Chap 6 Lagrange's Theorem

Lagrange's Theorem

If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

number of elements in H

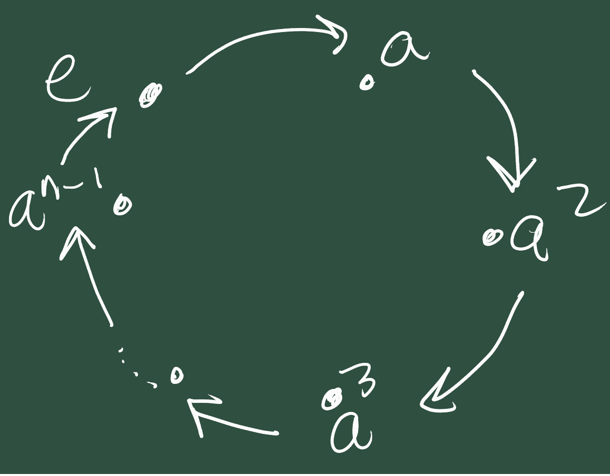
number of elements in G

So eg. If $|G| = 100$, then we may see subgroups H of G with

$|H| = 1, 2, 5, 10, 20, 25, 4, 50, 100$.

Any other order cannot arise.

We've already seen this in the case of cyclic groups. So if we have $G = \langle a \rangle$ and $|G| = n$.



In chapter 4 on cyclic groups we proved that for any k,

$H = \langle a^k \rangle$ is a subgroup of G

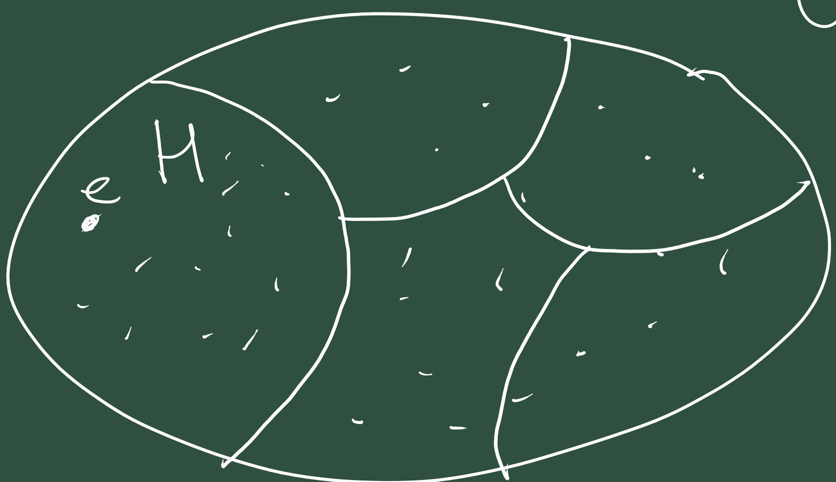
and $|H| = \frac{n}{d}$, $d = \gcd(n,k)$.

and notice $\frac{n}{d}$ is a divisor of n

as $n = d \cdot \frac{n}{d}$

Sketch of the proof of Lagrange's Theorem.

G, $|G| = n$



$|H| = k$.

There is a way to a construct a partition of G from H, with H itself as one of the subsets, and that all the subsets in partition have the same number of elements, i.e. all have k elements.

$$\Longrightarrow |G| = \left(\begin{array}{l}\text{number of subsets} \\ \text{of partition}\end{array}\right) \times |H|$$

6.1 Cosets.

Let G be a group and H one of its subgroups.

Let $g \in G$, the left coset of H in G with representative g is

$$gH = \{gh : h \in H\}$$

Similarly, the right coset ...... is

$$Hg = \{hg : h \in H\}$$

Ex 6.1 $\mathbb{Z}_6$ (integers under addition mod 6).

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$H = \{0, 3\}$

Left cosets are $0+H$, $1+H$, $2+H$, ..., $5+H$.

$0+H=\{0,3\}=3+H.$

$1+H=\{1,4\}=4+H$

$2+H=\{2,5\}=5+H.$

A partition of $\mathbb{Z}_6$.

As $\mathbb{Z}_6$ is abelian, the right cosets of H in $\mathbb{Z}_6$ are exactly these above.

<u>Ex 6.2</u> $G=S_3=\{e,(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$

composition non-Abelian

Consider the subgroup H.

$H=\boxed{\{e,(1\,2\,3),(1\,3\,2)\}}.$

The left cosets are.

$(1)H=(1\,2\,3)H=(1\,3\,2)H=\boxed{H}.$

$(1\,2)H=(1\,3)H=(2\,3)H=\boxed{\{(1\,2),(1\,3),(2\,3)\}}$

These two cosets partition S_3.

Follow the rest of the example.

<u>Lemma 6.3</u> "<u>Ways to talk about cosets being the same</u>"

$$g_1H = g_2H$$

<u>Proof</u> One way to prove is to prove a cycle of implications

<u>Eg. $1 \Rightarrow 2$.</u>

So we assume ①, i.e. $\boxed{g_1H = g_2H.}$

we want to prove ②, i.e. $Hg_1^{-1} = Hg_2^{-1}$

We will prove $\boxed{\underline{Hg_1^{-1} \subset Hg_2^{-1}}}$ <u>AND</u> $Hg_2^{-1} \subset Hg_1^{-1}$

Let $x \in Hg_1^{-1}$

$\Rightarrow x = hg_1^{-1}$, for some $h \in H$.

$= (\underbrace{g_1h^{-1}}_{\in g_1H})^{-1} \qquad \left(= (h^{-1})^{-1}g_1^{-1} = hg_1^{-1}\right)$

$= (g_2k)^{-1}$, for some $k \in H$ by assumption $g_1H = g_2H$

$= k^{-1} g_2^{-1} \in Hg_2^{-1}$

Similarly we can prove that $Hg_2^{-1} \subset Hg_1^{-1}$

Therefore $Hg_2^{-1} = Hg_1^{-1}$, as required.

Notice $1 \Rightarrow 3$ is trivial. Rest left as exercises.

Theorem 6.4 The left cosets of H in G partition G.

Proof Firstly we show that different cosets are disjoint

Let g_1H, g_2H be two cosets we will show that either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$, ie. disjoint.

Suppose $g_1H \cap g_2H \neq \phi$. Let $a \in g_1H \cap g_2H$. This means $a = g_1h_1 = g_2h_2$, for some $h_1, h_2 \in H$.

$$\Rightarrow \quad g_1 = g_2 \underbrace{h_2 h_1^{-1}}_{\in H}$$

$$\Rightarrow \quad g_1 \in g_2 H$$

$$\Rightarrow \quad g_1 H = g_2 H$$, by lemma 6.3.

Secondly, every element of G, is located in a coset, since.

$$g \in gH = \{gh : h \in H\}$$

$e \in$

$ge = g$

These two facts show that G is partitioned by left cosets of H in G.

Definition

The number of left cosets of H in G, is called the index of H in G and written

$$[G : H]$$

Theorem 6.8

The number of left cosets equals the number of right cosets.

Proof We will construct a bijective mapping ϕ (1-1 and onto) between

$$\phi : \mathcal{L}_H \longrightarrow \mathcal{R}_H ..$$

set of left cosets

set of right cosets.

Define ϕ by.

$$\phi(gH) = Hg^{-1}$$

Firstly, this is a well defined map, since if $g_1H = g_2H$ then by lemm 6.3 $Hg_1^{-1} = Hg_2^{-1}$

To prove 1-1, we suppose $\phi(gH) = \phi(kH)$

ie. $Hg^{-1} = Hk^{-1}$

$\Longrightarrow \quad gH = kH$, by lemma 6.3.

So ϕ is injective.

ϕ is clearly surjective/onto.

since $\phi(k^{-1}H) = Hk$

for any right coset Hk of H in G.

So ϕ is ~~also~~ a bijection

Therefore $|\mathcal{L}_H| = |R_H|$

Prop 6.9 All ~~co~~ left cosets of H in G ~~of~~ have the same size, namely $|H|$.

Proof ~~We~~ Show that $\phi : H \longrightarrow gH$ defined by $\phi(h) = gh$ is a bijection.

1-1 Suppose $\phi(h_1) = \phi(h_2)$

i.e. $gh_1 = gh_2$

$\Rightarrow h_1 = h_2$

onto Take any $gh \in gH$.

then clearly

$\phi(h) = gh$. ✓

$\Rightarrow |H| = |gH|$.

Theorem 6.10 Lagrange's theorem.

$|H|$ divides $|G|$.

Proof

$|G| = [G:H]\,|H|$

$\blacksquare$

Cor 6.11

$|g| = |\langle g \rangle|$ divides $|G|$.

Cor 6.12 If $|G| = p$, a prime.

Let $g \in G$, $g \neq e$,

consider $\langle g \rangle$ a subgroup G.

by Lagrange's theorem $|\langle g \rangle|$ divides $|G| = p$.

$\Rightarrow |\langle g \rangle| = 1$ or p, since p is prime

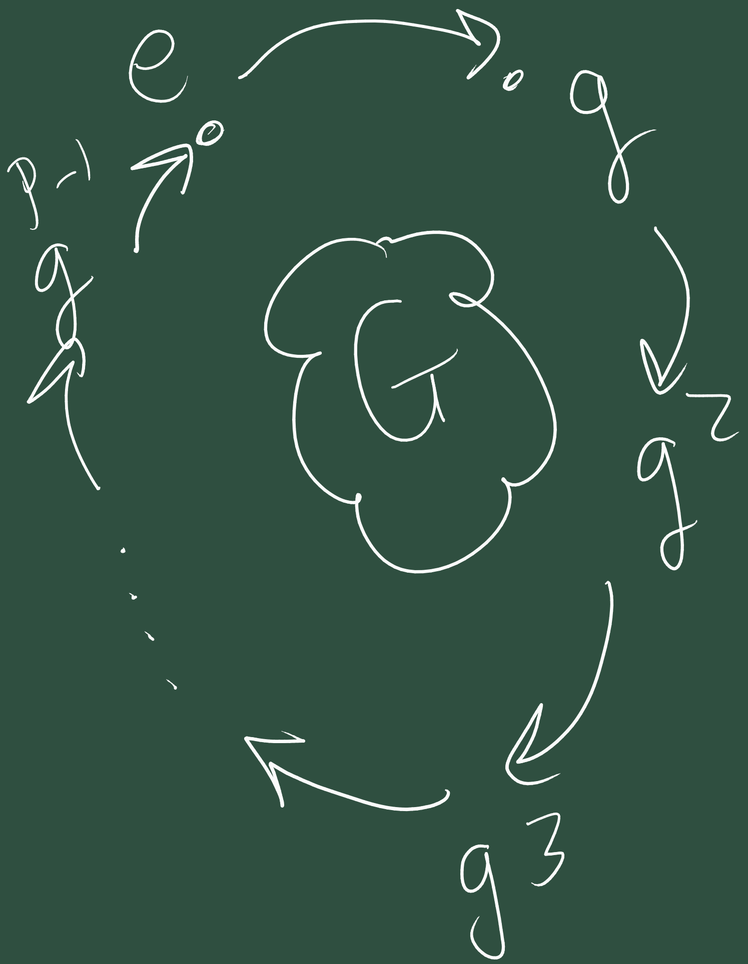
But $\langle g \rangle = \{ e, g, \dots \}$, ie at least two elements

$\Rightarrow |\langle g \rangle| = p = |G|$

$\Rightarrow G = \langle g \rangle$.

ie. G is cyclic.

So if $|G| = p$. take any element $g \in G$, $g \neq e$.



A_4 = "Alternating group on four letters."

$= \{ \sigma \in S_4 : \sigma \text{ is } \underline{\text{even}} \}$.

$|A_4| = \frac{1}{2} |S_4| = \frac{1}{2} 4! = 12$

$= 2^2 \cdot 3$

$(123), (124), (132),$

$(142),$

$(234), (243),$

$(143), (134).$