Some Basic Group Theory with Lagrange's Theorem

Kayla Wright

April 29, 2014

Recall the 4 group properties of some group $(G, \text{🦇})$:

Identity: $\exists$ some element $e \in G$ such that $\forall a \in G$, $a \,\text{🦇}\, e = a$.

Inverses: $\forall a \neq e \in G$, $\exists$ a unique number $a^{-1} \in G$ such that $a \,\text{🦇}\, a^{-1} = e$.

Associativity: $\forall a, b, c \in G$, $a \,\text{🦇}\, (b \,\text{🦇}\, c) = (a \,\text{🦇}\, b) \,\text{🦇}\, c$.

Closure: $\forall a, b \in G$, $a \,\text{🦇}\, b \in G$.

Continuous vs. Finite Groups:

Definitions: As suggested by the name, **finite groups** contain a finite number of elements whereas **continuous groups** contain an infinite number of elements.

Subgroups:

Definitions: A **subgroup** is a subset of the group (G,🦇) and is a group in its own right under the operation 🦇.

Defining Notation:

Generators:

- A generating set, $\langle a \rangle \in G$, of a group is a subset such that every element of the group can be expressed as the combination (under the group operation) of finitely many elements of the subset and their inverses.

Order :

- The order of a group, $\mid G \mid$, denotes the number of elements within a group.

Recall Fermat's Little Theorem:

Theorem:

- Let p be a prime number. Then $n^p \equiv n \mod p$ for any integer $n \geq 1$.

Two cases:

Either:
- p divides n
- Implying that p divides $n^p - n$
- YAY :D (Paddy face)

Or:
- p does not divide n
- WE HAVE WORK TO DO

When p does not divide n:

Let's begin:

- Consider the group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ and any subset $[a] \in G$.
- Let o denote the order of $\langle [a] \rangle$.
- We know that whatever generates that subgroup, $\langle [a] \rangle$ must also be a subgroup of Z_p.
- By the previous theorem, $\mid \langle [a] \rangle \mid \; = k$.

Lemma (Lagrange's Theorem):

Lemma:

- If H is a subgroup of a finite group G....
- By this theorem, $|H|$ divides $|G|$.
- We will be proving this later!

Applying it to the Problem:

This implies that

- $| \langle [a] \rangle | = | (\mathbb{Z}/p\mathbb{Z})^\times |$

And also implies that

- k divides $p - 1$ due to the order of the two groups

Now

- By definition of modular congruence: $\exists d \in \mathbb{Z}$ such that $p - 1 = kd$.
- From this, we can deduce that $n^k \equiv 1 \mod p$, $\forall n \in [a]$.
- And applying what we know, we can state that $n^{kd} \equiv 1^d \equiv 1 \mod p$.
- Because we know $kd = p - 1$, we can arrive at the conclusion that Fermat's Little Theorem is true.

Cosets:

Definiton:

- If H is a subgroup of G and $a \in G$, the **coset** defined as aH is the subset of G such that $aH = \{ah \mid h \in H\}$.

Examples of Cosets:

Consider $\langle \mathbb{Z}, + \rangle$

- Let H be $\{\cdots - 6, -4, -2, 0, 2, 4, 6 \ldots\}$
- Cosets would look like this...
- $a = 0$ will form
  $0 + H = \{\cdots - 6, -4, -2, 0, 2, 4, 6 \ldots\}$
- $a = 1$ will form
  $1 + H = \{\cdots - 5, -3, -1, 1, 3, 5 \ldots\}$

More on Cosets:

Left or Right

- Cosets can be either left or right.
- $gH = gh : h$ an element of H is a left coset of H in G.
- and $Hg = hg : h$ an element of H is a right coset of H in G.

But

- For simplicity's sake, we will just consider all cosets for the talk as right cosets

How to Attack the Proof:

Langrange's Theorem:

- In order to prove Lagrange's Theorem, we will need to prove two parts.

Lemma 1:

- All cosets are of equal cardinality.
- Formally, for a subgroup H, and some element $k \in H$: $\mid H \mid = \mid H_k \mid$

Lemma 2:

- All the cosets partition the entire group.
- This statement implies that for two cosets H_k, H_l for $k, l \in G$, there will be no intersection unless $H_k = H_l$.

Proof of Lemma 1:

Claim:

- $\mid H \mid \; = \; \mid H_k \mid$ for some $k \in G$.
- Suppose that $\mid H \mid \; \geq \; \mid H_k \mid$ when considering $h, k \forall h \in H$.
- Note that in order to satisfy equality, we know that $h_1 k \neq h_2 k$ and therefore, $h_1 \neq h_2$.

But!!

- When inverses are applied, we can manipulate the statement in the following way:
- $h_1 k \neq h_2 k$
- $h_1 k k^{-1} \neq h_2 k k^{-1}$
- $h_1 \neq h_2, \forall k \in H$

Proof of Lemma 2:

- Two cosets are either equal or disjoint.

Claim:

- If we take any 2 cosets H_k, H_l for $k, l \in G$. If $\exists$ some $x \in H_k, H_l$, then $H_k = H_l$

Proof:

- Take $x = h_1 k = h_2 k$ for some $h_1, h_2 \in H$
- By applying inverses: $h_2^{-1} h_1 = lk^{-1}$ and we know that $lk^{-1} \in H$
- Take any element $y \in H_k$.
- Write $y = hk$ for some $h \in H$.
- Multiply by lk^{-1} and its inverse to obtain $h(lk^{-1})^{-1} lk^{-1} k$.
- With this, we can deduce that $h(lk^{-1})^{-1} \in H$ and that $lk^{-1}k = l$.
- This means that $y \in H_l$, $(lk^{-1})^{-1} = kl^{-1} \in H$

The Result of the Two Lemmas:

Lagrange's Theorem

- Who can explain why?
- This result is very powerful and as shown before, helped prove Fermat's Little Theorem!

Homework Problem:

Music! ▶

	C	$C^{\sharp}$	D	$D^{\sharp}$	E	F	$F^{\sharp}$	G	$G^{\sharp}$	A
C	C	$C^{\sharp}$	D	$D^{\sharp}$	E	F	$F^{\sharp}$	G	$G^{\sharp}$	A
$C^{\sharp}$	$C^{\sharp}$	D	$D^{\sharp}$	E	F	$F^{\sharp}$	G	$G^{\sharp}$	A	$A^{\sharp}$
D	D	$D^{\sharp}$	E	F	$F^{\sharp}$	G	$G^{\sharp}$	A	$A^{\sharp}$	B
$D^{\sharp}$	$D^{\sharp}$	E	F	$F^{\sharp}$	G	$G^{\sharp}$	A	$A^{\sharp}$	B	C
E	E	F	$F^{\sharp}$	G	$G^{\sharp}$	A	$A^{\sharp}$	B	C	$C^{\sharp}$
F	F	$F^{\sharp}$	G	$G^{\sharp}$	A	$A^{\sharp}$	B	C	$C^{\sharp}$	D
$F^{\sharp}$	$F^{\sharp}$	G	$G^{\sharp}$	A	$A^{\sharp}$	B	C	$C^{\sharp}$	D	$D^{\sharp}$
G	G	$G^{\sharp}$	A	$A^{\sharp}$	B	C	$C^{\sharp}$	D	$D^{\sharp}$	E
$G^{\sharp}$	$G^{\sharp}$	A	$A^{\sharp}$	B	C	$C^{\sharp}$	D	$D^{\sharp}$	E	F
A	A	$A^{\sharp}$	B	C	$C^{\sharp}$	D	$D^{\sharp}$	E	F	$F^{\sharp}$
$A^{\sharp}$	$A^{\sharp}$	B	C	$C^{\sharp}$	D	$D^{\sharp}$	E	F	$F^{\sharp}$	G
B	B	C	$C^{\sharp}$	D	$D^{\sharp}$	E	F	$F^{\sharp}$	G	$G^{\sharp}$

Problem:

- Pick some subgroup H, what are the cosets of H?
- For those with musical background, what does this represent musically?