Abstract algebra is a framework for generalizing many parts of algebra.

Ordinary algebra: Number systems: rational, real, complex. We have four arithmetic operations $+, -, \times, \div$.

If we write down the basic properties these operations satisfy, we can use that as a list of axioms to define an "Abstract Number System"—more specifically, a "field" in modern parlance. If we drop the axioms relating to division, we get a "ring" (Example $\mathbb{Z}$ = integers).

We will talk about rings and fields more later, but we will start with a type of structure that has fewer operations: a group.

**Definition.** A group is a set $G$ together with a function $\star : G \times G \to G$

$$(a, b) \mapsto a \star b$$

satisfying the axioms:

(a) **associativity**: For all $a, b, c \in G$ it holds that

$$(a \star b) \star c = a \star (b \star c)$$

(b) **identity**: There is an element $e \in G$ with the property that $e \star a = a \star e = a$ for any $a \in G$. 


(3) **Inverse:** Given \( a \in G \), there is an element \( a^{-1} \in G \) such that \( a \ast a^{-1} = e = a^{-1} \ast a \) where \( e \) is the element from axiom 2.

**Rule:** The element \( e \) from axiom (2) is called the identity element of \( G \), and the element \( a^{-1} \) from axiom (3) is called the inverse of \( a \).

**Pedantic Remark:** The group operation is a function \( *: G \times G \to G \) so it would be natural to write \( *(a, b) \) for the value of this function on the inputs \((a, b)\). By convention, we don’t do that, but instead write \( * \) as a binary operation: \( a \ast b = *(a, b) \).

**What does the concept of group correspond to classically?**

**Examples**

1. **Addition in a number system.**

   \( G = \mathbb{Z} = \ldots, -2, -1, 0, 1, 2, 3, \ldots \) \( * = + \) ordinary addition

   **Axiom 1:** \( (a + b) + c = a + (b + c) \) \ YES

   **Axiom 2:** \( 0 + a = a = a + 0 \) so \( e = 0 \) is an identity \ YES

   **Axiom 3:** \( a + (-a) = 0 = (-a) + a \) so \( a^{-1} = -a \) works \ YES

   **Conclusion:** \((\mathbb{Z}, +)\) is a group.

   Also \((\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)\) are all groups

2. **What about \([-1, 1] = \{ x \in \mathbb{R} \mid -1 \leq x \leq 1 \}\)?**

   - Contains \( 0 \), contains \(-a\) when it contains \( a\).
   - Not closed under addition: BAD—NOT A GROUP.
3. Multiplication on invertible elements in a number system.
\( \mathbb{Q} = \text{rational numbers} \quad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \)

Group operation: \( \cdot \) multiplication.

Axiom 1: \((ab)c = a(bc) \) \quad \text{YES}

Axiom 2: \(1a = a = a1 \) so \( e = 1 \) is identity.

Axiom 3: If \( a = \frac{p}{q} \), \( a^{-1} = \frac{q}{p} \), but this only works if \( p \neq 0 \), \( a \neq 0 \).

Conclusion: \( (\mathbb{Q}^*, \cdot) \) is a group.

Also \( (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot) \).

What about \( \mathbb{Z} \setminus \{0\} \)? No because \( \frac{1}{2} \notin \mathbb{Z} \setminus \{0\} \)

But \( \{\pm 1\} \subseteq \mathbb{Z} \) is a group under multiplication.

3. "Symmetries" of a mathematical object
- invertible transformations that preserve a given structure or "shape".

Let \( X \) be a set. A function \( f: X \to X \) is a bijection if it is one-to-one and onto.

\[ \text{Sym}(X) = \{f: X \to X \mid f \text{ is a bijection} \} \]

Functions can be composed.
\[ (f \circ g)(x) = f(g(x)) \]

Claim. \( (\text{Sym}(X), \circ) \) is a group.

Axiom 1: \( (f \circ g) \circ h = f \circ (g \circ h) \)

Test on \( x \in X \): \[ (f \circ (g \circ h))(x) = f(g(h(x))) = f((g \circ h)(x)) \]

So \( \text{YES} \).
Axim 2: Let \( e = \text{Id}_X : X \to X \) be the identity function.
\[ \forall x \in X, \quad \text{Id}_X(x) = x \]
Then \( f \circ \text{Id}_X = f \) for indeed \( (f \circ \text{Id}_X)(x) = f(\text{Id}_X(x)) = f(x) \).
Similarly \( \text{Id}_X \circ f = f \), YES.

Axim 3: Given \( f \in \text{Sym}(X) \), denote by \( f^{-1} \) the inverse function
\[ f^{-1}(y) = x \iff f(x) = y. \]
Because \( f \) is a bijection, \( f^{-1} \) is actually a function \( X \to X \).

To check \( f \circ f^{-1} = \text{Id}_X \),
look at \( (f \circ f^{-1})(x) = f(f^{-1}(x)) = f(y) \) where \( f(y) = x \)
so \( x = x = \text{Id}_X(x) \).
Similarly \( f^{-1} \circ f = \text{Id}_X \), so YES.

4 Matrix groups: \( n \geq 1 \) integer-
\( GL(n, \mathbb{R}) = \) set of \( n \times n \) matrices with real entries
with non-zero determinant.

Composition A \( \cdot \) B matrix multiplication
\( (GL(n, \mathbb{R}), \cdot) \) is a group

Axim 1 \( (A \cdot B) \cdot C = A \cdot (B \cdot C) \) YES
Axim 2 \( I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \) Identity matrix
\[ \text{satisfies } I \cdot A = A = A \cdot I \]
Axim 3, Since \( A \in GL(n, \mathbb{R}) \) has non-zero determinant,
\( A^{-1} \) exists as a matrix, and \( A \cdot A^{-1} = I = A^{-1} \cdot A \).

... and many more examples, and connections between the examples!