Rings and fields!

Spencer Bagley

With many thanks to Matthew Macauley,
`http://www.math.clemson.edu/~macaule/`

28 Apr 2025

Groups!

What is a group? Why is a group?

Definition

A group is … a set of elements G together with a binary operation $*$ such that:

- $*$ has an identity element e such that $g * e = g$, and $e * g = g$, for all $g \in G$
- every element g has an inverse element g^{-1} such that $g * g^{-1} = g^{-1} * g = e$
- the operation $*$ is associative, ie., $(g * h) * k = g * (h * k)$
- (the set G is closed under $*$, but that's implied by the precise definition of a binary operation)

Why are we making this definition?

Why is a group?

One reason to make this definition is that there are lots ways to combine stuff that remind us a bit of multiplying numbers.

If we forget some specific things we know about numbers, what is still true about multiplying?

How much can we forget and still have something that "works like" multiplying numbers?

Let's play rock-paper-scissors

Let $M := \{r, p, s\}$ and define the binary operation $*$ as the winner between the two throws. For instance, $r * p = p$ because paper beats rock.

$*$	r	p	s
r	r	p	r
p	p	p	s
s	r	s	s

This is not a group. Why not?

- Is there an identity element?
- Do elements have inverses?
- Is the operation associative? (Check $r * (p * s)$ vs. $(r * p) * s$.)

We had to forget even more stuff about multiplying numbers! This is called a magma.

Forgetting more stuff

$$
\begin{tikzcd}
& \text{group} & \\
\text{monoid} & \text{loop} & \text{assoc. quasigroup} \arrow[ul, "\text{id.}"] \\
\text{unital magma} & \text{semigroup} \arrow[ul, "\text{id.}"] & \text{quasigroup} \arrow[ul, "\text{id.}"] \\
& \text{magma} \arrow[ul, "\text{id.}"] &
\end{tikzcd}
$$