## Subgroups

**Definition:** Let $G$ be a group and let $H$ be a subset of $G$. Then $H$ is a subgroup of $G$ if:

1. whenever $h_1, h_2 \in H$, we have $h_1 h_2 \in H$. In other words, the binary operation on $G$, when restricted to $H$, gives a binary operation on $H$.

2. With this binary operation inherited from $G$, $H$ is a group.

## Examples of subgroups

Let $\mathbb{R}$ be the additive group of real numbers. Then each of the following subsets of $\mathbb{R}$ are subgroups:

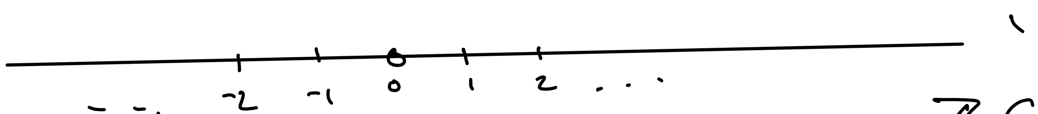
1. $\mathbb{Z} \subset \mathbb{R}$.
2. $\mathbb{Q} \subset \mathbb{R}$.
3. $\{0\} \subset \mathbb{R}$.
4. $\mathbb{R} \leq \mathbb{R}$.

$\mathbb{R}$ group with $+$

$0$ is the identity element

$x \in \mathbb{R}$, $-x \in \mathbb{R}$

$(x + (-x)) = 0$

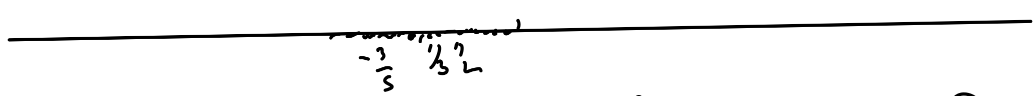



$\mathbb{Z} \leq \mathbb{R}$

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

sum of integers is integer

$0 \in \mathbb{Z}$ if $x \in \mathbb{Z}$, $-x \in \mathbb{Z}$ also



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

sum of fractions is a fraction; $0 \in \mathbb{Q}$; $\mathbb{Q}$ is a subgroup of $\mathbb{R}$.

$\frac{a}{b} \in \mathbb{Q}$, $-\frac{a}{b} \in \mathbb{Q}$

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

$\{0\} \leq \mathbb{R}$. $0 + 0 = 0$

$0$ is its own inverse.



Every group $G$ always has $\{e\} \leq G$ as a subgroup.

$G \leq G$ is a subgroup.

## Examples of subgroups continued

Let $\mathbb{R}^*$ be the set of *non-zero* real numbers with group operation given by multiplication. Then the following are subgroups:

1. $\{-1, 1\} \subset \mathbb{R}^*$
2. the non-zero rational numbers with multiplication $\mathbb{Q}^* \subset \mathbb{R}^*$.

$\mathbb{R}^* = \mathbb{R} - \{0\}$.

$\{-1, 1\} \leq \mathbb{R}^*$ is a subgroup.

$$\begin{array}{c|cc} & -1 & 1 \\ \hline -1 & 1 & -1 \\ 1 & -1 & 1 \end{array}$$

$(-1)(-1) = 1$

$\mathbb{Q}^* \leq \mathbb{R}^*$

$\mathbb{Q}^* = \mathbb{Q} - \{0\}$ multiplication are a group.

$\frac{a}{b} \cdot \frac{b}{a} = 1$

$1 \cdot \frac{a}{b} = \frac{a}{b}$.

**Note:** The nonzero integers $\mathbb{Z}^*$ are *not* a subgroup.

$\mathbb{Z} - \{0\} = \mathbb{Z}^*$.

$a \in \mathbb{Z}^*$, $b \in \mathbb{Z}^*$, $ab \in \mathbb{Z}^*$

$\mathbb{Z}^*$ NOT a group. $2^{-1} = \frac{1}{2} \notin \mathbb{Z}^*$.

### Examples of subgroups continued

Remember that $\underline{\mathrm{GL}_2(\mathbb{R})}$ is the group of invertible $2x2$ matrices with real entries.

**Proposition:** The subset $\mathrm{SL}_2(\mathbb{R})$ consisting of invertible $2x2$ matrices with determinant 1 is a subgroup.

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad-bc \neq 0 \right\}$$ , matrix multiplication.

$$\cup\!|$$

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad-bc = 1 \right\}.$$

$A, B \in GL_2(\mathbb{R})$, $\det(A) = \det(B) = 1$

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

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$ ✓ $\det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ ✓ $\det(A^{-1}) = 1$

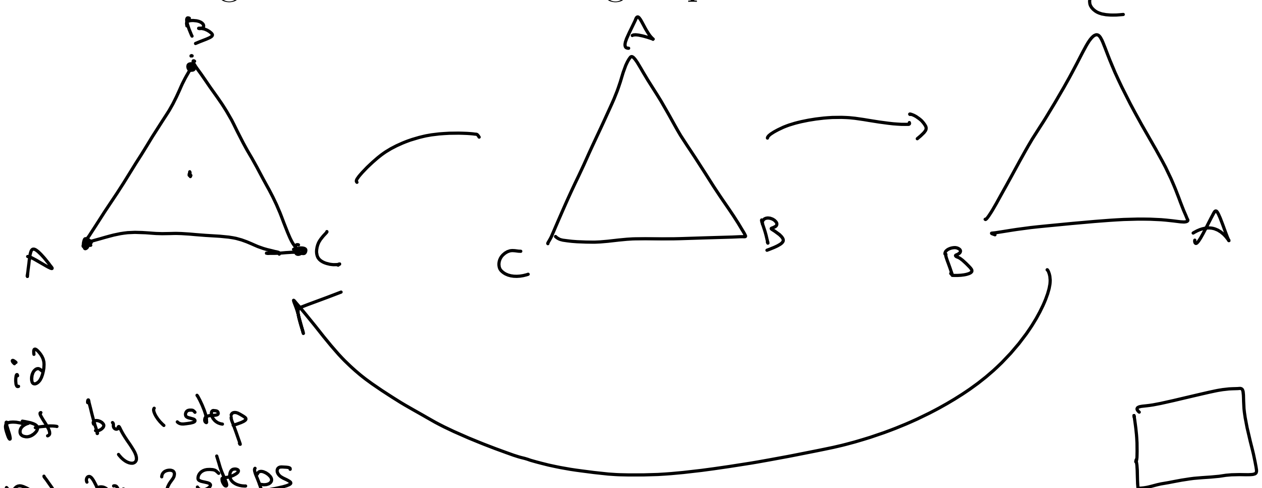
$A^{-1} \in SL_2(\mathbb{R})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

**Examples of subgroups continued**

Let $G$ be the group of symmetries of the equilateral triangle.

**Proposition:** Let $H \subset G$ be the subset consisting of the rotations of the triangle. Then $H$ is a subgroup of $G$.




$e$ id

$r$ rot by 1 step

$r^2$ rot by 2 steps

$r^3 = e$