Abstraction: Extract and study "objects" that share key common features in a unified way.

- stripped away extraneous information providing clarity
- provides a framework to analyze many different objects in relation to one another

Algebra? Some of the recurring themes will involve familiar algebra: numbers and solving equations, polynomials, linear algebra, ... But really the abstraction lets us study many other mathematical objects and situations.

Definition: A group is a nonempty set $G$ together with an operation $*: G \times G \to G$, $(a, b) \mapsto a \ast b$ (or often just $(a, b) \mapsto ab$) satisfying the axioms (or rules):

(i) Associativity: For all $a, b, c \in G$, we have

$$(a \ast b) \ast c = a \ast (b \ast c).$$

(ii) Identity: There exists an identity element $e \in G$, such that for all $a \in G$, $a \ast e = e \ast a = a$

(iii) Inverse: For all $a \in G$, there exists an element $a^{-1} \in G$

called the inverse of $a$, such that $a \ast a^{-1} = a^{-1} \ast a = e$

We will write $(G, *)$ to denote the group $G$ with operation $*$, but will often simply write $G$, with the operation understood from the context.
Examples: (1) \((\mathbb{Z}, +)\) the integers with addition:

(i) addition is associative \((a+b)+c = a+(b+c)\)
(ii) the identity? \([\text{students}]\ e = 0 \text{ since } 0 + a = a + 0 = a\)
(iii) inverses? \([\text{students}]\ a^{-1} = -a \text{ since } a + (-a) = 0 = (-a) + a\).

(2,3) Similarly: \((\mathbb{Q}, +), (\mathbb{R}, +)\) rational numbers and real numbers with usual addition.

(4) \(\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}, i^2 = -1\}\) complex numbers with addition +

\((a + bi) + (c + di) = (a+c) + (b+d)i\)

\((\mathbb{C}, +)\) is a group — check! identity = 0 + 0i = 0
inverse \((a+bi)^{-1} = -a-bi\)

(5) vector space \(V\) (with any "scalars") \(+ = \text{vector addition}\),
visit your linear algebra book — group axioms are part of the vector space axioms! eg. \(\mathbb{R}^n, \mathbb{C}, \mathbb{Q}^n\) + ....

(6) \(\mathbb{R}^* = \mathbb{R} \setminus \{0\}\) with multiplication \(*: (a, b) \cdot c = a \cdot (b, c)\), \(e = 1, a^{-1} = \frac{1}{a}\)

(7) \((\mathbb{R}^*, \cdot)\), \(\mathbb{R}^* = \mathbb{R} \setminus \{0\}\)

(8) \(\mathbb{C}^* = \mathbb{C} \setminus \{0\}\), \((a+bi) \cdot (c+di) = (ac-bd) + (ad+bc) i\) (expand, use \(i^2 = -1\))

\(e = 1\) \((a+bi) \cdot (1+0i) = (a \cdot 1 - b \cdot 0) + (0 \cdot 0 + b \cdot 1)i = a + bi\)

\((1+0i) \cdot (a+bi) = (1 \cdot a + 0 \cdot b) + (0 \cdot a + 1 \cdot b)i = a + bi\)

inverse? \([\text{students}]\ (a+bi)^{-1} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i\)

check \((a+bi)(a-bi)^{-1} = \left(\frac{a^2}{a^2+b^2} - \frac{b^2}{a^2+b^2}\right) + \left(-\frac{ab}{a^2+b^2} + \frac{ab}{a^2+b^2}\right) i = 1\)

(9) \(\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}\) — no \(\{±1\} \subset \mathbb{Z}^*\), \((±1, \cdot)\) yes! Two elements!
10. \[ \{ \cos(\theta) + i \sin(\theta) \in \mathbb{C} \mid \theta \in \mathbb{R} \} = \{ a + bi \in \mathbb{C} \mid a^2 + b^2 = 1 \}. \]

\( S^1 \) is a group!

\((\cos(\theta) + i \sin(\theta)) \cdot (\cos(\phi) + i \sin(\phi)) = \cos(\theta + \phi) + i \sin(\theta + \phi) \in S^1\]

\[
(\cos \theta + i \sin \theta)^{-1} = \frac{\cos(-\theta) + i \sin(-\theta)}{-\cos(\theta) - i \sin(\theta)}
\]

11. For any integer \( n \geq 1 \)

\[
C_n = \{ \cos(\frac{2\pi n}{n}) + i \sin(\frac{2\pi n}{n}) \mid k \in \mathbb{Z} \} \subset S^1
\]

12. Let \( X \) be any nonempty set and

\[
\text{Sym}(X) = \{ f : X \to X \mid f \text{ is a bijection}, \text{i.e., } 1_1 \text{ and onto (or surjective)} \}
\]

\( o = \text{composition } f \circ g \)(x) = f(g(x)).

**Proposition**: \( (\text{Sym}(X), o) \) is a group, \( e = \text{identity } e(x) = x \), inverse of \( f = f^{-1} \).

**Proof**: First we need to show an operation, i.e., \( f \circ g \in \text{Sym}(X) \):

Suppose \( x, y \in X \), \( f \circ g(x) = f(g(y)) \). Then \( f(g(x)) = f(g(y)) \) so \( y(x) = g(y) \) (\( f \) is \( 1_1 \))

and then \( x = y \) (\( f \) is \( 1_1 \)), so \( f \circ g \) is \( 1_1 \). Given \( y \in X \), \( \exists x \in X \) so \( f(x) = y \), and \( \exists x \in X \) so \( g(x) = z \). So, \( f \circ g = f(g(x)) = f(z) = y \), and \( f \circ g \) is onto. Hence \( f \circ g \in \text{Sym}(X) \).

We know composition is associative: \( (f \circ g) \circ h = f \circ (g \circ h) \).

\( f(g \circ h)(x) = f(g(h(x))) = f(g(h(x))) = f \circ (g \circ h)(x) \).
\[ e(x) = x, \text{ then } e \circ f(x) = e(f(x)) = f(x) = e \circ f \]

\[ f \circ e(x) = f(e(x)) = f(x) = f \circ e \]

By definition, \( f^{-1} \circ f = f \circ f^{-1} = e \). \( \square \) signifies end of proof.

Often call \( \text{Sym}(X) \) the symmetric group of \( X \) or the permutation group of \( X \), with bijections called permutations.

13. \( V \) a vector space, \( \text{GL}(V) = \) invertible linear transformations (i.e., bijective).

If \( S, T : V \rightarrow V \) linear, then \( S \circ T \) is linear. As in proof above then, \( (\text{GL}(V), \circ) \) is a group.

14. \( n \geq 1 \) integer, \( \text{GL}(n, \mathbb{R}) = \) invertible \( n \times n \) matrices with entries in \( \mathbb{R} \).

and \( A \cdot B = \) matrix product.

From linear algebra we know \( (A \cdot B) \cdot C = A \cdot (B \cdot C) \),

identity \( I = (1_0) \) has \( I \cdot A = A \cdot I = A \) and for all \( A \neq A' \) s.t. \( A'A = AA' = I \) (in particular \( (A \cdot B)^{-1} = B^{-1}A^{-1} \).

... so many more!!