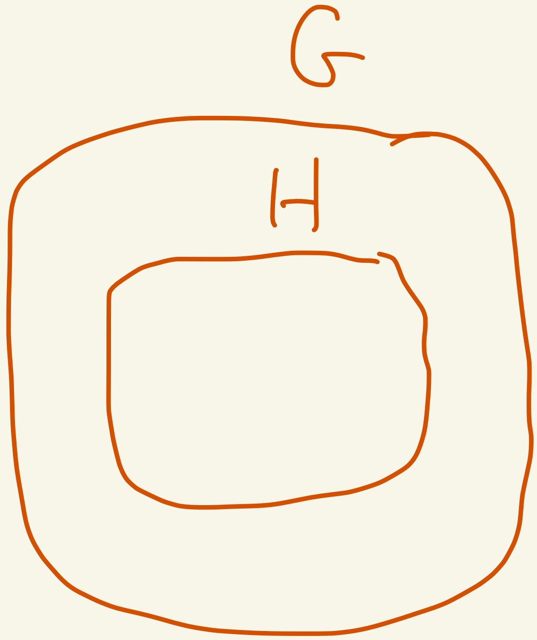
Math 4550

9/8/25

Topic 2 - Subgroups

<u>Def:</u> Let G be a group and H be a subset of G. We say that H is a <u>subgroup</u> of G if H itself is a group under the same operation as G.



We write $H \leq G$ to mean "H is a subgroup of G"

Ex:

$G = \mathbb{R}$ is a group under addition.

$H = \mathbb{Z}$ is a group under addition.

$\mathbb{Z}$ is a subset of $\mathbb{R}$.

So, $\mathbb{Z} \leq \mathbb{R}$.

$\mathbb{Z}$ is a subgroup of $\mathbb{R}$

Note: Under addition:

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

integers

rationals

real numbers

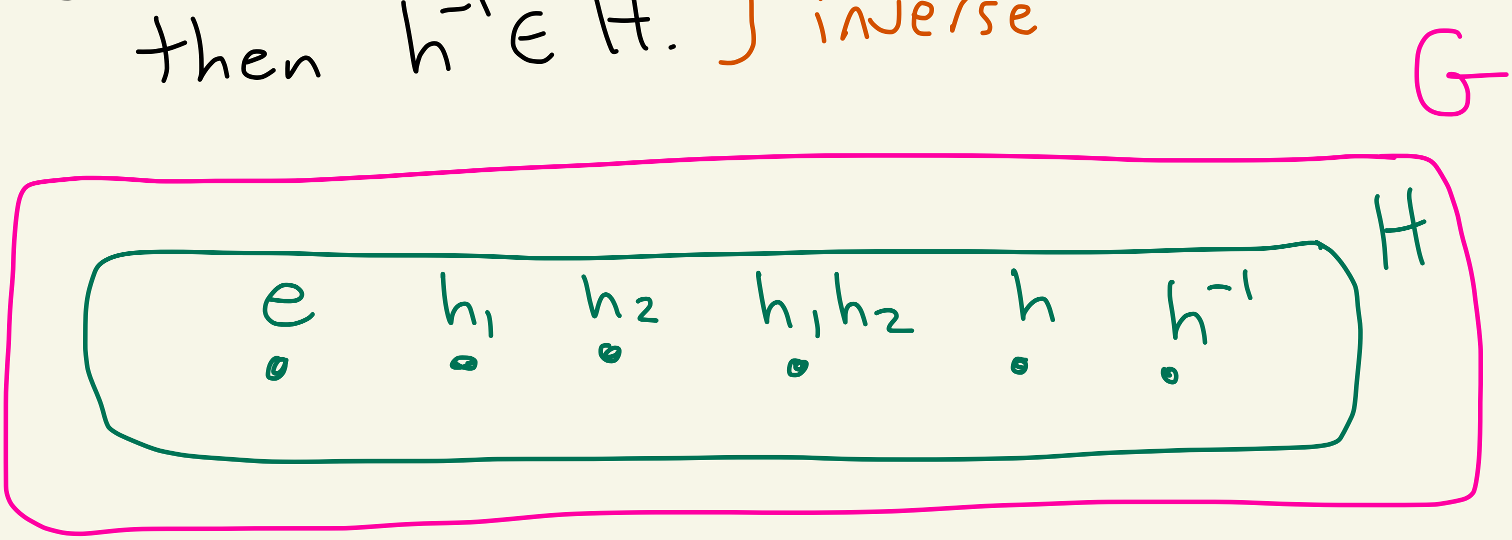
complex numbers

Theorem: Let G be a group with identity element e. Let H be a subset of G. Then, H is a subgroup of G if and only if the following three conditions hold:

① $e \in H$

② If $h_1, h_2 \in H$, then $h_1 h_2 \in H$. } closed under group operation

③ If $h \in H$, then $h^{-1} \in H$. } closed under inverse



<u>proof:</u>

($\Rightarrow$) Suppose $H \leq G$.

Let's show that ①, ②, ③ hold.

Since H is a group under the operation of G, it must have some identity element e_H.

Let's show that $e_H = e$. identity of G

We have

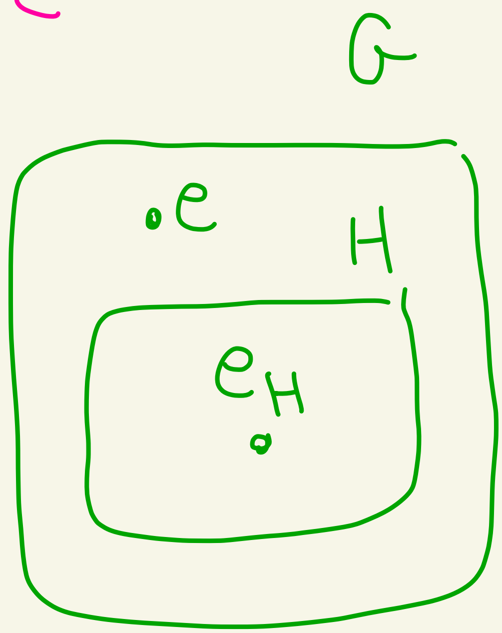
$$e e_H \underset{\substack{\text{since } e, e_H \in G \\ \text{and } e \text{ is the} \\ \text{identity of } G}}{=} e_H \overset{\substack{\text{since } e_H \\ \text{is the} \\ \text{identity} \\ \text{of } H}}{=} e_H e_H$$

Since $e_H \in G$ and G is a

group we know e_H^{-1} exists in G.

So, apply e_H^{-1} to $ee_H = e_H e_H$ on the right side to get

$$e\underbrace{e_H e_H^{-1}}_{e} = e_H \underbrace{e_H e_H^{-1}}_{e}$$



So, $ee = e_H e$.

Thus, $e = e_H$.

So, $e \in H$.

So, ① holds.

② holds because H is a group under the operation of G.

③ Let $h \in H$.

Let's show $h^{-1} \in H$.

$\boxed{\text{$h^{-1}$ means h's inverse in G}}$

Since H is a group under the same operation as G we know h has an inverse inside of H.

That is, there exists $h' \in H$ with $\boxed{hh' = h'h = e.}$

Let's show that $h' = h^{-1}$!

In G we have $\boxed{hh^{-1} = h^{-1}h = e}$

So, $hh' = e = hh^{-1}$.

Then, $\underbrace{h^{-1}(h}_{e}h') = \underbrace{h^{-1}(h}_{e}h^{-1})$

So, $eh' = eh^{-1}$

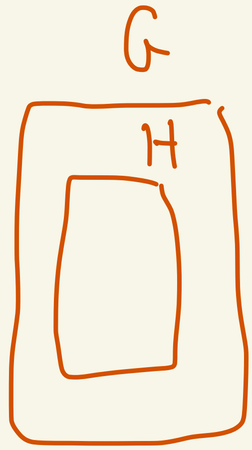
Thus, $h' = h^{-1}$.

So, $h^{-1} \in H$.

Thus, ③ holds.

($\Leftarrow$) Suppose ①, ②, ③ hold.

The only condition left to check to show that $H \leq G$ is to show that H is associative. But H is a subset of G and G has associativity. Thus, H does also.



Ex: Consider

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

$\mathbb{Z}_6$ is a group under addition with identity $e = \bar{0}$.

Let $H = \{\bar{0}, \bar{2}, \bar{4}\}$

Let's show that $H \leq G$.

H	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

Ex: $\bar{2} + \bar{4} = \bar{6} = \bar{0}$

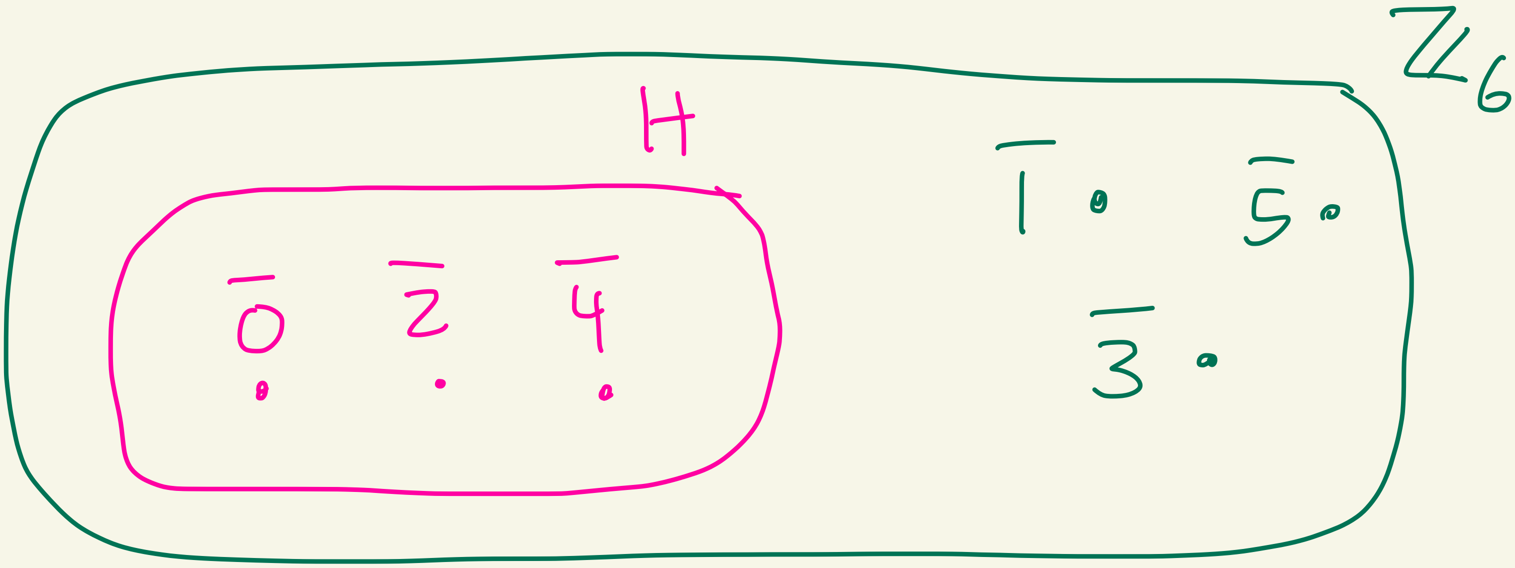
$\bar{4} + \bar{4} = \bar{8} = \bar{2}$

Claim: $H \leq G$

pf:

1. $\bar{0} \in H$
2. H is closed under $+$ by the table.
3. $\bar{0}^{-1} = \bar{0} \in H$
   $\bar{2}^{-1} = \bar{4} \in H$
   $\bar{4}^{-1} = \bar{2} \in H$

$\blacksquare$


$\mathbb{Z}_6$
H
$\bar{0}$
$\bar{2}$
$\bar{4}$
$\bar{1}$
$\bar{5}$
$\bar{3}$

<u>Ex:</u> Recall that

$$GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{matrix} a,b,c,d \in \mathbb{R} \\ ad-bc \neq 0 \end{matrix} \right\}$$

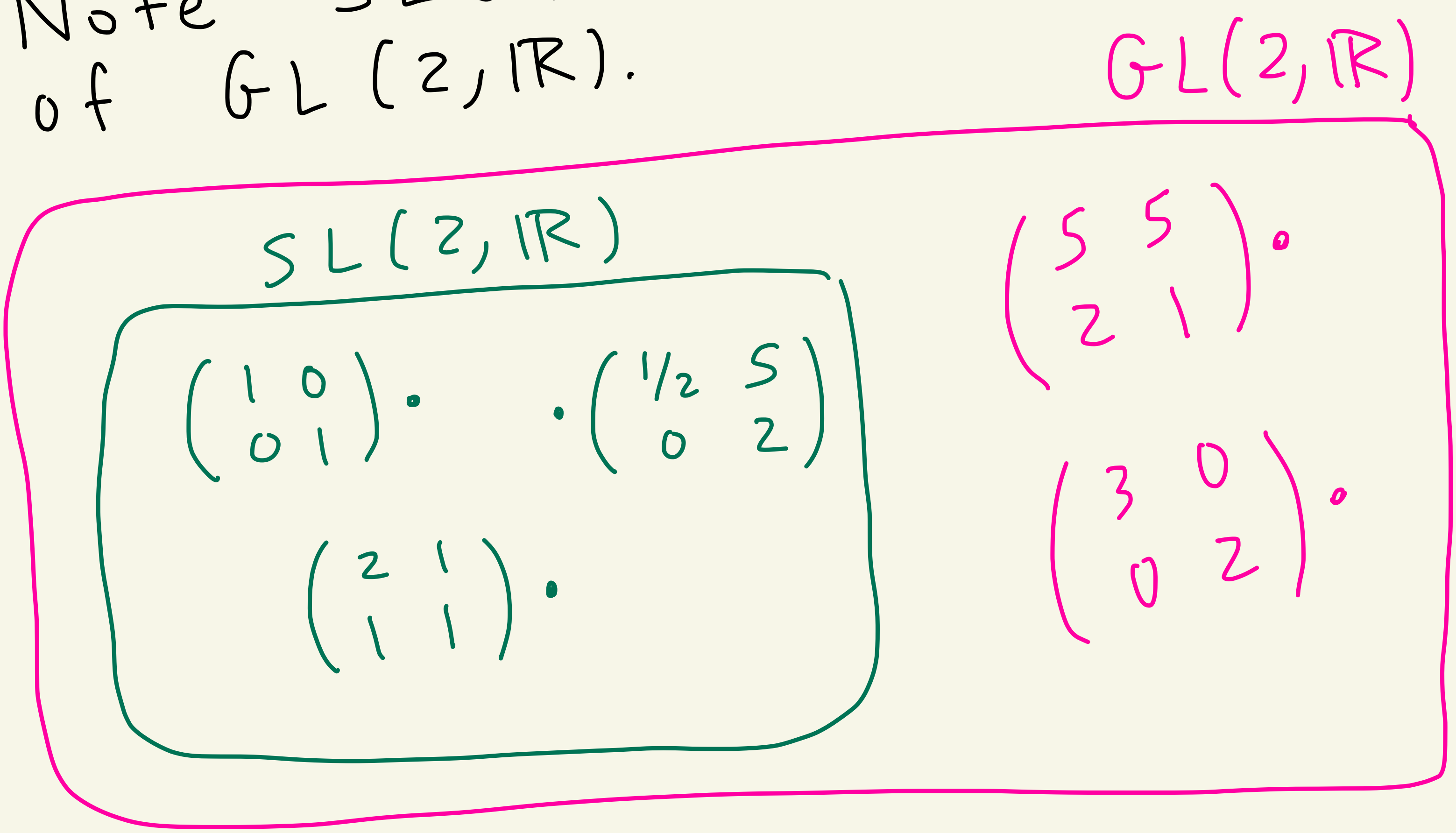
is a group under matrix mult.

Let

$$SL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{matrix} a,b,c,d \in \mathbb{R} \\ ad-bc = 1 \end{matrix} \right\}$$

"special linear"

Note $SL(2,\mathbb{R})$ is a subset of $GL(2,\mathbb{R})$.



Claim: $SL(2,\mathbb{R}) \leq GL(2,\mathbb{R})$

proof:

① The identity is $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which has determinant 1.

So, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL(2,\mathbb{R})$.

② Let $A, B \in SL(2,\mathbb{R})$.

Then, $\det(A) = 1$ and $\det(B) = 1$.

Then,

$$\det(AB) = \det(A) \cdot \det(B)$$
$$= 1 \cdot 1 = 1.$$

So, $AB \in SL(2,\mathbb{R})$.

③ Let $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be in $SL(2,\mathbb{R})$.

Then, $ad - bc = 1$,

We know

$$C^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Then,

$$\det(C^{-1}) = da - (-b)(-c)$$

$$= ad - bc = 1.$$

So, $C^{-1} \in SL(2,\mathbb{R})$.

By 1, 2, 3 we have

$$SL(2,\mathbb{R}) \leq GL(2,\mathbb{R}) \quad \blacksquare$$

Note: Every group has these subgroups:

$H = \{e\} \leftarrow$ trivial subgroup

$H = G \leftarrow$ improper subgroup