Abstract Groups Defined by Generating Operators

BY A. SINKOV

Unclassified

This paper explains and illustrates the concept of an abstract group. It shows how such a group can be defined in terms of conditions satisfied by a set of generating operations. The enumerative method of determining the order of a group defined in such a way can be made automatic.

A few months ago, we had the privilege in the CMI of hearing a talk by Professor Albert on "Groups with two Generators." This talk aroused in me memories of the early 30's when I was a graduate student, and of the years immediately following, when I did some research in the general field of defining groups in terms of generating operations. My doctorate thesis had concerned a problem in this area and I published some papers on the subject in the middle and late 30's. I was stimulated by Professor Albert's talk to address the Institute on some phase of this same general problem. And yet I was somewhat hesitant to do so, because I could not think of any application of this subject to cryptology. In fact, there are very few instances of any general applicability of abstract group theory to our field of effort. Some studies have been made of problems in the theory of wired rotors, using group theoretic concepts, but they have produced no cryptanalytically significant results.

The most interesting application of group theory that I can recall was one which utilized to advantage the notation of group theory rather than techniques therefrom. It was a method for solving double transpositions which was developed in the Signal Intelligence Service in the early 30's. Its importance stemmed from the fact that soon after the method had been worked out we had occasion to apply it against a double transposition system being used by rum runners on the West Coast. The system was one which used the same columnar transposition key twice. The text was sent in four-letter groups. To ensure that the cipher had four letters in every group, the last group was filled out with X's before transposition. We were enabled by this fact alone to solve the system. The method of solution depended on guessing correctly the location in the original message of some of the cipher letters, and the X's used as nulls obviously had to go at the end of the plain text. I can still recall with what great glee we used to seize on the messages containing X's. They yielded very easily—especially in the instance that none of the X's in the message was textual. Interesting as this example is—and its exposition might make a worth while subject for the CMI—it would not by itself justify using a general topic in group theory for a talk on cryptomathematics.

I have rationalized away my hesitation about presenting a paper on groups generated by two operators because I thought a basic exposition on group theoretic method might be of general interest and because the main idea presented in this talk has interest from the point of view of manipulative method.

In order that you may appreciate what is meant by a group, I shall give a few simple examples. Consider first a type of example with which you are all familiar: the idea of monoalphabetic substitution. And to keep the example very simple, we will suppose that we are dealing with an alphabet of only three letters. In such a limited situation, we can write down every possible monoalphabet. There are only six possibilities which I will call *E, S, T, U, V, W*.

$$\begin{array}{ccccccccc}
 & A & B & C & \quad & & A & B & C \\
E & A & B & C & & U & A & C & B \\
 & A & B & C & & & A & B & C \\
S & B & C & A & & V & B & A & C \\
 & A & B & C & & & A & B & C \\
T & C & A & B & & W & C & B & A
\end{array}$$

The following properties of these substitutions are fairly obvious:

1. If we apply one of the substitutions to textual material, and then superimpose a second substitution (which may or may not be the same as the first), the result of the two steps can be obtained by a properly selected single substitution. Only a moment's trial is required to see which substitution is the equivalent of two of these substitutions applied successively. For example, *S* followed by *V* is the same as *U*.

2. There is a substitution which produces no change whatever. If we replace *A* by *A*, *B* by *B*, *C* by *C*, the cipher is the same as the plain. This identity operation is written as either *E* or 1.

3. For each monalphabet there is an inverse (or as we call it a deciphering alphabet), which when applied to the cipher gets you back to plain language. For example, *T* is the inverse of *S*; *V*, which is a reciprocal alphabet, is its own inverse. The inverse of an operation is represented by the exponent -1.

These are the essential properties in the definition of a group.[1] To repeat them, a group is a collection of operations such that:

a. Two of them applied in succession gives a result equal to some one of the group.

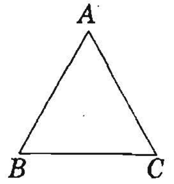
b. There is an identity operation which causes no change.

c. To each operation there corresponds an inverse such that an operation followed by its inverse equals the identity.

d. The application of three of them is associative, that is, $(ST)U = S(TU)$.

An equivalent group to the one we have just described is the following:

Given an equilateral triangle:



Consider the operations of the group to be those movements in the plane which cause the triangle to occupy the same space even though the identity of the vertices may change. Thus suppose we rotate the triangle clockwise about its center through an angle of 120°. Call this *S*, and let *T* be a clockwise rotation through 240°. There are also three ways *U, V, W*, in which the triangle can be rotated through 180° about an altitude. This keeps one vertex fixed and interchanges the other two.

Any two of these operations in succession are equivalent to one of the group; there is an identical operation; and each one of these transformations has an inverse.

Consider as a third example the process of replacing a variable *X* by a function of itself. It can be shown that the following six functional operations form a group.

[1] A further property is required for completeness of definition, viz., associativity. Since it is not really required in this presentation, it will be assumed throughout.

E	(X, X)	U	$\left(X, \frac{1}{X}\right)$
S	$\left(X, \frac{X-1}{X}\right)$	V	$(X, 1 - X)$
T	$\left(X, \frac{1}{1-X}\right)$	W	$\left(X, \frac{-X}{X-1}\right)$

All three of these examples of groups, and others that can be cited, based on different types of mathematical operations, have some very important common properties. Suppose we form a "multiplication" table which gives the result of any two successive operations, the first being the column coordinate and the second the row coordinate. It can be shown that this one table applies to each of the examples we have described. This table can thus be considered an abstract representation of the entire group, independent of the actual type of operation which the operators represent. Every group has such a defining table with as many rows and columns as there are operations in the group.

	E	S	T	U	V	W
E	E	S	T	U	V	W
S	S	T	E	W	U	V
T	T	E	S	V	W	U
U	U	V	W	E	S	T
V	V	W	U	T	E	S
W	W	U	V	S	T	E

Note in this table that

$$T = S \cdot S.$$

If we abbreviate $S \cdot S$ as S^2 then we can write $S^2 = T$ and $T \cdot S = S^2 \cdot S = S^3 = E$. Further,

$$V = S \cdot U, \text{ and}$$
$$W = S \cdot V = S. \quad (S \cdot U) = S^2 U.$$

Thus all six elements of the group are definable in terms of S and U. This is described by saying that S and U generate the group.

Any substitution operation applied a sufficient number of times in succession will finally produce the identity. The number of times this is required is called the *order* of the operation. Thus S is of order 3, since $S^3 = E$, U is of order 2, $U^2 = E$, SU is of order 2, $(SU)^2 = E$.

We can say that the generators of our group satisfy the relations $S^3 = U^2 = (SU)^2 = E$.

Suppose now that we had started with the statement: Given $S^3 = U^2 = (SU)^2 = E$, determine the group generated by S and U. We would first have to determine how many distinct combinations of S and U are possible. The answer would be six: E, S, S^2, U, SU, S^2U. Every other combination of S's and U's can be reduced to one of these six. By determining the product of every pair, the multiplication table can be reconstructed and from it the group can be completely defined.

Consider now a more general problem of determining the group defined by a pair of generators, say a pair S and U satisfying the relations

$$S^l = U^m = (SU)^p = E.$$

To solve such a problem it would be necessary to determine how many different combinations of S and U can be formed. For example, take the case

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

By a process of exhaustion it can be shown that there are only 12 distinct combinations:

E	U	U^2	US^2
S	SU	SU^2	SUS^2
S^2	S^2U	S^2U^2	S^2US^2.

Any other combination of S and U reduces to one of these 12.

To show this consider an instance. SUS is included since $SUSU = 1$; $SUSU \cdot U^2 = U^2$; $SUS = U^2$.

It is interesting to note a simplification in procedure which this array suggests. If we think of the first column E, S, S^2 as a unit, then the second column is the first column times U; the third column is the first column times U^2; the last column is the first column times US^2. The first column is a subgroup of order 3. If we start with it as a unit, we can enumerate all the possible combinations in the group by expanding on it. Write it S^x and let it stand for the set of all the possible powers of S. Then the group is:

$$S^x, S^x U, S^x U^2, S^x US^2.$$

This kind of expansion, known as an expansion by co-sets is a commonly used technique in abstract group theory.

By a similar method of expansion, the group defined by $S^4 = U^3 = (SU)^2 = E$ can be shown to be of order 24; $S^5 = U^3 = (SU)^2 = E$ is of order 60.

By way of a concrete representation of these groups, it is possible to prove that the group of order 12 is the group of all the movements of a regular tetrahedron into itself.

The group of order 24 is the group of all the movements of a cube into itself; it is also the group of all the movements of a regular octahedron into itself. That these two are the same, i. e., the rotations of a cube or regular octahedron into itself can be understood as follows. If you take the midpoints of each of the faces of a regular octahedron, these points form the vertices of a cube. Each movement of the octahedron into itself carries the cube into itself and vice versa.

The group of order 60 is the group of movements of either the regular icosahedron or the regular dodecahedron into itself.

As you are all aware, there are only five regular solids. The groups that determine all the possible rotations of such a solid into itself are therefore three in number; one of order 12, one of order 24, and one of order 60.

These examples of groups related to the regular solids seem simple enough but they are the only simple ones there are. In fact, it is possible to prove the following:

The group generated by

$$S^l = U^m = (SU)^p = 1$$

is finite only if

$$\frac{1}{l} + \frac{1}{m} + \frac{1}{p} > 1$$

and its order is

$$\frac{2}{\frac{1}{l} + \frac{1}{m} + \frac{1}{p} - 1}$$

Outside of the special case where 2 of the numbers l, m, p are $= 2$, this inequality is satisfied only in the cases

l	m	p
2,	3,	3
2,	3,	4
2,	3,	5

In all other cases, it becomes necessary to add further conditions on the generators before a finite group can be determined.

Several proofs of this result have been published. As might be expected from the connection with the regular solids, there ought to be a geometric proof. I should like to sketch such a proof.

Suppose we have a group definition in terms of the orders of each of two generators and of their product. It can be shown that there is a method of representing such a group by triangles whose angles are:

$$\frac{180°}{l}, \frac{180°}{m}, \frac{180°}{p}.$$

These triangles are contiguous and fill the entire space. Now the sum of the three angles of the triangle will determine the type of space in which the representation must take place. If it equals 180°, the representation would be in a Euclidean plane. If the sum of the angles of the triangle is not equal to 180°, the representation would have to be on a non-Euclidean surface—a sphere if the sum exceeds 180° and a pseudosphere if the sum is less than 180°.

Of these three types of space, only the sphere is finite in extent. Hence the only time you can have a finite group is when

$$\frac{180°}{l} + \frac{180°}{m} + \frac{180°}{p} > 180°$$

and the group can then be represented on a sphere. The sum of the angles in any spherical triangle exceeds 180° and the excess over 180° determines its area. Hence the number of triangles required to cover the sphere completely is calculable just from the angle sum.

From this it results that the order of the group is

$$\frac{2}{\frac{1}{l} + \frac{1}{m} + \frac{1}{p} - 1},$$

which agrees with the answers already mentioned; 12, 24, and 60.

There are, however, proofs based entirely on abstract group theory and independent of geometry. It might be of interest to sketch one such proof, say for the case

$$S^3 = U^2 = (SU)^5 = E.$$

To carry out this proof, one new concept needs to be introduced. Suppose we represent a group consisting of monoalphabetic substitutions on an alphabet of n characters $A_1, A_2, \cdots, A_n$. Suppose it is known that there exists at least one substitution in the group which replaces A_1 by any designated letter of the alphabet, i. e., there exist substitutions which replace A_1 by A_1, A_1 by A_2, A_1 by any specific letter. A group having this property is called transitive, and it is a basic theorem that the order of a transitive group is a multiple of the number of letters in the alphabet. (In effect what this says is that in such a group there are the same number of substitutions which replace A_1 by A_2, as replace A_1 by A_3 or A_4 or any other letter. Thus the order of the group is the number of letters multiplied by the number of substitutions which replace A_1 by itself, because the number replacing A_1 by any one letter is the same as the number replacing A_1 by any other letter.)

Now consider two substitutions:

$$S:\quad \begin{array}{lllllll} A_1A_2A_3 & A_4A_5A_6 & A_7A_8A_9 & \cdots & A_{6k-2} & A_{6k-1} & A_{6k} \\ A_2A_3A_1 & A_5A_6A_4 & A_8A_9A_7 & & A_{6k-1} & A_{6k} & A_{6k-2} \end{array},$$

$$U:\quad \begin{array}{llllll} A_3A_4 & A_5A_7 & A_6A_8 & A_9A_{10} & & A_{6k-3} & A_{6k-2} \\ A_4A_3 & A_7A_5 & A_8A_6 & A_{10}A_9 & \cdots\cdots & A_{6k-2} & A_{6k-3} \end{array}.$$

S interchanges the letters in groups of three, so that if applied three times in succession it would yield the identity, i. e., $S^3 = E$. Similarly U interchanges the letters in pairs $U^2 = E$.

The substitution $S\,U$, i. e., the result of applying substitution S and then T, can be shown to be of order 6.

$$\begin{array}{l} A_1A_2A_4A_7A_6A_3 \cdots\cdots\cdots\cdots \\ A_2A_4A_7A_6A_3A_1 \cdots\cdots\cdots\cdots \end{array}$$

Thus the group generated by these two operators S and T satisfies the relations.

$$S^3 = T^2 = (ST)^6 = E.$$

This group can be shown to be transitive. We can write down the necessary combination of S and T which will replace A_1 by any desired letter of the alphabet. Suppose we wished to determine which substitution replaces A_1 by A_9.

Example.

S^2 replaces A_1 by A_3 since S replaces A_1 by A_2 and the second application of S replaces A_2 by A_3

U replaces A_3 by A_4

Hence S^2U replaces A_1 by A_4

S^2 replaces A_4 by A_6

S^2US^2 replaces A_1 by A_6

S^2US^2U replaces A_1 by A_8

S^2US^2US replaces A_1 by A_9

Since the group is transitive its order is a multiple of $6k$. But k may be made any integer whatever and the order of the group can be made to exceed any number no matter how large.

Thus it results that two generators of orders 2 and 3, whose product is of order 6, if they have no other restrictions on them, generate a group of infinite order.

By a slight change in the form of S and U, the proof can be extended to apply to all cases where the order of $S\cdot U$ is any multiple of 3. A further extension takes care of the cases $3x + 1$ and $3x + 2$, x being any number equal to or greater than 2. This then confirms the conclusion already stated that only in the cases

$$\begin{array}{l} 2,\ 3,\ 3 \\ 2,\ 3,\ 4 \\ 2,\ 3,\ 5 \end{array}$$

is a finite group generated by two operators of periods 2 and 3.

In order to define a finite group satisfying $S^l = U^m = (SU)^p = E$, in any case other than the three mentioned, it becomes necessary to impose additional restrictions on the generators S and U, and the definition accordingly becomes more complicated. It might be of interest to discuss this aspect briefly.

The first question one must examine is how to pick the additional restrictions which will be used as defining relations. One approach that has been used is to employ the order of a special combination of S and T known as the commutator. The commutator of S and U is defined as

$$S^{-1}U^{-1}SU,$$

and has rather important properties in abstract group theory. We therefore consider the definition

$$S^3 = U^2 = (SU)^p = (S^{-1}U^{-1}SU)^q = E$$

which we shall write

$$(2, 3, p;\quad q).$$

The reason fcr the semicolon is that the roles of the numbers 2, 3, p are interchangeable. We could have two generators of orders 2 and 3 with product of order p; or we could have two generators of order p and three with product of order 2, etc.

Now the subgroup formed by commutators of every possible pair of operators of a group is called the commutator subgroup. This is usually smaller than the group itself. In the event that the commutator subgroup is identical with the group itself, the group is called a perfect group. It can be shown that if p is one more than a multiple of 6, then the group

$$S^3 = U^2 = (SU)^p = E$$

is perfect. This suggested a study of the case $p = 7$.

The problem now is to determine the order of the group

$$(2, 3, 7;\ \ q).$$

This study was initiated by Brahana of Illinois with these results:

$q = 2$ no group is possible. (This means that the relations (2, 3, 7; 2) involve a contradiction. They are not compatible with one another.)
$q = 3$ no group
$q = 4$ G is of order 168
$q = 5$ no group
$q = 6$ G is of order 1092.

I was able to prove in a later paper that when $q = 7$, G is of order 1092, and is the same group as is defined by $q = 6$. But the case $q = 8$ proved a hurdle.

It is not yet known whether

$$(2, 3, 7;\ \ 8)$$

is finite. What I have proved is that the appending of a fifth restriction defines the perfect group of order 10,752, and that the five conditions are probably independent. It can also probably be said that any value of q (the order of the commutator) at least equal to 8 is inadequate to define a finite group without appending at least fifth condition.

One might conclude from this that any group larger than 10,752 requires at least five defining relations, but that is not so. It is possible to devise more powerful defining relations than the order of the commutator but they may become very involved. For example, one very powerful condition is the order of Q^2P^5 where

$$Q = STSTS$$
$$P = T^{-1}S^{-1}.$$

I have been able to prove that with only four conditions

$$(2, 3, 7) \qquad (Q^2P^5)^5 = E$$

we can generate a group of order 12,180. A consequence of these four conditions is that the order of the commutator is 14.

But the four relations

$$(2, 3, 7;\ \ 14)$$

are not sufficient to define this same group. At least a fifth restriction would have to be introduced if we started with this type of definition.

The problem of determining the size of a group, as its definition involves additional conditions on the generators, is thus seen to increase rapidly in complexity. As a result, the number of groups for which abstract definitions are known is relatively small. A remarkable feature of the results already obtained is the extreme simplicity of such definitions in the case of several groups of quite high order. A small number of conditions gives a complete definition for groups of relatively very large size. This fact constitutes an additional incentive to the search for abstract definitions and many elegant results have doubtless yet to be discovered.

The method of enumeration which has been discussed is of general application and has been the method most commonly employed. Its success has however been limited, for in all but the simplest cases it has involved considerable manipulative ingenuity, and for many groups of even moderately high order, the length of the necessary calculations makes the method impracticable.

I come now to the main concept of my talk. I propose to show how such calculations can be dispensed with entirely, and the method can be reduced to a purely mechanical process independent of any real appreciation of group theory.

Take first the case of the group of order 6 which we used as our example of a group at the beginning of the talk. It is defined by

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

We set up a box for each of these defining relations and represent the identity by the number 1.

The operation S on 1 will be called 2. S on 2 will be called 3.

	S	S	S
1	2	3	1

U	U

S	U	S	U

Since $S^3 = 1$, S on 3 must produce 1. In general, in each of these boxes the last entry of any row will be equal to the number to the left of the row.

Now, let U on 1 be called 4. Then U on 4 is 1.

	S	S	S
1	2	3	1

	U	U
1	4	1

S	U	S	U

Proceed next to enter values into the third box.

	S	S	S
1	2	3	1

	U	U
1	4	1

	S	U	S	U
1	2		4	1

To the right S on 1 produces 2 and to the left U produces 1 from 4. We can go no further until we introduce new elements.

To this end let S on 4 give 5 and S on 5 give 6. Then since S produces 4 from 6, we can fill in the first line of the third box and deduce that U on 2 gives 6. Put this into box 2.

	S	S	S
1	2	3	1
4	5	6	4

	U	U
1	4	1
2	6	2

	S	U	S	U
1	2	6	4	1

Now start with 2 outside box 3. S on 2 gives 3. U produces 2 from 6. S produces 6 from 5. Hence U on 3 gives 5.

	S	U	S	U
2	3	5	6	2

Adding this to the U box, and continuing in this way the boxes fill in completely as follows:

	S	S	S
1	2	3	1
4	5	6	4

	U	U
1	4	1
2	6	2
3	5	3

	S	U	S	U
1	2	6	4	1
2	3	5	6	2
3	1	4	5	3

The order of the group is thus seen to be 6. This scheme is clearly applicable to situations involving more than two generators and any number of defining relations.

An improvement on this method can be effected by carrying out this enumeration on co-sets rather than on single operations. For example, let us designate by 1, in this mechanical process, all the powers of S, so that $1 = E, S, S^2, S^3$. Now consider the case

2, 3, 4.

The steps of enumeration would proceed as shown below:

	S	S	S	S
1	1	1	1	1
2	3			

	U	U	U
1	2	3	1

	S	U	S	U
1	1	2	3	1

	S	S	S	S
1	1	1	1	1
2	3	4	5	2

	U	U	U
1	2	3	1
4	5		4

	S	U	S	U
1	1	2	3	1
3	4	5	2	3

	S	S	S	S
1	1	1	1	1
2	3	4	5	2

	U	U	U
1	2	3	1
4	5	6	4

	S	U	S	U
1	1	2	3	1
3	4	5	2	3
4	5	6	6	4

and finally

	S	S	S	S
1	1	1	1	1
2	3	4	5	2
6	6	6	6	6

	U	U	U
1	2	3	1
4	5	6	4

	S	U	S	U
1	1	2	3	1
3	4	5	2	3
4	5	6	6	4

Since S is of order 4, the group is 6 times as large or 24.

$$1 = S^x$$
$$2 = S^x U$$
$$3 = S^x U^2$$
$$4 = S^x U^2 S = S^x U S^2$$
$$5 = S^x U S^3 = S^x U^2 S U$$
$$6 = S^x U S^2 U^2$$

What happens in studying a group by this method if the set of defining relations is not consistent? Let us take a simple instance:

$$(S^3 = U^2 = [SU]^3 = [S^2U]^2 = 1)$$
$$1 = S^2.$$

Following the procedure described, the boxes shown below are obtained, and it turns out from the S^2U box that 3 = 1 since U on 4 gives 3 in the last cell. If 3 = 1 then from the S box 2 = 1 and X = 1; and everything reduces to 1. This is a case of collapse and it follows that the defining relations are inconsistent.

	S	*S*	*S*
1	1	1	1
2	3	4	2

	U	*U*
1	2	1
3	4	3

	S	*U*	*S*	*U*	*S*	*U*
1	1	2	3	4	2	1

	S	*S*	*U*	*S*	*S*	*U*
1	1	1	2	3	3	1

3 = 1 .

These examples are deceptively easy because they have been applied to particularly simple problems. Nonetheless they serve adequately to demonstrate the principle of how an otherwise troublesome type of problem can be simplified and made completely automatic. Many of the underlying difficulties of this basic problem in group theory are thereby circumvented.

The obvious question that now comes to mind is whether the procedure I have described can be performed by machine. I have been giving some thought to this problem and am studying the possibility of writing a computer program which will duplicate the process I have just described for you.

I suggest this problem to those of you who are interested in computer techniques: Write a program that will duplicate the enumerative process which I have just described and which will therefore be able to determine the size of a group defined by a given set of generating relations.