MA294 Lecture

Timothy Kohl

Boston University

February 22, 2024

Lagrange's Theorem

Theorem

If G is a finite group and $H \leq G$ then $|H| \mid |G|$.

Proof.

We've already established most of the important facts.

We know that with respect to H, there exists elements of G, $g_1, \ldots, g_r$ such that

$$G = g_1 H \cup g_2 H \cup \cdots \cup g_r H$$

where each coset is disjoint from the others, and so

$$|G| = |g_1 H| + |g_2 H| + \cdots + |g_r H|$$

and the proof is finished by recalling the other fact we noted, which is that $|g_i H| = |H|$ for each g_i and so $|G| = r|H|$, that is $|H| \mid |G|$. □

One other point to mention about cosets is related to notation.

Definition

If $H \leq G$ then the number of distinct cosets of H in G is the index of H in G and is denoted $[G : H]$.

We note, that if G is finite, then Lagrange's theorem implies that $[G : H] = \frac{|G|}{|H|}$.

We note, for reference, that $[G : H]$ also makes sense for infinite groups.

Consider $G = \mathbb{Z}$ and $H = 2\mathbb{Z} \leq G$, namely $H = \{\dots, -4, -2, 0, 2, 4, \dots\}$ and start with the trivial coset

$$0 + H = \{\dots, -4, -2, 0, 2, 4, \dots\} \text{ (all even integers!)}$$

and since this is not all of $\mathbb{Z}$ we pick an element not in H, say 1 and consider the coset

$$1 + H = \{\dots, -3, -1, 1, 3, 5 \dots\} \text{ (all odd integers!!)}$$

and we realize that there are no other elements not already accounted for, so we're done and we can write

$$\mathbb{Z} = (0 + H) \cup (1 + H) \text{ i.e. the union of the even and odd integers}$$

so $[\mathbb{Z} : 2\mathbb{Z}] = 2$.

Exericse: What is $[\mathbb{Z} : m\mathbb{Z}]$ where $m\mathbb{Z} = \langle m \rangle$?

One other thing to note is that everything we say about left cosets, holds for right cosets as well, so there's no particular 'preference' for left cosets over right cosets.

That is, the number of left cosets of a subgroup $H \leq G$ is the same as the number of right cosets, and a group can be partitioned into a disjoint union of right cosets.

The only point to reiterate is that for a given subgroup, $H \leq G$ it need not be the case that $gH = Hg$.

Here is one of the first applications of Lagrange's theorem, and what is kind of extraordinary is how simple the proof is, considering the depth of the statement being proved.

We have seen that, for example, there are two groups with 4 elements, for example $\mathbb{Z}_4$ and $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ and a general question that's important in group theory is:

How many distinct groups are there of a given order (size)?

where by distinct, we mean not isomorphic, for example $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

For $|G| = 4$ for example, it turns out that there are only 2 non-isomorphic groups, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ but, in general, it gets harder to figure out the number of different groups of order (size) n as n gets larger.

We can say this however.

Theorem

If $|G| = p$ for p a prime number, then $G \cong C_p$. (where $C_p \cong \mathbb{Z}_p$)

Proof.

Let $x \in G$ and consider $H = \langle x \rangle \leq G$.

If $x = e$ then $|H| = 1$ of course. If $x \neq e$ then $|H| > 1$ but, by Lagrange's theorem, $|H| \big| |G|$.

However, since $|G| = p$ then, since $|H| > 1$ we must have $|H| = p$, so that $H = \{e, x, x^2, \ldots, x^{p-1}\}$.

But $|H| = |G| = p$ and H is a subset of G, which means $H = G$, but this means $G = \langle x \rangle$ and so $G \cong C_p$, the cyclic group of order p. $\square$

This is somewhat extraordinary since it implies, for example that there is exactly 1 group of order 127, but, in contrast, it is known that there are 2328 groups of order 128!

Again, the number of distinct groups of a given size is, in fact, an open problem in group theory.

One of the other facts we can infer from looking at the proof of the above theorem is this.

Proposition

If G is a finite group, say $|G| = n$ then for $x \in G$, one has $|x| \big| n$. (i.e. $|x| \big| |G|$)

Why?

Quite simply, if $x \in G$, then x gives rise to the subgroup $H = \langle x \rangle = \{e, x, \ldots, x^{m-1}\}$ for some m where $|x| = m = |H|$, so by Lagrange's theorem, $m|n$.

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 $\sigma : X \to X$ 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 $\sigma : X \to X$ 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.

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

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 $Perm(X)$, (also called $Sym(X)$) 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 $I : X \to X$ 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 $X = \{x_1, x_2, \ldots, x_n\}$ 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 $X = \{1, \ldots, n\}$, $Perm(X) = S_n$, 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'

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

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

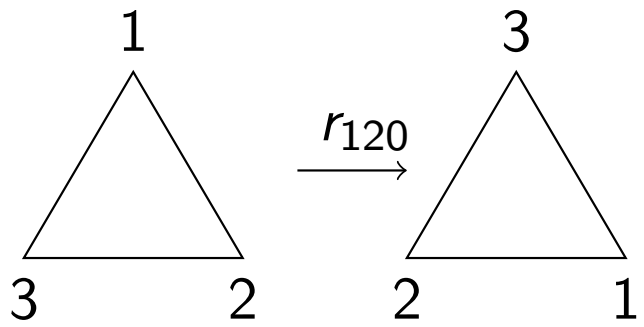
The permutations of $\{1, 2, 3\}$ should remind one of the dihedral group D_3, especially since both have 6 elements and permute three 'points'.

Definition

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

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

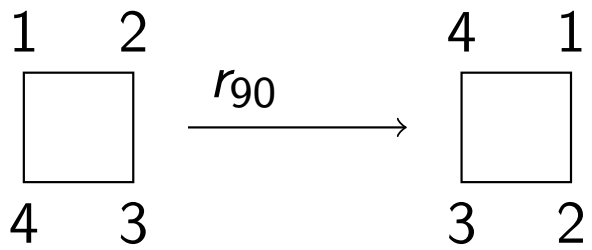
As alluded to on the previous page, our first example is S_3 above, which can be viewed as D_3 if we view the elements of D_3 as permutations of the vertices $\{1, 2, 3\}$, for example:



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

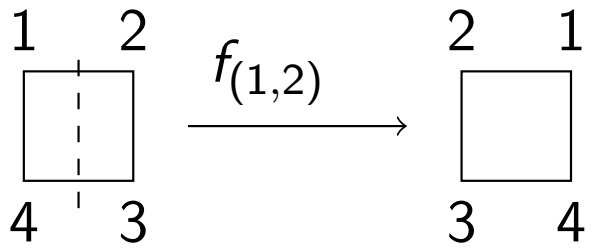
As we mentioned a while ago, for every n there is the n^{th} Dihedral group D_n of symmetries of the n-gon.

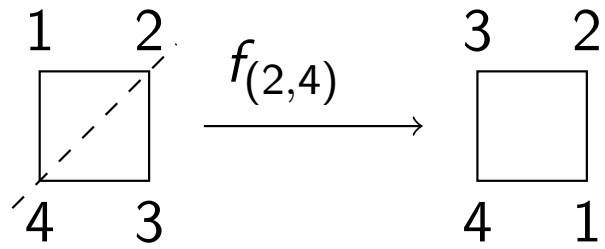
Example: $D_4 = \{r_0, r_{90}, r_{180}, r_{270}, f_{(1,2)}, f_{(2,3)}, f_{(3,4)}, f_{(1,3)}\}$



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:





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

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 $|S_4| = 4! = 24$.