

19780892

GENERATORS AND RELATIONS
FOR DISCRETE GROUPS

H. S. M. COXETER

AND

W. O. J. MOSER



0152

E608

19780892

外文书库

GENERATORS AND RELATIONS FOR DISCRETE GROUPS

H. S. M. COXETER

AND

W. O. J. MOSER



WITH 54 FIGURES



SPRINGER-VERLAG
BERLIN · GÖTTINGEN · HEIDELBERG

1957

ALLE RECHTE, INSBESONDERE DAS DER ÜBERSETZUNG
IN FREMDE SPRACHEN, VORBEHALTEN
OHNE AUSDRÜCKLICHE GENEHMIGUNG DES VERLAGES IST ES AUCH NICHT
GESTATTET, DIESES BUCH ODER TEILE DARAUS AUF PHOTOMECHANISCHEM
WEGE (PHOTOKOPIE, MIKROKOPIE) ZU VERVIELFÄLTIGEN

© BY SPRINGER-VERLAG OHG.
BERLIN · GÖTTINGEN · HEIDELBERG 1957
PRINTED IN GERMANY

BRÜHLSCHES UNIVERSITÄTSDRUCKEREI GIESSEN

ERGEBNISSE DER MATHEMATIK UND IHRER GRENZGEBIETE

UNTER MITWIRKUNG DER SCHRIFTLEITUNG DES
„ZENTRALBLATT FÜR MATHEMATIK“

HERAUSGEGEBEN VON

L.V.AHLFORS · R.BAER · R.COURANT · J.L.DOOB · S.EILENBERG
P.R.HALMOS · T.NAKAYAMA · H.RADEMACHER
F.K.SCHMIDT · B.SEGRE · E.SPERNER

NEUE FOLGE · HEFT 14

REIHE: GRUPPENTHEORIE

BESORGT
VON

R. BAER



SPRINGER-VERLAG
BERLIN · GÖTTINGEN · HEIDELBERG

1957

Preface

When we began to consider the scope of this book, we envisaged a catalogue supplying at least one abstract definition for any finitely-generated group that the reader might propose. But we soon realized that more or less arbitrary restrictions are necessary, because interesting groups are so numerous. For permutation groups of degree 8 or less (i. e., subgroups of \mathfrak{S}_8), the reader cannot do better than consult the tables of JOSEPHINE BURNS (1915), while keeping an eye open for misprints. Our own tables (on pages 134—143) deal with groups of low order, finite and infinite groups of congruent transformations, symmetric and alternating groups, linear fractional groups, and groups generated by reflections in real Euclidean space of any number of dimensions.

The best substitute for a more extensive catalogue is the description (in Chapter 2) of a method whereby the reader can easily work out his own abstract definition for almost any given finite group. This method is sufficiently mechanical for the use of an electronic computer.

There is also a topological method (Chapter 3), suitable not only for groups of low order but also for some infinite groups. This involves choosing a set of generators, constructing a certain graph (the Cayley diagram or *DEHNSche Gruppenbild*), and embedding the graph into a surface. Cases in which the surface is a sphere or a plane are described in Chapter 4, where we obtain algebraically, and verify topologically, an abstract definition for each of the 17 space groups of two-dimensional crystallography.

In Chapter 5, the fundamental groups of multiply-connected surfaces are exhibited as symmetry groups in the hyperbolic plane, the generators being translations or glide-reflections according as the surface is orientable or non-orientable.

The next two chapters deal with special groups that have become famous for various reasons. In particular, certain generalizations of the polyhedral groups, scattered among the numerous papers of G. A. MILLER, are derived as members of a single family. The inclusion of a slightly different generalization in § 6.7 is justified by its unexpected connection with SHEPHARD's regular complex polygons.

Chapter 8 pursues BRAHANA's idea that any group generated by two elements, one of period 2, can be represented by a regular map or topological polyhedron.

In Chapter 9 we prove that every finite group defined by relations of the form

$$R_i^2 = (R_i R_j)^{p_{ij}} = E \quad (1 \leq i < j \leq n)$$

can be represented in Euclidean n -space as a group generated by reflections in n hyperplanes. Many well-known groups belong to this family. Some of them play an essential role in the theory of simple Lie groups.

We wish to express our gratitude to Professor REINHOLD BAER for inviting us to undertake this work and for constructively criticizing certain parts of the manuscript. In the latter capacity we would extend our thanks also to Dr. PATRICK DU VAL, Professor IRVING REINER, Professor G. DE B. ROBINSON, Mr. F. A. SHERK, Dr. J. A. TODD and Professor A. W. TUCKER. We thank Mr. J. F. PETRIE for two of the drawings: Figs. 4.2, 4.3; and we gratefully acknowledge the assistance of Mrs. BERYL MOSER in preparing the typescript.

University of Toronto
University of Saskatchewan

H. S. M. C.
W. O. J. M.

February 1957

Contents

1. Cyclic, Dicyclic and Metacyclic Groups	1
1.1 Generators and relations	1
1.2 Factor groups	2
1.3 Direct products	3
1.4 Automorphisms	5
1.5 Some well-known finite groups	6
1.6 Dicyclic groups	7
1.7 The quaternion group	8
1.8 Cyclic extensions of cyclic groups	8
1.9 Groups of order less than 32	11
2. Systematic Enumeration of Cosets	12
2.1 Finding an abstract definition for a finite group	12
2.2 Examples	14
2.3 The corresponding permutations	17
2.4 Finding whether a given subgroup is normal	17
2.5 How an abstract definition determines a group	17
3. Graphs, Maps and Cayley Diagrams	18
3.1 Graphs	19
3.2 Maps	19
3.3 Cayley diagrams	21
3.4 Planar diagrams	23
3.5 Unbounded surfaces	24
3.6 Non-planar diagrams	28
3.7 SCHREIER's coset diagrams	31
4. Abstract Crystallography	33
4.1 The cyclic and dihedral groups	33
4.2 The crystallographic and non-crystallographic point groups	33
4.3 Groups generated by reflections	35
4.4 Subgroups of the reflection groups	38
4.5 The seventeen two-dimensional space groups	40
4.6 Subgroup relationships among the seventeen groups	51
5. Hyperbolic Tessellations and Fundamental Groups	52
5.1 Regular tessellations	52
5.2 The Petrie polygon	54
5.3 Dyck's groups	54
5.4 The fundamental group for a non-orientable surface, obtained as a group generated by glide-reflections	56
5.5 The fundamental region for an orientable surface, obtained as a group of translations	58

6. The Symmetric, Alternating, and other Special Groups	61
6.1 ARTIN's braid group	62
6.2 The symmetric group	63
6.3 The alternating group	66
6.4 The polyhedral groups	67
6.5 The binary polyhedral groups	68
6.6 MILLER's generalization of the polyhedral groups	71
6.7 A new generalization	76
6.8 BURNSIDE's problem	80
7. Modular and Linear Fractional Groups	83
7.1 Lattices and modular groups	83
7.2 Defining relations when $n = 2$	85
7.3 Defining relations when $n \geq 3$	88
7.4 Linear fractional groups	92
7.5 The groups LF $(2, p)$	93
7.6 The groups LF $(2, 2^m)$	96
7.7 The Hessian group and LF $(3, 3)$	97
7.8 The first Mathieu group	98
8. Regular Maps	100
8.1 Automorphisms	100
8.2 Universal covering	102
8.3 Maps of type $\{4, 4\}$ on a torus	102
8.4 Maps of type $\{3, 6\}$ or $\{6, 3\}$ on a torus	106
8.5 Maps having specified holes	108
8.6 Maps having specified Petrie polygons	110
8.7 Maps having two faces	113
8.8 Maps on a two-sheeted Riemann surface	115
8.9 Symmetrical graphs	116
9. Groups Generated by Reflections	117
9.1 Reducible and irreducible groups	117
9.2 The graphical notation	117
9.3 Finite groups	118
9.4 A brief description of the individual groups	122
9.5 Commutator subgroups	124
9.6 Central quotient groups	126
9.7 Exponents and invariants	129
9.8 Infinite Euclidean groups	131
9.9 Infinite non-Euclidean groups	132
Tables 1—12	134
Bibliography	144
Index	152

Chapter 1

Cyclic, Dicyclic and Metacyclic Groups

After briefly defining such fundamental concepts as generators, factor groups and direct products, we show how an automorphism of a given group enables us to adjoin a new element so as to obtain a larger group; e.g., the cyclic and non-cyclic groups of order 4 yield the quaternion group and the tetrahedral group, respectively. Observing that the standard treatises use the term *metacyclic* group in two distinct senses, we exhibit both kinds among the groups of order less than 32, whose simplest known abstract definitions are collected in Table 1.

Opinions seem to be evenly divided as to whether products of group elements should be read from left to right or from right to left. We choose the former convention, so that, if A and B are transformations, AB signifies the transformation A followed by B .

1.1 Generators and relations. Certain elements S_1, S_2, \dots, S_m , of a given discrete group \mathfrak{G} , are called a set of *generators* if every element of \mathfrak{G} is expressible as a finite product of their powers (including negative powers). Such a group is conveniently denoted by the symbol

$$\{S_1, S_2, \dots, S_m\}.$$

When $m = 1$, we have a *cyclic* group

$$\{S\} \cong \mathfrak{C}_q,$$

whose order q is the period of the single generator S . If q is finite, S satisfies the relation $S^q = E$, where E denotes the identity element.

A set of relations

$$g_k(S_1, S_2, \dots, S_m) = E \quad (k = 1, 2, \dots, s), \quad (1.11)$$

satisfied by the generators of \mathfrak{G} , is called an *abstract definition* of \mathfrak{G} if every relation satisfied by the generators is an algebraic consequence of these particular relations. For instance, if q is finite, $S^q = E$ is an abstract definition of \mathfrak{C}_q . It is important to remember that, in such a context, the relation $S^q = E$ means that the period of S is exactly q , and not merely a divisor of q . This is sometimes expressed by saying that the relation is not merely "satisfied" but "fulfilled" (see MILLER, BLICHFELDT and DICKSON 1916, p. 143).

Returning to the general group \mathfrak{G} , defined by 1.11, let \mathfrak{H} be another group whose abstract definition in terms of generators T_1, T_2, \dots, T_n is given by the relations

$$h_l(T_1, T_2, \dots, T_n) = E \quad (l = 1, 2, \dots, t). \quad (1.12)$$

Then it is known that a necessary and sufficient condition for \mathfrak{G} to be isomorphic to \mathfrak{H} is the existence of relations

$$T_j = T_j(S_1, S_2, \dots, S_m) \quad (j = 1, 2, \dots, n), \quad (1.13)$$

$$S_i = S_i(T_1, T_2, \dots, T_n) \quad (i = 1, 2, \dots, m), \quad (1.14)$$

such that 1.11 and 1.13 together are algebraically equivalent to 1.12 and 1.14 together (COXETER 1934b). For instance,

$$R^6 = E \quad (1.15)$$

and

$$S^3 = T^2 = S^{-1} T S T = E \quad (1.16)$$

are two possible definitions for \mathfrak{G}_0 , since the relations

$$R^6 = E, \quad S = R^4, \quad T = R^3$$

are equivalent to

$$S^3 = T^2 = S^{-1} T S T = E, \quad R = S T.$$

1.2 Factor groups. Let $\mathfrak{G}' \cong \{R_1, R_2, \dots, R_m\}$ be defined by the $s + r$ relations

$$g_k(R_1, R_2, \dots, R_m) = E \quad (k = 1, 2, \dots, s + r).$$

The correspondence

$$S_i \rightarrow R_i \quad (i = 1, 2, \dots, m)$$

defines a homomorphism of \mathfrak{G} (defined by 1.11) onto \mathfrak{G}' . The elements

$$g_k(S_1, S_2, \dots, S_m) \quad (k = s + 1, \dots, s + r) \quad (1.21)$$

of \mathfrak{G} all correspond to the identity element

$$g_k(R_1, R_2, \dots, R_m) = E \quad (k = s + 1, \dots, s + r)$$

of \mathfrak{G}' . Hence the kernel of the homomorphism is the normal subgroup

$$\mathfrak{N} \cong \{W^{-1} g_k(S_1, S_2, \dots, S_m) W\} \quad (k = s + 1, \dots, s + r),$$

where W runs through all the elements of \mathfrak{G} . In fact, \mathfrak{N} is the smallest normal subgroup of \mathfrak{G} that contains the elements 1.21, and it follows that

$$\mathfrak{G}' \cong \mathfrak{G}/\mathfrak{N}.$$

In other words, the effect of adding new relations to the abstract definition of a group \mathfrak{G} , is to form a new group \mathfrak{G}' which is a *factor group* of \mathfrak{G} (KUROSCHE 1953, p. 76).

In particular, the effect of adding to 1.11 the relations

$$S_i^{-1} S_j^{-1} S_i S_j = E \quad (i, j = 1, 2, \dots, m)$$

is to form the *commutator quotient group* of \mathfrak{G} , which is the largest Abelian factor group of \mathfrak{G} .

Every group with m generators is a factor group of the free group \mathfrak{F}_m , which has m generators and no relations (REIDEMEISTER 1932a, p. 31). Apart from some special considerations in § 7.3, p. 88, we shall not attempt to describe the modern development of the theory of free groups, which began with the remarkable theorem of NIELSEN (1921) and SCHREIER (1927) to the effect that *every subgroup of a free group is free* (see especially MAGNUS 1939, BAER 1945, M. HALL 1949, CHEN 1951, 1954, FOX 1953, 1954 and KUROSCH 1953, pp. 271—274).

1.3 Direct products. If two groups \mathfrak{G} , \mathfrak{H} , defined by the respective sets of relations 1.11, 1.12, have no common element except E , and if all elements of \mathfrak{G} commute with those of \mathfrak{H} , then the $m + n$ elements S_i and T_j generate the *direct product*

$$\mathfrak{G} \times \mathfrak{H}.$$

Clearly, a sufficient abstract definition is provided by 1.11, 1.12, and

$$S_i^{-1} T_j^{-1} S_i T_j = E \quad (i = 1, \dots, m; j = 1, \dots, n).$$

However, in many cases the number of generators may be reduced and the relations simplified. As an example, consider the cyclic groups \mathfrak{C}_3 and \mathfrak{C}_2 , defined by the respective relations

$$S^3 = E \text{ and } T^2 = E.$$

Their direct product $\mathfrak{C}_3 \times \mathfrak{C}_2$, of order 6, has the abstract definition 1.16; but it is also generated by the single element $R = ST$ and defined by the single relation 1.15, which shows that $\mathfrak{C}_3 \times \mathfrak{C}_2 \cong \mathfrak{C}_6$. More generally, the direct product of cyclic groups of orders q and r is an Abelian group $\mathfrak{C}_q \times \mathfrak{C}_r$, of order qr , which is cyclic if q and r are coprime:

$$\mathfrak{C}_q \times \mathfrak{C}_r \cong \mathfrak{C}_{qr}, \quad (q, r) = 1.$$

Still more generally, if p, q, \dots are distinct primes, any Abelian group of order

$$p^\alpha q^\beta \dots$$

is a direct product

$$\mathfrak{G}_{p^\alpha} \times \mathfrak{G}_{q^\beta} \times \dots$$

of Abelian p -groups (BURNSIDE 1911, pp. 100—107), and every such p -group is a direct product of cyclic groups:

$$\mathfrak{G}_{p^\alpha} \cong \mathfrak{C}_{p^{\alpha_1}} \times \mathfrak{C}_{p^{\alpha_2}} \times \dots,$$

where

$$\alpha = \alpha_1 + \alpha_2 + \dots$$

This p -group is described as the Abelian group of order p^α and type $(\alpha_1, \alpha_2, \dots)$; in particular, the direct product of α cyclic groups of order p is the Abelian group of order p^α and type $(1, 1, \dots, 1)$:

$$\mathfrak{C}_p^\alpha \cong \mathfrak{C}_p \times \mathfrak{C}_p \times \dots \times \mathfrak{C}_p.$$

Combining the above results, we see that every finite Abelian group is a direct product of cyclic groups.

The infinite cyclic group \mathfrak{C}_∞ is generated by a single element X without any relations. Thus it is the same as the free group \mathfrak{F}_1 on one generator. The inverse X^{-1} is the only other element that will serve as a generator. The direct product

$$\mathfrak{C}_\infty^2 \cong \mathfrak{C}_\infty \times \mathfrak{C}_\infty$$

of two infinite cyclic groups is defined by the single relation

$$XY = YX. \quad (1.31)$$

Its finite factor groups are obtained by adding relations of the type

$$X^b Y^c = E.$$

For example, in the Abelian group

$$X^b Y^c = X^{-c} Y^b = E, \quad XY = YX, \quad (1.32)$$

we have

$$X^c = Y^b, \quad X^c = Y^{bc} = X^{-b^2},$$

and therefore $X^n = E$, where $n = b^2 + c^2$. Suppose $(b, c) = d = \gamma b - \beta c$. Then X^d is a power of Y , namely

$$X^d = X^{\gamma b - \beta c} = Y^{-(\beta b + \gamma c)}.$$

Also

$$Y^b = X^c = Y^{-c(\beta b + \gamma c)/d} = Y^{b - \gamma n/d},$$

$$Y^c = X^{-b} = Y^{b(\beta b + \gamma c)/d} = Y^{c + \beta n/d}.$$

Since $(\beta, \gamma) = 1$, the period of Y divides n/d , and any element of the group is expressible as

$$X^x Y^y \quad (0 \leq x < d, 0 \leq y < n/d).$$

Consider the direct product $\mathfrak{C}_d \times \mathfrak{C}_{n/d}$ in the form

$$Z^d = Y^{n/d} = E, \quad ZY = YZ.$$

The element $X = ZY^{-(\beta b + \gamma c)/d}$ satisfies $XY = YX$ and

$$X^b Y^c = Z^b Y^{(-b(\beta b + \gamma c) + c(\gamma b - \beta c))/d} = Z^b Y^{-\beta n/d} = E,$$

$$X^{-c} Y^b = Z^{-c} Y^{(c(\beta b + \gamma c) + b(\gamma b - \beta c))/d} = Z^{-c} Y^{\gamma n/d} = E.$$

Hence our original group $\{X, Y\}$ is $\mathfrak{C}_d \times \mathfrak{C}_{n/d}$, the direct product of cyclic groups generated by

$$XY^{(\beta b + \gamma c)/d} \text{ and } Y.$$

It can be shown similarly that the Abelian group

$$X^c = Y^b = X^{-b} Y^{-c}, \quad XY = YX$$

or

$$Y^c = Z^b, \quad Z^c = X^b, \quad X^c = Y^b, \quad XYZ = ZYX = E \quad (1.33)$$

is $\mathfrak{G}_d \times \mathfrak{G}_{t/d}$, the direct product of cyclic groups generated by

$$XY^{(\beta b + \gamma c)/d} \text{ and } Y,$$

where $t = b^2 + bc + c^2$ and $d = (b, c) = \gamma b - \beta c$ (FRUCHT 1955, p. 12).

1.4 Automorphisms. Consider again the group $\mathfrak{G} \cong \{S_1, S_2, \dots, S_m\}$ defined by 1.11. Suppose it contains m elements S'_1, S'_2, \dots, S'_m which satisfy the same relations:

$$g_k(S'_1, S'_2, \dots, S'_m) = E \quad (k = 1, 2, \dots, s).$$

Then the correspondence

$$S_i \rightarrow S'_i \quad (i = 1, 2, \dots, m)^* \quad (1.41)$$

defines an *automorphism* of \mathfrak{G} if the elements S'_i are a set of generators, i.e., if every S_i can be expressed in terms of them.

One fruitful method for deriving a larger group \mathfrak{G}^* from a given group \mathfrak{G} is to adjoin a new element T , of period ac (say), which transforms the elements of \mathfrak{G} according to an automorphism of period c . If we identify T^c with an element U of period a in the centre of \mathfrak{G} , the order of \mathfrak{G}^* is evidently c times that of \mathfrak{G} . If the automorphism is given by 1.41, the larger group is defined by the relations 1.11 and

$$T^{-1}S_iT = S'_i, \quad T^c = U. \quad (1.42)$$

This procedure is easily adapted to infinite groups. Although a may be infinite, \mathfrak{G} is still a normal subgroup of index c in \mathfrak{G}^* .

In the case of an *inner* automorphism, \mathfrak{G} contains an element R such that, for every S in \mathfrak{G} ,

$$R^{-1}SR = T^{-1}ST,$$

i.e., $TR^{-1}S = STR^{-1}$. Thus the element

$$Z = TR^{-1} = R^{-1}T$$

of \mathfrak{G}^* commutes with every element of \mathfrak{G} . The lowest power of Z that belongs to \mathfrak{G} is

$$V = Z^c = UR^{-c},$$

of period b , say. V , like Z , commutes with every element of \mathfrak{G} ; since it belongs to \mathfrak{G} , it belongs to the centre.

If $(b, c) = 1$ (for instance, if b is prime to the order of the centre, as in COXETER 1939, p. 90), consider integers β, γ , such that

$$\gamma b - \beta c = 1.$$

Instead of adjoining T to \mathfrak{G} , we could just as well adjoin $Z = TR^{-1}$, or adjoin

$$ZV^\beta = Z^{1+\beta c} = Z^{\gamma b},$$

whose c th power is

$$Z^{rbc} = V^{rb} = E$$

(since $V^b = E$). Hence in this case

$$\mathfrak{G}^* \cong \mathfrak{G} \times \mathfrak{C}_c, \quad (1.43)$$

where \mathfrak{C}_c is the cyclic group generated by Z^{rb} .

1.5 Some well-known finite groups. The cyclic group \mathfrak{C}_q , defined by the single relation

$$S^q = E, \quad (1.51)$$

admits an outer automorphism of period 2 with transforms every element into its inverse. Adjoining a new element R_1 , of the same period, which transforms \mathfrak{C}_q according to this automorphism, we obtain the *dihedral* group \mathfrak{D}_q , of order $2q$, defined by 1.51 and

$$R_1^{-1} S R_1 = S^{-1}, \quad R_1^2 = E,$$

that is,

$$S^q = R_1^2 = (S R_1)^2 = E. \quad (1.52)$$

The same group \mathfrak{D}_q is equally well generated by the elements R_1 and $R_2 = R_1 S$, in terms of which its abstract definition is

$$R_1^2 = R_2^2 = (R_1 R_2)^q = E. \quad (1.53)$$

The "even" dihedral group \mathfrak{D}_{2m} , defined by 1.53 with $q = 2m$, has a centre of order 2 generated by $Z = (R_1 R_2)^m$. If m is odd, the two elements R_1 and $R = R_2 Z$ satisfy the relations

$$R_1^2 = R^2 = (R_1 R)^m = E,$$

so that $\{R_1, R\}$ is \mathfrak{D}_m , and we have

$$\mathfrak{D}_{2m} \cong \mathfrak{C}_2 \times \mathfrak{D}_m \quad (m \text{ odd}). \quad (1.54)$$

Since \mathfrak{D}_{2m} (m odd) can be derived from \mathfrak{D}_m by adjoining R_2 , which transforms \mathfrak{D}_m in the same manner as R , we see that 1.54 is an example of 1.43 (with $a = b = 1$, $c = 2$, $\beta = \gamma = -1$, $T = R_2$, $U = V = E$).

When $m = 1$, 1.54 is the *four-group*

$$\mathfrak{D}_2 \cong \mathfrak{C}_2 \times \mathfrak{D}_1 \cong \mathfrak{C}_2 \times \mathfrak{C}_2,$$

defined by

$$R_1^2 = R_2^2 = (R_1 R_2)^2 = E.$$

In terms of the three generators R_1 , R_2 and $R_0 = R_1 R_2$, these relations become

$$R_0^2 = R_1^2 = R_2^2 = R_0 R_1 R_2 = E. \quad (1.55)$$

In this form, \mathfrak{D}_3 clearly admits an outer automorphism of period 3 which cyclically permutes the three generators. Adjoining a new element S which transforms \mathfrak{D}_3 in this manner, we obtain a group of order 12 defined by 1.55 and

$$S^3 = E, \quad S^{-i} R_0 S^i = R_i \quad (i = 1, 2).$$

The same group is generated by S and R_0 , in terms of which it has the abstract definition

$$S^3 = R_0^3 = (S R_0)^3 = E. \quad (1.56)$$

Since the permutations $S = (1\ 2\ 3)$ and $R_0 = (1\ 2)(3\ 4)$ generate the alternating group \mathfrak{A}_4 of order 12 and satisfy the relations 1.56, we conclude that the group defined by these relations is \mathfrak{A}_4 . The above derivation shows that \mathfrak{A}_4 contains \mathfrak{D}_3 as a normal subgroup.

\mathfrak{A}_4 is equally well generated by S and $U = S^{-1} R_0$, in terms of which its definition is

$$S^3 = U^3 = (S U)^2 = E. \quad (1.57)$$

Clearly, \mathfrak{A}_4 admits an outer automorphism of period 2 which interchanges the generators S and U . Adjoining such an element T , we obtain a group of order 24 defined by 1.57 and

$$T^2 = E, \quad T S T = U. \quad (1.58)$$

In terms of the generators S and T , this group is defined by

$$S^3 = T^2 = (S T)^4 = E. \quad (1.59)$$

Since the permutations $S = (2\ 3\ 4)$, $T = (1\ 2)$, which generate the symmetric group \mathfrak{S}_4 of order 24, satisfy 1.59, we conclude that the group defined by these relations is \mathfrak{S}_4 . In terms of the generators S and $U = S^{-1} T$, \mathfrak{S}_4 is defined by

$$S^3 = U^4 = (S U)^2 = E.$$

1.6 Dicyclic groups. When q is even, say $q = 2m$, the automorphism $S \rightarrow S^{-1}$ of \mathfrak{C}_q can be used another way. Adjoining to

$$S^{2m} = E \quad (1.61)$$

a new element T , of period 4, which transforms S into S^{-1} while its square is S^m , we obtain the dicyclic group $\langle 2, 2, m \rangle$, of order $4m$, defined by 1.61 and

$$T^2 = S^m, \quad T^{-1} S T = S^{-1}.$$

Since the last relation may be written as $(S T)^2 = T^2$, S and T satisfy

$$S^m = T^2 = (S T)^2. \quad (1.62)$$

To show that these two relations suffice to define $\langle 2, 2, m \rangle$, we observe that they imply

$$S^m = T^2 = T^{-1} T^2 T = T^{-1} S^m T = (T^{-1} S T)^m = S^{-m},$$

which is 1.61 (COXETER 1940c, p. 372; cf. MILLER, BLICHFELDT and DICKSON 1916, p. 62).

In terms of the three generators S , T , and $R = ST$, $\langle 2, 2, m \rangle$ is defined by the relations

$$R^2 = S^m = T^2 = RST, \quad (1.63)$$

or in terms of R and T alone:

$$R^2 = T^2 = (R^{-1} T)^m. \quad (1.64)$$

Of course, the symbol $\langle 2, 2, m \rangle$ could just as well have been written as $\langle m, 2, 2 \rangle$ or $\langle 2, m, 2 \rangle$. Other groups $\langle l, m, n \rangle$ will be discussed in § 6.5.

1.7 The quaternion group. The smallest dicyclic group

$$\mathfrak{Q} \cong \langle 2, 2, 2 \rangle,$$

called the *quaternion* group, is defined by $S^2 = T^2 = (ST)^2$ or

$$R^2 = S^2 = T^2 = RST. \quad (1.71)$$

Note the resemblance to the famous formula

$$i^2 = j^2 = k^2 = ijk = -1$$

of HAMILTON (1856, p. 446).

\mathfrak{Q} is the smallest *Hamiltonian* group, that is, it is the smallest non-Abelian group all of whose subgroups are normal. In fact, the Hamiltonian groups are precisely the groups of the form

$$\mathfrak{Q} \times \mathfrak{A} \times \mathfrak{B},$$

where \mathfrak{A} is an Abelian group of odd order, and \mathfrak{B} is an Abelian group of order 2^m ($m \geq 0$) and type $(1, 1, \dots, 1)$ (HILTON 1908, p. 177; CAR-MICHAEL 1937, p. 114; ZASSENHAUS 1937, p. 123; SCORZA 1942, p. 89).

\mathfrak{Q} is also the smallest group of *rank* 1, that is, it is the smallest non-Abelian group all of whose proper subgroups are Abelian. The groups of rank 1 have been investigated by MILLER and MORENO (1903), SCHMIDT (1924) and REDEI (1947). REDEI showed that, apart from \mathfrak{Q} , every such group belongs to one of three well-defined families. It thus appears that \mathfrak{Q} is the only finite non-Abelian group all of whose proper subgroups are Abelian and normal.

1.8 Cyclic extensions of cyclic groups. If $(q, r) = 1$, the cyclic group 1.51 admits an automorphism

$$S \rightarrow S^r, \quad (1.81)$$

whose period c is the exponent to which r belongs modulo q , so that

$$r^c \equiv 1 \pmod{q}.$$

We derive a group of order qc by adjoining a new element T , of period a (where a divides both q and $r-1$), such that

$$T^{-1}ST = S^r, \quad T^a = S^{q/a}.$$

Writing $m = q/a$, we have the abstract definition

$$S^m = T^c = U, \quad U^a = E, \quad T^{-1}ST = S^r \quad (1.82)$$

(implying $U^r = S^{rm} = (T^{-1}ST)^m = T^{-1}UT = U$) for this group of order mac . (When $c = 2$ and $r = -1$, the group is dihedral or dicyclic according as $a = 1$ or $a = 2$.)

These relations can be simplified if

$$(a, m) = 1.$$

For if $\mu a + \alpha m = 1$, we have

$$S = S^{\mu a + \alpha m} = S^{\mu a} U^{\alpha} = (S^a)^{\mu} T^{c\alpha},$$

so that 1.82 is generated by $S_1 = S^a$ and T , in terms of which it has the abstract definition

$$S_1^m = T^{ac} = E, \quad T^{-1}S_1T = S_1^r.$$

Dropping the subscript, we are thus led to consider the group

$$S^m = T^n = E, \quad T^{-1}ST = S^r, \quad (1.83)$$

of order mn , derived from \mathfrak{C}_m by adjoining T , of period n , which transforms \mathfrak{C}_m according to the automorphism 1.81, of period c . The new feature is that we no longer identify T^c with an element of \mathfrak{C}_m . Since

$$S^{rm} = T^{-n}ST^n = S,$$

the consistency of the relations 1.83 requires

$$r^m \equiv 1 \pmod{m}; \quad (1.84)$$

i.e., n must be a multiple of the exponent to which r belongs modulo m (CARMICHAEL 1937, p. 176). Thus 1.83 is a factor group of

$$T^n = E, \quad T^{-1}ST = S^r \quad (1.85)$$

(where r may be positive or negative). The group 1.85 is infinite if $r^n = 1$, and of order

$$n \cdot |r^n - 1|$$