

MA294 Lecture

Timothy Kohl

Boston University

July 12, 2021

Permutation Groups

Groups like D_3 are one example of a broad (and critically important) class of groups called permutation groups.

Definition

Given a (finite) set X , a function $\sigma : X \rightarrow X$ that is one-to-one and onto is a permutation of X .

i.e. $\sigma(x_1) = \sigma(x_2)$ implies $x_1 = x_2$ and given $y \in X$, there exists $x \in X$ such that $\sigma(x) = y$.

Example: $X = \{1, 2, 3\}$, let $\sigma : X \rightarrow X$ be given by $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.

Note: We can think of this as a 're-ordering' of the elements of X , i.e.

$$\{1, 2, 3\} \rightarrow \{2, 3, 1\}$$

and if one has two permutations σ, τ of X then, because they are functions, they can be composed.

Proposition

Given two permutations σ, τ of X , the composite $\sigma \circ \tau$ defined by $(\sigma \circ \tau)(x) = \sigma(\tau(x))$ is also a permutation.

Proof.

It's clear that $\sigma \circ \tau$ is a function from X to X . If now $(\sigma \circ \tau)(x_1) = (\sigma \circ \tau)(x_2)$ then $\sigma(\tau(x_1)) = \sigma(\tau(x_2))$ so, since σ is 1-1, we have that $\tau(x_1) = \tau(x_2)$, and since τ is 1-1, then $x_1 = x_2$.

Similarly, $\sigma \circ \tau$ is onto since both σ and τ are each onto. □

Note: If X is finite then σ being 1-1 is equivalent to it being onto, so you only need to check that it's 1-1 to verify it's a permutation.

Example: If $X = \{1, 2, 3\}$, and $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 2$, and $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ then

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 2$$

$$(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(3) = 1$$

$$(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(2) = 3$$

and in comparison $(\tau \circ \sigma)(1) = 3$, $(\tau \circ \sigma)(2) = 2$, $(\tau \circ \sigma)(3) = 1$, the point being that $\sigma \circ \tau \neq \tau \circ \sigma$ as functions from X to X .

Theorem

Given a (finite) set X , the set $\text{Perm}(X)$, (also called $\text{Sym}(X)$) of all permutations of X forms a group under composition.

Proof.

We've already verified closure, and we've already mentioned that function composition is associative.

The permutation $I : X \rightarrow X$ given by $I(x) = x$ for all $x \in X$ is the identity since $(\sigma \circ I)(x) = \sigma(I(x)) = \sigma(x)$, so $\sigma \circ I = \sigma$ and similarly $I \circ \sigma = \sigma$.

And as each σ is a bijection, it has an inverse as a function σ^{-1} which can be shown (Exercise!) is also a permutation and that, of course $\sigma \circ \sigma^{-1} = I = \sigma^{-1} \circ \sigma$. □

Ex:

$$\sigma(1) = 2$$

$$\sigma(2) = 3$$

$$\sigma(3) = 1$$

implies

$$\sigma^{-1}(1) = 3$$

$$\sigma^{-1}(2) = 1$$

$$\sigma^{-1}(3) = 2$$

The following fact is very reminiscent of certain arguments one sees in statistics, especially in questions about 'how many ways are there to do something'.

Theorem

If $|X| = n$ then $|Perm(X)| = n!$.

Proof.

Say $X = \{x_1, x_2, \dots, x_n\}$ then for $\sigma \in Perm(X)$ we have

- n choices for $\sigma(x_1)$
- $n - 1$ choices for $\sigma(x_2)$
- $n - 2$ choices for $\sigma(x_3)$
- $\downarrow$
- 2 choices for $\sigma(x_{n-1})$
- 1 choices for $\sigma(x_n)$

so that there are $n \cdot (n - 1) \cdot (n - 2) \cdots 2 \cdot 1 = n!$ possible different permutations σ . □

Notation: For $X = \{1, \dots, n\}$, $\text{Perm}(X) = S_n$, the n^{th} symmetric group.

For small n one can readily enumerate the elements of S_n .

For $\sigma \in S_3$, $\sigma(1) = a$, $\sigma(2) = b$, $\sigma(3) = c$ so we can express σ in 'table notation'

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

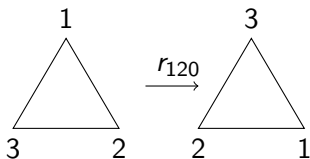
The permutations of $\{1, 2, 3\}$ should remind one of the dihedral group D_3 , especially since both have 6 elements and permute three 'points'.

Definition

A group G is a permutation group if $G \leq \text{Perm}(X)$ for some X .

Note, this is not saying $G = \text{Perm}(X)$, but that G acts *as* permutations on set X , but does not necessarily represent *all* permutations of X .

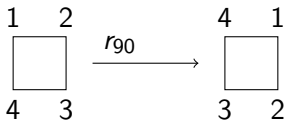
As alluded to on the previous page, our first example is S_3 above, which can be viewed as D_3 if we view the elements of D_3 as permutations of the vertices $\{1, 2, 3\}$, for example:



so that we can associate $r_{120} \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

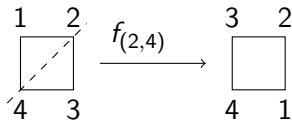
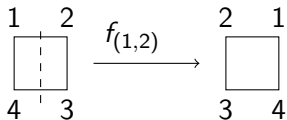
As we mentioned a while ago, for every n there is the n^{th} Dihedral group D_n of symmetries of the n -gon.

Example: $D_4 = \{r_0, r_{90}, r_{180}, r_{270}, f_{(1,2)}, f_{(2,3)}, f_{(3,4)}, f_{(1,3)}\}$



which, since $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1$, is representable by the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$.

The other rotations are fairly clear.
As to the flips consider:



$$f_{(1,2)} \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$f_{(2,4)} \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

where the subscript indicates the 'axis' about which the square is flipped.

As a subgroup of S_4 , we can represent D_4 as follows:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \right. \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\ \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \right\}$$

so $|D_4| = 8$ is a permutation group, but is not all of S_4 since $|S_4| = 4! = 24$.

Cycle Structure and Orbits

We have seen the 'table' notation for elements of S_n , e.g.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix} \in S_6$$

but as n increases, this notation becomes cumbersome.

There is a more efficient notation for permutations built on the notion of a 'cycle'.

Definition

For $S_n = \text{Perm}(\{1, \dots, n\})$ the k -cycle $(i_1, i_2, \dots, i_k)$ is that permutation σ which acts as follows:

$$\sigma(i_1) = i_2$$

$$\sigma(i_2) = i_3$$

$$\vdots$$

$$\sigma(i_{k-1}) = i_k$$

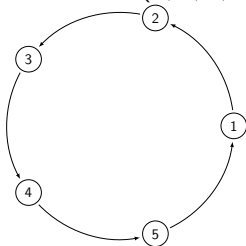
$$\sigma(i_k) = i_1$$

and where $\sigma(x) = x$ for those $x \notin \{i_1, \dots, i_k\}$.

The usage of the term 'cycle' is to highlight the fact that the permutation moves each i_t to i_{t+1} in a loop back all the way to i_1 .

And again, those i not 'in the loop' are left fixed by the cycle.

For example, consider $\sigma = (1, 2, 3, 4, 5) \in S_8$



i.e. $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 5, \sigma(5) = 1$, and $\sigma(6) = 6, \sigma(7) = 7, \sigma(8) = 8$

Table Notation: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 8 \end{pmatrix}$.

Beyond individual cycles, we can look at products of cycles.

Definition

Two cycles $(i_1, i_2, \dots, i_k)$ and $(j_1, j_2, \dots, j_l)$ in S_n are disjoint if $\{i_1, i_2, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$.

e.g. $(1, 3, 5)$ and $(2, 7)$ are disjoint but $(1, 2)$ and $(2, 3, 4)$ are not.

Proposition

If $\sigma = (i_1, \dots, i_k)$ and $\tau = (j_1, \dots, j_l)$ are disjoint cycles, then $\sigma \circ \tau = \tau \circ \sigma$.

Why? Basically

$$(i_1, \dots, i_k) \circ (j_1, \dots, j_l)(x) = \begin{cases} j_{t+1} & \text{if } x = j_t \\ i_{r+1} & \text{if } x = i_r \\ x & \text{if } x \notin \{i_1, i_2, \dots, i_k\} \cup \{j_1, \dots, j_l\} \end{cases}$$

which is the same as $(j_1, \dots, j_l) \circ (i_1, \dots, i_k)(x)$.

Cycles can be used to represent all permutations in S_n .

Theorem

Every permutation in S_n is a product of disjoint cycles.

In lieu of a formal proof, let's consider an example to see how this works.

Say $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 7 & 1 & 4 & 2 & 8 \end{pmatrix}$ then to compute the cycles σ gives rise to we start with say 1 and see what happens when we keep applying σ :

- $\sigma(1) = 3$
- $\sigma(3) = 5$
- $\sigma(5) = 1$

so we stop and see that we get the cycle $(1, 3, 5)$.

Now consider another element of $\{1, 2, \dots, 7, 8\}$, say 2, and see what repeated applications of σ do

- $\sigma(2) = 6$
- $\sigma(6) = 4$
- $\sigma(4) = 7$
- $\sigma(7) = 2$

and we stop and see that we get the cycle $(2, 6, 4, 7)$.

The only remaining element is 8, but $\sigma(8) = 8$ so we can ignore it.

So

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 7 & 1 & 4 & 2 & 8 \end{pmatrix}$$

can be written (compactly!) as the product

$$\sigma = (1, 3, 5)(2, 6, 4, 7)$$

which conveys exactly the same information as the table notation.

Note, what if we had started the analysis by following what happens with 2, and then 1, then we would have gotten the cycles $(2, 6, 4, 7)$ and $(1, 3, 5)$ and written $(2, 6, 4, 7)(1, 3, 5)$ which, as we mentioned earlier, is the same permutation since disjoint cycles commute.

As another example, for practice, consider

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 5 & 3 & 8 & 2 & 6 & 4 & 9 \end{pmatrix}$$

which can be written as the product $(2, 7, 6)(3, 5, 8, 4)$.

Note also, in a given cycle, the order doesn't matter as far as the cycle is concerned. e.g.

$$\begin{aligned}(1, 4, 7, 3, 2) &\in S_7 \\ &= (4, 7, 3, 2, 1) \\ &= (7, 3, 2, 1, 4) \\ &= (3, 2, 1, 4, 7) \\ &= (2, 1, 4, 7, 3)\end{aligned}$$

And if one has a given cycle

$$\sigma = (i_1, i_2, \dots, i_k)$$

then the inverse image is easy to compute, namely

$$\sigma^{-1} = (i_1, i_k, i_{k-1}, \dots, i_2)$$

for example $(1, 4, 7, 3, 2)^{-1} = (1, 2, 3, 7, 4)$.

Note: In a given cycle, we never include elements which are left fixed, by that cycle, e.g. $\sigma = (1, 3, 4) \in S_4$ fixes 2 and we purposely do **not** write this as $(1, 3, 4)(2)$ which would *technically* be correct, but is unnecessary, since the omission of 2 tells us that it is not 'moved' by σ .

Note also that the identity permutation is traditionally written as an 'empty' cycle, namely $()$.

Two other basic, but important facts come from using cycle notation:

Proposition

For $(i_1, \dots, i_k)$ we have $|(i_1, \dots, i_k)| = k$.

For example, for $\sigma = (1, 3, 5)$,

$$\sigma(1) = 3, \sigma(\sigma(1)) = \sigma(3) = 5, \text{ and } \sigma(\sigma(\sigma(1))) = \sigma(5) = 1$$

i.e. $\sigma^3(1) = 1$, and similarly $\sigma^3(3) = 3$ and $\sigma^3(5) = 5$, so $\sigma^3 = I$.

Proposition

If $\sigma = \sigma_1 \sigma_2 \cdots \sigma_t$ where the σ_i are disjoint cycles where σ_i is a k_i -cycle (of length/order k_i) then $|\sigma| = \text{lcm}(k_1, k_2, \dots, k_t)$

Proof.

Suppose $g_1, g_2 \in G$ where $|g_1| = k_1$ and $|g_2| = k_2$ where $g_1 g_2 = g_2 g_1$ then $(g_1 g_2)^2 = g_1 g_2 g_1 g_2 = g_1 g_1 g_2 g_2 = g_1^2 g_2^2$.

And in general $(g_1 g_2)^m = g_1^m g_2^m$, so the question is what is $|g_1 g_2|$?

Well, $(g_1 g_2)^m = g_1^m g_2^m$ so if $(g_1 g_2)^m = e$ then $g_1^m = e$ and $g_2^m = e$ which means $|g_1| \mid m$ and $|g_2| \mid m$ so the least m for which this is true is $\text{lcm}(|g_1|, |g_2|) = \text{lcm}(k_1, k_2)$.

The argument is the same for the product of more than 2 group elements which commute, e.g. disjoint cycles in S_n . □

One kind of neat application of this is this, what is the largest order of any element in S_n ?

Example: S_2 ? Well S_2 has just $2! = 2$ elements, namely $\{(), (1, 2)\}$, so the maximum order is 2.

Example: S_3 ? Since there are no '1-cycles' the only elements are 2-cycles (a, b) and 3-cycles (a, b, c) so the max. order is 3.

Example: S_4 ? In S_4 we have 4-cycles, 3-cycles, 2-cycles and products of two 2-cycles, $(a, b)(c, d)$ so the max is 4.

Example: S_5 ? In S_5 we have elements with cycle structures like (a, b, c, d, e) , (a, b, c, d) , (a, b, c) , $(a, b)(c, d)$, (a, b) ... any others?

Yes, S_5 has 'room' for a product $(a, b, c)(d, e)$ (where a, b, c, d, e are distinct!) and an element like this has order
 $\text{lcm}(|(a, b, c)|, |(d, e)|) = \text{lcm}(3, 2) = 3 \cdot 2 = 6$ since $\text{gcd}(3, 2) = 1$.

Example: S_6 ? The max order is 6. (Exercise.)

Example: S_7 ? The general principle to mention for this and all larger ones is the question of what kind of products of disjoint cycles can you make?

And therefore how big an lcm can you have?

This is also tied in with a question we shall examine later on, which is, how many ways can one write a natural number as a sum of natural numbers? Each such sum is called a 'partition' of n , for example:

$$\begin{aligned}5 &= 5 \\&= 4 + 1 \\&= 3 + 2 \\&= 3 + 1 + 1 \\&= 2 + 2 + 1 \\&= 2 + 1 + 1 + 1 \\&= 1 + 1 + 1 + 1 + 1\end{aligned}$$

and this ties in very closely with how many products of disjoint cycles exist in a given S_n .