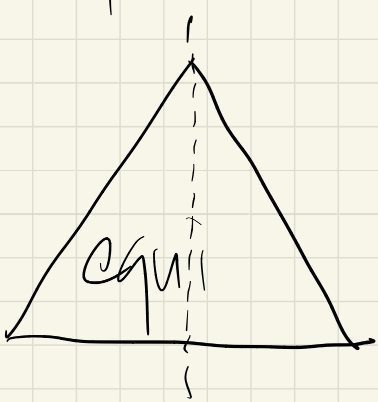
§4 Algebraic structures, groups, rings and fields.

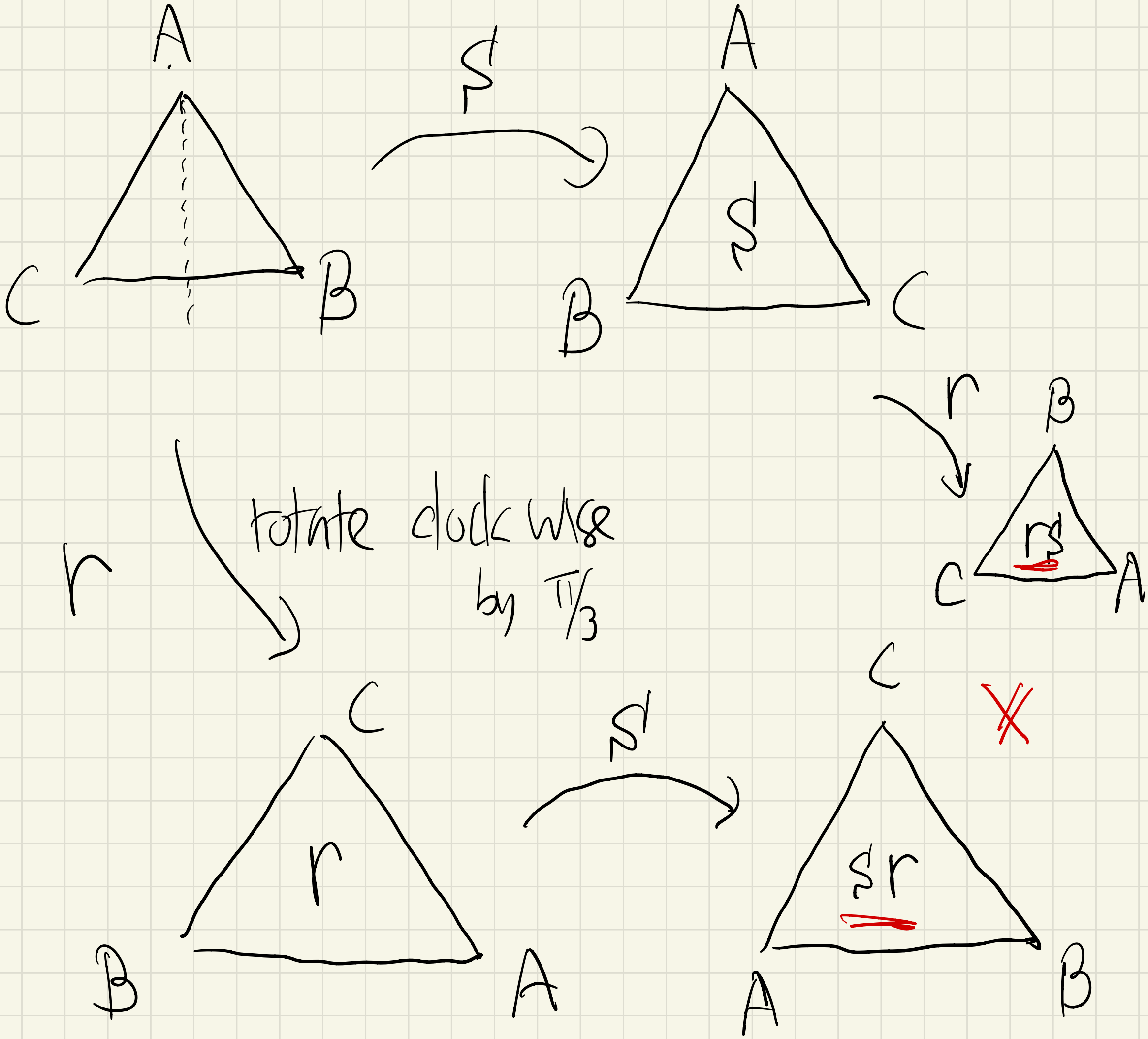
What are groups?

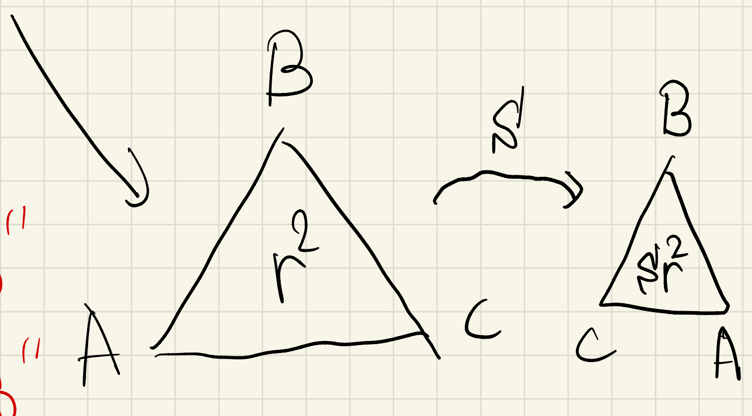
Groups are "symmetries"



Which one is "more" symmetric ?

Symmetries are "action" we perform on an object.





r^3 = "identity"

= "doing nothing"

s^2 = "doing nothing"

Since there are $3! = 6$ ways of rearranging $\{A, B, C\}$, the list covers all the actions that preserve the triangle.

Group theory looks at these action r's and s's because these actions represent symmetries of the triangle.

Def A group is a set G with an operation $*$ satisfying the following axioms.

(G0): If $a, b \in G$,

$$a * b \in G.$$

(G1): If $a, b, c \in G$,

$$a * (b * c) = (a * b) * c$$

(G0) says this is an element in G.

(G2) There is an element e of G,

s.t. $e * a = a * e = a$

for any $a \in G$.

(G3) For every element a of G,

there exists $b \in G$ s.t.

$$a * b = b * a = e$$

Rk The element e in (G2) is called the identity element of $(G, *)$.

Rk The element b in (G3) is called the inverse of a.

If $(G, *)$ is a group,

and satisfies

(G4) If $a, b \in G$,

$$a * b = b * a,$$

then we call $(G, *)$

an *abelian* group

commutative

We'll almost always see

abelian groups.

Examples

$(G, *) = (\mathbb{Q}, +)$

$\uparrow$ addition as we know it.

i.e. $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ $b \neq 0, d \neq 0$

$$\left(\frac{a}{b}\right) * \left(\frac{c}{d}\right) = \left(\frac{a}{b}\right) + \left(\frac{c}{d}\right)$$

$$= \frac{ad+bc}{bd} \leftarrow bd \neq 0$$

$(\mathbb{Q}, +)$

"0" is the identity element (G2)

because

$$\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a}{b}$$

Given $\frac{a}{b} \in \mathbb{Q}$, what is the inverse of $\frac{a}{b}$?

In fact $\frac{(-a)}{b}$ is the inverse of $\frac{a}{b}$

because $\frac{a}{b} + \left(\frac{-a}{b}\right) = 0$

$$\left(\frac{-a}{b}\right) + \left(\frac{a}{b}\right) = 0$$

$$(G, *) = (\mathbb{Q} - \{0\}, \times)$$

the set of non-zero rational numbers.

multiplication as we know it.

$$\frac{a}{b}, \frac{c}{d} \in \mathbb{Q} - \{0\}$$

$b \neq 0$, $d \neq 0$ $a \neq 0$ $c \neq 0$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$ $ac \neq 0$

$bd \neq 0$

$$\Rightarrow \frac{ac}{bd} \in \mathbb{Q} - \{0\}$$ ✓ $(G0)$

$(\mathbb{Q} \setminus \{0\})$

What is the identity element ?

1 is the identity element

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

$\forall \frac{a}{b} \in \mathbb{Q} - \{0\}$

(G2) ✓

What is the inverse of $\frac{a}{b}$ $(\mathbb{Q}-\{0\})$?

In fact $\frac{b}{a \neq 0}$ is the inverse

as $\frac{a}{b} \cdot \frac{b}{a} = \frac{b}{a} \cdot \frac{a}{b} = 1$ (G3) ✓

$\uparrow$
(G2)

(G4) ✓ $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$

$(G, *) = (\mathbb{Q}, \times)$

is NOT a group!

It passes (G0), (G1), (G2)

1 is the identity

but it fails on (G3)

where 0 does NOT have the inverse!

Note $(\mathbb{Q}, +)$ is a group

but $(\mathbb{Q}, \times)$ is NOT a group.

So it really depends on what kind of $*$ we choose.

$(G, *) = ($ the set of 2-by-2 matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\mathbb{R}$

s.t.

$\det A \neq 0$ $, \times)$

$\parallel$

$(ad - bc)$

is a group but this is

<u>NOT</u> an abelian group, i.e.

it fails (G4).

$$\boxed{AB \neq BA}$$