{g^{k-1}}.$$

In the former example $p^s=9$, we may take $g=2$. Then the preceding roots are ρ, ρ^2, ρ^4, ρ^8, ρ^7, ρ^5, respectively.

Since each root of (4) can therefore be expressed as the gth power of the preceding root, we readily find as in § 161

that the group of (4) for R is a regular cyclic group of order k. If $s>1$, k is not a power of 2, and by the usual argument the regular p^s-gon cannot be constructed by ruler and compasses.

Combining our results, we have the

THEOREM. *A regular polygon of n sides can be constructed by ruler and compasses if and only if $n=2^s p_1 p_2 \ldots$, where $p_1, p_2, \ldots$ are distinct primes of the form* (3).

Since therefore a regular 9-gon cannot be constructed, we have a new proof that angle 120° cannot be trisected by ruler and compasses.

Gauss * was the first to prove that a regular p-gon can be constructed if p is a prime of the form (3); he stated,† but apparently did not publish a proof of, the remaining part of the above theorem. For the elegant method invented by Gauss for finding the series of quadratic equations leading to a 17th root of unity and the actual geometrical construction of a regular 17-gon, as well as for a longer proof of the above theorem without the aid of group theory, the reader may consult the monograph by Dickson,‡ where references to other books are given.

* *Disquisitiones Arithmeticæ*, 1801, Art. 335–366 [=*Werke*, 1]; German translation by Maser, 1889, pp. 397–448, 630–652.

† Gauss-Maser, p. 447.

‡ *Monographs on Modern Mathematics*, edited by J. W. A. Young, New York, 1911. A brief, but more elementary, treatment is given in Dickson's *Elementary Theory of Equations*, 1914, pp. 84–92. A still more elementary discussion is that by Dickson, *Amer. Math. Monthly*, vol. 21 (1914), 259–262.

CHAPTER XVIII

THE INFLEXION POINTS OF A PLANE CUBIC CURVE

173. Homogeneous Coördinates of Points in a Plane. Let

$$a_i x + b_i y + c_i = 0 \qquad (i = 1, 2, 3)$$

be any three linear equations such that

$$\Delta = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \neq 0.$$

Interpret x and y as the Cartesian coördinates of a point referred to rectangular axes. Then the three equations represent three straight lines L_i forming a triangle. Choose the sign before the radical so that

$$p_i = \frac{a_i x + b_i y + c_i}{\pm\sqrt{a_i^2 + b_i^2}}$$

is positive for a point (x, y) inside the triangle, and hence is the length of the perpendicular from that point to L_i. The homogeneous coördinates of a point (x, y) are three numbers x_1, x_2, x_3 such that

$$\rho x_1 = k_1 p_1, \quad \rho x_2 = k_2 p_2, \quad \rho x_3 = k_3 p_3,$$

where k_1, k_2, k_3 are constants, the same for all points, while ρ is an arbitrary factor of proportionality. Thus only the ratios of x_1, x_2, x_3 are defined. The coefficients of the linear function $k_i p_i$, which are proportional to a_i, b_i, c_i, will henceforth be denoted by those same letters. Then

$$(1) \qquad \rho x_i = a_i x + b_i y + c_i, \quad \Delta \neq 0 \qquad (i = 1, 2, 3).$$

Solving these equations by determinants, we get

$$\Delta x = \rho \sum A_i x_i, \quad \Delta y = \rho \sum B_i x_i \quad \Delta = \rho \sum C_i x_i,$$

where A_i is the cofactor of a_i in Δ, B_i that of b_i, and C_i that of c_i. Hence

$$x=\frac{\sum A_i x_i}{\sum C_i x_i}, \quad y=\frac{\sum B_i x_i}{\sum C_i x_i}. \tag{2}$$

Thus any equation $f(x, y)=0$ can be expressed as a homogeneous equation $\phi(x_1, x_2, x_3)=0$ of the same total degree, and conversely. In particular, any straight line is represented by an equation of the first degree in x_1, x_2, x_3, and conversely. For example, $x_1=0$ represents a side of the triangle of reference.

Let y_1, y_2, y_3 be the homogeneous coördinates of the same point (x, y) referred to a new triangle of reference having the sides L'_i. As before,

$$\rho y_i=a'_i x+b'_i y+c'_i \qquad (i=1, 2, 3), \tag{1'}$$

where the right member equated to zero represents L'_i. Solving equations (1') as we did (1), we obtain x and y as linear fractional functions of y_1, y_2, y_3. Inserting these values into (1), we get formulas like

$$x_i=c_{i1}y_1+c_{i2}y_2+c_{i3}y_3, \quad |c_{ij}|\neq 0 \qquad (i=1, 2, 3). \tag{3}$$

Thus a change of triangle of reference gives rise to a linear transformation of the homogeneous coördinates.

Let $f(x_1, x_2, x_3)$ be a homogeneous rational integral function of the nth degree. Under the transformation (3), let it become $\phi(y_1, y_2, y_3)$. Then $\phi=0$ represents the same curve as $f=0$, but referred to the new triangle of reference. Let

$$t=kx_1^a x_2^b x_3^c \qquad (a+b+c=n)$$

be any term of f. Then

$$x_1\frac{\partial t}{\partial x_1}=at, \quad x_2\frac{\partial t}{\partial x_2}=bt, \quad x_3\frac{\partial t}{\partial x_3}=ct.$$

Their sum is nt. Hence we have Euler's theorem:

$$x_1\frac{\partial f}{\partial x_1}+x_2\frac{\partial f}{\partial x_2}+x_3\frac{\partial f}{\partial x_3}=nf. \tag{4}$$

If x_1, x_2, x_3 is a set of solutions, not all zero, of

$$\frac{\partial f}{\partial x_1}=0, \quad \frac{\partial f}{\partial x_2}=0, \quad \frac{\partial f}{\partial x_3}=0, \tag{5}$$

and hence by (4) of $f=0$, the point (x_1, x_2, x_3) is called a *singular point* of the curve $f=0$. At this point,

$$\frac{\partial \phi}{\partial y_j}=\sum_{i=1}^{3}\frac{\partial f}{\partial x_i}\frac{\partial x_i}{\partial y_j}=0 \qquad (j=1, 2, 3).$$

Hence the definition of a singular point is independent of the special triangle of reference chosen. It is readily proved, but not presupposed in what follows, that two or more branches of the curve pass through any singular point, which is therefore called a double or multiple point.

174. Hessian Curve. The Hessian of f is

$$h=\begin{vmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} & \frac{\partial^2 f}{\partial x_1 \partial x_3} \\ \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial x_2^2} & \frac{\partial^2 f}{\partial x_2 \partial x_3} \\ \frac{\partial^2 f}{\partial x_3 \partial x_1} & \frac{\partial^2 f}{\partial x_3 \partial x_2} & \frac{\partial^2 f}{\partial x_3^2} \end{vmatrix}.$$

Let transformation (3), of determinant Δ, replace f by $\phi(y_1, y_2, y_3)$. The product $h\Delta$ is a determinant of the third order, in which the element in the ith row and jth column is the sum of the products of the elements of the ith row of h by the corresponding elements of the jth column of Δ, and hence is

$$\frac{\partial^2 f}{\partial x_i \partial x_1}c_{1j}+\frac{\partial^2 f}{\partial x_i \partial x_2}c_{2j}+\frac{\partial^2 f}{\partial x_i \partial x_3}c_{3j}.$$

The latter is the partial derivative with respect to x_i of

$$\frac{\partial f}{\partial x_1}\frac{\partial x_1}{\partial y_j}+\frac{\partial f}{\partial x_2}\frac{\partial x_2}{\partial y_j}+\frac{\partial f}{\partial x_3}\frac{\partial x_3}{\partial y_j}=\frac{\partial \phi}{\partial y_j}.$$

Let Δ' be the determinant obtained from Δ by interchanging its rows and columns. By the same rule of multiplication,

the element in the rth row and jth column of the determinant equal to $\Delta' \cdot h\Delta$ is

$$c_{1r}\frac{\partial}{\partial x_1}\left(\frac{\partial \phi}{\partial y_j}\right)+c_{2r}\frac{\partial}{\partial x_2}\left(\frac{\partial \phi}{\partial y_j}\right)+c_{3r}\frac{\partial}{\partial x_3}\left(\frac{\partial \phi}{\partial y_j}\right)=\frac{\partial}{\partial y_r}\left(\frac{\partial \phi}{\partial y_j}\right),$$

since c_{ir} is the partial derivative of x_i with respect to y_r. Hence

$$\Delta^2 h=\left|\frac{\partial^2 \phi}{\partial y_r \partial y_j}\right|_{r,\,j=1,\,2,\,3}=\text{Hessian } H \text{ of } \phi.$$

In words, $\Delta^2 h$ becomes H under the transformation (3), so that $H=0$ represents the same curve as $h=0$, but referred to the new triangle of reference. Hence there is associated with any curve $f=0$ a definite *Hessian curve* $h=0$ independent of the choice of the triangle of reference.

175. Points of Inflexion of a Cubic Curve. Let $f(x_1, x_2, x_3)$ be of the third degree. Choose a triangle of reference having the vertex $P=(0, 0, 1)$ at a point on the curve $f=0$, not a singular point. Then there is no term involving x_3^3, and the coefficients of the terms $rx_1x_3^2$ and $sx_2x_3^2$ are not both zero, since otherwise the derivatives (5) would all vanish at P. Hence we may take rx_1+sx_2 as a side of a new triangle of reference with the same vertex P and obtain

$$x_3^2x_1+x_3(ax_1^2+bx_1x_2+cx_2^2)+\phi(x_1, x_2)=0$$

as the new equation of our curve. Replacing x_3 by

$$x_3-(ax_1+bx_2)/2,$$

we get

$$F_1=x_3^2x_1+ex_3x_2^2+C(x_1, x_2).$$

Denote the second derivative of the cubic function C with respect to x_i and x_j by C_{ij}. Then the Hessian of F_1 is

$$H_1=\begin{vmatrix} C_{11} & C_{12} & 2x_3 \\ C_{21} & C_{22}+2ex_3 & 2ex_2 \\ 2x_3 & 2ex_2 & 2x_1 \end{vmatrix}=-8ex_3^3+\ \ldots$$

Hence $P=(0, 0, 1)$ is on $H_1=0$ if and only if $e=0$.

If d is the coefficient of x_2^3 in C, then $x_1=0$ meets $F_1=0$ in the points for which $x_2^2(ex_3+dx_2)=0$, and these three points

coincide (at P) if and only if $e=0$. In that case P is called a *point of inflexion* of $F_1=0$ and $x_1=0$ the *inflexion tangent* to $F_1=0$ at P.

Thus P is a point of inflexion of $F_1=0$ if and only if it is on $H_1=0$. Hence, by § 174, *each intersection of a cubic curve $f=0$ without a singular point with its Hessian curve $h=0$ is a point of inflexion of $f=0$, and conversely.*

There is certainly at least one intersection. For, by eliminating x_3 between $f=0$ and $h=0$, we get a homogeneous equation in x_1 and x_2, having therefore at least one set of solutions x'_1, x'_2. Then, for $x_1=x'_1$, $x_2=x'_2$, the equations $f=0$, $h=0$ have at least one common root $x=x'_3$. Thus (x'_1, x'_2, x'_3) is an intersection and therefore a point of inflexion of $f=0$. Taking this point as a vertex (0, 0, 1) of a triangle of reference and proceeding as before, we get F of type F_1 with $e=0$. If the coefficient d of x_2^3 in F is zero, F has the factor x_1. But, if $F=x_1Q$, the derivatives

$$\frac{\partial F}{\partial x_1}=Q+x_1\frac{\partial Q}{\partial x_1}, \quad \frac{\partial F}{\partial x_2}=x_1\frac{\partial Q}{\partial x_2}, \quad \frac{\partial F}{\partial x_3}=x_1\frac{\partial Q}{\partial x_3}$$

all vanish at a point of intersection of $x_1=0$, $Q=0$, whereas $F=0$ has no singular point. Hence $d\neq 0$. Taking $d^{\frac{1}{3}}x_2$ as a new x_2, and then adding a suitable multiple of x_1 to x_2 to delete the term with $x_2^2x_1$, we get

$$F=x_3^2x_1+C, \quad C=x_2^3+3bx_2x_1^2+ax_1^3.$$

$$H=2x_1\begin{vmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{vmatrix}-4x_3^2C_{22}=72x_1\begin{vmatrix} bx_2+ax_1 & bx_1 \\ bx_1 & x_2 \end{vmatrix}-24x_3^2x_2.$$

Eliminating x_3^2 between $F=0$, $H=0$, we get

$$\begin{vmatrix} x_1 & C \\ -x_2 & 3x_1(bx_2^2+ax_1x_2-b^2x_1^2) \end{vmatrix}$$
$$=x_2^4+6bx_2^2x_1^2+4ax_2x_1^3-3b^2x_1^4=0.$$

If $x_1=0$, then $x_2=0$ and the intersection is (0, 0, 1). For the remaining intersections, we may set $x_1=1$; then each root of

$$r^4+6br^2+4ar-3b^2=0 \tag{6}$$

leads to the inflexion points $(1, r, \pm s)$, where

$$-s^2 = C = r^3 + 3br + a.$$

If $s=0$, (6) would have a double root and $a^2+4b^3=0$. But the partial derivatives of F all vanish at $(1, x_2, 0)$ if $x_2^2+b=0$, $2bx_2+a=0$, and hence if $b=0$, $x_2=0$, or if $b\neq 0$, $x_2=-a/(2b)$, whereas F has no singular point. Hence

$$a^2+4b^3\neq 0 \tag{7}$$

and (6) has four distinct roots r for each of which $s\neq 0$. Thus *there are exactly nine distinct points of inflexion.*

The two points $(1, r, \pm s)$ with a fixed r are collinear with $P=(0, 0, 1)$, being on $x_2=rx_1$. For the remaining roots ρ of (6), we have

$$\rho^3+r\rho^2+(r^2+6b)\rho+r^3+6br+4a=0.$$

The product of this by r can be written in the form

$$r(\rho^3+3b\rho+a)+(r\rho+k)^2=0, \qquad k=\tfrac{1}{2}(r^2+3b).$$

Hence the quadratic factor in

$$\frac{1}{24}H+rF=(rx_1-x_2)\left\{x_3^2-\frac{1}{r}(rx_2+kx_1)^2\right\} \tag{8}$$

vanishes at $(1, \rho, \pm\sigma)$, where

$$-\sigma^2=\rho^3+3b\rho+a.$$

Thus the nine points of inflexion lie by threes upon the three straight lines given by (8), which are said to form an *inflexion triangle.* There are four inflexion triangles, one for each root r of (6).

The roots of (6) are the only values of r for which $H+24rF$ has a linear factor l. In fact, $l=0$ meets $F=0$ in three points on $H=0$ which are therefore points of inflexion. Thus l has two companion linear functions such that $ll_1l_2=0$ is one of the four inflexion triangles. Hence $ll_1l_2=H+24\rho F$, where ρ is one of the roots of (6). By hypothesis, $lQ=H+24rF$. If

$r \neq \rho$, we see by subtraction that F has the factors l and $Q - l_1 l_2$ and hence has a singular point, contrary to assumption.

Corresponding results follow at once for the general cubic curve $f=0$. We saw that f can be reduced to F by a linear transformation of a certain determinant δ. But F is replaced by a like form by the transformation which multiplies x_1, x_2, x_3 by δ^{-2}, 1, δ, respectively, and thus has the determinant δ^{-1}. The product of the two transformations is of determinant unity and replaces f by a form F. Hence (§ 174), it replaces the Hessian h of f by the Hessian H of F. Thus for each root r of (6), in which a and b are certain functions of the coefficients of f, $h+24rf=0$ represents an inflexion triangle of f.

Furthermore, a and b are rational functions of the coefficients of f. For, there are exactly four values of r for which $\phi \equiv h+24rf$ has a linear factor $x_1 - mx_2 - nx_3$. Replacing x_1 by mx_2+nx_3 in ϕ, we obtain a cubic function of x_2 and x_3 whose coefficients must vanish. Eliminating m and n, we obtain two equations in which r and the coefficients of f enter rationally and integrally. The greatest common divisor of their left members must be a function of r whose coefficients are rational in those of f. The latter is therefore true (§ 145, first foot-note) of the quartic equation * for r with no multiple root.

176. Group G of the Equation X for the Abscissas of the Points of Inflexion. Let R be the domain defined by the coefficients of the equation $f=0$ of a cubic curve without singular points. We employ a new triangle of reference whose side $x_1=0$ does not contain a point of inflexion. This can be accomplished by a linear transformation on x_1, x_2, x_3 with coefficients in R. We pass to Cartesian coördinates by setting $x_2/x_1=x$, $x_3/x_1=y$. After applying a transformation with coefficients in R, corresponding to a rotation of the axes, we may assume that the y-axis is not parallel to any line joining two inflexion points of $f=0$. Then the abscissas $x_1, \ldots, x_9$ of the points of inflexion are distinct. By eliminating y^3 and y^2 between the equations of the curve and its Hessian curve, we

* We do not employ the fact, which now follows readily, that the coefficients of (6) are rational integral invariants of f.

obtain y expressed as a rational function $\phi(x)$ of x with coefficients in R. In fact, the ordinate of an inflexion point is uniquely determined by its abscissa. By substituting $\phi(x)$ for y in $f=0$, we obtain the equation X for the nine abscissas of the points of inflexion.

For three collinear points of inflexion,

$$\begin{vmatrix} x_i & y_i & 1 \\ x_j & y_j & 1 \\ x_k & y_k & 1 \end{vmatrix} = 0.$$

Replacing y_i by $\phi(x_i)$, etc., we obtain a rational relation

$$\psi(x_i, x_j, x_k) = 0, \tag{9}$$

with coefficients in R. Conversely, if relation (9) holds for the abscissas of three points of inflexion, the latter are collinear. For, the line joining two of them, (x_j, y_j) and (x_k, y_k), meets the curve at a single point (x, y) and that point is a point of inflexion, so that $\psi(x, x_j, x_k)=0$ and $X(x)=0$ have a unique common solution x. Thus $x=x_i$ and hence $y=y_i$.

Let a substitution of the group G of equation X for the domain R replace three roots x_i, x_j, x_k, for which (9) holds, by the roots x_r, x_s, x_t. By property B (§ 149) of the group G, $\psi(x_r, x_s, x_t)=0$. Hence *every substitution of G replaces the abscissas of three collinear points of inflexion by the abscissas of three collinear points of inflexion.*

Denote by 1, 2, 3 the points of inflexion on one side of a triangle of inflexion; by 4, 5, 6 those on a second side. Those on the third side may be denoted by 7, 8, 9 in such an order that 1, 4, 7 are collinear; 1, 5, 9 collinear, and hence 1, 6, 8 collinear. The third point on the line joining 2 and 4 is 8 or 9 (since 4 and 7 are collinear with 1); if it be 8, we interchange symbols 5 and 6, 8 and 9, and see that all the earlier collinearities are preserved, and that 2, 4, 9 are now collinear. Then the point on the line joining 2 and 6 must be 7 (since not 8 or 9), and that on the line joining 2 and 5 must be 8. We see that the 12 sets of collinear points of inflexion are those given by the

rows, columns, and positive and negative terms of the expansion of the determinant

$$\begin{vmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{vmatrix}$$

Henceforth we shall denote the abscissas of the nine points of inflexion by the nine symbols $[\xi\,\eta]$, where $\xi=0,\ 1,\ 2$ and $\eta=0,\ 1,\ 2$. Then the abscissas of collinear points of inflexion are those in the rows, columns, and positive and negative terms of

$$(10) \qquad \begin{vmatrix} [00] & [01] & [02] \\ [10] & [11] & [12] \\ [20] & [21] & [22] \end{vmatrix}$$

and have the sum of their first indices divisible by 3, and also the sum of their second indices divisible by 3.

Hence G is a subgroup of the group L of those substitutions on the nine roots which replace any three distinct roots $[\xi_i\eta_i]$, $i=1,\ 2,\ 3$, for which

$$(11) \qquad \xi_1+\xi_2+\xi_3\equiv 0,\quad \eta_1+\eta_2+\eta_3\equiv 0 \pmod 3,$$

by three distinct roots $[\xi'_i\ \eta'_i]$ also satisfying congruences (11).

We obtain a substitution of L if we take

$$(12) \qquad \xi'\equiv a\xi+b\eta+c,\quad \eta'\equiv A\xi+B\eta+C,\quad \begin{vmatrix} a & b \\ A & B \end{vmatrix}\not\equiv 0 \pmod 3,$$

where $a,\ \ldots,\ C$ are integers. For,

$$\sum_{i=1}^{3}\xi'_i=a\sum_{i=1}^{3}\xi_i+b\sum_{i=1}^{3}\eta_i+3c\equiv 0,\quad \sum_{i=1}^{3}\eta'_i\equiv 0 \pmod 3.$$

Further, the $[\xi'_i\ \eta'_i]$ are distinct. For, if $\xi'_1\equiv\xi'_2$, $\eta'_1\equiv\eta'_2$, then

$$a(\xi_1-\xi_2)+b(\eta_1-\eta_2)\equiv 0,\quad A(\xi_1-\xi_2)+B(\eta_1-\eta_2)\equiv 0 \pmod 3.$$

But the determinant $aB-bA$ is not congruent to zero. Hence $\xi_1\equiv\xi_2$, $\eta_1\equiv\eta_2$, contrary to hypothesis.

Conversely, every substitution S of L is induced by a linear transformation (12) on the indices. Let S replace [00] by $[c\,C]$; the same is true of the substitution P induced by

$$\xi' \equiv \xi + c, \quad \eta' \equiv \eta + C \pmod 3. \tag{13}$$

Hence $S = TP$, where T is a substitution of L which leaves [00] unaltered. Let T replace [10] by $[aA]$, where therefore a and A are not both zero. Thus we can find two integers b and B such that $aB - bA$ is not divisible by 3; if $a \not\equiv 0$, we may take $B = 1$, $b = 0$; if $A \not\equiv 0$, we may take $b = 1$, $B = 0$. Then the substitution P' induced by

$$\xi' \equiv a\xi + b\eta, \quad \eta' \equiv A\xi + B\eta, \quad aB - bA \not\equiv 0 \pmod 3 \tag{14}$$

replaces [10] by $[aA]$. Hence $T = T'P'$, where T' is a substitution of L which alters neither [00] nor [10] and hence not [20], in view of the first column of (10). Let T' replace [01] by $[de]$, so that $e \not\equiv 0$. The substitution P_1 induced by

$$\xi' \equiv \xi + d\eta, \quad \eta' \equiv e\eta$$

leaves unaltered each $[\xi 0]$ and replaces [01] by $[de]$. Hence $T'P_1^{-1}$ leaves unaltered each $[\xi 0]$ and [01] and is the identity. For, it leaves fixed [02] by the first row of (10), and hence [21] and [12] by positive terms of the expansion of determinant (10), and then [11] and [22] by the second and third rows. Hence $T' = P_1$ and $S = P_1P'P$, so that S is induced by a linear transformation (12).

Now $[cC]$ was any one of 3×3 roots, $[aA]$ any one of $3^2 - 1$ roots, and $[de]$ any one of 3×2 roots.

THEOREM.* *The group G of the equation X for the abscissas $[\xi\eta]$ of the nine points of inflexion is a subgroup of the group L of all of the $9 \times 8 \times 6$ linear transformations* (12) *on ξ, η.*

The $3^2 - 1$ incongruent linear homogeneous functions of ξ and η with integral coefficients modulo 3 are

$$\pm\xi, \quad \pm\eta, \quad \pm(\xi + \eta), \quad \pm(\xi - \eta).$$

* Jordan, *Traité des Substitutions*, p. 302, where L is defined to be the group leaving (formally) unaltered the cubic function given by the sum of the products of the roots in each row, etc., of (10). But formal invariance may well introduce some confusion since the roots are not independent. For a wholly different determination of L, see Weber's *Algebra*, 2d ed., vol. 2, p. 413.

Hence they are permuted by the linear homogeneous transformations (14), which form a group H. Since H permutes their four squares $\xi^2, \ldots, (\xi-\eta)^2$, it is isomorphic with a group of substitutions on four letters. To show that the isomorphism is (2, 1), note that a transformation leaving ξ^2 and η^2 unaltered at most changes the signs of ξ and η. But if the sign of one is changed and the sign of the other is not changed, $(\xi+\eta)^2$ is replaced by $(\xi-\eta)^2$. Hence the identity I and

$$J: \qquad \xi' \equiv -\xi, \quad \eta' \equiv -\eta \pmod 3$$

alone leave each of the four squares unaltered.

The order of H is 48. There are $2\times2\times3$ transformations (14) with $b\equiv0$, whence $a\equiv1$ or 2, $B\equiv1$ or 2, $A\equiv0$, 1 or 2. There are $2\times2\times3^2$ transformations (14) with $b\not\equiv0$, whence a and B are arbitrary, while $aB-bA\equiv\pm1$ then determines A.

Hence * the quotient group $H/\{I, J\}$ is simply isomorphic with the symmetric group on four letters. Thus H is a solvable group.

The group T of the nine translations (13) is invariant under L. In fact, (14) transforms (13) into the translation

$$\xi' \equiv \xi + ac + bC, \quad \eta' \equiv \eta + Ac + BC.$$

It follows that L is a solvable group. By § 68, Ex. 4, or by § 178, its subgroup G is solvable. Hence *the equation X for the abscissas of the nine points of inflexion is solvable by radicals.*

177. Group of the Resolvent Quartic Equation (6). Let $r_1, \ldots, r_4$ be the roots of (6) and set $y_1 = r_1r_2 + r_3r_4$, etc., as in Example 2, § 150. Then y_1, y_2, y_3 are the roots of

$$y^3 - 6by^2 + 12b^2y - 16a^2 - 72b^3 = 0.$$

Setting $y = z + 2b$, we obtain the reduced cubic $z^3 = D$, where

$$D = 16(a^2 + 4b^3) \not\equiv 0,$$

by (7). From † its discriminant, we see that

$$P \equiv (y_1 - y_2)(y_1 - y_3)(y_2 - y_3) = D\sqrt{-27}.$$

* Another proof follows from the fact that the linear fractional transformation on $z = \xi/\eta$, derived from (14) by division, permutes the values 0, 1, 2, ∞ of z.

† Or from $(z-\omega z)(z-\omega^2 z)(\omega z-\omega^2 z)$, where $\omega^2+\omega+1=0$.

Consider the special cubic form given by F in § 175 with $a=1$, $b=-1$. Then $D=-48$, so that P and each y_i is irrational. Equation (6) is now

$$r^4-6r^2+4r-3=0 \tag{6'}$$

and is irreducible in the domain $R(1)$ of rational numbers. For, no root is ± 1, ± 3, so that no root is rational. Further, a y_i occurs in the coefficients of any quadratic factor, as shown by Ferrari's method of solving quartic equations. Hence the group of (6') for the domain $R(1)$ is the symmetric group (Ex. 5, § 153).

Let f be a cubic form whose ten coefficients are independent variables. Let R be the domain of the rational functions with rational coefficients of these ten variables. Then (Ex. 2, § 153), *the group of the quartic equation* (6) *for* R *is the symmetric group.*

178. Group G of Equation X is the Linear Group L. After the adjunction of a root r of the resolvent quartic (6), the product of the equations of the three sides of an inflexion triangle has its coefficients in the domain (R, r), and the group G reduces to the subgroup which permutes the triples of abscissas of the points of inflexion on the sides of that triangle. First, let the triangle be that one whose sides contain the points of the rows in (10); these triples are merely permuted when the sign of either index is changed and also by the transformation

$$\xi' \equiv \xi + c, \quad \eta' \equiv A\xi + \eta + C$$

and hence by the group of the $4 \cdot 3^3$ transformations (12) with $b \equiv 0$, whose index under L is 4. By the interchange of the two indices, these triples are replaced by those in the columns of (10), so that the latter are merely permuted by the group of the transformations (12) with $A \equiv 0$. When $b \equiv A \equiv 0$, we have

$$\xi' \equiv a\xi + c, \quad \eta' \equiv B\eta + C, \quad aB \not\equiv 0 \pmod 3.$$

Unless $a \equiv B$, the triples in the positive terms of the determinant (10) are replaced by those in the negative terms, since this is true for $\xi' = \xi$, $\eta' \equiv -\eta$, and since each transformation

$$\xi' \equiv \pm\xi + c, \quad \eta' \equiv \pm\eta + C \tag{15}$$

permutes the three triples in the rows, the three in the columns, etc., of (10). Hence *after the adjunction of the four roots of* (6), *the group G reduces to a subgroup* Σ *of the group of the* 18 *transformations* (15).

The group Σ *is of order a multiple of* 2. Take $a=-2$, $b=0$ in § 175. Then (6) becomes $r(r^3-8)=0$, all of whose roots are in $R(\omega)=R(\sqrt{-3})$. The Hessian (§ 175) is

$$H=-24x_2(x_3^2+6x_1^2).$$

After the adjunction of the four r's, the domain is $R(\sqrt{-3})$, to which does not belong the irrationality * $\sqrt{2}\sqrt{-3}$ occurring in the sides of the inflexion triangle $H=0$.

The group Σ *is of order a multiple of* 3. For

$$f=x_1^3+2x_2^3+4x_3^3+6x_1x_2x_3,$$

the Hessian is $6^3h'$, where

$$h'=-x_1^3-2x_2^3-4x_3^3+10x_1x_2x_3.$$

Then $3h'+rf$ has a linear factor if $r=3$, -1, $-1\pm4\sqrt{-3}$. This is evident for $r=3$. For $r=-1$, we get

$$3h'-f=4(-x_1^3-2x_2^3-4x_3^3+6x_1x_2x_3),$$

having the factor

$$\frac{x_1}{\sqrt[3]{2}}+x_2+\sqrt[3]{2}x_3.$$

After the adjunction of the four r's, the domain is $R(\sqrt{-3})$, to which $\sqrt[3]{2}$ does not belong. Thus the order † of Σ is a multiple of 3.

We return to a cubic form f with arbitrary coefficients and the domain R defined by them. By the adjunction of the nine roots of X, the group G_{24} of the resolvent (6) is reduced to the identity. In fact, the abscissas and hence the ordinates of the nine inflexion points are in the enlarged domain. Thus the ratios of the coefficients of the equation of the line joining

* No radical other than these two occurs in the sides of triangle (8) for $r^3=8$. Hence the group G for this special cubic curve is of order 4.

† Its order is in fact exactly 3; that of G is 6.

three collinear inflexion points are in the enlarged domain; the same is true for their products by threes giving the inflexion triangles $h+24rf$, so that each root r of (6) is in that domain. It now follows from the theorem of Jordan (§ 167) that the adjunction to R of the four roots of (6) reduces the group G of X for R to an invariant subgroup Σ of index 24 under G, such that G/Σ is simply isomorphic with G_{24}.

This group Σ was shown to contain a transformation (15) of period 3, necessarily a translation (13). By interchanging ξ and η if necessary, we may assume that ξ is altered. Then the translation or its square is of the form

$$\xi' \equiv \xi + 1, \quad \eta' \equiv \eta + t.$$

Introducing ξ and $\eta - t\xi$ as new variables, we obtain a group Σ_1 conjugate with Σ under L and containing the translation $\xi' \equiv \xi + 1$, $\eta' \equiv \eta$. The only transformations (12) which are commutative with this one are those with $a \equiv 1$, $A \equiv 0$, $B \not\equiv 0$, b, c, C arbitrary, $2 \cdot 3^3$ in number. The above translation is transformed into its inverse by $\xi' \equiv -\xi$, $\eta' \equiv \eta$. Hence exactly $4 \cdot 3^3$ transformations of L transform into itself the cyclic group of order 3 generated by it. Since this number is one-fourth of the order of L, a subgroup of index 3 under L cannot transform this cyclic group into itself.

But Σ is of order 6 or 18. In the first case, Σ contains a single cyclic group of order 3, which is therefore invariant under G; while G is of order $24 \cdot 6$ and hence of index 3 under L. Thus the first case is excluded by the preceding result. Hence Σ is of order 18 and $G = L$.

THEOREM.* *If the coefficients of a cubic curve $f = 0$ are independent variables, the group of the equation upon which depends the nine points of inflexion* $[\xi\eta]$, $\xi, \eta = 0, 1, 2$, *for the domain of the coefficients, is the group of all linear transformations on ξ and η modulo* 3.

After the adjunction of the roots of the resolvent quartic (6), the group is that of the 18 transformations (15). The

* Stated, but not completely proved, by Weber, *Algebra*, ed. 2, vol. 2, pp. 416–7. The proof is due to Dickson, *Annals of Math.*, ser. 2, vol. 16 (1914), pp. 50–66.

product $P \equiv h + 24rf$ of the linear functions which vanish at the sides of an inflexion triangle has as its coefficients quantities in the enlarged domain. The determination of the linear factors requires the solution of a cubic equation. Consider the inflexion triangle associated with the rows in (10); after the adjunction of the roots of the corresponding cubic equation, the group permutes the roots $[\xi\eta]$ in the same row. The only transformations (15) having this property are $\xi' \equiv \xi$, $\eta' \equiv \eta + C$, which form a group C_3. The group of the resolvent cubic is therefore of order $\frac{1}{3} \cdot 18 = 6$. In the new domain, the group of the corresponding resolvent cubic for another inflexion triangle is C_3. After the adjunction of one and hence all of its roots, we have the sides of two inflexion triangles, and their intersections give the nine inflexion points.

Hence *the determination of the inflexion points of an arbitrary cubic curve requires the extraction of a cube root and three square roots to solve the resolvent quartic equation, then the extraction of a square root and two cube roots to solve the two cubic equations which determine the sides of two inflexion triangles. No one of these three cube roots and four square roots can be avoided or expressed rationally in terms of the others.*

179. Real Points of Inflexion. Let the coefficients of the equation of the cubic curve be real. After a suitable choice of axes, the nine abscissas of the points of inflexion are the nine distinct roots of an equation with real coefficients (§ 176). Hence at least one point of inflexion is real. The reduction to the form F in § 175 can therefore be effected by a real transformation. By § 177 the discriminant of the real quartic equation (6) is $-27D^2$ and hence is negative. Thus * there are two distinct real and two imaginary roots. One of the real roots is positive and the other is negative, as shown by the values $-\infty$, 0, $+\infty$ of the variable r. By use of the same values we see that the slope of the curve $y = x^4 + 6br^2 + \ldots$, corresponding to (6), is positive at the point whose abscissa is the positive root and negative at that with the negative root. At the points of inflexion $(1, r, \pm s)$ the slope is $-4s^2$, by the

* Dickson's *Elementary Theory of Equations*, p. 45, or Ex. 5, p. 101.

formula below (6). To obtain a real point, we must therefore take the negative real root r. Thus a real cubic curve $F=0$ has exactly three real points of inflexion, viz., (0, 0, 1) and $(1, r, \pm s)$, where r is the single negative root. *Any real cubic curve without a double point has exactly three real points of inflexion.*

CHAPTER XIX

THE TWENTY-SEVEN STRAIGHT LINES ON A GENERAL CUBIC SURFACE AND THE TWENTY-EIGHT BITANGENTS TO A GENERAL QUARTIC CURVE

180. Existence of the 27 Lines. We shall first show that there is at least one real or imaginary straight line

$$x = mz + n, \quad y = pz + q \tag{1}$$

on the general cubic surface $\phi(x, y, z) = 0$. Eliminating x and y, and equating to zero the coefficients of the resulting cubic function of z, we obtain four relations between the four parameters m, n, p, q. These are consistent and have one or more sets of solutions, except possibly for special sets of coefficients of ϕ. In fact, they are evidently consistent when $\phi = xyz$. See also § 183.

To determine the number of the straight lines on the cubic surface, we employ homogeneous coördinates, choosing the tetrahedron of reference so that $x_3 = 0$, $x_4 = 0$ are the equations of a line on the surface. Then no one of the terms x_1^3, $x_1^2 x_2$, $x_1 x_2^2$, x_2^3 occurs in the equation of the surface, which is therefore of the form

$$x_3 f + x_4 g = 0,$$

where f and g are homogeneous quadratic functions of $x_1, \ldots, x_4$. Part of the intersection of the surface by the plane $x_4 = cx_3$ is the line $x_3 = x_4 = 0$, and the remaining part is the conic $f_1 + cg_1 = 0$ in that plane, where f_1 and g_1 are derived from f and g by replacing x_4 by cx_3. Hence in f_1 and g_1, the coefficients of x_3^2 are quadratic in c, the coefficients of $x_1 x_3$ and $x_2 x_3$ are linear in c, and the coefficients of x_1^2, $x_1 x_2$, x_2^2 are free of c. The conic degenerates into a pair of straight lines if and only

if the Hessian (discriminant) of f_1+cg_1 is zero. The degrees in c of the second partial derivatives of f_1+cg_1 exceed by unity those of g_1. Hence the degrees in c of the elements of the Hessian determinant are

$$\begin{matrix} 1 & 1 & 2 \\ 1 & 1 & 2 \\ 2 & 2 & 3. \end{matrix}$$

Thus the determinant is of the fifth degree in c. There are cubic surfaces S for which this quintic has five distinct roots, so that the surface contains five pairs of straight lines intersecting the line C given by $x_3=x_4=0$. This is true if

$$f=x_1x_2+ex_1x_4+tx_2x_4+ax_3x_4+bx_4^2, \quad g=x_1^2+x_2x_4.$$

For then

$$f_1+cg_1=cx_1^2+x_1x_2+cex_1x_3+(c^2+tc)x_2x_3+(ac+bc^2)x_3^2,$$

whose discriminant is

$$-2c[c^4+2tc^3-(e-t^2)c^2+(b-te)c+a].$$

The second factor becomes any assigned quartic function by choice of t, e, b, a. Consequently, after the exclusion of the special surfaces for which the quintic is identically zero in c (for example, $xyz=0$), or has fewer than five distinct finite roots, there remain surfaces of type S. For such a surface, each root c leads to a pair of lines A and B forming with C a triangle, which is the complete intersection of its plane $x_4=cx_3$ with the cubic surface.

The line C was any straight line on the surface. Hence every line on the surface is met by ten other straight lines lying on the surface.

Any straight line L on the surface meets the plane of the triangle ABC and meets it at a point on one of the sides, since the triangle is the complete intersection of its plane with the surface. Thus L is either A, B, C, or one of the eight lines, other than B and C, which meet A, or one of the eight new lines meeting B, or one of the eight new lines meeting C. These 24 new lines are distinct, since otherwise one of them would meet

two of the lines A, B, C, whereas the triangle ABC is the complete intersection of its plane with the surface. We readily exclude the case in which L passes through the intersection of A and B. For, if so, we may take those three lines as concurrent edges of a tetrahedron of reference. Then $x_1=x_2=0$, $x_1=x_3=0$, $x_2=x_3=0$ are lines on the surface, whose equation $\phi=0$ therefore has no terms in x_3 and x_4 only, none in x_2 and x_4 only, and none in x_1 and x_4 only. Thus x_4 occurs only in the terms $x_1x_2x_4$, $x_1x_3x_4$, $x_2x_3x_4$. Hence the first partial derivatives of ϕ with respect to each x_i vanish at $(0, 0, 0, 1)$, which is therefore a singular point. But not every cubic surface has a singular point. Hence *there are exactly 27 distinct straight lines on a general cubic surface.*

181. Double-six Configuration. Consider a line b_1 on the cubic surface and the five pairs a_i, c_i $(i=2, \ldots, 6)$ of lines

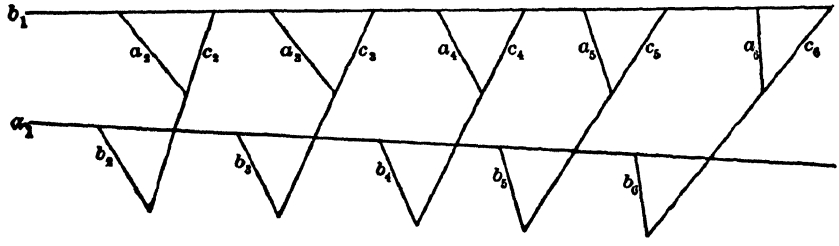


FIG. 16.

on the surface which meet b_1. The five planes $b_1a_ic_i$ are distinct and three lines on the surface do not concur (§ 180). Hence no two of the lines $c_2, \ldots, c_6$ intersect. The locus of a line L intersecting c_2, c_3, c_4 is a surface of the second order *

* By choice of the axes, the equations of c_2 become $y=mx$, $z=c$, and those of c_3 become $y=-mx$, $z=-c$. The line L joining the general point (a, ma, c) of c_2 with the general point $(b, -mb, -c)$ of c_3 is

$$x=dz+ce, \quad y=mez+mcd, \quad d\equiv\frac{a-b}{2c}, \quad e\equiv\frac{a+b}{2c}.$$

This meets c_4: $x=lz+t$, $y=rz+s$, if

$$(d-l)z+ce-t=0, \quad (me-r)z+mcd-s=0.$$

In the determinant of the coefficients of z and the constants, replace d and e by the values obtained by solving the equations of L. We get

$$\Delta\equiv\begin{vmatrix} mxz-cy-lmZ, & cyz-mc^2x-mtZ \\ yz-mcx-rZ, & mcxz-c^2y-sZ \end{vmatrix}=0,$$

and hence is an hyperboloid H of one sheet. By suitable choice of the axes, the equation of H is

$$0=\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}-1=\left(\frac{x}{a}+\frac{z}{c}\right)\left(\frac{x}{a}-\frac{z}{c}\right)-\left(1+\frac{y}{b}\right)\left(1-\frac{y}{b}\right),$$

or $tu-vw=0$, if the binomials are designated t, etc. Hence

$$\begin{cases} u=rw, \\ v=rt, \end{cases} \qquad \begin{cases} u=sv, \\ w=st \end{cases}$$

are intersecting lines lying on H. When r varies, we obtain one set of *generators;* when s varies, we obtain a second set. Through each point of H passes one and only one generator of each set. We may assume that c_2, c_3, c_4 belong to the first set of generators. Let c_5 cut H at P_1 and P_2. Through P_i passes one generator of the second set, which therefore meets c_2, c_3, c_4, as well as c_5. Hence c_2, c_3, c_4, c_5 have two non-intersecting transversals, one of which is b_1; call the second a_1. Since a_1 contains four points of the surface (the intersections of a_1 with c_2, c_3, c_4, c_5), it lies wholly on the surface. The line a_1 therefore meets one of the sides of triangle $b_1a_6c_6$. As observed above, a_1 does not meet b_1. Denote by c_6 that one of the remaining two sides which meets a_1, and by a_6 the other side. Then no two of the lines $a_1, \ldots, a_6$ intersect.

The line a_1 is met by five lines $b_2, \ldots, b_6$ of the surface besides $c_2, \ldots, c_6$. No two of the lines $b_1, \ldots, b_6$ intersect.

Now b_2 meets one side of triangle $b_1a_3c_3$ other than c_3, since c_3 meets the side a_1 of triangle $a_1b_2c_2$. Hence b_2 meets a_3.

The name *double-six* is given to this configuration of 12 lines a_i, b_i $(i=1, \ldots, 6)$ such that no two a's meet, no two b's meet, a_i and b_i do not meet, while a_i and b_j meet if $i \neq j$.

182. The 45 Triangles on the Cubic Surface. Since each line on the surface is a side of five triangles (§ 180) and each triangle has three sides, there are $5 \cdot 27/3$ or 45 triangles.

where $Z=z^2-c^2$. Suppressing the terms involving Z in Δ, we get

$$c(mxz-cy)^2-c(yz-mcx)^2=c(m^2x^2-y^2)Z.$$

Hence Δ is the product of Z by the required equation of degree 2.

Write $c_{1i} \equiv c_{i1}$ for the c_i $(i=2, \ldots, 6)$ in § 181. Then $a_1 b_i c_{1i}$ and $a_i b_1 c_{i1}$ are triangles on the surface. Let c_{23} be the third side of the triangle determined by a_2 and b_3. Hence c_{23} is distinct from each a_i and b_i; also from c_i, since c_2 is the only c_i meeting a_2, and since c_2 meets the side a_1 of $a_1 b_3 c_3$ and hence does not meet b_3. This new line c_{23} is thus not one of the ten lines meeting b_1; nor does it meet c_3, which intersects the side b_3 of $a_2 b_3 c_{23}$. Hence c_{23} meets the side a_3 of $a_3 c_3 b_1$. Similarly, c_{23} meets b_2. For like reasons, we may write $c_{ij} \equiv c_{ji}$ for the third side of the triangle determined by a_i and b_j for $i, j = 1, \ldots, 6$; $i \neq j$.

We now have notations a_i, b_i, c_{ij} for the 27 lines on the surface, and have the 30 triangles $a_i b_j c_{ij}$.

Next, if i, j, k are distinct, c_{ij} and c_{ik} do not meet. For, if they met, their plane would contain a_i and b_i, whereas the latter do not intersect. Finally, two c's having four distinct subscripts intersect. For example, c_{34} meets one side of $a_2 b_1 c_{12}$, but does not meet b_1 or a_2, since a_2 meets the side b_3 of $a_4 b_3 c_{34}$; hence c_{34} meets c_{12}.

Thus the sides of the remaining 15 triangles on the surface are c's with the following sets of subscripts:

12 34 56, 13 24 56, 14 23 56, 15 23 46, 16 23 45,

12 35 46, 13 25 46, 14 25 36, 15 24 36, 16 24 35,

12 36 45, 13 26 45, 14 26 35, 15 26 34, 16 25 34.

183. The Group for the Problem. Let R be the domain defined by the ratios of the coefficients of the equation for the cubic surface. After a suitable choice of axes of coördinates, we may assume that no two of the 27 lines (1) on the surface have the same parameter q. By eliminating m, n, p between the four relations mentioned in § 180, we obtain an equation * $E(q) = 0$ of degree 27 in q with coefficients in R. Since n may be eliminated last, it is a rational function of q with coefficients in R. The same is true of m and p. Thus the coefficients of the equation of a line on the surface are rational functions with

* It may be assumed to have no multiple root (§ 145 first foot-note).

coefficients in R of the corresponding root q of $E(q)=0$. Hence we seek the group G of $E(q)=0$ for R.

Line (1) is in a plane with another line

$$x=m_1z+n_1, \quad y=p_1z+q_1 \tag{2}$$

on the surface, if the eight parameters satisfy the relation obtained by eliminating x, y, z between the four equations:

$$\begin{vmatrix} 1 & 0 & m & n \\ 0 & 1 & p & q \\ 1 & 0 & m_1 & n_1 \\ 0 & 1 & p_1 & q_1 \end{vmatrix} = 0.$$

In view of the remark that m, n, p are rational functions of q, this yields a rational relation $f(q, q_1)=0$ with coefficients in R. Let this relation be satisfied. Since there is a single line (q_2) on the surface coplanar with two intersecting lines (q) and (q_1),

$$f(q, q_2)=0, \quad f(q_1, q_2)=0$$

have a single solution q_2. The next to the last step in the elimination of q_2 gives q_2 expressed as a rational function of q and q_1 with coefficients in R, say $q_2=r(q, q_1)$.

Since any substitution of G must leave $q_2-r(q, q_1)$ unaltered, it must replace the three q's corresponding to three lines of a triangle on the surface by three q's of another triangle. Henceforth we shall denote the 27 q's by the 27 letters a_i, b_j, c_{ij} of § 182. Thus G is a subgroup of the group Γ on the a_i, b_j, c_{ij} which permutes the 45 triples having the same notation as the 45 triangles in § 182.

We readily determine the order and generators * of Γ. First,

$$J=(a_1b_1) \ \ldots \ (a_6b_6)$$

interchanges the triples $\Delta_{ij}\equiv a_ib_jc_{ij}$ and Δ_{ji}, and leaves unchanged the 15 triples at the end of § 182. Thus J is in Γ.

* Much simpler and more natural than the generators used by Jordan, *Traité des Substitutions*, p. 317.

Next, the 45 triples are evidently permuted by the substitution $[ij]$ on the 27 letters which is induced by the interchange of the subscripts i and j. For example,

$$[12]=(a_1a_2)(b_1b_2)(c_{13}c_{23})(c_{14}c_{24})(c_{15}c_{25})(c_{16}c_{26}).$$

Finally, the group Γ contains

$$A=(a_1a_3c_{24})(a_2c_{14}c_{34})(a_4c_{12}c_{23})(b_3b_1c_{56})(b_5c_{36}c_{16})(b_6c_{35}c_{15}),$$

which permutes the 45 triples as follows:

$$(\Delta_{12}\Delta_{32}\Delta_{42})(\Delta_{14}\Delta_{34}\Delta_{24})(\Delta_{13}\quad\Delta_{31}\quad c_{13}c_{24}c_{56})$$
$$\cdot(\Delta_{43}\quad\Delta_{21}\quad c_{14}c_{23}c_{56})(\Delta_{23}\quad\Delta_{41}\quad c_{12}c_{34}c_{56})PQ,$$

where

$$P=(\Delta_{15}\quad\Delta_{36}\quad c_{16}c_{24}c_{35})(\Delta_{25}\quad c_{14}c_{25}c_{36}\quad c_{16}c_{25}c_{34})$$
$$\cdot(\Delta_{51}\quad\Delta_{56}\quad\Delta_{53})(\Delta_{45}\quad c_{12}c_{36}c_{45}\quad c_{16}c_{23}c_{45}),$$

while Q is derived from P by interchanging the subscripts 5 and 6.

From these substitutions of Γ we evidently can derive one which replaces a_1 by any one of the 27 letters. If a substitution of Γ does not alter a_1, it must permute amongst themselves the pairs b_j, $c_{1j}(j=2, \ldots, 6)$ occurring in triples with a_1. From

$$B=(a_5a_3c_{24})(a_2c_{45}c_{34})(a_4c_{25}c_{23})(b_3b_5c_{16})(b_1c_{36}c_{56})(b_6c_{13}c_{15}),$$

which is the transform of A by [15], and the $[ij]$, we readily derive a substitution which leaves a_1 fixed and replaces b_2 by any one of the ten letters b_j, c_{1j} $(j>1)$.

If a substitution of Γ leaves a_1 and b_2 fixed, it leaves c_{12} fixed and replaces b_3 by one of the eight letters b_j, $c_{1j}(j=3, \ldots, 6)$. Such a substitution can be derived from the $[ij]$, $i,j=3, \ldots, 6$, and B.

If a substitution of Γ leaves fixed a_1, b_2, c_{12}, b_3, it leaves fixed c_{13} and permutes the pairs a_i, $c_{i2}(i=3, \ldots, 6)$ occurring in triples with b_2, and permutes the pairs a_i, c_{i3} $(i=2, 4, 5, 6)$ occurring in triples with b_3. Hence it permutes the letters c_{23}, a_4, a_5, a_6 common to the two sets of pairs. Now [15][34] transforms A into

$$(a_5a_4a_{23})(a_2c_{35}c_{34})(a_3c_{25}c_{24})(b_4b_5c_{16})(b_1c_{46}c_{56})(b_6c_{14}c_{15}),$$

from which and the $[ij]$, $ij=4, 5, 6$, we get a substitution leaving fixed a_1, b_2, c_{12}, b_3 and c_{13} and replacing c_{23} by any one of the four letters c_{23}, a_4, a_5, a_6. Next, the $[ij]$, $i, j=4, 5, 6$, leave also c_{23} fixed and permute a_4, a_5, a_6 in six ways.

Finally, a substitution of Γ which leaves fixed

$$a_1,\ a_4,\ a_5,\ a_6,\ b_2,\ b_3,\ c_{12},\ c_{13},\ c_{23}$$

is the identity. For, by the above two sets of four pairs, it leaves fixed a_3, c_{i2}, a_2, c_{i3} $(i=4, 5, 6)$. Then by the triples containing c_{12}, c_{i3} $(i \geqq 4)$, it leaves fixed c_{56}, c_{46}, c_{45}. By the triples containing one of the last three c's and c_{23}, it leaves fixed c_{14}, c_{15}, c_{16}. Hence it leaves fixed the fifteen c's and the six a's and consequently the six b's, in view of the triples $a_i b_j c_{ij}$.

The group Γ *is generated by* A, J *and the* $[ij]$, $i, j=1, \ldots, 6$ *and is of order* $27 \cdot 10 \cdot 8 \cdot 24 = 51{,}840$.

It was noticed that J gives rise to an odd substitution on the 45 triples. Hence Γ has an invariant subgroup H of index 2 and order 25,920, composed of those substitutions of Γ which give rise to even substitutions on the triples. Various proofs * have been given of the simplicity of H.

We shall next discuss the remarkable relation between the 27 lines on a general cubic surface and the 28 bitangents to a general quartic curve. From the group of the latter problem, we shall be able to conclude (§ 189) that the group G of the former is identical with Γ. Thus G has the factors of composition 2 and 25,920. In particular, the equation $E(q)=0$ for the 27 lines is not solvable by radicals. The equation has a resolvent of degree 45, corresponding to the 45 triangles, and a resolvent of degree 36, corresponding to the 36 double-sixes. But it has no resolvent of degree less than 27 other than the quadratic the adjunction of whose roots reduces the group to the subgroup H of index 2; this fact has been proved in three distinct ways.† The problem is thus of special complexity on the algebraic side.

* Jordan, *Traité des Substitutions*, § 444, § 504; Dickson, *Linear Groups*, p. 307.

† Jordan, *Traité des Substitutions*, pp. 319–329; Dickson, *Trans. Amer. Math. Soc.*, vol. 5 (1904), p. 126; cf. vol. 6 (1905), p. 48; Mitchell, *ibid.*, vol. 15 (1914), p. 379.

184. Relation between Cubic Surfaces and Plane Quartic Curves.* Using homogeneous coördinates, let

$$f(x) \equiv f(x_1, x_2, x_3, x_4) = 0$$

be the equation of a cubic surface without a singular point, so that the first partial derivatives of f with respect to $x_1, \ldots, x_4$ are not all zero for a set of x's not all zero. The point $(y+\lambda z)$ on the line joining the points $(y) \equiv (y_1, \ldots, y_4)$ and (z) is on the surface if

$$f(y+\lambda z) \equiv f(y) + \lambda L + \tfrac{1}{2}\lambda^2 Q + \lambda^3 f(z) = 0,$$

where, by Taylor's theorem,

$$L = z_1 \frac{\partial f}{\partial y_1} + \ldots + z_4 \frac{\partial f}{\partial y_4}, \quad Q = z_1{}^2 \frac{\partial^2 f}{\partial y_1{}^2} + 2 z_1 z_2 \frac{\partial^2 f}{\partial y_1 \partial y_2} + \ldots$$

Take (y) to be a fixed point P on the surface $f=0$. Then the line joining P and (z) meets the surface in two further points which coincide if

$$(\tfrac{1}{4}Q)^2 = Lf(z). \tag{3}$$

Hence this equation of degree four in $z_1, \ldots, z_4$ represents the tangent cone T_4 to the surface $f=0$ with the vertex P on $f=0$.

Any plane through a straight line l on the cubic surface meets the surface in l and a conic c. Let I and I' be the two intersections of l and c. The tangent to c at I is the limiting position of a line meeting the surface in three points and hence meets the surface at three coincident points. Thus l and this tangent line are principal tangent lines to the cubic surface and their plane is a tangent plane. Hence any plane through l is tangent to the surface at two points I, I', and thus is a bitangent plane.

In particular, the plane through the fixed point P and any line l on the cubic surface is a bitangent plane to the surface and hence also to the tangent cone T_4.

The section of T_4 by an arbitrary plane E is a quartic curve C_4. The intersections of E with the above 27 bitangent planes to T_4 give 27 bitangent lines to C_4.

* Geiser, *Mathematische Annalen*, vol. 1 (1869), p. 129.

But there is an additional bitangent to C_4, making 28 in all. In fact, the plane $L=0$ passes through (y), in view of Euler's theorem (4), § 173. Hence $L=0$ intersects T_4, given by (3), in two pairs of coincident lines, the intersections of $L=0$, $Q=0$. Thus $L=0$ is a bitangent plane to T_4.

Before we can conclude that the general plane quartic curve has exactly 28 bitangents, we must show that, conversely, any given quartic curve C_4 is the intersection of the plane U of the curve with the tangent cone to a suitably chosen cubic surface f at a point P on it.

Let x, y, z be the homogeneous coördinates of a point in the plane U referred to a triangle of reference whose side $z=0$ is

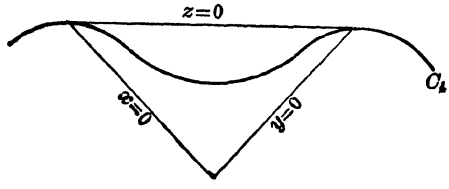


FIG. 17.

one of the bitangents to C_4 and whose sides $x=0$ and $y=0$ are any lines through the points of contact of this bitangent. Then the equation of C_4 reduces to $x^2y^2=0$ when $z=0$ and hence is

$$z\phi - x^2y^2 = 0, \tag{4}$$

where ϕ is a cubic form in x, y, z.

Let P be any point not in the plane U of C_4. As the tetrahedron of reference for homogeneous coördinates x, y, z, u of points in space, take that determined by the plane U and the planes through P and the sides of our triangle of reference. Then the desired cubic surface is

$$f \equiv \phi + 4uxy + 4u^2z = 0. \tag{5}$$

In fact, we shall proceed with this f as we did with the general f and find its tangent cone with the vertex $P=(0, 0, 0, 1)$ in place of (y). Now

$$\frac{\partial f}{\partial x} = \frac{\partial \phi}{\partial x} + 4uy, \quad \frac{\partial f}{\partial y} = \frac{\partial \phi}{\partial y} + 4ux,$$

$$\frac{\partial f}{\partial z} = \frac{\partial \phi}{\partial z} + 4u^2, \quad \frac{\partial f}{\partial u} = 4xy + 8uz.$$

At the point P these derivatives vanish, with the exception of the third, which becomes 4. Hence $L=4z$.

The second partial derivatives vanish at P, except

$$\frac{\partial^2 f}{\partial x\,\partial y}=4, \qquad \frac{\partial^2 f}{\partial z\,\partial u}=8.$$

Hence

$$\tfrac{1}{4}Q=2xy+4zu.$$

Thus the tangent cone T_4 from P is

$$(2xy+4zu)^2=4zf.$$

Deleting the factor 4 and inserting the value of f, we get the equation (4) of C_4 in the plane $u=0$.

EXERCISES

1. In the equation of the tangent plane to $Q=0$ at $(t_1, \ldots, t_4)$, the coefficient of $2z_1$ is

$$t_1\frac{\partial^2 f}{\partial y_1^2}+t_2\frac{\partial^2 f}{\partial y_1\partial y_2}+\ldots+t_4\frac{\partial^2 f}{\partial y_1\partial y_4},$$

which, for $(t)=(y)$, equals

$$\sum_{i=1}^{4} y_i\frac{\partial}{\partial y_i}\left(\frac{\partial f}{\partial y_1}\right)=2\frac{\partial f}{\partial y_1}.$$

Hence the tangent plane to $Q=0$ at (y) is $L=0$.

2. Let l_1, l_2, l_3 be three lines on the cubic surface f which form a triangle and let P be a point of f not on one of the 27 lines. For $i=1, 2, 3$, the plane Pl_i meets f in l_i and a conic c_i. Call r_i and s_i the points of intersection of l_i and c_i; they are on T_4 and f and hence on $Q=0$. Thus the r_i, s_i are six points on the conic c in which $Q=0$ is met by the plane of l_1, l_2, l_3. This plane meets the principal tangents t_1, t_2 to f at P (the lines of intersection of $L=0$, $Q=0$) at two points on c.

Any plane E cuts T_4 in a quartic curve C_4. From l_1, l_2, l_3, we obtain bitangents l'_1, l'_2, l'_3 to C_4 whose points of contact are the projections of r_i, s_i $(i=1, 2, 3)$ from P. From t_1, t_2, we obtain a bitangent τ. The conic c projects into a conic c'. Hence C_4 has the four bitangents l'_1, l'_2, l'_3, τ, whose eight points of contact are on a conic c'.

3. Thus τ and any one of the 45 triangles on f determine a conic c'. But any one of the 28 bitangents can be used in place of τ. Since any one of the conics is related in this way to each of the four bitangents, there

are $28 \cdot 45/4 = 315$ conics each containing the eight points of contact of four bitangents.

4. If (x, y, z) is a singular point with $z_y \neq 0$ on (4), then (5) has the singular point (x, y, z, u), where $2zu + xy = 0$.

185. Steiner Sets of Bitangents to a Quartic Curve. Let two sides, $x=0$ and $y=0$, of a triangle of reference for homogeneous coördinates x, y, z be two bitangents to the quartic curve $f=0$. Then, for $x=0$, f reduces to a perfect square, so that

$$f \equiv x\phi + (rz^2 + syz + ty^2)^2,$$

where $\phi = c + yq$, c being a cubic form in x and z only, and q a quadratic form in x, y, z. Similarly,

$$f_{y=0} = (rz^2 + uxz + vx^2)^2.$$

Hence the latter is identical with $xc + r^2z^4$. Thus

$$f \equiv xyq + (rz^2 + uxz + vx^2)^2 - r^2z^4 + (rz^2 + syz + ty^2)^2$$
$$\equiv xyq_1 + (rz^2 + syz + ty^2 + uxz + vx^2)^2,$$

where

$$q_1 = q - 2(sz + ty)(uz + vx).$$

Hence $f=0$ can be given the form $xyU = V^2$, where U and V are quadratic forms in x, y, z. Conversely, this equation evidently represents a quartic curve having $x=0$ and $y=0$ as bitangents.

If λ is any constant, the equation may be written as follows:

$$xy(U + 2\lambda V + \lambda^2 xy) = (V + \lambda xy)^2.$$

Now $U + 2\lambda V + \lambda^2 xy$ is a quadratic form in x, y, z. Its discriminant (Hessian) is a determinant of the third order whose elements are linear in λ with the exception of two elements which involve λ^2. Hence the discriminant is of the fifth degree in λ. It has no double root in general. For, if

$$U = 2xz, \quad V = ax^2 + by^2 + z^2 + 2dxy + 2exz,$$

the discriminant is

$$-\tfrac{1}{2}\lambda[\lambda^4 + 8d\lambda^3 + 16(d^2 - ab + be^2)\lambda^2 + 16be\lambda + 4b],$$

and the last factor can be identified with any quartic in λ whose constant term is not zero. Hence if our quartic curve is general,

there are five distinct values of λ for which the quadratic form is a product of two linear functions. We thus have *

THEOREM 1. *Given any two bitangents $x=0$, $y=0$ to a general quartic curve, we can determine in exactly five ways a pair of lines $\xi=0$, $\eta=0$, such that the quartic becomes $xy\xi\eta=Q^2$. Then the eight points of contact of the four bitangents x, y, ξ, η lie on the conic $Q=0$.*

Such a set of six pairs of bitangents is called a *Steiner set* (the older term was Steiner group).

Let a, b; c, d; e, f be three pairs of bitangents of the Steiner set determined by a, b. Then the quartic is $abcd=Q^2$ or

$$ab(cd+2\lambda Q+\lambda^2 ab)=(Q+\lambda ab)^2.$$

As above, we can determine λ ($\lambda\neq 0$) so that

$$cd+2\lambda Q+\lambda^2 ab=ef.$$

Eliminating Q between this and $abcd=Q^2$, we get

$$4abcd=\left(\lambda ab+\frac{cd}{\lambda}-\frac{ef}{\lambda}\right)^2.$$

Replacing a, c, e by a/λ, λc, λe, we get

$$4abcd=(ab+cd-ef)^2, \tag{6}$$

which may be written in the symmetrical forms

$$a^2b^2+c^2d^2+e^2f^2=2abcd+2abef+2cdef, \tag{7}$$

$$\sqrt{ab}+\sqrt{cd}+\sqrt{ef}=0. \tag{7'}$$

Transposing the first radical, we derive

$$Acdef=(ef+cd-ab)^2.$$

Hence the points of contact of c, d, e, f are on a conic.

THEOREM 2. *The eight points of contact of any two pairs of bitangents of a Steiner set are on a conic. Thus the same Steiner set is determined by any one of its six pairs.*

Since the $\frac{1}{2}28\cdot 27$ pairs of bitangents lie by sixes in a Steiner set, there are 63 Steiner sets.

* Also by § 180 and Exs. 2, 3 of § 184, with τ and l'_1 as the given bitangents.

Three bitangents are said to form a *syzygetic* or an *asyzygetic triple* according as their six points of contact are or are not on a conic. Thus a, b, c are syzygetic if they belong to a Steiner set and two of them, as a and b, form a pair of that set. We shall prove the important

THEOREM 3. *Three bitangents a, c, e of a Steiner set are asyzygetic if no two of the three form a pair.*

First, a, c, e do not all pass through the same point P. For, if they did, P would be a singular point of the curve (6). We may therefore take them as the sides of a triangle of reference and write

$$b=la+mc+ne, \quad d=pa+qc+re, \quad f=sa+tc+ue.$$

No one of the constants l, q, u is zero. For, if $l=0$, for example, the lines b, c, e would meet at a singular point of the curve (6).

Suppose that the points of contact of a, c, e with (6) lie on a conic $C\equiv ga^2+hc^2+ke^2+\ \ldots\ =0$. Then, by (6) for $a=0$, etc.,

$$C_{a=0}=\lambda\{c(qc+re)-e(tc+ue)\},$$
$$C_{c=0}=\mu\{a(la+ne)-e(sa+ue)\},$$
$$C_{e=0}=\nu\{a(la+mc)-c(pa+qc)\},$$

where λ, μ, ν are constants. Hence

$$h=\lambda q, \qquad g=\mu l, \qquad g=\nu l,$$
$$k=-\lambda u, \quad k=-\mu u, \quad h=-\nu q,$$

whence $\lambda=-\nu$, $\mu=\nu$, $\lambda=\mu$, or $\lambda=\mu=\nu=0$. Thus $g=h=k=0$ and the conic $C=0$ passes through each vertex of our triangle of reference ace. The vertex $a=c=0$ is not on $f=0$, since $u\neq 0$. But the points of contact of a with (6) are given by $cd-ef=0$ and, being on $C=0$, are the vertices lying on a; so that the vertex $a=c=0$ is on $f=0$. The assumption that Theorem 3 is false has thus led to a contradiction.

COROLLARY. A Steiner set a, b; c, d; . . . has in common with the Steiner set a, c; b, d; . . . no bitangent except a, b, c, d.

For, if e is common to them, a, c, e are asyzygetic by the first, and syzygetic by the second set.

186. The Notation of Hesse and Cayley. The 28 bitangents are designated $[ij]\equiv[ji]$, $i, j=1, \ldots, 8$; $i\neq j$. We shall usually omit the brackets. We shall prove that the notation may be assigned to the bitangents in such a way that the 63 Steiner sets are given by

$$(8)\quad ag\,ah,\quad bg\,bh,\quad cg\,ch,\quad dg\,dh,\quad eg\,eh,\quad fg\,fh;$$

$$(9)\quad ab\,cd,\quad ac\,bd,\quad ad\,bc,\quad ef\,gh,\quad eg\,fh,\quad eh\,fg;$$

where $a, \ldots, h$ form a permutation of $1, \ldots, 8$. For examples, see S_5 and S_1 below. Since g and h may be any two of the eight figures, there are $8\cdot 7/2$ or 28 sets of the first type. Since there are 70 ways of selecting four figures out of eight, there are 35 sets of the second type, which is determined by a, b, c, d or by e, f, g, h.

Having in mind also another application (§ 191), we shall proceed abstractly and consider the distribution of 28 symbols into sets of six pairs, in which the arrangement of the pairs and the order of the symbols of a pair are immaterial, and such that

A. Every pair occurs in one and but one set.

B. If α, β, and γ, δ are two pairs of a set, then α, γ, and β, δ are pairs of a set.

C. Two sets α, β; γ, δ; . . . and α, γ; β, δ; . . . have only four symbols in common.

For Steiner sets of bitangents, these properties hold in view of § 185.

As the first set we shall take

S_1. 12 34, 13 24, 14 23, 56 78, 57 68, 58 67.

Rearranging the components of the first and fourth pairs by B, we see that there is a set S_2 with 12 56, 34 78, and a set S_3 with 12 78, 34 56, which, by C, have no further symbol in common with each other or with S_1. Hence they introduce all of the 8+8 symbols not found in S_1. It is at our choice to select the eight to go into S_2; we take

S_2. 12 56, 15 26, 16 25, 34 78, 37 48, 38 47;

S_3. 12 78, 17 28, 18 27, 34 56, 35 46, 36 45.

The set S_4 with 12 57 and 34 68 has no further symbol in common with S_1 and hence contains eight new symbols chosen from those of S_2 and S_3 not in the first or fourth pairs. The two of a pair cannot be two, as 26 and 25, from S_2, since by B they would imply the pair 15 16, contrary to C. Again, if 25 occurs in S_4, 16 does not occur; for, 25 jk and 16 lm would imply a set with 25 16 and jk lm, necessarily S_2, whereas jk, lm are not in S_2, by the last result. Hence after applying a substitution which permutes the eight symbols in S_2 not in the first or fourth pairs, and the eight in S_3 not in the first or fourth pairs, we may take

S_4. 12 57, 15 27, 17 25, 34 68, 36 48, 38 46.

The set S_5 having 12 25 contains, in view of S_2 and S_4, the pairs 56 16 and 57 17, and no further symbols from S_2 and S_4, and therefore six symbols chosen from

13 24, 14 23, 58 67, 18, 35, 45, 28,

the earlier ones being paired for the sake of simplicity of reference. But 57 17, 28 t imply a set with 17 28, 57t, contrary to S_3. Hence 28 is excluded. If we take at least four of the first six symbols, we must pair two of them with each other; these two occur in S_1 and cannot be a pair in S_1, so that we have a contradiction with C. Hence we must take one and but one from each pair 13 24, etc. Since we may interchange the symbols of any one of these three pairs without altering sets S_1–S_4, we may assume that S_5 contains 58, 13, 14. These and sets S_1–S_4 are not altered by

(15 38) (26 47) (18 35) (27 46),

(38 48) (47 37) (46 36) (35 45),

which give rise to any permutation of 18, 35, 45. Hence we may take

S_5. 21 25, 31 35, 41 45, 61 65, 71 75, 81 85.

Without the use of further substitutions to fix the choice of equivalent notations, we can now prove that the 63 sets are

uniquely determined by properties A, B, C and that each is of one of the two types (8), (9).

Using S_2, S_4, S_3, S_5, S_1 in turn, and property B, we get

S_6. 15 48, 26 37, 27 36, 18 45, 14 58, 23 67;

S_7. 15 38, 26 47, 27 46, 18 35, 13 58, 24 67;

S_8. 37 47, 38 48, 36 46, 35 45, 13 14, 23 24.

The set S_9 with 12 68 has, by S_1, S_4, the pair 34 57 and the symbols 16, 26, 47, 37 paired with 28, 18, 35, 45, since not paired with each other in view of S_2. But 16 is not paired with one of the last three in view of S_5. Hence S_9 contains the pair 16 28. A pair 26 35 would imply 47 18 by S_7 and hence 37 45, contrary to S_8. A pair 26 45 would imply 37 18 by S_6 and hence 47 35, contrary to S_7. Hence, by S_6,

S_9. 12 68, 34 57, 16 28, 26 18, 37 45, 47 35.

With 12 16 occurs 56 25 by S_2, S_5, and 68 28 by S_9, while 67, 24, 23 are paired with 27, 46, 36, by S_1. But 67, 23 are paired with 27, 36 by S_6, and 67, 24 with 27, 46 by S_7. Hence

S_{10}. 12 16, 56 25, 68 28, 67 27, 24 46, 23 36.

By S_2, S_4, S_3 we have the first four pairs of

S_{11}. 26 16, 15 25, 17 27, 28 18, 13 23, 24 14,

and four of the symbols 13, 14, 23, 24, 58, 67. Pairs 58 t, 28 18 would imply 58 18, 28 t, contrary to S_5. Pairs 67t, 17 27 would imply 67 27, t17, contrary to S_{10}. Finally, 13 14, 13 24 are excluded by S_8 and S_1. Hence we have S_{11}. By the same steps,

S_{12}. 47 16, 38 25, 17 46, 28 35, 58 23, 67 14;

S_{13}. 37 16, 48 25, 17 36, 28 45, 58 24, 67 13.

By S_7, S_6, S_{11}, S_5 or S_{10}, S_1, we get

S_{14}. 26 27, 47 46, 37 36, 16 17, 56 57, 78 68;

S_{15}. 15 18, 38 35, 48 45, 25 28, 56 68, 78 57.

By S_1 and S_5, the set S_{16} with 12 58 has 34 67 and 25 18 and the symbols 15, 47, 37, 28, 46, 36, since 26, 38, 48, 27 are excluded by S_9, S_{12}, S_{13}, S_{10}, respectively (since 25 18, 26 imply

that 25 is in a set S_9 with 26 18). By S_{15}, 15 is paired with 28 in S_{16}. By S_8 and S_{14}, 47 is not paired with 37 or 46. Hence

S_{16}. 12 58, 34 67, 25 18, 15 28, 47 36, 37 46.

In exactly the same manner, we get

S_{17}. 12 13, 34 24, 25 35, 38 28, 26 36, 37 27;

S_{18}. 12 14, 34 23, 25 45, 48 28, 26 46, 47 27.

By S_1, S_{10}, S_{16} we get the first three pairs of

S_{19}. 12 67, 34 58, 16 27, 17 26, 38 45, 48 35,

and see that the further symbols are those in the last three pairs. By S_4, 17 is not paired with 38 or 48, and by S_3 not with 35 or 45. Hence 17 is paired with 26. By S_8 and S_{15}, 38 is not paired with 48 or 35 and hence is paired with 45.

Similarly, using S_1, S_{10}, S_{12}, S_{17}, we get

S_{20}. 12 24, 34 13, 16 46, 47 17, 15 45, 48 18,

except as to the pairing of the last four symbols, which is determined by S_6 and S_{15}. By S_1, S_{10}, S_{13}, S_{18} (and S_7, S_{15} for the pairing the final four symbols), we get

S_{21}. 12 23, 34 14, 16 36, 37 17, 18 38, 15 35.

We may now determine uniquely the remaining 42 sets from S_1–S_{21} by use of the simple property B. Thus by S_2, S_4, S_{21} and S_{16}, S_{20} or S_{17}, S_6, we get

S_{22}. 12 15, 56 26, 57 27, 58 28, 23 35, 24 45;

S_{23}. 12 38, 56 47, 57 46, 13 28, 23 18, 67 45.

The remaining sets may be derived independently of each other from $S_1, \ldots, S_{23}$ by use of property B; they need not be tabulated here since they, like the earlier sets, are of one of the two types (8), (9).

THEOREM 4. *There is a distribution of* 28 *symbols into* 63 *sets of* 6 *pairs such that the arrangement of the pairs in a set is immaterial and such that properties* A, B, C *hold. Any such distribution can be derived from that given by* (8) *and* (9) *by a substitution on the* 28 *symbols.*

Hence the notation ij may be assigned to the bitangents in such a way that the Steiner sets are given by (8) and (9).

Since the sets S_1, S_2, S_3 together contain all the bitangents any bitangent syzygetic with 12 and 34 occurs in S_1 (Theorem 3, § 185). Similarly, every syzygetic triple is composed of three bitangents of a Steiner set, two of which form a pair. The converse was noted before Theorem 3. Any syzygetic triple of a Steiner set (8) is of the type *ag, ah, bg*; any one of a Steiner set (9) is of type *ab, cd, ac* or *ab, cd, ef*. The latter is represented by |||, i.e., by three segments whose six end points are all distinct. The former is represented by the broken line $\sqcap$ composed of the segments *ba, ac, cd*; and the same representation is given to *ha, ag, gb*.

THEOREM 5. *A triple is syzygetic if and only if it is of type* ||| *or type* $\sqcap$. *Hence a triple is asyzygetic if and only if it is of one of the three types* Δ, $\vee|$, $\diagdown|\diagup$.

Seven bitangents are said to form an ***Aronhold set*** if every triple contained in it is asyzygetic. An example is

(10) 18, 28, 38, 48, 58, 68, 78,

each triple of which is of type $\diagdown|\diagup$ and hence asyzygetic.

An Aronhold set is represented by a figure formed by seven segments with at most eight end points. It is not composed of more than two separate parts; for, if it be, it would contain three syzygetic bitangents |||. If a separate part has two or more points from each of which at least two segments radiate, that part is of type Δ, since otherwise it would contain a triple of type $\sqcap$. Hence each separate part is a Δ or a fan F_n consisting of n segments radiating from one vertex.

First, let there be a single part. Then the set is a fan F_7. Its vertex may be any one of the points 1, . . . , 8, so that there are eight such Aronhold sets. That with the vertex 8 is given by (10).

Finally, let there be two parts. If they are fans F_r and F_s, the number of segments $r+s$ is 7, and hence the number of points is $r+1+s+1=9$, whereas at most 8 points occur. Hence one part is a Δ and the other a fan F_4; for example,

(11) 12, 23, 31, 48, 58, 68, 78.

The triangle can be chosen in 56 ways (the number of ways of selecting three points out of eight), and then the vertex of the fan is any one of the remaining five points. Hence (11) is one of 280 such sets.

THEOREM 6. *There are exactly* 288 *Aronhold sets. Each is a fan* F_7 *or is composed of a triangle and a fan* F_4.

187. Group of an Equation for the 28 Bitangents. Take as the x-axis of Cartesian coördinates a line not through the intersection of any two bitangents. Then the bitangents cross the x-axis at 28 distinct points $(\xi, 0)$, and each bitangent $y=m(x-\xi)$ is uniquely determined by its ξ. If the equation to the quartic curve is $F(x, y)=0$, then $F[x, m(x-\xi)]$ must be a perfect square in x. From the resulting two conditions on m and ξ, we obtain m as a rational function of ξ and the coefficients of $F(x, y)$, since there is a single m for each ξ; and hence obtain an equation $E(\xi)=0$ of degree 28 whose coefficients are in the domain R of the rational functions of the ratios of the coefficients of F. Let G be the group of this equation for the domain R.

Let $p=0$, $q=0$ be the two bitangents determined by the roots ξ_1, ξ_2. Then (§ 185) there are two conics $U=0$, $V=0$, with coefficients in the domain (R, ξ_1, ξ_2), such that $F=pqU-V^2$. As there proved, there are five values of λ for which

$$U+2\lambda V+\lambda^2 pq=0$$

is a pair of lines. In the product

$$P=\Pi(U+2\lambda V+\lambda^2 pq),$$

extended over these five values of λ, the coefficients are in the domain (R, ξ_1, ξ_2). Now P is a product of ten linear functions of x and y, which represent ten bitangents forming with p and q a Steiner set. Setting $y=0$ in $P=0$, we obtain an equation $f(\xi_1, \xi_2, x)=0$, with coefficients in R, whose ten roots x are the ξ's of these ten bitangents. Thus $f(\xi_1, \xi_2, \xi_3)$ is zero when ξ_1, ξ_2, ξ_3 are roots of $E(\xi)=0$ corresponding to a syzygetic triple of bitangents and not zero for three roots corresponding to an asyzygetic triple. In the first case, we shall call the roots syzygetic; in the second case, aszygetic.

If a substitution S of G replaces three syzygetic roots ξ_1, ξ_2, ξ_3 by the roots ξ'_1, ξ'_2, ξ'_3, then, by property B of § 149, $f(\xi'_1, \xi'_2, \xi'_3)=0$ and ξ'_1, ξ'_2, ξ'_3 are syzygetic. The converse is shown to be true by use of S^{-1}.

THEOREM 7. *Every substitution of G replaces syzygetic roots by syzygetic roots and replaces asyzygetic roots by asyzygetic roots.*

COROLLARY. Every substitution of G replaces any Steiner set by a Steiner set and every Aronhold set by an Aronhold set.

We proceed to exhibit a fixed group Γ which contains G as a subgroup no matter how we vary the coefficients of the quartic equation and hence vary G. For the extreme case in which the coefficients are independent variables, we shall later see that G is identical with Γ. But in every case we shall in the meantime be able to determine the possible number of real bitangents from a knowledge of the substitutions of period 2 in Γ.

The group G may contain a substitution S which interchanges the roots 18 and 28 of the Aronhold set (10) and leaves unaltered the remaining roots $i8$, $i=3, \ldots, 7$. If so, S replaces the Steiner set $1a\ 8a (a=2, \ldots, 7)$ by a Steiner set Σ in which the figure 8 occurs six times and hence is of type (8) with $h=8$ (since we may permute g and h). Since 8 is paired in Σ with any figure except 2 and 8, we have $g=2$. Hence Σ is $2a\ 8a$ $(a=1, 3, \ldots, 7)$, so that S replaces $1a$ by $2a$ if $a>2$, and leaves 12 unaltered. Next, S replaces Σ by a Steiner set of type (8) with $h=8$ and containing 21 82, and hence with $g=1$, so that the new set is 21 82, $1a\ 8a$ $(a=3, \ldots, 7)$. Thus S replaces $2a$ by $1a$ if $a>2$. Finally, S replaces the Steiner set 31 81, 32 82, $3a\ 8a$ $(a=4, \ldots, 7)$ by one with 32 82, 31 81, and hence with $3a\ 8a$, so that S leaves unaltered $3a$ $(a=4, \ldots, 7)$. Similarly, S leaves unaltered ba $(b,\ a=3, \ldots, 7;\ b\neq a)$. Thus S is the product of the transpositions $(1j, 2j), j=3, \ldots, 8$, and is therefore the substitution on the 28 symbols $[ij]$ which is induced by the transposition of the two indices 1 and 2.

We obtain in this way 7! substitutions which leave unaltered the Aronhold set (10), merely permuting its seven symbols.

The group G may contain a substitution S which replaces the symbols (10) by the corresponding symbols of the Aronhold set

$$17, \quad 27, \quad 37, \quad 47, \quad 57, \quad 67, \quad 87.$$

If so, S replaces the Steiner set $ia\ 8a$ $(a=1, \ldots, 7;\ a \neq i)$, where i is a fixed integer $\leqq 6$, by a Steiner set of type (8) with $h=7$, $g=i$, since 7 is paired with every integer except 7 and i. Hence the new set is $ia\ 7a$ $(a=1, \ldots, 6, 8;\ a \neq i)$. Hence S leaves fixed ia $(a \leqq 6)$ and replaces $i7$ by $i8$. Thus S is induced by the transposition of the indices 7, 8.

We now have 8! substitutions which permute the eight Aronhold sets typified by fans F_7 with vertices $1, \ldots, 8$. These 8! substitutions on the 28 symbols are those induced by the 8! substitutions on the indices $1, \ldots, 8$, and form a group E.

The group G may contain the substitution

$$P_{1238} = \begin{pmatrix} 18 & 28 & 38 & 48 & 58 & 68 & 78 & \ldots \\ 23 & 13 & 12 & 48 & 58 & 68 & 78 & \ldots \end{pmatrix},$$

which replaces the Aronhold set (10) by the Aronhold set (11) composed of the triangle with vertices 1, 2, 3 and a fan F_4 with the vertex 8. Since P replaces the Steiner set $1a\ 8a$ $(a=2, \ldots, 7)$ by one of type (8) with $h=8$ and having the symbols 13, 12 and hence with $g=1$, P replaces 12 by 38, 13 by 28, and leaves unaltered $1a (a=4, \ldots, 7)$. Next P replaces the Steiner set $8a\ 4a$ $(a=1, 2, 3, 5, 6, 7)$ by that determined by 23 14 and hence leaves 24 and 34 unaltered and replaces 45 by 67, 46 by 57, 47 by 56. In this way we find that

$$P_{1238} = (12\ 38)\ (13\ 28)\ (23\ 18)\ (45\ 67)\ (46\ 57)\ (47\ 56),$$

which may therefore be designated also by P_{4567}.

Similarly, or by symmetry, we obtain the substitution

$$P_{\alpha_1\alpha_2\alpha_3\alpha_4} = P_{\beta_1\beta_2\beta_3\beta_4} = (\alpha_1\alpha_2\ \ \alpha_3\alpha_4)(\alpha_1\alpha_3\ \ \alpha_2\alpha_4)$$
$$(\alpha_1\alpha_4\ \ \alpha_2\alpha_3)(\beta_1\beta_2\ \ \beta_3\beta_4)(\beta_1\beta_3\ \ \beta_2\beta_4)(\beta_1\beta_4\ \ \beta_2\beta_3),$$

where $\alpha_1, \ldots, \beta_4$ form a permutation of $1, \ldots, 8$. There are 35 such substitutions, since there are 70 combinations of 8 things 4 at a time.

We thus have a group, of order $288 \cdot 7! = 36 \cdot 8!$,

$$\Gamma = E + \sum EP_{\alpha_1\alpha_2\alpha_3\alpha_4}.$$

188. Number of Real Bitangents. We shall employ the

LEMMA.* *If an algebraic equation with distinct roots and with coefficients in a real domain R has exactly ν pairs of conjugate imaginary roots x_{2j-1}, x_{2j} $(j = 1, \ldots, \nu)$, its group for R contains the substitution*

$$S = (x_1x_2) \ldots (x_{2j-1}x_{2j}) \ldots (x_{2\nu-1}x_{2\nu}).$$

If we apply the Corollary in § 149 to the group $\{1, S\}$, we see that our Lemma is proved if we show that S leaves numerically unaltered every rational function $\phi(x_1, \ldots, x_n)$ of the roots such that ϕ has its coefficients in R and equals a quantity in R. Since the numerical value of ϕ is real, ϕ remains numerically unaltered when $i = \sqrt{-1}$ is changed into $-i$ in each imaginary root; but the resulting change in ϕ is the same as if we had applied the substitution S.

COROLLARY. *Either the roots are all real or else the number of real roots equals the number of letters unaltered by one of the substitutions of period 2 of the group for R of the equation.*

We shall prove that every substitution S of period 2 of the group Γ of § 187 leaves fixed exactly 4, 8 or 16 of the 28 symbols. First, if S is in the subgroup E, it is induced by 1, 2, 3 or 4 transpositions on the 8 figures and hence leaves unaltered † 16, 8, 4 or 4 symbols, respectively. Second, $S = P_{1234}$ leaves 16 symbols unaltered. Third, let $S = \sigma^{-1}P_{1234}$, where σ is not the identity and is induced by the substitution which replaces $1, \ldots, 8$ by $\alpha_1, \ldots, \alpha_8$. Then

$$S = S^{-1} = P_{1234}\ \sigma = \sigma P_{\alpha_1\alpha_2\alpha_3\alpha_4}, \quad P_{1234} = \sigma S = \sigma^2 P_{\alpha_1\alpha_3\alpha_2\alpha_4}.$$

Hence (end of § 187) σ^2 is the identity and $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ form a permutation of either 1, 2, 3, 4 or of 5, 6, 7, 8. In the latter case, σ is induced by

$$(1\ \alpha_1)\ (2\ \alpha_2)\ (3\ \alpha_3)\ (4\ \alpha_4),$$

* A less precise theorem limited to irreducible equations was given by E. Maillet, *Annales de Toulouse*, ser. 2, vol. 6 (1904), p. 280. The present Lemma was given by Dickson, *Annals of Mathematics*, ser. 2, vol. 6 (1905), p. 144.

† The verification can be made for the substitutions used below.

so that the substitution induced by

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ 5 & 6 & 7 & 8 \end{pmatrix}$$

transforms $S = \sigma P_{1234}$ into that induced by $(15)(26)(37)(48)P_{1234}$, which leaves unaltered only the symbols 15, 26, 37, 48. In the former case, $\alpha_1, \ldots, \alpha_4$ is a permutation of 1, 2, 3, 4. If this permutation is the identity, σ permutes only 5, 6, 7, 8, and, after applying a transformation not altering P_{1234}, we may take $\sigma = (78)$ or $(56)(78)$, whence S leaves 8 or 4 symbols unaltered. In the contrary case, we may assume that σ is the product of (12) or (12)(34) by a substitution σ_1 on 5, 6, 7, 8. If σ_1 is the identity, we transform by (18)(27)(36)(45) and are led to the preceding case. There remain the cases

$$\sigma = (12)(56), \quad (12)(56)(78), \quad (12)(34)(56)(78),$$

for which S leaves unaltered 4, 4 or 8 symbols, and the case (12)(34)(56), which is equivalent to the second case.

THEOREM 8. *There are exactly* 4, 8, 16 *or* 28 *real bitangents to a real quartic curve without singular points.**

189. Real Lines on a Cubic Surface. If we adjoin to the domain one root of the equation upon which depend the 28 bitangents to a quartic curve, the group reduces to a subgroup simply isomorphic † with the group of the equation upon which depend the 27 straight lines on the related cubic surface (§ 184). The substitutions of period 2 of Γ which leave one symbol fixed leave unaltered 3, 7 or 15 of the remaining 27 symbols.

THEOREM 9. *There are exactly* 3, 7, 15 *or* 27 *real straight lines on a general real cubic surface.*‡

* It is then not of the type excluded in the proof of Theorem 1. The group discussion by Maillet (*l.c.*, p. 323) is incomplete, as it fails to exclude the case of no real bitangents. Weber, *Algebra*, 2d ed., vol. 2 (1899), devotes pages 458–465 to a proof that no other than these four cases can occur, and three pages to a proof that all four cases actually occur. For geometrical treatments see Zeuthen, *Mathematicshe Annalen*, vol. 7 (1874), p. 411; Salmon's *Higher Plane Curves*, p. 220.

† Note that the quotient of the order $288 \cdot 7!$ of Γ in § 187 by 28 is the order of the group Γ in § 183.

‡ That these four, but no other, cases actually occur was shown by *Schläfli*, *Quarterly Journal of Mathematics*, vol. 2 (1858), p. 117.

190. Actual Group G for the 28 Bitangents. We have seen that G is a subgroup of the known group Γ and have applied this fact to the study of the reality of the bitangents. It is a proper conclusion of this investigation to give the proof that G is identical with Γ in case the coefficients of the quartic equation are independent variables. For this purpose we need the following Lemmas, the proof of which differs from that given by Weber * mainly in a slight change of notation made in the interests of symmetry, and in the elaboration of the proof of Lemma 2.

LEMMA 1. *Given the seven bitangents of any Aronhold set of bitangents to a quartic curve without singular points, we can determine rationally the remaining bitangents.*

Let (10) be the given Aronhold set and write x_i for $[i8]$, and x_{ij} for $[ij]$, $i<8, j<8$. We are to express the x_{ij} rationally in terms of $x_1, \ldots, x_7$. Since x_1x_{23}, x_2x_{13}, x_3x_{12} are pairs 18 23, 28 13, 38 12 of a Steiner set of type (9), we may multiply x_{23}, etc., by constants as in the derivation of (6), and obtain the equation $f=0$ of the curve in a form such that

$$f=4x_2x_{13}x_3x_{12}-u^2=4x_3x_{12}x_1x_{23}-v^2 \tag{12}$$
$$=4x_1x_{23}x_2x_{13}-w^2,$$

where

$$u=-x_1x_{23}+x_2x_{13}+x_3x_{12},\quad v=x_1x_{23}-x_2x_{13}+x_3x_{12}, \tag{13}$$
$$w=x_1x_{23}+x_2x_{13}-x_3x_{12}.$$

Similarly, x_2x_{12} and x_4x_{14} are pairs of a Steiner set (8) with $g=8$, $h=1$, and

$$f=4x_2x_{12}x_4x_{14}-q^2, \tag{12'}$$

where q is a quadratic form. Then by (12_1),

$$4x_2x_{12}(x_3x_{13}-x_4x_{14})\equiv(u-q)(u+q).$$

If one of the factors on the right were divisible by x_2 and the other by x_{12}, the intersection of x_2 and x_{12} would be on $u=0$

* *Algebra*, ed. 2, vol. 2, 1899, p. 442. Down to this point in our exposition of the theory, we have made only an indirect use of Weber's treatment.

and hence be a singular point of $f=0$ by (12_1). Hence, after changing the sign of q if necessary, we may assume that

$$u-q=2\lambda_1 x_2 x_{12},$$

where λ_1 is a constant not zero. Then

$$u+q=2(x_3x_{13}-x_4x_{14})/\lambda_1.$$

Adding and replacing u by its expression (13), we get

$$x_4x_{14}=x_3x_{13}+\lambda_1{}^2x_2x_{12}-\lambda_1(-x_1x_{23}+x_2x_{13}+x_3x_{12}). \tag{14}$$

In the same manner (or by permuting 1, 2, 3 cyclically), we get

$$\begin{cases} x_4x_{24}=x_1x_{12}+\lambda_2{}^2x_3x_{23}-\lambda_2(x_1x_{23}-x_2x_{13}+x_3x_{12}), \\ x_4x_{34}=x_2x_{23}+\lambda_3{}^2x_1x_{13}-\lambda_3(x_1x_{23}+x_2x_{13}-x_3x_{12}), \end{cases} \tag{14'}$$

where λ_2 and λ_3 are new constants not zero.

To determine the λ's, divide equations (14′) by λ_2 and λ_3, respectively, and then add. We get the identity

$$x_4\left(\frac{x_{24}}{\lambda_2}+\frac{x_{34}}{\lambda_3}\right)=x_1\left(\frac{x_{12}}{\lambda_2}+\lambda_3x_{13}-2x_{23}\right)+x_{23}l, \tag{15}$$

where $l=\lambda_2x_3+x_2/\lambda_3$. Since x_4, x_1, x_{23} occur in the Steiner set (8) with $g=8$, $h=3$, and no two are paired, they are not concurrent (proof of Theorem 3); similarly, no three of the x_i concur. Hence l, x_4, x_1 are concurrent, so that x_4 is a linear function of l and x_1. But

$$x_4=a_1x_1+a_2x_2+a_3x_3, \tag{16}$$

where the a's are known constants each not zero. This sum must vanish for $l=0$, $x_1=0$, whence $a_3=a_2\lambda_2\lambda_3$. Thus

$$\lambda_2=h_1a_3, \quad \frac{1}{\lambda_3}=h_1a_2,$$

where h_1 is a new constant. Then, by (15) and (16),

$$h_1x_4\left(\frac{x_{24}}{\lambda_2}+\frac{x_{34}}{\lambda_3}-h_1x_{23}\right)=x_1\left[\frac{x_{13}}{a_2}+\frac{x_{12}}{a_3}-h_1(2+a_1h_1)x_{23}\right].$$

Hence, if k_1 is a new constant,

$$\frac{x_{24}}{\lambda_2}+\frac{x_{34}}{\lambda_3}-h_1x_{23}=\frac{k_1}{h_1}x_1, \tag{17}$$

$$k_1x_4=\frac{x_{13}}{a_2}+\frac{x_{12}}{a_3}-h_1(2+a_1h_1)x_{23}.$$

Permuting 1, 2, 3 cyclically, we get

$$k_2x_4=\frac{x_{12}}{a_3}+\frac{x_{23}}{a_1}-h_2(2+a_2h_2)x_{13},$$

$$k_3x_4=\frac{x_{23}}{a_1}+\frac{x_{13}}{a_2}-h_3(2+a_3h_3)x_{12}.$$

Since the three expressions for x_4 must be identical, the three k's are equal and will be designated by k. Also,

$$0=1+a_ih_i(2+a_ih_i)=(1+a_ih_i)^2 \qquad (i=1, 2, 3),$$

so that $h_i=-1/a_i$. Thus

$$kx_4=\frac{x_{23}}{a_1}+\frac{x_{13}}{a_2}+\frac{x_{12}}{a_3}. \tag{18}$$

Since λ_1 is derived from λ_3 by permuting 1, 2, 3 cyclically, we have

$$\lambda_1=\frac{-a_2}{a_3}, \quad \lambda_2=\frac{-a_3}{a_1}, \quad \lambda_3=\frac{-a_1}{a_2}.$$

Permuting 1, 2, 3 cyclically in (17), we get

$$\frac{x_{24}}{\lambda_2}+\frac{x_{34}}{\lambda_3}=\frac{-x_{23}}{a_1}-ka_1x_1, \tag{19'}$$

$$\frac{x_{34}}{\lambda_3}+\frac{x_{14}}{\lambda_1}=\frac{-x_{13}}{a_2}-ka_2x_2, \quad \frac{x_{14}}{\lambda_1}+\frac{x_{24}}{\lambda_2}=\frac{-x_{12}}{a_3}-ka_3x_3.$$

Adding and employing (18) and (16), we get

$$\frac{x_{14}}{\lambda_1}+\frac{x_{24}}{\lambda_2}+\frac{x_{34}}{\lambda_3}=-k(a_1x_1+a_2x_2+a_3x_3).$$

Hence

$$\frac{x_{14}}{\lambda_1}=\frac{x_{23}}{a_1}-k(a_2x_2+a_3x_3), \quad \frac{x_{24}}{\lambda_2}=\frac{x_{13}}{a_2}-k(a_1x_1+a_3x_3), \tag{19}$$

$$\frac{x_{34}}{\lambda_3}=\frac{x_{12}}{a_3}-k(a_1x_1+a_2x_2).$$

We may employ x_5, x_6 or x_7 in place of x_4 in the preceding discussion. Instead of (16), we use

$$x_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 \qquad (i = 4, 5, 6, 7), \tag{20}$$

where the a_{ij} are known constants. Corresponding to (18) are

$$k_i(a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3) = \frac{x_{23}}{a_{i1}} + \frac{x_{13}}{a_{i2}} + \frac{x_{12}}{a_{i3}} \quad (i = 4, 5, 6, 7), \tag{21}$$

in which $k_4, \ldots, k_7$ are constants to be determined. If the determinant

$$\begin{vmatrix} \frac{1}{a_{i1}} & \frac{1}{a_{i2}} & \frac{1}{a_{i3}} \end{vmatrix}$$

were zero, where for example $i = 4, 5, 6$, then the corresponding x_i would be linearly dependent, whereas they were shown not to concur. Hence the ratios of four numbers $l_4, \ldots, l_7$ are determined by

$$\frac{l_4}{a_{4j}} + \frac{l_5}{a_{5j}} + \frac{l_6}{a_{6j}} + \frac{l_7}{a_{7j}} = 0 \qquad (j = 1, 2, 3). \tag{22}$$

Multiplying the ith equation (21) by l_i and summing, we see that the new right member is identically zero, so that

$$\sum_{i=4}^{7} k_i l_i a_{i1} = 0, \quad \sum_{i=4}^{7} k_i l_i a_{i2} = 0, \quad \sum_{i=4}^{7} k_i l_i a_{i3} = 0. \tag{23}$$

These equations determine the ratios of the k's, one of which is arbitrary and may be taken to be unity. Then (21) determine x_{23}, x_{13}, x_{12}, while (19) and the corresponding formulas determine x_{1i}, x_{2i}, x_{3i} $(i = 4, \ldots, 7)$ rationally. We now have all the bitangents except 45, 46, 47, 56, 57, 67. But if we had used x_5, x_6, x_7 in place of x_1, x_2, x_3, we would have obtained rationally all except 12, 13, 14, 23, 24, 34. The two steps together give all the bitangents x_{ij}.

LEMMA 2. *If we choose seven straight lines in a plane in a sufficiently general manner, we can determine rationally the equation of a quartic curve without singular points for which the seven chosen lines form an Aronhold set of bitangents.*

For proof, we have only to reverse the argument made for Lemma 1, now taking the a_{ij} as independent variables. Then x_{23}, x_{13}, x_{12} are determined rationally in terms of the a_{ij} by means of (21)–(23), and then x_4, x_5, x_6, x_7, x_{4i}, x_{5i}, x_{6i}, x_{7i} are determined rationally by means of (20), (19) and the analogous equations mentioned above.

Substituting the expressions for x_{23}, x_{13}, x_{12} into (12_1) and (13), we obtain the equation $f=0$ of a quartic curve, whose coefficients are rational functions of the a_{ij}. Its discriminant is not identically zero, since we saw in the proof of Lemma 1 that we can deduce equations (21)–(23) from the equation of a quartic curve without singular points.

For $i=4$, (20) and (21) give (16) and (18). From these and (19) we get (19′). Substitute the left member of the latter into (15). In the resulting term $-x_4x_{23}/a_1$, replace x_4 by its value (16); in the term $-ka_1x_1x_4$, replace kx_4 by its value (18). We obtain the right member of (15). Hence we have (15) and the equations derived from it by permuting 1, 2, 3 cyclically. From the relation between (14′) and (15), it follows at once that (14) and (14′) hold. Define q by the equation preceding (14). Then $u-q$ has the value indicated, so that (12′) follows from the equation written below it. The equations obtained from (12′) by replacing 4 by 5, 6, 7 follow similarly from (20), (21) and the equations of type (19). Hence x_4, x_5, x_6, x_7 form with x_1, x_2, x_3 an Aronhold set.

THEOREM 10. *If the ratios of the* 15 *coefficients of a ternary quartic form f are independent variables and if R is the domain of the rational functions of these* 14 *ratios with rational coefficients, the group G for R of the equation $E(\xi)=0$ upon which depends the determination of the* 28 *bitangents to $f=0$ is the group* Γ *of* § 187.

It was proved in § 187 that every substitution of G is in Γ. To prove the converse, it is sufficient, in view of the Corollary in § 149, to show that every rational relation with coefficients in R between the roots of $E(\xi)=0$ is preserved by each substitution of Γ. To this end, let $\xi_1, \ldots, \xi_7$ be the roots corresponding to the bitangents 18, . . . , 78. Since the latter

form an Aronhold set, the remaining 21 roots $\xi_{ij}=\xi_{ji}$ $(i, j=1, \ldots, 7;\ i\neq j)$ are rational functions of $\xi_1, \ldots, \xi_7$ with coefficients in R (Lemma 1). If $c_1, \ldots, c_{14}$ are the ratios of the coefficients of f, any rational relation between the roots with coefficients in R is of the type

$$\Phi(\xi_1, \ldots, \xi_7, \xi_{12}, \ldots, \xi_{67}, c_1, \ldots, c_{14})=0,$$

where Φ is a rational function of its arguments with rational coefficients. First, we replace the ξ_{ij} by their rational expressions in terms of the ξ_k, c_k. Next, we replace each c_k by its rational expression (Lemma 2) in terms of the coefficients ξ_i, m_i $(i=1, \ldots, 7)$ of the seven bitangents of our Aronhold set. But these 14 quantities can be chosen at will. Hence after our replacements, relation $\Phi=0$ becomes an identity in the ξ_i, m_i. Thus $\Phi=0$ remains true if we substitute for $\xi_1, \ldots, \xi_7$ the seven roots in any order of any Aronhold set, provided of course we replace each ξ_{ij} by the root which arises from it by our substitution. But Γ is the group of all such substitutions. Hence $G=\Gamma$.

COROLLARY. The adjunction of one root of a certain equation of degree 36 reduces the group of the equation for the 28 bitangents to the group of the general equation of degree 8.

In fact, the subgroup E(§ 187) of Γ is simply isomorphic with the symmetric group on 8 letters and is of index 36 under Γ.

Since we know the generators of Γ and the representation of each substitution of Γ in terms of the generators (end of § 187), we can prove by a straightforward argument that Γ is a simple group (Weber, *l.c.*, pp. 454–6).

191. Symmetrical Notation for the Bitangents to a Quartic Curve. The separation of the Steiner sets into two types and likewise for the Aronhold sets was due to the lack of symmetry in the notation of Hesse and Cayley and not to a geometrical difference. A perfectly symmetrical notation was discovered *

* Riemann, *Werke*, 1876, p. 471. Weber, *Theorie der Abelschen Functionen vom Geschlecht* 3, Berlin, 1876, p. 82. Clebsch, "Ueber die Anwendung der Abelschen Functionen in der Geometrie," *Crelle*, vol. 63 (1864), p. 211, who used the notation $(x_1, x_2, x_3;\ y_1, y_2, y_3)$. Appell and Goursat, *Théorie des Fonctions Algébriques*, 1895, p. 511.

in connection with the theory of theta functions of odd characteristics

$$(x_1y_1 \quad x_2y_2 \quad x_3y_3), \tag{24}$$

where each x_i and y_i is 0 or 1, and

$$x_1y_1+x_2y_2+x_3y_3\equiv 1 \pmod 2. \tag{25}$$

If $x_3\equiv 1 \pmod 2$, the congruence determines y_3 in terms of x_1, y_1, x_2, y_2, so that there are 2^4 such sets of solutions. If $x_3\equiv 0 \pmod 2$,

$$x_1y_1+x_2y_2\equiv 1 \pmod 2 \tag{26}$$

has the four sets of solutions $x_2\equiv 1$, $y_2\equiv 1-x_1y_1$, and the two sets $x_2\equiv 0$, $y_2\equiv 0$ or 1, $x_1\equiv y_1\equiv 1$; since $y_3=0$ or 1, we obtain 2×6 sets of solutions of (25) with $x_3\equiv 0$. Hence there are 28 symbols (24).

THEOREM 11. *The* 28 *bitangents to a general quartic curve can be designated by the* 28 *symbols* (24) *in such a way that the* 8 *points of contact of the four bitangents*

$$A=(a_1b_1 \quad a_2b_2 \quad a_3b_3), \quad B=(c_1d_1 \quad c_2d_2 \quad c_3d_3),$$

$$C=(x_1y_1 \quad x_2y_2 \quad x_3y_3), \quad D=(z_1w_1 \quad z_2w_2 \quad z_3w_3)$$

are on a conic if and only if

$$a_i+c_i+x_i+z_i\equiv 0, \quad b_i+d_i+y_i+w_i\equiv 0 \ (mod\ 2) \quad (i=1,2,3). \tag{27}$$

This theorem, which leads to a symmetrical notation for the bitangents and presents the problem of the bitangents in a form suitable for extensive generalizations (§ 192), was deduced in the papers last cited from the theory of abelian functions. We shall here give a very elementary proof,* depending upon two lemmas.

LEMMA 3. *If A and B are any two distinct symbols* (24), *there exist exactly five pairs of symbols C_0, D_0; . . . ; C_4, D_4, distinct from each other and from A and B, such that the sums of corresponding elements of the symbols A, B, C_j, D_j are all even, as in Theorem* 11.

* Dickson, *Bull. Amer. Math. Soc.*, vol. 20 (1914), pp. 463–4.

This lemma implies that the sums of corresponding elements of C_0, D_0, C_j, D_j, are all even. Thus the set of six pairs determined by A and B is identical with the set of six pairs determined by C_0, D_0. For such sets of six pairs, properties (A) and (B) of § 186 therefore hold. The fact that also property (C) holds and hence also Theorem 11, may be stated as

LEMMA 4. *The sets* AB, CD, . . . *and* AC, BD, . . . *have no further symbol in common.*

In the proof of these two lemmas, it suffices to consider symbols A, B having $b_3 \not\equiv d_3 \pmod 2$, and hence (after interchanging A and B if necessary) with $b_3 \equiv 0$, $d_3 \equiv 1$. For, if $b_3 \equiv d_3$, but $b_1 \not\equiv d_1$, the symbols $A' = (a_3 b_3 \; a_2 b_2 \; a_1 b_1)$ and B', derived from A and B by interchanging the first and third pairs of elements, lead by the proof below to just five pairs C'_j, D'_j, from which we derive the required C_j, D_j, by interchanging the first and third pairs of elements. Next, if each $b_i \equiv d_i$, then $a_1 \not\equiv c_1$, for example, and we proceed as before with $A^* = (b_1 a_1 \; b_2 a_2 \; b_3 a_3)$, $B^* = (d_1 c_1 \; d_2 c_2 \; d_3 c_3)$.

To prove Lemma 3, we may therefore assume that $b_3 \equiv 0$, $d_3 \equiv 1$. If C and D are symbols for which congruences (27) hold, then $y_3 + w_3 + 1 \equiv 0 \pmod 2$, so that either $y_3 \equiv 0$ or $w_3 \equiv 0$. Since the mutual order of C and D is immaterial, we may set $y_3 \equiv 0$, whence $w_3 \equiv 1 \pmod 2$. The conditions that C and D shall satisfy the condition (25) for a symbol are (26) and $z_1 w_1 + z_2 w_2 + z_3 \equiv 1$. By (27), the latter becomes

$$(28) \qquad \sum_{i=1}^{2} (a_i + c_i + x_i)(b_i + d_i + y_i) + a_3 + c_3 + x_3 \equiv 1 \pmod 2,$$

which determines x_3 in terms of x_1, y_1, x_2, y_2. There are six sets of values of the latter which satisfy (26). One of these sets is $x_i \equiv a_i$, $y_i \equiv b_i$ $(i = 1, 2)$, whence $x_3 \equiv a_3$, $C = A$ (and hence $D = B$), since

$$(29) \qquad c_3 \equiv 1 + c_1 d_1 + c_2 d_2 \pmod 2.$$

Since this set is to be excluded, Lemma 3 is proved. For use in the proof of Lemma 4, we shall exhibit the five pairs C_j, D_j.

In view of $a_1 b_1 + a_2 b_2 \equiv 1$, b_1 and b_2 are not both even.

After interchanging the first and second pairs of elements in all of our symbols, if necessary, we may set $b_2 \equiv 1$. Then we may set

$$A = (a \;\; b \;\; ab+1 \;\; 1 \;\; e \;\; 0), \quad B = (c_1 d_1 \;\; c_2 d_2 \;\; c_3 1),$$

in which, as well as below, c_3 is given by (29). The sets of solutions of (26), other than the above excluded set, are evidently the five sets of the first four elements in $C_0, \ldots, C_4$ below. After determining x_3 for each by use of (28), we see that the five pairs of symbols specified in Lemma 3 are

$$C_k = (1 \;\; 1 \;\; k \;\; 0 \;\; z_k \;\; 0), \quad D_k = (a+c_1+1, \; b+d_1+1, \; ab+1+c_2+k, \; d_2+1, \; e+c_3+z_k, \; 1)$$
$$[z_k = a+b+c_1+d_1+c_2+d_2+ad_1+bc_1+abd_2+k+d_2k+e, \; k=0, \; 1];$$

$$C_2 = (a+1, \; b, \; ab+b+1, \; 1, \; e+d_1+bd_2, \; 0) \quad D_2 = (c_1+1, \; d_1, \; c_2+b, \; d_2, \; c_3+d_1+bd_2, \; 1);$$

$$C_3 = (a, \; b+1, \; ab+a+1, \; 1, \; e+c_1+ad_2, \; 0), \quad D_3 = (c_1, \; d_1+1, \; c_2+a, \; d_2, \; c_3+c_1+ad_2, \; 1);$$

$$C_4 = (a+1, \; b+1, \; ab+a+b, \; 1, \; e+\alpha, \; 0), \quad D_4 = (c_1+1, \; d_1+1, \; c_2+a+b+1, \; d_2, \; c_3+\alpha, \; 1)$$
$$[\alpha = c_1+d_1+d_2+1+ad_2+bd_2].$$

To prove Lemma 4, we have to show that if C is one of these 10 symbols and E is one of the 8 not paired with C and not identical with C, the new set AC, BD, . . . does not contain E. If it did, there would be a symbol paired with E whose elements are the sums of corresponding elements of A, C, E. But we readily verify that condition (25) is never satisfied for this symbol paired with E. After treating the cases in which $C = C_4$, we need not consider the cases $C = D_4$, since if P and Q form any pair of our ten symbols, $A+B \equiv P+Q \equiv C_4+D_4$ imply $A+D_4+P \equiv A+C_4+Q$. Hence, treating $C_k (k=0, \; 1)$ together, we need consider only six cases with $C = C_2$, four with $C = C_3$, two with $C = C_4$, and $C = C_0$, $E = D_1$. For example, $A+C_2+C_k = (0 \;\; 1 \;\; b+k \;\; 0 \;\; s \;\; 0)$ is not a symbol satisfying (25).

192. Further Problems of Contacts of Curves. The preceding symmetrical notation for the bitangents to a quartic curve is in accord with that used by Steiner * and Clebsch † in their treatment of a series of problems on contacts of curves.

* *Journal für Math.*, vol. 49 (1855).
† *Ibid.*, vol. 63 (1864).

Let C_n be a real plane curve of order n having no double point. Set

$$p=\tfrac{1}{2}(n-1)(n-2), \quad R_p=2^{2p-1}-2^{p-1}.$$

There are R_p curves of order $n-3$ having simple contact with C_n at $n(n-3)/2$ points. The determination of these curves depends upon an algebraic equation E of degree R_p whose roots are designated by $(x_1y_1\ x_2y_2\ \ldots\ x_py_p)$, where $x_1, \ldots, y_p$ form any set of integral solutions of

$$x_1y_1+x_2y_2+\ \ldots\ +x_py_p\equiv 1 \pmod 2.$$

The simplest case is $n=4$; then $p=3$ and the problem is that of the $R_3=28$ bitangents to a quartic curve. For $n\geqq 4$, Clebsch proved that, if μ is any positive integer $\leqq R_p$ for which $\mu(n-3)/2$ is an integer, the points of contact of C_n with the μ curves corresponding to the roots

$$\ldots(x'_1y'_1\ \ldots\ x'_py'_p), \ \ldots, \ (x_1^{(\mu)}y_1^{(\mu)}\ \ldots\ x_p^{(\mu)}y_p^{(\mu)})$$

lie on a curve of order $\mu(n-3)/2$ if the congruences

$$x'_\rho+x''_\rho+\ \ldots\ +x_\rho^{(\mu)}\equiv 0, \quad y'_\rho+y''_\rho+\ \ldots\ +y_\rho^{(\mu)}\equiv 0 \pmod 2 \qquad (\rho=1, \ldots, p)$$

hold simultaneously. For $n=4$, the first case $\mu=2$ is evidently trivial, while the next case $\mu=4$ is the one treated in Theorem 11.

The group * of equation E can be represented as a subgroup of the abelian † linear homogeneous group on $2p$ variables with integral coefficients taken modulo 2. Its substitutions of period 2 are conjugate to certain simple types, from which fact in connection with the Corollary in § 188 we find that the number of real roots of equation E is one of the numbers

$$2^{2p-1-k}(k=1, \ldots, p), \quad 2^{2p-2j-1}-2^{p-1} \qquad (j=0, 1, \ldots, \pi),$$

where $\pi=p/2$ or $(p-1)/2$, according as p is even or odd. For $n=4$, we again get the number of real bitangents to a quartic curve (§ 188). For $n=5$, we have $p=6$ and see that, of the 2016 conics tangent at 5 points to a quintic curve without

* Dickson, *Annals of Math.*, ser. 2, vol. 6 (1905), p. 146.

† Leaving invariant a certain bilinear function of two sets of cogredient variables. It is not a commutative group.

double points, either all, 1024, 512, 480, 256, 128, 96, 64, 32 or none are real.

These results, obtained so easily by group theory, are in complete agreement with those obtained by an elaborate geometrical proof by Klein.*

The case in which the curve C_n has $n(n-3)/2$ double points was treated by Clebsch † and from the group standpoint by Jordan.‡ The latter treated also the group of the equation upon which depend the 16 singular tangent planes to Kummer's quartic surface with 16 singular points (*l.c.*, pp. 313–5); also several technical problems of contacts of curves and the problem of the 16 straight lines on a quartic surface with a double conic (*l.c.*, pp. 305–313).

The various geometrical problems treated or mentioned in this Chapter and the preceding one have led to linear congruence groups. Such groups enter into the majority of the questions treated in Jordan's *Traité des Substitutions* and form the exclusive subject of Dickson's *Linear Groups*.

* *Math. Annalen*, vol. 42 (1893), p. 3, p. 26; *Riemann'sche Flächen*, II (1892), pp. 117–255.

† *Journal für Math.*, vol. 64 (1865).

‡ *Traité des Substitutions*, 1870, pp. 331–3.

CHAPTER XX

MONODROMIE GROUP

193. Definition of the Monodromie Group M. Consider an algebraic equation $F(z, k)=0$ in z whose coefficients are rational functions of the complex variable k. Let $z_1, \ldots, z_n$ be the roots of $F(z, k_0)=0$, where k_0 is a constant. Let k vary continuously from this initial value in any manner, but finally return to the same value k_0 (i.e., let the point representing k in the complex plane describe any closed path starting from and ending with the point representing k_0). Then the roots vary continuously and, after the circuit, take on their initial values in the same or a new order. Thus to each closed path corresponds a substitution on the roots.

For example, if k describes a circle around the origin, the roots of $z^2=2k$ are interchanged.

Two circuits may be combined into a single third circuit to which corresponds the product of the two substitutions corresponding to the two circuits. Hence the substitutions corresponding to all possible circuits form a group M, called the monodromie group * of $F(z, k)=0$ with respect to k. It was first studied by Hermite and Jordan.†

194. Monodromie Group an Invariant Subgroup of the Galois Group. Let ϕ be a rational function of k and the roots $z_1, \ldots, z_n$, and let $\phi, \phi', \phi'', \ldots$ be the functions derived from ϕ by the various substitutions of M. If $\phi=\phi'=\phi''=\ldots$, ϕ is said to possess monodromie with respect to k. This is evidently the case with any ϕ which equals a rational function

* "Group in the function-theoretic sense," by Klein-Fricke, *Elliptischen Modulfunctionen*, vol. 1, 1890, p. 132; applications in vol. 2, 1892, p. 53, p. 599.

† *Traité des Substitutions*, 1870, pp. 277–9.

of k, whether or not the coefficients of $\phi(k, z_1, \ldots, z_n)$ involve irrational constants.

Let R be the domain defined by k and the coefficients of the powers of z in $F(z, k)$. Any rational function ϕ of the roots with coefficients in R, which equals a quantity in R, equals a rational function of k and hence is unaltered by every substitution of M. Then, by the Corollary in § 149, M is a subgroup of the Galois group G for R of the equation $F=0$.

Moreover, *M is an invariant subgroup of G.* For, let ϕ be a rational function of the roots with coefficients in R which belongs to the subgroup M of index ν under G. Then ϕ is a root of an equation E of degree ν with coefficients in R, so that ϕ is an algebraic function of k. But ϕ possesses monodromie with respect to k. Hence ϕ is a rational function $f(k)$ of k with perhaps irrational coefficients. Replace the coefficients of $f(k)$ by independent variables and substitute the resulting expression in place of ϕ in E, and let the result be an identity in k. We obtain certain algebraic equations which the variable coefficients of $f(k)$ must satisfy. Adjoin to R all of the roots of these numerical equations. Since ϕ is in the enlarged domain, G reduces to a subgroup of M, necessarily M itself, since the group of monodromie is evidently unaltered by the adjunction of constants. But the adjunction of all of the roots of a second equation reduces the Galois group of the first equation to an invariant subgroup (§ 167). A number of such adjunctions reduced G to M; whence M is invariant in G.

For example, the Galois group for $R(k)$ of $z^3-2k^3=0$ is the symmetric group G_6, since the equation is irreducible in R and the product of the differences of its roots is $6\sqrt{-3}k^3$. The only circuits causing a permutation of the roots are those around the origin. Hence M is the cyclic group of order 3 and is invariant in G.

195. Applications of Monodromie. Jordan * employed monodromie to determine the Galois group of the equation for the n-section of the periods of elliptic † and hyperelliptic functions with $2p$ periods. For the case of the trisection of

* *Traité des Substitutions*, pp. 337–369.

† Cf. H. Weber, *Elliptische Functionen*, 1891, p. 219.

the periods of hyperelliptic functions of four periods, the group is the quaternary abelian linear group modulo 3 and is isomorphic * with the group for the equation of the 27 lines on a cubic surface (§ 183).

Monodromie has been applied to linear differential equations

$$\frac{d^n z}{dk^n}+f_1(k)\frac{d^{n-1}z}{dk^{n-1}}+ \ . \ . \ . \ + f_n(k)\cdot z=0.$$

For simplicity, the coefficients $f(k)$ will be assumed to be rational functions of the complex variable k. Let $z_1, \ . \ . \ . \ , z_n$ be a set of linearly independent solutions (integrals) and let k_0 be a constant such that each z_i is an ordinary power series in $k-k_0$. If now the point representing k describes a closed path starting from and ending with the point representing k_0, as in § 193, the set of solutions $z_1, \ . \ . \ . \ , z_n$ becomes a set of solutions $z'_1, \ . \ . \ . \ , z'_n$, which are therefore linear functions of $z_1, \ . \ . \ . \ , z_n$ with constant coefficients:

$$z'_1=a_{11}z_1+ \ . \ . \ . \ +a_{1n}z_n, \ . \ . \ . \ , \ z'_n=a_{n1}z_1+ \ . \ . \ . \ +a_{nn}z_n.$$

With the chosen circuit is thus associated a linear transformation (§ 75). The transformations obtained from all such circuits form a linear group, called the monodromie group M of the differential equation.

This group M is finite in case the integrals $z_1, \ . \ . \ . \ , z_n$ are algebraic functions of k. The theory of finite linear groups (Part II) is therefore applicable to the problem † of the determination of all linear differential equations whose integrals are all algebraic. In the case just mentioned, M coincides with another important group G, which we proceed to define; but, in general, M is only a subgroup of G.

According to Picard and Vessiot, the transformation group G of a linear differential equation with the linearly independent solutions $z_1, \ . \ . \ . \ , z_n$ possesses the following two characteristic properties (analogous to properties A and B of the Galois group of an algebraic equation, § 149):

If a rational function F of $z_1, \ . \ . \ . \ , z_n$ and their derivatives

* Jordan, *l.c.*, p. 369; Dickson, *Linear Groups*, pp. 306–7.

† Jordan, *Jour. für Math.*, vol. 84 (1877), pp. 89–215.

remains unaltered (as a function of k) by all the transformations of G, then F equals a rational function of k.

Conversely, if such a function F equals a rational function of k, it remains unaltered by all the transformations of G.

For the development and application of these concepts, see C. Jordan, *Cours d'Analyse*, vol. 3, 1896, pp. 193, 203, and L. Schlesinger, *Handbuch der Linearen Differentialgleichungen*, vol. 2, I, 1897, pp. 1–226, especially pp. 71, 96–102; vol. 2, II, 1898, pp. 148–159.

196. Quintic Equations, Form Problem. In the "form problem" for the icosahedral group, we are given the values of the fundamental invariants T, H, f, consistent with the relation between them (§ 105, E), and require the values of the variables x_1, x_2. However, we desire primarily only their ratio $z = x_1/x_2$. Hence, given Z, we seek the values of z for which

$$\frac{H^3}{1728 f^5} = Z. \tag{1}$$

This icosahedral equation of degree 60 is remarkable both on account of the property that all its roots are linear fractional functions of a single root and the fact that the roots of any quintic equation can be expressed in terms of radicals and a root z of (1). In his *Vorlesungen über das Ikosaeder*, 1884, Klein therefore regards z as a new fundamental irrationality, a stage higher in algebraic complexity than radicals. Moreover, z can be expressed in terms of elliptic modular functions (*ibid.*, p. 132).

Naturally there are many resolvent equations of degree < 60. For example, if we use the tetrahedral invariant t of § 105 and set $r = t^2/f$, we get the resolvent of the fifth degree

$$r(r^2 - 10r + 45)^2 + 1728(Z - 1) = 0.$$

The form problem of the tenary linear group of order 168 (§ 123, J, § 125) is connected in a similar manner with the equations of degree 7 whose Galois group is the simple group of order 168.

For references to these and related subjects, consult *Encyklopädie der Mathematischen Wissenschaften*, vol. 1, I, pp. 533–552, 513–4; Weber, *Algebra*, ed. 2, vol. 2, 470–496, 530–550.

SUBJECT INDEX

(The numbers refer to pages)

PART I

Abelian group defined, 62, 87
Abstract definitions of groups, 143
— group defined, 52
Alternating group, 18, 43, 166
Anharmonic group, 65
Arithmetic substitutions, 12
Automorphisms of a group, 46
Average number of letters in all the substitutions of a transitive group, 32, of an intransitive group, 73
Axial group, 65

Base of an abelian group, 89
Bauer's theorem, 124
Bertrand's problem, 166

Cayley's table, 64
— theorem, 64
Central of a group, 68
— quotient group, 68
Characteristic subgroups and characteristic operators, 71, 109
Class of a substitution and of a substitution group, 47
Cogredient isomorphisms, 68, 76
Commutative operators and commutative groups, 54, 62
— substitutions, 2, 18
Commutator quotient group, 69
Commutators and commutator subgroup, 68
Complementary groups, 67
Complete group, 46
— set of conjugates, 22
Composite groups, 43
Conformal groups, 107
Congruence groups, 10
Congruent elements, 67
Conjoints, 37
Conjugate operators or subgroups, 59
— substitutions and substitution groups, 5, 21
Construction of groups of order p^m, 138
— — — with invariant subgroups, 59
Contragredient isomorphisms, 76
Co-set and augmented co-set, 24, 66
Cross-cut of two groups, 23
Cyclic group, 7, 54
— substitution, 16

Degree and order of a group, 2
— of a substitution, 8, 16
Derived groups, 69
Dicyclic groups, 62, 170
Dihedral groups, 61, 168
Direct product, 13, 77
Divisible groups, 117
Divisor of a group, 3
Double co-set, 25
— holomorph, 46
Doubly transitive groups, 40, 164

Elementary divisors of the order of an abelian group, 88
Elements of a group, 52, 68
Equivalent or congruent elements, 67
Even or positive substitutions, 17
Examples of groups, 1

Factor groups, 176
Factors of composition, 174, 184
Four-group, 65
Frobenius's theorem, 77
Fundamental characteristic subgroup, 110

Generalizations of the groups of the regular polyhedrons, 152
Generating substitutions of a group, 7
Group defined, 2, 52
— generated by two operators having a common square, 143
— of a function, 5
— — isomorphisms, 46, 95, 101, 134, 160
— — the square, 4
— property, 86
Groups involving no more than four letters, 41
— — only abelian subgroups, 112
— of degree five, 45
— — movements of plane figures, 9
— — subtraction and division, 15, 81
— — the regular polyhedrons, 147
— represented by matrices, 13
— whose orders are powers of prime numbers, 118
— — — — — divisible by 2 but not by 4, 66
— having simple abstract definitions, 143

Hamilton groups, 115
Holomorph of a group, 46

Icosahedron group, 150, 158
Icosian calculus, 159
Identity, 2, 53
Imprimitive substitution groups, 38
Independent cyclic subgroups, 88
Index of a subgroup, 23
Indivisible group, 117
Inner isomorphisms, 76, 183
Insolvable groups, 174, 186
Intransitive substitution group, 31
Intrinsic and relative properties of operators, 159

Invariant abelian subgroups of a prime-power group, 120
— operators in the group of isomorphisms of an abelian group, 101
— subgroups, 21, 66
Invariants of an abelian group, 88
Inverse of a substitution, 11
— — an element or operator, 54
Isomorphisms defined, 33, 160
— of the alternating and the symmetric groups, 166
— — an abelian group, 101

Jordan's theorem, 35

Kuhn's theorem, 37

Lagrange's theorem, 23
Left co-sets, 66

Maximal subgroup, 39
Metabelian group, 68
Metacyclic group, 12
Movements of the regular polygon, 9
Multiple isomorphisms, 34
Multiplication of substitutions, 2
Multiply transitive groups, 40

Nebengruppen, 24
Negative or odd substitutions, 17
Number of elements of a given order in an abelian group, 93
— — operators in a set of independent generators of a group of order p^m is invariant, 127
— — subgroups in a prime-power group, 123
— — — of order p^α in any group, 125

Octahedron group, 149, 154
Octic group, 4
Operator or operation of a group, 68
Order of a group and of an operator, 2, 53
— — a substitution, 8
— — the product of n operators, 70
Outer isomorphisms, 76

Perfect group, 69
Period of an element of a group, 53
Permutations and substitutions, 36
ϕ-subgroup, 71
P-isomorphisms, 134
Positive and negative substitutions, 16
Power of a group, 32
Primary groups, 118
Prime-power groups, 118
Primitive and imprimitive substitution groups, 38
Product of two substitutions, 2

Quadratic group, 65
Quaternion group, 62
Quotient group, 34, 66

Rank of an abelian group, 92
Relative and intrinsic properties of operators, 159
Regular substitution group, 35
Representation of a group as a regular substitution group, 63
— — an abstract group as a transitive substitution group, 81
Right co-sets, 66
Roots of operators of an abelian group, 114

Self-conjugate subgroup, 21
Series of composition, 177
Set of independent generators of a group, 9, 90, 127
Similar substitutions and similar groups, 21
Simple group, 43
— isomorphisms and simply isomorphic groups, 33, 73, 95
Simplicity of the alternating group, 43
Solvable group , 174
Subgroup, 3
Subgroups and quotient groups of an abelian group, 99
Substitution and substitution group, 1, 2
— groups of degree five, 45
Substitutions commutative with a given substitution, 19
Sylow's theorem, 27
Sylow subgroups, 27, 181
Symmetric group, 1, 3, 166
Systems of imprimitivity, 38

Tetrahedral group, 147, 152
Totient of a number, 11
Totitives of a number, 95
Transform of a substitution and of a substitution group, 20, 57
Transitive constituent of an intransitive group, 33
— substitution group, 31
Transitivity of the symmetric group, 40
Transposition, 16

Vierergruppe, 65

PART II

Abelian groups, canonical form of, 213
Algebraic integer, 241

Canonical form, 196; theorems on, 212, 213
Change of variables, 203
Characteristic and characteristic equation, 205
Collineations and collineation-groups, 198
Conjugate-imaginary groups, 209
Determinant of a linear transformation, 194; theorems on the determinants of the transformations belonging to a finite group, 196, 200, 202
Dihedral group, 220, 225
Diophantine equation, 227

Equivalent groups, 262

Group-matrix, theorem on, 268

Groups, binary, 215
—, linear, 198
—, linear fractional, 201
— of collineations, 198
— — linear transformations of determinant unity, 200
— — the regular polyhedra, 220
— — order p^a, 231
— — order $p^a q^b$, 272
— — degree n and class $n-1$, 274
—, ternary, 235

Hermitian form, 207
— invariant, 209
Hessian group, 239
Homology, 248

Icosahedral group, 223, 226
Identical transformation or the identity, 196
Imprimitive groups, 228; theorem on, 229
Imprimitivity, sets of, 228
Intransitive groups, 206
Intransitivity, sets of, 206
Invariants (absolute, relative), 258; theorems on the number of, 258, 259
— of the binary groups, 224
— — — ternary groups, 253
Inverse of a linear transformation, 194, 210
Irreducible groups, 211.

Linear transformation, 194

Matrix of a linear transformation, 194; theorems on the matrices of the transformations belonging to a finite transitive group, 271
Monomial groups, 229
Multipliers of a linear transformation, 196; theorems on, 197, 257

Non-equivalent groups, 262; theorem on, 271

Octahedral group, 222, 225
Order of a linear transformation, 196
— — — primitive group, 256

Power of a linear transformation, 196
Primitive groups, 228; order of, 256
Product of linear transformations, 195

Reducible groups, 210
Regular substitution groups, theorems on, 264, 265, 269, 272
Roots of unity, 239

Similarity-transformations, 196; theorems on, 197, 202, 233, 234
Sylow groups, 231

Tetrahedral group, 222, 225
Transitive groups, 207; theorems on, 260, 261

Unitary form, 210

PART III

Abel's theorem, 320
Abelian functions, 373
— linear group, 376-7, 380
Adjunction, 299, 313–4, 317–20, 323–4, 338–41, 379
Aronhold set, 361, 367–71
Asyzygetic, 356, 361–3

Belongs to group, 296–7, 299
Binomial equation, 281, 312, 316
Bitangents, 350–76

Cardan's formulas, 301
Congruence group, 335, 377
Conics, 353–6, 373, 376
Conjugate, 297, 305
Constructions by ruler and compasses, 321–6
Contact, 353–77
Cross-ratio, 283
Cubic curve, 330–42
— equation, 296, 301–3, 320–3
— surface, 343–53, 366, 380

Curve of order n, 376–7
Cyclic group, 306–9, 311, 316, 319, 326
Cyclotomic equation, 308–10

Differential equation, 380
Discriminant, 290, 292, 302, 312
Domain, 280, 293, 299
Double point, 329
— six, 345
Duplication of cube, 321–3

Elliptic function, 379, 381
Equality, 294
Equation with variable coefficients, 292
— of the fifth and seventh degree, 381
Euler's theorem, 328

Factors of composition, 306, 311–2, 317, 350
Fan, 361
Form problem, 381

Galois' criterion for solvability, 315
— generalization of Lagrange's theorem, 298
— theorem, 319
Galoisian equation, 320
— resolvents, 284, 288
Gauss' lemma, 309
General equation, 292, 294, 317, 320, 372
Geometrical constructions, 321–6
— questions, 321–77
Group of an algebraic equation, 286–9, 294, 300, 305, 333–41, 347, 362, 365, 367–71, 376–81
— — a differential equation, 380
— on four letters, 290

Hessian, 329, 344, 354
— curve, 330–3
Homogeneous coördinates, 327
Hyperboloid, 346
Hyperelliptic functions, 379

Icosahedral equation, 381
— group, 381
Imaginary roots, 292, 365
Inflexion, 330–42
Integral root, 282
Invariant, 330, 333, 381
— subgroup, 305–6, 318–9, 378
Irreducible, 280–1, 289, 292, 294, 297, 310, 320, 325
— case for cubic equations, 320
Isomorphic, 304

Jordan's theorem, 317

Lagrange's formulas, 307
— theorem, 298
Linear group, 335–8, 380–1
— transformation, 328, 336, 380
Lines on a cubic surface, 343, 366

Monodromie, 378–81

Notation of Hesse and Cayley, 357

Primitive root, 308, 325

Quartic curve, 350–76
— equation, 290, 296, 312–4, 337
— surface, 377
Quintic equation, 381
— curve, 376
Quotient group, 306, 318, 337

Radicals (see Solvable)
Rational function, 284, 289, 294, 296, 298, 378, 380–1
— root, 282
Reality, 341, 365–6, 376–7
Reciprocal equation, 290–2
Reducible, 280–1, 289, 291, 309
Regular group, 306, 309, 316
— polygon, 321–6
Resolvent, 284, 290, 303–6, 312. 350, 381
Root, definition of, 292
— of unity, 307–11, 323–6

Series of composition, 306, 317
Simple group, 306, 350, 372, 381
Singular point, 329

Solvable equation, 301–3, 307, 310–4, 315, 317, 320, 337, 341
— group, 279, 306, 310, 337
Steiner sets of bitangents, 354–77
Symmetric group, 295–6, 299, 305, 315, 317, 337–8, 364, 372
Symmetrical form for the equation to a quartic curve, 355
— notation for bitangents, 372
Syzygetic, 356, 361–3

Tangent cone, 351–3
Theta functions, 373
Transitive, 289, 306
Triangle of reference, 328
— on a cubic surface, 344–6
Trisection of an angle, 321–3, 326

Unaltered, 287, 289, 294, 296, 298, 381

Values of functions, 282, 314

AUTHOR INDEX

(The numbers refer to pages)

PART I

Abbati, P., 84
Abel, N H., 85
Alasia, C., 86
Battaglini, G., 86
Bertrand, J., 166
Betti, E., 15, 20
Bianchi, L., 86
Bôcher, M., 13, 65, 86
Bolza, O., 33, 65
Burnside, W., 46, 65, 86, 123, 127
Capelli, A., 65, 160
Carmichael, R. D., 28
Cauchy, A. L., 12, 17, 23, 25, 27, 43, 47, 85
Çayley, A., 64, 85, 159
Čebyšëv, P. L., 166
Chapman, H. W., 84
Cole, F. N., 86
Dedekind, R., 69, 97, 115
Dickson, L. E., 117
Dyck, W., 81
Easton, B. S., 86
Euler, L., 84, 87
Fite, W. B., 68
Frattini, G., 35, 71
Frobenius, G., 25, 32, 71, 77, 87, 88, 113, 118
Galois, E., 2, 12, 24, 27, 45, 66, 85
Gauss, C. F., 11, 85, 87, 89
Hamilton, W. R., 45, 62, 115, 147, 150, 159
Heffter, L., 93
Hermite, C., 15
Hilton, H., 124
Hölder, O., 34, 160, 176, 191
Huntington, E. V., 85
Jordan, C., 20, 34, 35, 50, 85, 86, 160, 176
Klein, F., 15
Kronecker, L., 85, 89
Kuhn, H. W., 31
Lagrange, J. L., 4, 23, 84
Loewy, A., 183
Lucas, E., 98
Manning, W. A., 50
Mathieu, E., 106
Miller, G. A., 65, 114, 117, 138
Moore, E. H., 105, 160, 161
Moreno, H. C., 114
Netto, E., 86, 93
Pierpont, J., 65
Poincaré, H., 84
Ranum, A., 101
Remak, R., 176
Ruffini, P., 84
Schering, E., 89
Séguier, J. de, 2
Serret, J. A., 166
Stickelberger, L., 87, 88, 118
Sylow, L., 27, 119
Sylvester, J. J., 11
Vandermonde, A. J., 17, 84
Weber, H., 12, 24, 34, 95, 98, 174

PART II

Bieberbach, L., 256
Blichfeldt, H. F., 231, 256
Burnside, W., 231, 257, 268, 272
Dickson, L. E., 253
Frobenius, G., 256, 257, 274
Fuchs, L., 209, 215
Gordan, P., 215
Jordan, C., 207, 215, 239, 256
Klein, F., 215, 225, 254
Kronecker, L., 240
Loewy, A., 209
Maschke, H., 207, 253
Mitchell, H. H., 256
Molien, T., 257
Moore, E. H., 209, 250
Picard, E., 209
Schur, J., 256, 257
Valentiner, H., 209, 215, 256
Wiman, A., 254

PART III

Abel, N. H., 317, 320
Aronhold, S, 361, 367–71
Cardan, G., 301
Cayley, A., 357
Clebsch, A., 372, 375–7
Dickson, L. E., 320, 326, 350, 365, 373, 376–7, 380
Euler, L., 328
Galois, E., 298, 315–20, 378
Gauss, C. F., 309, 326
Geiser, C. F., 351
Hermite, C., 378
Hesse, O., 329, 357
Hölder, O., 318
Jordan, C., 317, 336, 348, 350, 377–81
Kempner, A. J., 292
Klein, F., 377, 378, 381
Kronecker, L., 310
Lagrange, J. L., 298, 307
Maillet, E., 365–6
Mitchell, H. H., 350
Picard, E., 380
Riemann, B., 372
Ruffini, P., 317
Schläfli, L., 366
Schlesinger, L., 381
Serret, J. A., 320
Steiner, J., 354–77, 375
Vessiot, E., 380
Weber, H., 320, 336, 366–7, 372, 379 381
Zeuthen, H. G., 366