

17. Symmetries

17.1 Permutations

A **permutation** of a set is a reordering of its elements. Another way to look at it is as a function Φ that takes as its argument a set of natural numbers of the form $\{1, 2, \dots, n\}$ and produces another set consisting of the same elements, but in a different order. The permutation function is such that every element of the set is mapped to itself or another element of the set, and no two of them are mapped to the same element.

Permutations can be notated in two ways:

One is by listing the new ordering that replaces $\{1, \dots, n\}$. We do this by writing the n elements of our set in their new order like this: $\{i_1, \dots, i_n\}$, where for each integer j in our set, i_j is the element of the set to which it is mapped. Thus, for $n = 5$, we can write $\{1\ 3\ 5\ 4\ 2\}$ to represent the permutation that takes 1 to itself, 2 to 3, 3 to 5, 4 to itself, and 5 to 2.

Another way to represent a permutation is to put all the cycles of the permutation inside parentheses. It could happen, as in our last example, that 2 maps to 3, 3 to 5, and 5 back to 2. This is an example of a **cycle**.¹ We would represent this cycle by writing it out as: $(2,3,5)$. A cycle can have any length between 1 and n . A cycle with length k of the form (i_1, \dots, i_k) means that i_1 maps to i_2 , i_2 to i_3 , and so on, with i_k mapping back to i_1 . A permutation can have multiple cycles, which can range from size 1 to n . The permutation in the previous example can be written as $(1)(2,3,5)(4)$ in cycle notation.

Using basic combinatorics, we can see that there are $n!$ permutations of n symbols. Still another way to describe them is by using an n -by- n matrix whose entries are either 0 or 1 (this is called a **permutation matrix**). There is exactly one 1 in each column and row; the 1 entry of the j -th column is in the row that corresponds to the number to which element j is mapped.

Thus, the example above corresponds to the matrix:

$$\begin{matrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{matrix}$$

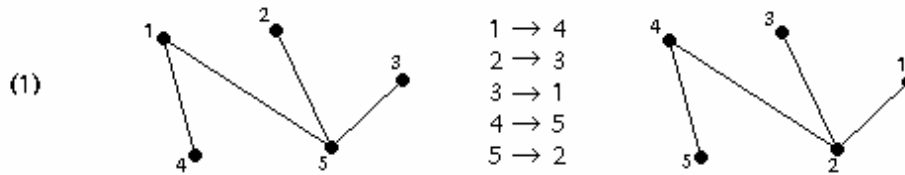
We shall now look at how permutations relate to trees.

¹ If we represented a permutation as a directed graph by making each element of the set a vertex and the mappings as edges, then the cycles of a permutation would exactly be the cycles of the graph.

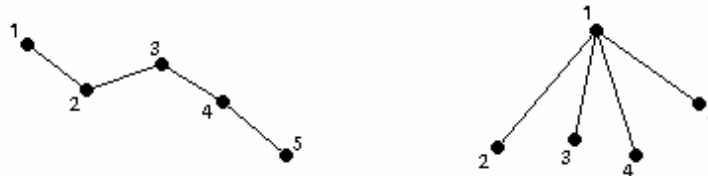
17.2 Symmetry Groups

We saw in notes 16 that the set of trees on 5 vertices has 125 elements, which fit into 1 of 3 patterns. There is a collection of operations that can take one tree and transform it into another tree that looks just like it. Such operations are called **symmetries**.

In the case of trees, the symmetries are all the permutations of the five labels. For example, consider the tree $\{ (4,1), (1,5), (2,5), (3,5) \}$. We can permute its vertices using the permutation $\{ 4\ 3\ 1\ 5\ 2 \}$, and it becomes the tree $\{ (5,4), (4,2), (3,2), (1,2) \}$. We see that these two trees can be drawn exactly the same way, just with different labels on the vertices:



If we have two trees on the same number of vertices and there exists no permutation that takes one to the other, then they cannot have the same pattern. If we look at the trees $\{ (1,2), (2,3), (3,4), (4,5) \}$ and $\{ (1,2), (1,3), (1,4), (1,5) \}$, we can see below that they have different patterns (one is a path and the other is a claw):



If we tried to come up with a permutation that maps one tree into the other, we would not be able to. Look at the edges of the second tree. There are four 1's in them. In order for a permutation to exist, there must be four of some label number in the edges of the first tree that we can map to 1. However, none of the vertex labels appears four times in the edges. Thus, no permutation can exist.

In general, symmetries of any system form a mathematical structure called a group. First, we will list the properties of a group, then explain in detail what each of these properties means.

A **group**, G , is a set of elements $\{A, B, \dots\}$ that has a **law of composition** which allows you to assign a single element of the group to each pair of elements. The set must include an identity element, and each element of G must have an inverse which when composed with it produces the identity element. Finally, the composition law must be associative.

Our law of composition tells us that for any two elements of the group A and B , A composed with B (written as AB) always produces another element of the group. We can

compose two elements in two different orders, without necessarily getting the same result. If $AB = BA$, then we say that our group is a **commutative** group, or an **abelian** group.

The **identity** element of a group, usually written as I , is the unique element of the group such that for any A in G , $AI = IA = A$.

For every element A of G , the **inverse** of A is an element of G , written as A^{-1} , such that $AA^{-1} = A^{-1}A = I$. The inverse of I is I .

Associativity tells us that for any A, B , and C in G , AB composed with C is equal to A composed with BC . More compactly, $(AB)C = A(BC)$.

The symmetry operations that we described before are groups with the law of composition that reads: *A composed with B means that we perform operation B and then operation A*. The identity of this group is the operation that does nothing. So for trees, the law of composition would be the permutations of the vertex labels, and the identity operation would be the permutation $\{1\ 2\ 3\ 4\ 5\}$ which maps every label to itself.

There are two properties of symmetry operations that are essential in making them a group.

The first is that a symmetry operation followed by another symmetry operation is itself a symmetry operation. *This tells us that if A and B are symmetry operations, then AB is as well*. This implies that performing two permutations does define a law of composition and produces an element of the set of symmetries for every pair of elements composed.

The second property is reflexivity. *A symmetry operation must be reversible*. If doing something maintains symmetry, then undoing it does as well. This means that each symmetry operation has an inverse that is also a symmetry operation.

Taking all this together, we see that the symmetry operations form a group under the rules that we have just defined.

You are used to dealing with groups because integers, rational numbers, real numbers, complex numbers, and numbers mod n for any n , all form groups under the law of composition called addition. Additionally, the rational numbers, real numbers, complex numbers, and numbers mod p for any prime p , form groups under multiplication when 0 is omitted.²

Because of this fact, we often describe the law of composition of a group as multiplication, which is shorter to write or say than “law of composition”. Thus, we

² 0 must be omitted because, if we look at the real numbers, we have 1 as the identity element but then $1 * 0$ is 0, when it should be 1. If 0 is omitted then there are no problems of this kind.

often call AB the product of A and B , even if we are in fact talking about some obscure composition law or symmetry operation.

Any group can be described by what is called its **multiplication table**. This is a table much like the multiplication of integers that many of us encountered as children. The table has all of the group elements listed as rows of the table and as columns. In this way, every possible product of two group elements will appear in the table, including that of I with each element of G . This means that every element of the group will appear at least once in the table. Note that not all multiplication tables define groups. To do so, the table must obey the associative law.

For example, let us consider the group of natural numbers mod 5, with multiplication as the law of composition. The elements of this group are $\{1,2,3,4\}$. 1 is the identity element, since $A*1 = A$ for any A . The multiplication table is:

	1	2	3	4
1	$1*1 = \mathbf{1}$	$1*2 = \mathbf{2}$	$1*3 = \mathbf{3}$	$1*4 = \mathbf{4}$
2	$2*1 = \mathbf{2}$	$2*2 = \mathbf{4}$	$2*3 = 6 \text{ mod } 5 = \mathbf{1}$	$2*4 = 8 \text{ mod } 5 = \mathbf{3}$
3	$3*1 = \mathbf{3}$	$3*2 = 6 \text{ mod } 5 = \mathbf{1}$	$3*3 = 9 \text{ mod } 5 = \mathbf{4}$	$3*4 = 12 \text{ mod } 5 = \mathbf{2}$
4	$4*1 = \mathbf{4}$	$4*2 = 8 \text{ mod } 5 = \mathbf{3}$	$4*3 = 12 \text{ mod } 5 = \mathbf{2}$	$4*4 = 16 \text{ mod } 5 = \mathbf{1}$

17.3 Group Representations

When we considered graphs in notes 14 and 15, we noticed that we could look at graphs in two ways. There are graphs as an abstract concept and then there are the drawings of graphs, which have additional properties like faces or edge crossings.

With groups, there are **abstract groups** that are defined by their multiplication table, **permutation groups** whose elements are permutations of sets, and **matrix groups** whose elements are matrices with matrix multiplication as their law of composition.

We note that the permutation group is sometimes referred to as the **symmetric group** because of its relation to symmetric operations as described in section 17.2. For this reason, we often denote the permutation group on n elements as S_n .

Every finite group can be considered a permutation group on itself as objects. This means that every element of the group corresponds uniquely to a permutation of the group elements. It can be shown that each row of the multiplication table is a permutation of the group elements, and that none of the rows are the same (see the exercises for more info). This means that the members of the group can be seen as permuting the group elements according to its row of the multiplication table.

Since any permutation group can be described by matrices (see section 1), every finite group can be written as a group of matrices. However, a given group can be

written as a permutation group acting on many other types of objects, and its elements can thus be described by matrices in many ways.

In fact, a group G is said to be **represented** by a matrix group M if there is a function f that maps the elements of G into those of M that preserves the law composition; which means that $f(A)f(B) = f(AB)$.

A representation is said to be **faithful** if the function f is invertible. Not all representations are faithful. In fact, the mapping $i(A) = I$, which maps A to I for all A in G , makes the trivial one-dimensional matrix group consisting of the single element 1 a representation of every group.

A matrix representation of a group consists of square matrices of some given size, say n -by- n . Given two representations, of dimensions m and n , we can compose them by making a set of $m + n$ by $m + n$ matrices, where each one has the m by m matrix representation of some element A of G in the upper left corner and the n -by- n matrix representation of A in the lower right corner, and 0 's everywhere else in the matrix.

We can then find a different basis for these matrices that obscures this structure.

A matrix representation is said to be **reducible** if it can be broken up into two representations, an m -by- m one in the upper left corner and an n -by- n one in the lower right for each of its elements simultaneously, after some change of basis. If this cannot be done, the representation is said to be **irreducible**.

17.4 Subgroups

We say that H is a **subgroup** of G if H is a subset of G and H is itself a group under the same law of composition as G . Equivalently, we say that a subset H is a subgroup if any composition of two elements in H gives us an element of H , a statement which we sometimes write as $HH = H$.

Given a subgroup H of G , and an element g of G that is not in H , we can define the **coset** gH to be the set consisting of g composed with each element of H . We can similarly define Hg .

When gH and Hg are the same for every g in G we call H a **normal subgroup** of G .

If H is a normal subgroup of G , then we can define another group, called the **factor group** G/H , whose elements are the cosets of H in G . Thus, for every a in G and not in H , aH is in G/H . The law of composition for G/H is that aH composed with bH is equal to abH , for a and b in G and not H . This works because aH composed with bH is $aHbH$, and since H is a normal subgroup this is equal to $abHH$, and we know that any two elements of H composed together will give us an element of H , thus this equals abH .

All subgroups of a numerical group are normal, since all elements commute. These provide many examples of normal subgroups. Thus, if we consider the additive group of integers, there is a subgroup consisting of the even numbers (or more generally, of the numbers divisible by k for any k). The factor group corresponding to this group is the group whose elements are the cosets of odd and even numbers, mod 2. So, the factor group has the elements $\{0,1\}$, with its law of composition being addition mod 2. (Similarly, the numbers mod k under addition are the factor group for the subgroup of numbers divisible by k).

There is a wonderful and simple theorem about subgroups that will be of much use to us. It is called **Lagrange's Theorem**:

If G is any finite group, and H is any subgroup of G , then the number of elements of G is an integer multiple of the number of elements of H .

We can prove it by showing that any two cosets aH and bH have the same number of elements as H itself has, and are either identical or have no elements in common.

Let G be a finite group. Let H be a subgroup of G of size n . (We assume that H contains distinct elements, because otherwise we could throw out the duplicates). Let a be an element of G , that is not in H . Then aH is a coset of H with n elements in it, one for each element of H . The elements of aH are all distinct, because if $ah_1 = ah_2$, then $h_1 = h_2$, and we already said that the elements of H are distinct. Thus, aH is of size n . The same argument applies for any coset of H . This tells us that any two cosets of H will have the same number of elements as H .

If we have that $ah = bh'$, for some h and h' in H , then we can multiply both sides by h^{-1} to get that $ahh^{-1} = bh'h^{-1}$, and since $hh^{-1} = I$, we get that $aI = a = bh'h^{-1}$. This means that for any h'' in H , we have that $ah'' = bh'h^{-1}h''$, and since h', h^{-1} , and h'' are all in H , we get that their product is also in H , and thus $ah'' = bh''$, for some h'' in H . This means that any member of a 's coset is a member of b 's, which means that the two cosets are identical. Thus, if two cosets of H are not entirely distinct, then they are completely identical.

Now, since G is finite, there are finitely many g in G such that g is not in H . We note that every element of G is either in H or in a coset of H , because if g is an element of G that is not in H , then g 's coset contains the element $gI = g$ (since I is in H). Thus, if we take all the cosets of H along with H itself, we have all the elements of G . We now line up all the cosets of H into a rectangle like so (we assume H is of size n and there are k cosets):

$$\begin{array}{cccc}
h_1 & h_2 & \dots & h_n \\
g_1 h_1 & g_1 h_2 & \dots & g_1 h_n \\
g_2 h_1 & g_2 h_2 & \dots & g_2 h_n \\
\cdot & \cdot & \dots & \cdot \\
\cdot & \cdot & \dots & \cdot \\
\cdot & \cdot & \dots & \cdot \\
g_k h_1 & g_k h_2 & \dots & g_k h_n
\end{array}$$

This rectangle contains every element of G . However, it is possible that some of the cosets are not distinct. We showed above that if two cosets share any element, then they are duplicates. Thus, if we remove all duplicate cosets, then our new rectangle will contain every element of G exactly once. The width of the rectangle is the size of H , and the number of elements in the rectangle is its height times its width. Thus, the number of elements of G is an integer multiple of the size of H . This proves our theorem.

□

It follows from Lagrange's theorem that if the number of elements of G (called its **order**) is prime, then its only subgroups are itself and the group consisting of I alone.

Every element A of every finite group G generates a subgroup that consists of its positive powers: A, A^2, A^3, \dots . This sequence must end since G is finite. The list is obviously closed under multiplication, and thus is a subgroup. The order of this subgroup is also called the order of A . By Lagrange's theorem, the order of G must be an integer multiple of the order of any element.

A group is said to be **cyclic** if it is generated by one of its elements. That is, there exists an element of the group A such that every element of the group is a power of A . We can deduce here that any group of prime order is cyclic, since the order of any of its elements other than the identity must be the order of the subgroup it generates, which can only be the whole group G .

Any group of prime order is normal since it has no non-trivial subgroups as all (a non-trivial subgroup is one that is not I or G).

A group without non-trivial normal subgroups is said to be **simple**. Not that long ago mathematicians were able to complete a list of all the simple groups. These include three general classes of matrix groups and a finite number of other weird groups including several of enormous size. Every simple group has a faithful representation as one of these.

Is the group of permutations of n symbols simple? The answer is no, for n at least 3 (we state this without proof).

Any permutation can be constructed by starting from the identity permutation³ and switching pairs of elements. These switches are called **transpositions** (in the permutation's matrix form, this corresponds to switching two of the rows of the matrix). For example, to get the permutation $\{1\ 5\ 3\ 2\ 4\}$, we could start with $\{1\ 2\ 3\ 4\ 5\}$ and then transpose 2 and 5 to get $\{1\ 5\ 3\ 4\ 2\}$ and then transpose 4 and 2 to get $\{1\ 5\ 3\ 2\ 4\}$. A permutation is said to be **even** if it can be constructed using an even number of transpositions; otherwise the permutation is said to be **odd** (this corresponds to the determinant of the permutation matrix being +1 or -1).

The even permutations of n elements form a subgroup called the **alternating group** on n elements, denoted as A_n . Since this group has only one coset other than itself (that of the odd permutations on n elements), that coset is unique, whether defined from the left or right, and thus the alternating group is always a normal subgroup.

17.5 Conjugacy

Two elements of a group, A and B , are called **conjugates** if there is a group element C such that $AC = CB$. Multiplying both sides on the right by C^{-1} , this gives us that $A = CBC^{-1}$. Similarly, we can get that $B = CAC^{-1}$. If A and B are conjugates and B and C are conjugates, then A and C are as well (see exercises for more info).

We can partition any finite group into blocks called conjugacy classes, such that each pair of members in every block are conjugates of one another.

Among permutation groups, two elements are conjugate if their cycle structure is the same. Thus, for example, any two permutations of 7 elements that consist of one cycle of length 3 and another of length 4 are conjugate to one another.

Thus, while there are $n!$ elements of the group of permutations of n objects (written as S_n), there are only a number of conjugacy classes given by the number of partitions of n into blocks.

This leads to the question: *How many partitions of n into blocks are there, i.e. how many conjugacy classes S_n does the permutation group on n elements possess?*

Let us look at what happens when n is small. Suppose, for example, that $n = 9$.

We will list out all the possible partitions of 9 elements into cycles. In order to save space, we shall omit all cycles of size 1, which correspond to fixed points. We shall use numbers to indicate the size of a cycle, and commas to separate different cycles. This means that the difference between n and the sum of the block sizes shown is made up of blocks of size 1. Thus, (2,3) indicates a cycle of size 2 and a cycle of size 3, omitting the 4 cycles of size 1. Note that the order of the cycles does not matter, only their size.

³ This is the permutation $\{1\ 2\ 3\ \dots\ n\}$ which leaves all the symbols exactly as they are without mixing up the order.

Then we have the partition that is all 1's, then (2), (3), (4), (2,2), (5), (3,2), (6), (4,2), (3,3), (2,2,2), (7), (5,2), (4,3), (3,2,2), (8), (6,2), (5,3), (4,4), (4,2,2), (3,3,2), (2,2,2,2), (9), (7,2), (6,3), (5,4), (5,2,2), (4,3,2), (3,3,3), (3,2,2,2). There are a total of 30 of them. On the other hand, there are 9! or 362880 elements of the permutation group on 9 symbols.

We can count these numbers on a spreadsheet by using the following properties:

Let the number of partitions of n into k blocks be denoted as $p(n,k)$.⁴

Then we have

$$p(0,0) = 1,$$

$$p(n,k) = 0 \text{ for } k > n \text{ or } k < 0,$$

and

$$p(n,k) = p(n-1, k-1) + p(n-k, k)$$

The last of these statements represents the fact that the partitions that include a block of 1 are, if we ignore that block, partitions of $n-1$ into $k-1$ blocks; while partitions which have all blocks at least 2 become partitions of $n-k$ into k blocks, if we subtract 1 from each block. This recursive algorithm can help us count blocks using a spreadsheet. Try to figure out yourself what spreadsheet commands to use. As a guide, here is the spreadsheet for $0 \leq n \leq 9, 0 \leq k \leq 9$:

		k = number of blocks										sum	
		0	1	2	3	4	5	6	7	8	9		
n = number of partitions	0	1	0										0
	1	0	1	0									1
	2	0	1	1	0								2
	3	0	1	1	1	0							3
	4	0	1	2	1	1	0						5
	5	0	1	2	2	1	1	0					7
	6	0	1	3	3	2	1	1	0				11
	7	0	1	3	4	3	2	1	1	0			15
	8	0	1	4	5	5	3	2	1	1	0		22
	9	0	1	4	7	6	5	3	2	1	1		30

We can express the condition that a subgroup is normal by the statement that its elements consist of complete conjugacy classes.

We now look some examples. Consider the alternating groups on 3, 4, and 5 objects.

⁴ Not to be mistaken for the probability function from notes 7.

The elements of these groups are the even permutations of the objects, which are those with an even number of even cycles. Once again, we will count by looking at the size of the cycles, but this time without omitting the cycles of size 1.

For $n=3$: (1,1,1) - there is one such element, the identity.

(3) - there are two such three cycles of three elements (123) and (132).

This group, then, has three elements.

In this case, the alternating group is a cycle and has no normal subgroups.

For $n = 4$: (1,1,1,1) – The identity

(2,2) – there are three of these (12)(34), (13)(24), and (14)(23)

(3,1) – there are 8 of these, namely (1)(234), (1)(243), (2)(134), (2)(143), etc.

The alternating group has 12 elements. The first two conjugacy classes here have four elements, and form a subgroup. This is a normal subgroup of S_4 .

For $n = 5$: (1,1,1,1,1) – The identity

(3,1,1) – 20 of these; two ways of cycling 3 elements and $\binom{5}{2}$ ways of picking out two not to cycle.

(2,2,1) – 15 of these; 5 objects to leave out and 3 ways to split 4 in two.

(5) – 24 of these; start with 1 and add the rest in any of 4! Orders

The alternating group has 60 elements.

Exercises

Exercise 1 Write down the multiplication table for the group of permutations of 3 symbols.

Exercise 2 Show that each row of a group multiplication table is a permutation of the elements of the group, and that no two rows are the same.

Exercise 3 If A and B are conjugates and B and C are conjugates, show that A and C are conjugate as well.

Exercise 4 Find the conjugacy classes for S_6 , which is the group of all permutations of six symbols. Prove that its alternating group (denoted by A_6) has no normal subgroups.

~Edited by Jacob Green