A practical method for enumerating cosets of a finite abstract group

By J. A. Todd (University of Manchester), and
H. S. M. Coxeter (University of Cambridge).

(*Received 22nd January,* 1936. *Read 7th February,* 1936.)

Introduction.

An important problem in finite-group theory is the determination of an *abstract definition* for a given group $\mathfrak{G}$, that is, a set of relations

$$f_i(S_1, \ldots, S_k) = E, \qquad (i = 1, \ldots, n) \tag{1}$$

between k generating operations $S_1, \ldots, S_k$ of $\mathfrak{G}$, such that every other relation between $S_1, \ldots, S_k$ is an algebraic consequence of (1).

The number of groups for which abstract definitions are actually known is relatively small, but a remarkable feature of the results already obtained is the extreme simplicity of the relations (1) in the case of several groups of quite high order. This fact constitutes an additional incentive to the search for abstract definitions, and many elegant results have doubtless yet to be discovered.

Of the various methods which have hitherto been employed to obtain abstract definitions, one only, that of enumeration by cosets, is of general application. This method has been employed with limited success hitherto, for in all but the simplest cases it has involved considerable manipulative ingenuity, and for many groups of moderately high order the length of the necessary calculations makes the method impracticable. The aim of the present paper is to show that such calculations can be dispensed with entirely; in fact, the method can be reduced to a purely mechanical process, which becomes a useful tool with a wide range of application. Bearing in mind what we have said above concerning the simplicity of the abstract definitions of many known groups, we venture to predict that our method will prove quite practicable for most groups (at any rate such as occur naturally in geometry or analysis) of order less than a thousand, and for many groups of much higher order.

https://doi.org/10.1017/S0013091500008221 Published online by Cambridge University Press

The first section of the paper gives an outline of the theory underlying the "method of cosets"; our rationalisation of the technique is described in § 2. The rest of the paper is devoted to illustrative examples, some being known definitions of groups and others being new. We have tested the method by verifying a large number of other abstract definitions, but space does not permit us to give details.

§ 1. The method of "enumeration by cosets" must in principle date back to the earliest years of abstract group-theory, but it first seems to have been seriously exploited with a view to obtaining abstract definitions by Moore and Dickson[1]. The principle of the method is as follows. A group $\mathfrak{G}$, of order g, being given, the equations (1) are proposed as an abstract definition of $\mathfrak{G}$. In practice, these equations are obtained by taking a set of generators of $\mathfrak{G}$ and noting down some of the relations satisfied by them. We naturally select as far as possible relations of a simple form, such as those which express the periods of the generators or of simple combinations of them. The number of such relations which will be necessary to define $\mathfrak{G}$ is a matter for experiment, and the "method of cosets" is the way we test the success of the experiment. In this (or some other) manner we verify that $\mathfrak{G}$ possesses a set of generators which satisfy (1). It follows that the abstract group $\mathfrak{G}'$ defined by (1) either coincides with $\mathfrak{G}$ or possesses an invariant sub-group $\mathfrak{G}_1$ such that the factor-group $\mathfrak{G}'/\mathfrak{G}_1$ is simply isomorphic with $\mathfrak{G}$. If then we can verify that the order of $\mathfrak{G}'$ does not exceed g, it follows that $\mathfrak{G}'$ is simply isomorphic with $\mathfrak{G}$. To verify whether this is or is not the case, we pick out a sub-set $T_1, \ldots, T_l$ of operations of $\mathfrak{G}'$ (in an extreme case the set might consist merely of the identity) such that the relations (1) imply the relations

$$\phi_j(T_1, \ldots, T_l) = E, \qquad (j = 1, \ldots, m) \qquad (2)$$

which are already known to be the abstract definition of a group $\mathfrak{H}'$ of order $h < g$. Conceivably the relations (1) imply other relations between the T's independent of (2), in which case the sub-group $\mathfrak{H}$ of $\mathfrak{G}'$ generated by the T's will not be $\mathfrak{H}'$ but some factor-group $\mathfrak{H}'/\mathfrak{H}_1$. In all cases the order of $\mathfrak{H}$ is at most h. We now consider the sets of operations $S\mathfrak{H}$, got by multiplying the operations of $\mathfrak{H}$ on the left by

[1] See, *e.g.*, Moore, *Proc. London Math. Soc.* (1), 28 (1897) 357-366; Dickson, *Linear Groups* (Leipzig, 1901).

the various elements of $\mathfrak{G}'$. Two such sets either coincide or have no common member, and every operation of $\mathfrak{G}'$ belongs to at least one such set. If then we can show that of these sets only g/h are distinct, it follows that the order of $\mathfrak{G}'$ is at most $h.g/h = g$, and hence that $\mathfrak{G}'$ is simply isomorphic with $\mathfrak{G}$. The method further gives a representation of $\mathfrak{G}$ as a permutation group on the g/h cosets, but it may be remarked that the isomorphism between $\mathfrak{G}$ and this permutation group may well be multiple[1].

To avoid the complications involved in carrying out this process in practice, we are always careful to choose $\mathfrak{H}$ to have as large an order as possible, *i.e.* to make g/h as small as we can. Even so, the task of showing the existence of just g/h cosets which are permuted among themselves by $S_1, \ldots, S_k$ would be impracticable in all but the simplest cases without some systematic technique. Such a technique, obviating calculation of any kind, will now be described.

§ 2. Let us write a typical one of the relations (1) in the form

$$T_c \ldots . T_2 T_1 = E, \tag{3}$$

where $T_1, \ldots, T_c$ are certain of the generators and their inverses, repeated if necessary. We denote the g/h cosets (in an order to be defined presently) by the numbers $1, 2, \ldots, g/h$. For each of the n relations (1) we gradually construct a table of cosets with g/h columns and $c+1$ rows, c being the number of operations in the expression (1) when written in the form (3). Each row contains every coset just once, and the first and last rows are identical. The rows, except the first, are labelled in order, $T_1, T_2, \ldots, T_c$, and in any part of the table, a coset in the pth row is obtained from the coset immediately above it by (left) multiplication with T_{p-1}, or from the coset immediately below it by multiplication with T_p^{-1}. The coset 1 is defined as the set of operators of the sub-group $\mathfrak{H}$, and the coset 2 as the set $S_a.1$ where S_a is a suitably chosen generator of $\mathfrak{G}'$ not belonging to $\mathfrak{H}$. Now, and hereafter, we fill up as much as possible of all the tables before introducing any new coset. Thus, before defining the coset 3 we make sure that every row of each table shall contain both 1 and 2. We next define a new coset by inserting the symbol 3 in any vacant space immediately above or below a 1 or a 2, and fill up as much as possible of the tables as before. We then insert 4, and so on. Whenever a column in one of the tables becomes complete,

[1] See, *e.g.*, Burnside, *Theory of Groups*, 2nd Ed. (Cambridge, 1911), Ch. XII.

some additional information is obtained, which in turn enables us to fill other columns. When all the tables are complete the process is at an end.

In the course of the work it may happen that the information given by the completion of a column implies that two of the numbers in the table represent the same coset. (In actual practice this occurs rather infrequently, and is soon detected). In that case we replace the larger of the two numbers by the smaller throughout, and note any other coincidences which may be involved. When all these have been adjusted we can proceed in the usual manner. If these coincidences ultimately involve the collapse of the whole table, it is a sign that the relations (1) are *inconsistent*[1].

If there is a generator S whose order is not directly specified by the relations (3), it is desirable, for purposes of reference, to construct an auxiliary table of two rows to record the effect of multiplying each coset by S. If any one of the relations (1) is of the form $(S_p S_q \ldots . S_r)^\lambda = E$, then the number of columns in the table may be reduced, since most of them occur in several trivially distinct forms.

If the proposed relations are insufficient to define $\mathfrak{G}$, the tables will fail to close up after g/h cosets have been introduced. If conversely the table fails to close when these cosets have been defined, then either the relations (1) are insufficient to determine $\mathfrak{G}$, or else there are some undiscovered coincidences between the cosets already introduced. If the tables are "nearly" complete, it is probably the latter circumstance that has occurred, and the introduction of a few more cosets will demonstrate the coincidences. If on the other hand there are large gaps in the table, it is a sign that the relations (1) are probably insufficient to define $\mathfrak{G}$. In that case, since $\mathfrak{G}'$ contains a factor-group simply isomorphic with $\mathfrak{G}$, its order must be at least $2g$, and hence the table cannot close with less than double the number of columns.

Note.—The arrangement of rows and columns explained above depends on regarding the elements of the group as left operators, and corresponding tables of columns and rows could be made for right operators, with the formal advantage that the headings of the columns (formerly rows) are then written out from left to right as they stand in (3), instead of from bottom to top.

[1] We use this word by analogy with the case of a set of homogeneous linear equations whose only solution is the trivial one: 0, 0, ..., 0.

§ 3. In further explanation we propose to give a few examples. We start by using the method to show that the relations

$$S^5 = T^3 = (ST)^2 = E \tag{4}$$

define a group of order 60 (the icosahedral group). As this is a well-known result we omit the verification that the group in question possesses generators satisfying (4), and proceed at once to the construction of the table.

We take for $\mathfrak{H}$ the cyclic group of order five generated by S. We have three tables to construct, corresponding to the three relations (4); as each of these relations expresses the order of a function of the generators, the number of columns is less than twelve.

	1	2	7	12
S	1	3	9	12
S	1	4	10	12
S	1	5	11	12
S	1	6	8	12
S	1	2	7	12

	1	2	5	6	8	11
T	2	3	8	7	9	12
S	3	4	7	9	10	12
T	1	6	4	5	11	10
S	1	2	5	6	8	11

	1	4	5	10
T	2	6	8	11
T	3	7	9	12
T	1	4	5	10

The set 1 being $\{S\}$, it is invariant on multiplication with S, and so the first column of the S table is given at once. We define 2 as $T \,.\, 1$ and 3 as $T \,.\, 2$. The T table then shows that $T \,.\, 3 = 1$, and the ST table gives $S \,.\, 2 = 3$. We now define $S \,.\, 3 = 4$, $S \,.\, 4 = 5$, $S \,.\, 5 = 6$, so that $S \,.\, 6 = 2$. The ST table then gives $T \,.\, 4 = 6$. We now define 7 as $T \,.\, 6$. Then $T \,.\, 7 = 4$. Put $8 = T \,.\, 5$. Then the ST table gives $S \,.\, 8 = 7$. If 9 is $T \,.\, 8$ then $T \,.\, 9 = 5$, and the ST table gives $S \,.\, 7 = 9$. Next put $S \,.\, 9 = 10$, $S \,.\, 10 = 11$. Then from the S table, $S \,.\, 11 = 8$, and from the ST table $T \,.\, 10 = 11$. Put now $12 = T \,.\, 11$. From the T table $T \,.\, 12 = 10$, and from the ST table $S \,.\, 12 = 12$. All the tables are now complete, and the verification that there are only twelve cosets is accomplished.

It should be noticed that the table itself contains all the necessary "working," and no auxiliary calculations are necessary. The reader may convince himself of this by constructing the tables for the following groups, neither of which is of large order. He will, we believe, soon be convinced that the method we have explained avoids the manipulative ingenuity usually associated with work of this description.

$$G_{168}: S^7 = T^4 = (ST)^2 = (S^{-1}T)^3 = E.$$
$$G_{80}: S^5 = T^5 = (ST)^2 = (S^{-1}T^{-1}ST)^2 = E.$$

In the two examples which follow, the explanation is confined to a note of the definitions of the successive cosets.

As an example of a group where the tables involve rather more columns, we show that *the relations*

$$S^5 = T^5 = (ST)^2 = (S^{-1}T)^4 = E \tag{5}$$

define a group of order 360, *simply isomorphic with the alternating group of degree six.* As permutations of the letters a, b, c, d, e, f, we may take $S = (abcde)$, $T = (afedc)$. These satisfy (5) and generate the alternating group. We take as the subgroup $\mathfrak{H}$ the cyclic G_5 generated by S. The tables, and the definitions of the cosets, are as follows.

	1	2	3	4	8	9	10	13	18	19	23	24	28	29	33	49
S	1	5	6	21	20	14	31	36	45	51	50	24	66	39	53	58
S	1	11	26	56	41	34	61	69	38	47	64	24	72	44	59	63
S	1	16	46	37	17	54	67	62	60	30	57	24	70	71	48	68
S	1	7	22	12	15	32	27	35	52	42	25	24	40	43	55	65
S	1	2	3	4	8	9	10	13	18	19	23	24	28	29	33	49

	1	6	11	16	21	26	31	36	41	46	51	56	61	66	71	72
T	2	7	12	17	22	27	32	37	42	47	52	57	62	67	71	72
T	3	8	13	18	23	28	33	38	43	48	53	58	63	68	71	72
T	4	9	14	19	24	29	34	39	44	49	54	59	64	69	71	72
T	5	10	15	20	25	30	35	40	45	50	55	60	65	70	71	72
T	1	6	11	16	21	26	31	36	41	46	51	56	61	66	71	72

	1	2	3	4	7	8	9	10	12	13	15	17	18	19	22	23	25	27
T	2	3	4	5	8	9	10	6	13	14	11	18	19	20	23	24	21	28
S	5	6	21	11	20	14	31	26	36	34	16	45	51	41	50	24	56	66
T	1	7	22	12	16	15	32	27	37	35	17	41	52	42	46	25	57	67
S	1	2	3	4	7	8	9	10	12	13	15	17	18	19	22	23	25	27

	28	29	30	32	33	35	37	38	40	43	47	48	49	52	57	62	65	70
T	29	30	26	33	34	31	38	39	36	44	48	49	50	53	58	63	61	66
S	39	42	46	53	54	61	60	44	69	71	55	58	64	59	63	68	67	72
T	40	43	47	54	55	62	56	45	70	71	51	59	65	60	64	69	68	72
S	28	29	30	32	33	35	37	38	40	43	47	48	49	52	57	62	65	70

	1	2	3	6	8	9	11	14	18	21	23	26	28	29	31	34	36	61
T	2	3	4	7	9	10	12	15	19	22	24	27	29	30	32	35	37	62
S^{-1}	7	22	12	16	32	27	37	17	42	46	24	67	43	47	54	62	56	69
T	8	23	13	17	33	28	38	18	43	47	25	68	44	48	55	63	57	70
S^{-1}	15	25	35	41	55	40	45	52	71	51	57	63	39	59	48	58	64	72
T	11	21	31	42	51	36	41	53	71	52	58	64	40	60	49	59	65	72
S^{-1}	5	4	10	30	19	13	20	33	44	60	49	50	70	38	65	53	68	66
T	1	5	6	26	20	14	16	34	45	56	50	46	66	39	61	54	69	67
S^{-1}	1	2	3	6	8	9	11	14	18	21	23	26	28	29	31	34	36	61

The coset 1 is the set $\{S\}$, and the others are defined as follows:

$n + 1 = T \,.\, n$ except in the following cases;

$6 = S \,.\, 3$, $\quad 11 = S \,.\, 5$, $\quad 16 = S \,.\, 11$, $\quad 21 = S \,.\, 4$, $\quad 26 = S \,.\, 6$,
$31 = S \,.\, 10$, $\quad 36 = S \,.\, 13$, $\quad 41 = S \,.\, 20$, $\quad 46 = S \,.\, 26$, $\quad 51 = S \,.\, 19$,
$56 = S \,.\, 21$, $\quad 61 = S \,.\, 31$, $\quad 66 = S \,.\, 28$, $\quad 71 = S \,.\, 44$, $\quad 72 = S \,.\, 66$.

The table contains all the necessary working, except that where two columns of the table are found to be identical save for a cyclic permutation of the sets, we have only written one of them.

The reader may find it a useful exercise to verify that the relations

$$S^{11} = T^2 = (ST)^3 = (S^3 T)^5 = (S^4 T)^5 = E$$

define a group of order 660 (actually the simple group of this order) by taking 1 as the coset formed by S and its powers and showing that all the tables are complete when 60 cosets have been introduced.

Our final example is of a group with three generators. We shall use the method to show that the relations

$$S_1^3 = S_2^2 = S_3^2 = (S_1 S_2)^4 = (S_1 S_3)^2 = (S_2 S_3)^3 = E \tag{6}$$

define the group [3, 4, 3]′, of order 576. This is the group of rotations of the regular 24-cell in four dimensions, and this definition was originally obtained by the "method of cosets" involving calculations

https://doi.org/10.1017/S0013091500008221 Published online by Cambridge University Press

which could not be printed. The notation here agrees with that used previously[1].

We take for $\mathfrak{H}$ the group generated by S_1 and S_2, subject to the relations

$$S_1^3 = S_2^2 = (S_1 S_2)^4 = E$$

which define the octahedral group of order 24, choosing this in preference to that generated by other pairs of the operations because it has a larger order. The other cosets are defined thus:

$2 = S_3 . 1$, $3 = S_2 . 2$, $4 = S_1 . 3$, $5 = S_1 . 4$, $6 = S_2 . 4$, $7 = S_2 . 5$, $8 = S_1 . 7$, $9 = S_2 . 8$, $10 = S_3 . 6$, $11 = S_3 . 7$, $12 = S_3 . 8$, $13 = S_3 . 9$, $14 = S_2 . 12$, $15 = S_2 . 13$, $16 = S_1 . 14$, $17 = S_1 . 16$, $18 = S_1 . 15$, $19 = S_1 . 18$, $20 = S_2 . 18$, $21 = S_2 . 19$, $22 = S_1 . 21$, $23 = S_2 . 22$, $24 = S_3 . 23$.

The tables are as follows:

	1	2	3	6	9	10	13	14	15	20	23	24
S_1	1	2	4	7	9	12	13	16	18	21	23	24
S_1	1	2	5	8	9	11	13	17	19	22	23	24
S_1	1	2	3	6	9	10	13	14	15	20	23	24

	1	2	4	5	8	10	12	13	16	18	19	22	24
S_2	1	3	6	7	9	11	14	15	17	20	21	23	24
S_2	1	2	4	5	8	10	12	13	16	18	19	22	24

	1	3	4	6	7	8	9	14	16	17	20	22	23
S_3	2	3	5	10	11	12	13	15	19	18	21	22	24
S_3	1	3	4	6	7	8	9	14	16	17	20	22	23

	1	2	5	10	11	13	17	19	24
S_2	1	3	7	11	10	15	16	21	24
S_1	1	4	8	10	12	18	17	22	24
S_2	1	6	9	11	14	20	16	23	24
S_1	1	7	9	10	16	21	17	23	24
S_2	1	5	8	11	17	19	16	22	24
S_1	1	3	6	10	14	15	17	20	24
S_2	1	2	4	11	12	13	16	18	24
S_1	1	2	5	10	11	13	17	19	24

[1] Todd, *Proc. Camb. Phil. Soc.*, 27 (1931), 221.

	1	4	5	8	9	16	17	22
S_3	2	5	4	12	13	19	18	22
S_2	3	7	6	14	15	21	20	23
S_3	3	11	10	15	14	20	21	24
S_2	2	10	11	13	12	18	19	24
S_3	1	6	7	9	8	17	16	23
S_2	1	4	5	8	9	16	17	22

	1	3	5	6	7	8	9	14	15	17	20	21	23
S_3	2	3	4	10	11	12	13	15	14	18	21	20	24
S_1	2	4	5	12	10	11	13	18	16	19	22	21	24
S_3	1	5	4	8	6	7	9	17	19	16	22	20	23
S_1	1	3	5	6	7	8	9	14	15	17	20	21	23

https://doi.org/10.1017/S0013091500008221 Published online by Cambridge University Press