Math 4550
9/10/25

Today we discuss the simplest kind of subgroup. These are the ones "generated" by a single element.

<u>Lemma</u>: Let G be a group. Let $x \in G$ and $n, m \in \mathbb{Z}$. Then, $x^n x^m = x^{n+m}$

<u>Proof</u>:

Note that

$$x^0 x^m = e x^m = x^m = x^{0+m}$$

$$x^n x^0 = x^n e = x^n = x^{n+0}$$

So we can assume $n, m \neq 0$.

Let $a > 0$, $b > 0$.

Then,

$$x^a x^b = (\underbrace{x x \cdots x}_{a \text{ times}})(\underbrace{x x \cdots x}_{b \text{ times}}) = x^{a+b}$$

$$x^{-a} x^b = (\underbrace{x^{-1} x^{-1} \cdots x^{-1}}_{a \text{ times}})(\underbrace{x x \cdots x}_{b \text{ times}}) = x^{-a+b}$$

$$x^a x^{-b} = (\underbrace{x x \cdots x}_{a \text{ times}})(\underbrace{x^{-1} x^{-1} \cdots x^{-1}}_{b \text{ times}}) = x^{a-b}$$

$$x^{-a} x^{-b} = (\underbrace{x^{-1} x^{-1} \cdots x^{-1}}_{a \text{ times}})(\underbrace{x^{-1} x^{-1} \cdots x^{-1}}_{b \text{ times}}) = x^{(-a)+(-b)}$$

$\blacksquare$

Theorem: Let G be a group and $x \in G$. Define:

$$H = \{ x^n \mid n \in \mathbb{Z} \}$$

$$= \{ \ldots, x^{-3}, x^{-2}, x^{-1}, x^0, x^1, x^2, x^3, \ldots \}$$

$$= \{ \ldots, (x^{-1})^3, (x^{-1})^2, x^{-1}, e, x, x^2, x^3, \ldots \}$$

Then, $H \leq G$.

We notate H by $\langle x \rangle$ and call it the cyclic subgroup of G generated by x.

H is the "smallest" subgroup of G that contains x.

Proof:

① $e = x^0$ is in H.

② Let $a, b \in H$.

Then, $a = x^{n_1}$ and $b = x^{n_2}$ where $n_1, n_2 \in \mathbb{Z}$.

So,

$$ab = x^{n_1} x^{n_2} = x^{n_1 + n_2}$$

which is in H.

③ Let $c \in H$.

Then, $c = x^n$ where $n \in \mathbb{Z}$.

So, $c^{-1} = (x^n)^{-1} = x^{-n} \in H$.

$$\boxed{\begin{array}{l} x^n x^{-n} = x^0 = e \\ \text{So, } (x^n)^{-1} = x^{-n} \end{array}}$$

By ①, ②, ③, $H \leq G$. $\blacksquare$

<u>Ex:</u> Consider the group $\mathbb{R}^* = \mathbb{R} - \{0\}$. Then, $\mathbb{R}^*$ is a group under multiplication

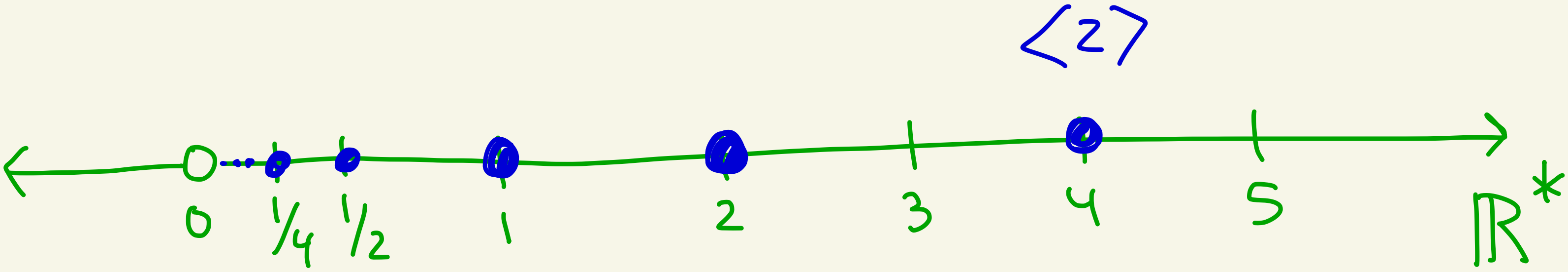
Let $x = 2$.

Then,

$$\underbrace{\langle 2 \rangle}_{H} = \{ 2^n \mid n \in \mathbb{Z} \}$$

$$= \{ \ldots, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, \ldots \}$$

$$= \{ \ldots, \left(\tfrac{1}{2}\right)^3, \left(\tfrac{1}{2}\right)^2, \tfrac{1}{2}, 1, 2, 2^2, 2^3, \ldots \}$$



Ex: Consider the group $\mathbb{Z}$ under addition. Let $x = 2$.

Here a^3 means $a + a + a$.

Then,

$$\langle 2 \rangle = \{\underbrace{\dots, -2-2-2, -2-2, -2}_{\text{"powers" of } -2}, \underset{\uparrow \atop \text{identity}}{0}, \underbrace{2, 2+2, 2+2+2, \dots}_{\text{"powers" of } 2}\}$$

$$= \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$$

which is the set of even integers.

A common notation in an additive group is $3a$ for $a+a+a$.

Ex: In general in $\mathbb{Z}$ we get

always addition

$$\langle n \rangle = \{\ldots, -n-n, -n, 0, n, n+n, \ldots\}$$
$$= \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$$
$$= \{kn \mid k \in \mathbb{Z}\}$$

$\langle n \rangle$ is a subgroup of $\mathbb{Z}$ under addition.

We call it $n\mathbb{Z}$.

For example:

$$3\mathbb{Z} = \langle 3 \rangle = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$0\mathbb{Z} = \langle 0 \rangle = \{0\}$$

<u>Def:</u> Let G be a group and $x \in G$.

If there exists a positive integer m where $x^m = e$, then the <u>order</u> of x is defined to be the smallest positive integer k where $x^k = e$.

If no such positive integer m exists, then we say that x has <u>infinite order</u>

Ex: $U_6 = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$

where $\rho = e^{2\pi i/6}$ and $\rho^6 = 1$.

U_6 is a group under multiplication with identity element 1.

Let $x = \rho^2$.

Then:

$$x^1 = \rho^2 \neq 1$$

$$x^2 = (\rho^2)^2 = \rho^4 \neq 1$$

$$x^3 = (\rho^2)^3 = \rho^6 = 1$$

Thus, the order of $x = \rho^2$ is 3.

Ex:

$\overset{\text{identity}}{}$ $\text{operation} = +$

$$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$$

$$x = \bar{2}$$

Find the order of x.

The positive "powers" of $\bar{2}$ are:

$$\bar{2} \neq \bar{0}$$

$$\bar{2} + \bar{2} = \bar{4} \neq \bar{0}$$

$$\bar{2} + \bar{2} + \bar{2} = \bar{6} \neq \bar{0}$$

$$\underbrace{\bar{2} + \bar{2} + \bar{2} + \bar{2}}_{4 \text{ times}} = \bar{8} = \bar{0}$$

The order of $\bar{2}$ in $\mathbb{Z}_8$ is 4.

What is the order of

$\bar{0}$ in $\mathbb{Z}_8$?

Its 1.

Ex: $\mathbb{R}^* = \mathbb{R} - \{0\}$ is a group under multiplication.

Identity is 1.

What's the order of 2?

$\boxed{\text{positive powers of } 2:}$

$2^1 \neq 1$

$2^2 = 4 \neq 1$

$2^3 = 8 \neq 1$

$\vdots \quad \vdots$

there is no positive power of 2 that gives the identity

So, 2 has infinite order.

Are there any elements of $\mathbb{R}^*$ that have finite order?

1 has order 1 (its the identity)

-1 has order 2 since $-1 \neq 1$
$(-1)^2 = 1$.
