Recall: $\mathbb{R}$ is the set of real numbers, a group under $+$ but not $*$.

Discuss in your group:

(a) Let $\mathbb{R}^* = \{a \in \mathbb{R} \mid a \text{ has a multiplicative inverse}\}$.
Describe the elements in $\mathbb{R}^*$.

Note: $\mathbb{R}^*$ is a group under multiplication.

(b) Let H be the smallest subgroup of $\mathbb{R}^*$ that contains 3.
Describe the elements in H.

$$H = \{ \qquad\qquad 3 \qquad\qquad \}$$

nonzero real numbers.

(b) Let H be the smallest subgroup of $\mathbb{R}^*$ that contains 3. Describe the elements in H.

$$H = \{ \ldots, \tfrac{1}{81}, \tfrac{1}{27}, \tfrac{1}{9}, \tfrac{1}{3}, 1, 3, 9, 27, 81, \ldots \}$$

$$= \{\ldots, 3^{-4}, 3^{-3}, 3^{-2}, 3^{-1}, \overset{1}{3^0}, 3^1, 3^2, 3^3, 3^4, \ldots\}$$

$$= \{3^k \mid k \in \mathbb{Z}\}$$ ← need positive and *negative* powers of 3

$$= \langle 3 \rangle$$ ← new notation

Cyclic subgroup $\langle g \rangle$

Notation. Fix an element g of a *multiplicative* group G.
Define $\langle g \rangle$ to be the set of all integer powers of g, i.e.,

$$\begin{aligned}\langle g \rangle &= \{g^k \mid k \in \mathbb{Z}\} \\ &= \{\dots, g^{-4}, g^{-3}, g^{-2}, g^{-1}, \overset{\varepsilon}{g^0}, g^1, g^2, g^3, g^4, \dots\}\end{aligned}$$

Example. Fix an element 3 in $\mathbb{R}^*$. Then...

$$\begin{aligned}\langle 3 \rangle &= \{3^k \mid k \in \mathbb{Z}\} \\ &= \{\dots, 3^{-4}, 3^{-3}, 3^{-2}, 3^{-1}, \overset{1}{3^0}, 3^1, 3^2, 3^3, 3^4, \dots\}\end{aligned}$$

* **Theorem.** $\langle g \rangle$ is a subgroup of G. (Proved last time.)

Definition of "cyclic" group

OLD Definition. A group G is *cyclic* if it has a generator.

Example: $U_5 = \{1, 2, 3, 4\}$ is cyclic, since 3 is a generator, i.e.,

$$3^1 = 3,\ 3^2 = 4,\ 3^3 = 2,\ 3^4 = 1.$$

NEW Definition.

$3 \in U_5$ $\qquad$ $U_5 = \langle 3 \rangle$

A group G is *cyclic* if there exists $g \in G$ such that $G = \langle g \rangle$.

Note: Here, g is a generator of G.

Example: U_5 is cyclic, because $U_5 = \langle 3 \rangle$.

- $\mathbb{Z}_{12} = \{1,\ 1+1,\ 1+1+1,\ \ldots,\ \underbrace{1+1+\cdots+1}_{12\text{ terms}}\}$

  $= \{k \cdot 1 \mid k \in \mathbb{Z}\}$

  $= \langle 1 \rangle$ ← the set of all possible *sums* of 1

We also have

$$\mathbb{Z}_{12} = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle.$$

- $\mathbb{Z} = \langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}$ ← need positive and *negative* sums of 1.

  But also $\mathbb{Z} = \langle -1 \rangle = \{k \cdot (-1) \mid k \in \mathbb{Z}\}$.

- U_{13} is cyclic with generator 2, i.e.,

  $U_{13} = \langle 2 \rangle$ with $2^{12} = 2^0 = 1$.

  $= \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}\}$

  $= \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$

$5 \in \mathbb{Z}_{12}$ $\quad 2^5 \in U_{13}$

$\boxed{k \in \mathbb{Z}_{12} \leftrightarrow 2^k \in U_{13}}$ gives

$$U_{13} = \langle 2^5 \rangle = \langle 2^7 \rangle = \langle 2^{11} \rangle$$

$$= \langle 6 \rangle = \langle 11 \rangle = \langle 7 \rangle.$$

Subgroups of $\mathbb{Z}_{12}$ and U_{13}:

$\boxed{k \in \mathbb{Z}_{12} \leftrightarrow 2^k \in U_{13}}$ gives

$$\mathbb{Z}_{12} = \langle 1 \rangle \qquad U_{13} = \langle 2^{1} \rangle$$

$$\{0, 2, 4, 6, 8, 10\} = \langle 2 \rangle \qquad \{2^0, 2^2, 2^4, 2^6, 2^8, 2^{10}\} = \langle 2^{2} \rangle = \{1, 4, 3, 12, 9, 10\}$$

$$\{0, 3, 6, 9\} = \langle 3 \rangle \qquad \{2^0, 2^3, 2^6, 2^9\} = \langle 2^{3} \rangle = \{1, 8, 12, 5\}$$

$$\{0, 4, 8\} = \langle 4 \rangle \qquad \{2^0, 2^4, 2^8\} = \langle 2^{4} \rangle = \{1, 3, 9\}$$

$$\{0, 6\} = \langle 6 \rangle \qquad \{2^0, 2^6\} = \langle 2^{6} \rangle = \{1, 12\}$$

$$\{0\} = \langle 0 \rangle \qquad \{2^0\} = \langle 2^{0} \rangle = \{1\}$$

Theorem: Let G be a cyclic group, and H a subgroup of G.
Then H is also cyclic.

Subgroup of $\mathbb{R}^*$.

Elizabeth:

The multiplicative group $\langle 3 \rangle$ behaves just like the additive group $\mathbb{Z}$.

In $\langle 3 \rangle$:

- $3^{17} \cdot 3^{25} = 3^{17+25} = 3^{42}$.
- The mult. identity is 3^{0}.
- The mult. inverse of 3^{17} is 3^{-17}.

In $\mathbb{Z}$:

- $17 + 25 = 42$.
- The additive identity is 0.
- The additive inverse of 17 is -17.