THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

The Free Group

Dr. Jyoti
Assistant Professor,
DAV (PG) College,
Karnal.

Abstract:

We have seen a few groups, such as the symmetric group S_3, the dihedral groups D_n, and the group M of rigid motions of the plane, in which one can compute easily using a list of generators and a list of relations for manipulating them. The rest of this chapter is devoted to the formal background for such methods. In this section, we consider groups which have a set of generators satisfying *no* relations other than ones [such as $x(xy) = (xy)z$] which are implied by the group axioms. A set S of elements of a group which satisfy no relations except those implied by the axioms is called *free*, and a group which has a free set of generators is called a *free group*. We will now describe the free groups.

Proposition(1). There is only one reduced form of a given word w.

Proof: We use induction on the length of w. If w is reduced, there is noting to show. If not, there must be some pair of letters which can be cancelled, say the underlined pair

$$w = \ldots \underline{xx^{-1}} \ldots .$$

(Let us allow x to denote any element of S', with the obvious convention that if $x = a^{-1}$ and $x^{-1} = a$.) If we show that we can obtain every reduced form w_0 of w by cancelling the pair $\underline{xx^{-1}}$ first, then the proposition will follow by induction on the shorter word $\ldots \underline{xx^{-1}} \ldots$ thus obtained.

Let w_0 be a reduced form of w. We know that w_0 is obtained from w by some sequence of cancellations. The first case is that our pair $\underline{xx^{-1}}$ is cancelled at some step in this sequence. Then we might as well rearrange the operations and cancel $\underline{xx^{-1}}$ first. So this case is settled. On the other hand, the pair $\underline{xx^{-1}}$ cannot remain in w_0, since w_0 is reduced. Therefore at least one of the two symbols must be cancelled at some time. If the pair itself is not cancelled, then the first cancellation involving the pair must look like

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

$$\ldots x^{-1}\underline{xx^{-1}}\ldots \quad \text{or} \quad \underline{xx^{-1}}x\ldots$$

Notice that the word obtained by this cancellation is the same as that obtained by cancelling the original pair $\underline{xx^{-1}}$. So we may cancel the original pair at this stage instead. Then we are back in the first case, and the proposition is proved. □

Now we call two words, w, w' in W′ equivalent, and we write $w \sim w'$, if they have the same reduced form. This is an equivalence relation.

Proposition(2). The product of equivalent words is equivalent: If $w \sim w'$ and $v \sim v'$, then $wv \sim w'v'$.

Proof. To obtain the reduced word equivalent to the product wv, we can first cancel as much as possible in w and in v, to reduce w to w_0 and v to v_0. Then wv is reduced to w_0v_0. Now we continue cancelling in w_0v_0 if possible. Since $w \sim w'$ and $v \sim v'$, the same process, applied to $w'v'$, passes through w_0v_0 too, and hence it leads to the same reduced word. □

It follows from this proposition that equivalence classes of words may be multiplied, that is, that there is a well-defined law of composition on the set of equivalence classes of words.

Proposition(3). Let F denote the set of equivalence classes of words in W'. Then F is a group with the law of composition induced from W'.

Proof. The facts that multiplication is associative and that the class of the empty word 1 is an identity follow from the corresponding facts in W'. It remains to check that all elements of F are invertible. But clearly, if $w = xy \ldots z$ then the class $z^{-1} \ldots y^{-1}x^{-1}$ is the inverse of the class of w. □

Definition. The group F of equivalence classes of words is called the *free group* on the set S.

So an element of the free group F corresponds to exactly one reduced word in W', by Proposition(1). To multiply reduced words, combine and cancel:

$$(abc^{-1})(cb) \rightsquigarrow abc^{-1}cb = abb.$$

One can also introduce power notation for reduced words: $aaab^{-1}b^{-1} = a^3b^{-2}$.

The free group on the set $S = \{a\}$ consisting of one element is the same as the set of all powers of a: $F = \{a^n\}$. It is an infinite cyclic group. In contrast, the free group on a set $S = \{a, b\}$ of two elements is very complicated.

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

GENERATORS AND RELATIONS

Having described free groups, we now consider the more likely case that a set of generators of a group is not free–that there are some nontrivial relations among them. Our discussion is based on the mapping properties of the free group and of quotient groups.

Proposition(4). *Mapping property of the free group:* Let *F* be the free group on a set *S* = {*a*, *b*, ... }, and let G be a group. Every map of set *f*: *S* → *G* extends in a unique way to a group homomorphism φ: *F* → *G*. If we denote the image *f*(x) of an element $x \in S$ by $\tilde{x}$, then φ sends a word in *S′* = {*a*, a^{-1}, *b*, b^{-1},.....} to the corresponding product of the elements $\{\tilde{a}, \tilde{a}^{-1}, \tilde{b}, \tilde{b}^{-1}, \dots .\}$ in *G*.

Proof. This rule does define a map on the set of words in *S′*. We must show that equivalent words are sent to the same product in *G*. But since cancellation in a word will not change the corresponding product in *G*, this is clear. Also, since multiplication in *F* is defined by juxtaposition, the map φ thus defined is a homomorphism. It is the only way to extend *f* to a homomorphism. □

If *S* is any subset of a group G, the mapping property defines a homomorphism φ : *F* → *G* from the free group on *S* to *G*. This reflects the fact that the elements of *S* satisfy no relations in *F* except those implied by the group axioms, and explains the reason for the adjective *free*.

A family *S* of elements is said to *generate* a group *G* if the map φ from the free group on *S* to *G* is surjective. This is the same as saying that every element of *G* is a product of some string of elements of *S′*, so it agrees with the terminology introduced in Section 2 of Chapter 2. In any case, whether or not *S* generates *G*, the image of the homomorphism φ of Proposition (4) is a subgroup called the *subgroup generated by S*. This subgroup consists precisely of all products of elements of *S′*.

Assume that *S* generates *G*. The elements of *S* are then called *generators*. Since φ is a surjective homomorphism, the First Isomorphism Theorem tells us that *G* is isomorphic to the quotient group *F*/*N*, where *N* = ker φ. The elements of N are called *relations* among the generators. They are equivalence classes of words *w* with the property that the corresponding product in *G* is 1:

$$\varphi(w) = 1 \quad \text{or} \quad w = 1 \text{ in } G.$$

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

In the special case that $N = \{1\}$, φ is an isomorphism. In this case G is called a free group too.

If we know a set of generators and also all the relations, then we can compute in the isomorphic group F/N and hence in our group G. But the subgroup N will be infinite unless G is free, so we can't list all its elements. Rather, a set of words

$$R = \{r_1, r_2, ...\}$$

is called a set of defining relations for G if $R \subset N$ and if N is the *smallest normal subgroup containing* R. This means that N is generated by the subset consisting of all the words in R and also all their conjugates.

It might seem more systematic to require the defining relations to be generators for the group N. But remember that the kernel of the homomorphism $F \to G$ defined by a set of generators is always a normal subgroup, so there is no need to make the list of defining longer. If we know that some relation $r = 1$ holds in G, then we can conclude that $xrx^{-1} = 1$ holds in G too, simply by multiplying both sides of the equation on the left and right by x and x^{-1}.

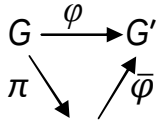
We already know a few examples of generators and relations, such as the dihedral group D_n. It is generated by the two elements x, y, with relations

$$x^n = 1, \qquad y^2 = 1, xyxy = 1.$$

Proposition(5). The elements x^n, y^2, $xyxy$ from a set of defining relations for the dihedral group.

This proposition is essentially what was checked in Previous Chapter. But to prove it formally and to work freely with the concept of generators and relations, we will need what is called the mapping property of quotient groups. It is a generalization of the First Isomorphism theorem:

Proposition(6). *Mapping property of quotient groups:* Let N be a normal subgroup of G, let $\bar{G} = G/N$, and let π be the canonical map $G \to G'$ defined by $\pi(a) = \bar{a} = aN$. Let $\varphi : G \to G'$ be a homomorphism whose kernel contains N. There is a unique homomorphism $\bar{\varphi}: G \to G'$ such that $\bar{\varphi}\pi = \varphi$:



ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

G

This map is defined by the rule $\bar{\varphi}(\bar{a}) = \varphi(a)$.

Proof. To define a map $\bar{\varphi}: \bar{G} \to G'$, we must define $\bar{\varphi}(\alpha)$ for every element α of $\bar{G}$. To do this, we represent α by an element $a \in G$, choosing a so that $\alpha = \pi(a)$. In the bar notation, this means that $\alpha = \bar{a}$. Now since we want our map $\bar{\varphi}$ to satisfy the relation $\bar{\varphi}(\pi(a)) = \varphi(a)$, there is no choice but to define $\bar{\varphi}$ by the rule $\bar{\varphi}(\alpha) = \varphi(a)$, as asserted in the proposition. To show that this is permissible, we must show that the value we obtained for $\bar{\varphi}(\alpha)$, namely $\varphi(a)$, depends only on α and not on our choice of the representative a. This is often referred to as showing that our map is "well-defined."

Let a and a' be two elements of G such that $\bar{a} = \bar{a}' = \alpha$. The equality $\bar{a} = \bar{a}'$ means that $aN = a'N$, or that $a' \in aN$. So $a' = an$ for some $n \in N$. Since $N \subset \ker \varphi$ by hypothesis, $\varphi(n) = 1$. Thus $\varphi(a') = \varphi(a)\varphi(n) = \varphi(a)$, as required.

Finally, the map $\bar{\varphi}$ is a homomorphism because $\bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b}) = \varphi(ab) = \bar{\varphi}(\overline{ab})$. □

Proof of Proposition(5). We showed in previous chapter that D_n is generated by elements x, y which satisfy Proposition(4). Therefore there is a surjective map $\varphi: F \to D_n$ from the free group on x, y to D_n, and $R = \{x^n, y^2, xyxy\}$ is contained in ker φ. Let N be the smallest normal subgroup of F containing R. Then since ker φ is a normal subgroup which contains R, $N \subset \ker \varphi$. The mapping property of quotients gives us a homomorphism $\bar{\varphi}: F/N \to D_n$. If we show that $\bar{\varphi}$ is bijecitive, the proposition will be proved.

Note that since φ is surjective, $\bar{\varphi}$ is too. Also, in F/N the relations $\bar{x}^n = 1, \bar{y}^2 = 1, and\ \bar{x}\bar{y}\bar{x}\bar{y} = 1$, hold. Using them, we can put any word in $\bar{x}, \bar{y}$ into the form $\bar{x}^i\bar{y}^j, with\ 0 \le i \le n-1\ and\ 0 \le j \le 1$. This shows that F/N has at most $2n$ elements. Since $|D_n| = 2n$, it follows that $\bar{\varphi}$ is bijective, as required. □

We will use the notation $\langle x_1, \dots, x_m; r_1, \dots, r_k \rangle$ to denote the group generated by elements $x_1, \dots, x_m$, with defining relations $r_1, \dots, r_k$. Thus

$$D_n = \langle x, y; x^n, y^2, xyxy \rangle.$$

As a new example, let us consider the group generated by x, y, with the single relation $xyx^{-1}y^{-1} = 1$. If x, y are elements of a group, then $xyx^{-1}y^{-1}$ is called

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

their *commutator*. This commutator is important because it is equal to 1 if and only if x and y commute. This is seen by multiplying both sides of the equation $xyx^{-1}y^{-1} = 1$ on the right by yx. So if we impose the relation $xyx^{-1}y^{-1} = 1$ on the free group, we will obtain a group in which x and y commute. Thus if N is the smallest normal subgroup containing the commutator $xyx^{-1}y^{-1}$ and if $G = F/N$, then the residues of x and y are commuting elements of G. This forces any two elements of G to commute.

Proposition(7). Let F be the free group on x, y and let N be the smallest normal subgroup generated by the commutator $xyx^{-1}y^{-1}$. The quotient group $G = F/N$ is abelian.

Proof. Let us denote the residues of the generators x, y in G by the same letters. Since the commutator is in N, the elements x, y commute in G. Then x commutes with y^{-1} too. For xy^{-1} and $y^{-1}x$ both become equal to x when multiplied on the left by y. So by the Cancellation Law, they are equal. Also, x obviously commutes with x and with x^{-1}. So x commutes with any word in $S' = \{x, x^{-1}, y, y^{-1}\}$. So does y. It follows by induction that any two words in S' commute. Since x, y generate the group, G is commutative. □

Note this consequence: The commutator $uvu^{-1}v^{-1}$ of any two words in S' is in the normal subgroup generated by the single commutator $xyx^{-1}y^{-1}$, because, since u, v commute in G, the commutator represents the identity element in G.

The group G constructed above is called the *free abelian group* on the set $\{x, y\}$, because the elements x, y satisfy no relations except those implied by the group axioms and the commutative law.

In the examples we have seen, knowledge of the relations allows us to compute easily in the group. This is somewhat misleading, because computation with a given set of relations is often not easy at all. For example, suppose that we change the defining relations for the dihedral group slightly, substituting y^3 for y^2;

$$G = \langle x, y; x^n, y^3, xyxy \rangle.$$

This group is much more complicated. When n > 5, it is an infinite group.

Things become very difficult when the relations are complicated enough. Suppose that we are given a set R of words, and let N be the smallest normal

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

subgroup containing *R*. Let *w*, *w'* be any other words. Then we can pose the problem of deciding whether or not *w* and *w'* represent the same element of *F*/*N*. This is called the *word problem for groups*, and it is known that there is no general procedure for deciding it in a predictable length of time. Nevertheless, generators and relations allow efficient computation in many cases, and so they are a useful tool. We will discuss an important method for computation, the Todd-Coxeter Algorithm, in the next section.

Recapitulating, when we speak of a group defined by generators *S* and relations *R*, we mean the quotient group *F*/*N*, where *F* is the free group *S* and *N* is the smallest normal subgroup of *F* containing *R*. Note that *any* set *R* of relations will define a group, because *F*/*N* is always defined. The larger *R* is, the larger *N* becomes and the more collapsing takes place in the homomorphism $\pi: F \to F/N$. If *R* gets "too big," the worst that can happen is that *N* = *F*, hence that *F*/*N* is the trivial group. Thus there is no such thing as a contradictory set of relations. The only problems which may arise occur when *F*/*N* becomes too small, which happens when the relations cause more collapsing than was expected.

THE TODD-COXETER ALGORITHM

Let *H* be a subgroup of a finite group *G*. The Todd-Coxeter Algorithm which is described in this section is an amazing direct method of counting the cosets of *H* in *G* and of determining the operation of *G* on the set of cosets. Since we know that any operation on an orbit looks like an operation on cosets, the algorithm is really a method of describing any group operation.

In order to compute explicitly, both the group *G* and the subgroup *H* must be given to us in an explicit way. So we consider a group

$$G = \langle x_1, \dots, x_m; r_1, \dots, r_k \rangle$$

Presented by generators x_1, …, x_m and explicitly given relations r_1,…, r_k, as in the previous section. Thus *G* is realized as the quotient group *F*/*N*, where *F* is the free group on the set {x_1,…, x_m} and *N* is the smallest normal subgroup containing {r_1,…, r_k}. We also assume that the subgroup *H* of *G* is given to us explicity by a set of words {h_1,…, h_s} in the free group *F*, whose images in *G* generate *H*.

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

Let us work out a specific example to begin with. We take for *G* the group generated by three elements x, y, z, with relations x^3, y^2, z^2, xyz, and for *H* the cyclic subgroup generated by z:

$$G = \langle x, y, z; x^3y^2z^2, xyz \rangle, \quad H = \{z\}.$$

Since we will determining the operation on cosets, which is permutation representation, we must decide how to write permutations. We will use the cycle notation of Section 6. This forces us to work with *right cosets Hg* rather than with left cosets, because we want *G* to operate on the right. Let us denote the set of right cosets of *H* in *G* by ζ. We must also decide how to describe the operation of our group explicitly, and the easiest way is to go back to the free group again, that is, to describe the permutations associated to the given generators x, y, z.

The operations of the generators on the set of cosets will satisfy these rules:

Rules. (*)

1. The operation of each generator (x, y, z in our example) is a permutation.

2. The relations (x^3, y^2, z^2, xyz in our example) operate trivially.

3. The generators of *H* (z in our example) fix the coset *H*1.

4. The operation on cosets is transitive.

The first rule is a general property of group operations. It follows from the fact that group elements are invertible. We list it instead of mentioning inverses of the generators explicitly. The second rule holds because the relations represent 1 in *G*, and it is the group *G* which operates. Rules 3 and 4 are special properties of the operation on cosets.

We now determine the coset representation by applying only these rules. Let us use indices **1, 2, 3,** ... to denote the cosets, with **1** standing for the coset *H*1. Since we don't know how many cosets there are, we don't know how many indices we need. We will add new ones as necessary.

Fist, Rule 3 tells us that z sends **1** to itself **1**z = **1**. This exhausts the information in Rule 3, so Rules 1 and 2 take over. Rule 4 will appear only implicitly.

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

We don't know what x does to the index **1**. Let's guess that $\mathbf{1}x \neq \mathbf{1}$ and assign a new index, say $\mathbf{1}x = \mathbf{2}$. Continuing with the generator x, we don't know $\mathbf{2}x$, so we assign a third index: $\mathbf{1}x^2 = \mathbf{2}x = \mathbf{3}$. Rule 2 now comes into play. It tells us that x^3 fixes every index. Therefore $\mathbf{1}x^3 = \mathbf{3}x = \mathbf{1}$. It is customary to sum up this information in a table

x	x	x	
1	**2**	**3**	**1**

Which exhibits the operation of x on the three indices. The relation xxx appears on the top, and Rule 2 is reflected in the fact that the same index **1** appears at both ends. At this point, we have determined the operation of x on the three indices **1, 2, 3,** except for one thing: We don't yet know that these indices represent distinct cosets.

We now ask for the operation for y on the index **1**. Again, we don't know it, so we assign a new index, say $\mathbf{1}y = \mathbf{4}$. Rule 2 applies again. Since y^2 operates trivially, we know tha $\mathbf{1}y^2 = \mathbf{4}y = \mathbf{1}$:

y	y	
1	**4**	**1.**

The remaining relation is xyz. We know that $\mathbf{1}x = \mathbf{2}$, but we don't yet know $\mathbf{2}y$. So we set $\mathbf{1}xy = \mathbf{2}y = \mathbf{5}$. Rule 2 then tells us tha $\mathbf{1}xyz = \mathbf{5}z = \mathbf{1}$:

x	y	z	
1	**2**	**5**	**1**

We now apply Rule 1: The operation of each group element is a permutation of the indices. We have determined that $\mathbf{1}z = \mathbf{1}$ and also that $\mathbf{5}z = \mathbf{1}$. It follows that **5** = **1**. We eliminate the index **5**, replacing it by **1**. This in turn tells us that $\mathbf{2}y = \mathbf{1}$. On the other hand, we have already determined that $\mathbf{4}y = \mathbf{1}$. So **4** = **2** by Rule 1, and we eliminate **4**.

The entries in the table below have now been determined:

x	x	x	y	y	z	z	x	y	z	
1	**2**	**3**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**
2	**3**	**1**	**2**	**1**	**2**		**2**	**3**		**2**
3	**1**	**2**	**3**		**3**		**3**	**1**	**2**	**3**

The bottom right corner shows that $\mathbf{2}z = \mathbf{3}$. This determines the rest of the table. There are three indices, and the operation is

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

x = (**1 2 3**), y = (**1 2**), z = (**2 3**).

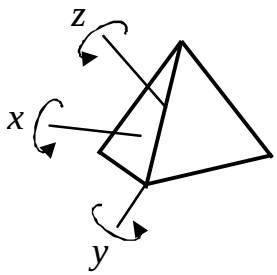
Since there are three indices, we conclude that there are three cosets and that the index of *H* in *G* is 3. We also conclude that the order of *H* is 2, and hence that *G* has order 6. For $z^2 = 1$ is one of our relations; therefore z has order 1 or 2, and since z does not operate trivially on the indices, $z \neq 1$. The three permutations listed above generate the symmetric group, so the permutation representation is an isomorphism from *G* onto S_3.

Of course, there conclusions depend on our knowing that the permutation representation we have constructed is the right one. We will show this at the end of the section. Let's compute a few more examples first.

Example. Consider the tetrahedral group *T* of the 12 rotational symmetries of a regular tetrahedron. If we let y and x denote counter-clockwise rotations by $2\pi/3$ about a vertex and the center of a face as shown below, then $yx = z$ is the rotation by π about an edge. Thus the relations

$$x^3 = 1, y^3 = 1, yxyx = 1 \qquad \text{----------(1)}$$

hold in *T*.



Let us show that (1) is a complete set of relations for T. To do so, we consider the group $G = \langle y, x; y^3, x^3, yxyx \rangle$ defined by these relations. Since the relations (1) hold in T, the mapping property of quotient groups provides a homomorphism $\varphi: G \to T$. This map is surjective because, as is easily seen, y and x generate *T*. We need only show that φ is injective. We will do this by showing that the order of the group *G* is 12.

It is possible to analyze the relations directly, but they aren't particularly easy to work with. We could also compute the order of *G* by enumerating the cosets of the trivial subgroup *H* = {1}. This is not efficient either. It is better to use a nontrivial subgroup *H* of *G*, such as the one generated by y. This subgroup has order at most 3 because $y^3 = 1$. If we show that its order is 3 and that its index in *G* is 4, it will follow that *G* has order 12, and we will be done.

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

Here is the resulting table. To fill it in, work from both ends of the relations.

x	x	x	y	y	y	y	x	y	x
1	**2**	**3**	**1**	**1**	**1**	**1**	**1**	**2**	**3**	**1**
2	**3**	**1**	**2**	**3**	**4**	**2**	**3**	**1**	**1**	**2**
3	**1**	**2**	**3**	**4**	**2**	**3**	**4**	**4**	**2**	**3**
4	**4**	**4**	**4**	**2**	**3**	**4**	**2**	**3**	**4**	**4**

Thus the permutation representation is

$$x = (\mathbf{1\ 2\ 3}),\ y = (\mathbf{2\ 3\ 4}). \qquad \text{----------(2)}$$

Since there are four indices, the index of H is 4. Also, notice that y does have order precisely 3. For since $y^3 = 1$, the order is at most 3, and since the permutation (**2 3 4**) associated to y has order 3, it is at least 3. So the order of the group is 12, as predicted. Incidentally, we can derive the fact that T is isomorphic to the alternating group A_4 by verifying that the permutations (2) generate that group. □

Example. We modify the relations (1) slightly. Let G be generated by $x, y,$ with relations

$$x^3 = 1,\ y^3 = 1,\ yxy^2x = 1,$$

and let H be the subgroup generated by y. Here is a start for a table. Since $y^3 = 1$, we have shortened the last relation, substituting y^{-1} for y^2. Clearly, y^{-1} acts as the inverse of the permutation associated to y. The entries in the bottom row have been determined by working from the right side.

x	x	x	y	y	y	y	x	y^{-1}	x
1	**2**	**3**	**1**	**1**	**1**	**1**	**1**	**2**	**3**	**1**
2			**2**			**2**	**3**	**1**	**1**	**2**

We rewrite the relation $\mathbf{2}y^{-1} = \mathbf{3}$ as $\mathbf{3}y = \mathbf{2}$. Since $\mathbf{2}y = \mathbf{3}$ as well, it follows that $\mathbf{3}y^2 = \mathbf{3}$ and that $\mathbf{3}y^3 = \mathbf{2}$. But $y^3 = \mathbf{1}$, so $\mathbf{3} = \mathbf{2}$, which in turn implies $\mathbf{1} = \mathbf{2} = \mathbf{3}$. Since the generators x, y fix **1**, there is one coset, and $H = G$. Combining this fact with the first relation, we find $x = 1$. Thus G is a cyclic group of order 3. This example illustrates how relations may collapse the group. □

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

In our examples, we have taken for *H* the subgroup generated by one of the chosen generators of *G*, but we could also make the computation with a subgroup *H* generated by an arbitrary set of words. They must be entered into the computation using Rule 3.

This method can also be used when *G* is infinite, provided that the index [*G*:*H*] is finite. The procedure can not be expected to terminate if there are infinitely many cosets.

We now address the question of why the procedure we have described does give the operation on cosets. A formal proof of this fact is not possible without first defining the algorithm formally, and we have not done this. So we will discuss the question informally. We describe the procedure this way: At a given stage of the computation, we will have some set $\mathbf{I}$ of indices, and the operation of some generators of the group on some indices will have been determined. Let us call this a *partial operation* on $\mathbf{I}$. A partial operation need not be consistent with Rules 1, 2, and 3, but it should be transitive; that is, all indices should be in the "partial orbit" of **1**. This is where Rule 4 comes in. It tells us not to introduce any indices we don't need.

The starting position is $\mathbf{I} = \{\mathbf{1}\}$, with no operations assigned. At any stage there are two possible steps: (**)

(i) We may equate two indices $\mathbf{i}, \mathbf{j} \in \mathbf{I}$ as a consequence of one of the first three rules, or

(ii) we may choose a generator x and an index **i** such that $\mathbf{i}x$ has not yet been determined and define $\mathbf{i}x = \mathbf{j}$, where **j** is a new index.

We stop the process when an operation has been determined which is consistent with the rules, that is, when we have a complete, consistent table and the rules hold.

There are two questions to ask: First, will this procedure terminate? Second, if it terminates, is the operation the right one? The answer to both questions is yes. It can be shown that the process always terminates, provided that the group is finite and that preference is given to Step (i). We will not prove this. The more important fact for applications is that if the process terminates, the resulting permutation representation is the right one.

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

Theorem. Suppose that a finite number of repetitions of Steps (i) and (ii) yields a consistent table. Then the table defines a permutation representation which is isomorphic, by suitable numbering, to the representation on cosets.

Sketch of proof. Let $\mathbf{I}^*$ denote the final set of indices, with its operation. We will prove the proposition by defining a bijective map $\varphi^*: \mathrm{I}^* \to \zeta$ from this set to the set of cosets which is compatible with the two operations. We define φ^* inductively, by defining at each stage a map $\varphi : \mathbf{I} \to \zeta$ from the set of indices determined at that stage to ζ, such that φ is compatible with the partial operation on $\mathbf{I}$. To start, $\{\mathbf{1}\} \to \zeta$ sends $\mathbf{1} \rightsquigarrow H1$. Now suppose that $\varphi : \mathbf{I} \to \zeta$ has been defined, and let $\mathbf{I}'$ be the result of applying one of Steps (**) to $\mathbf{I}$. In case of Step (ii), there is no difficulty in extending φ to a map $\varphi' : \mathbf{I} \to \zeta$. We simply define $\varphi'(\mathbf{k}) = \varphi(\mathbf{k})$ if $\mathbf{k} \neq \mathbf{j}$, and $\varphi'(\mathbf{j}) = \varphi(\mathbf{i})x$. Next, suppose that we use Step (ii) to equate two indices, say **i**, **j**, so that $\mathbf{I}$ is collapsed to form the new index set $\mathbf{I}'$. Then the next lemma allows us to define the map $\varphi' : \mathbf{I}' \to \zeta$:

Lemma. Suppose that a map $\varphi : \mathbf{I} \to \zeta$ is given, compatible with a partial operation on $\mathbf{I}$. Let $\mathbf{i}, \mathbf{j} \in \mathbf{I}$, and suppose that one of the Rules 1, 2, or 3 forces $\mathbf{i} = \mathbf{j}$. Then $\varphi(\mathbf{i}) = \varphi(\mathbf{j})$.

Proof. This is true because, as we have already remarked, the operation on cosets does satisfy all of the Rules (*). So if the rules force **i** = **j**, they also force $\varphi(\mathrm{i}) = \varphi(\mathrm{j})$. □

It remains to prove that the map $\varphi^*: \mathbf{I}^* \to \zeta$ is bijective. To do this, we construct the inverse map $\psi^*: \zeta \to \mathbf{I}^*$, using the following lemma:

Lemma. Let S be a set on which G operates, and let $s \in S$ be an element stabilized by H. There is a unique map $\psi: \zeta \to S$ which is compatible with the operations on the two sets and which sends $H1 \rightsquigarrow s$.

Proof. This proof repeats that of previous chapter, except that we have changed to right operations. Since g sends $H \rightsquigarrow Hg$ and since we want $\psi(Hg) = \psi(H)g$, we must try to set $\psi(Hg) = sg$. This proves uniqueness of the map ψ. To prove existence, we first check that the rule $\psi(Hg) = sg$ is well-defined. If $Ha = Hb$, then $ba^{-1} \in H$. By hypothesis, ba^{-1} stabilizes s, so $sa = sb$. Finally, ψ is compatible with the operations of G because $\psi(Hga) = sga = (sg)a = \psi(Hg)a$. □

ISSN:0971-1260
Vol-22-Issue-3-July-September-2019

Now, to prove the bijectivity of ψ^*, we use the lemma to construct a map $\psi^*: \zeta \to \mathbf{I}^*$. Consider the composed map $\varphi^*\psi^*: \zeta \to \zeta$. It sends $H1 \rightsquigarrow H1$. We apply the lemma again, substituting ζ for S. The uniqueness assertion of the lemma tells us that $\varphi^*\psi^*$ is the identity map. On the other hand, since the operation on **I*** is transitive and since ψ^* is compatible with the operations, ψ^* must be surjective. It follows that φ* and ψ^* are bijective. □

References:

1. I. N. Herstein, Second Edition, Topics in Algebra
2. P. B. Bhattacharya, S. K. Jain, S. R. Nagpal, Second Edition, Basic Abstract Algebra
3. I. S. Luthar, I. B. S. Passi, Volume 1: Groups, Algebra
4. Surjeet Singh, Qazi Zameeruddin, Eighth Edition, Modern Algebra
5. Vijay K. Khanna, S. K. Bhambri, Third Edition, A Course in Abstract Algebra