§1 Introduction

What is algebra (vs. analysis, geometry, etc.)?

What do you learn in algebra classes?

What do you expect to learn in this course?

Algebra concerns the study of algebraic structures.

An algebraic structure is a set of objects (such as numbers) with one or more (binary) operations.

Examples

\[ \mathbb{N} = \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}^+, \mathbb{Q}^*, \mathbb{R}, \mathbb{R}^+, \mathbb{R}^*, \mathbb{C}, \mathbb{C}^*, M_n(\mathbb{R}), \]

\[ \mathbb{Z}_n = \{0, 1, \ldots, n-1\}, \quad S \text{ is a set of sets}. \]

What is abstract algebra? What do you (expect to) learn in abstract algebra classes?

We study an abstract algebraic structure of objects with abstract (binary) operations which satisfy some rules (axioms).

We are interested in how to perform the operations, solve equations, determine special elements, subsets, etc.

We will begin with a structure - Group - with only one operation \( * \) in which we can solve the equation \( a * x = b \).

You will be amazed by the fact that very rich theory can be developed with a single operation satisfying some simple rules (axioms).
Review of Complex numbers

Define an imaginary number $i$ such that $i^2 = -1$.

The set of complex numbers $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$.

Equality, addition, subtraction, multiplication, division by nonzero numbers.

Examples

Evaluate $(-i)^{35}$, $(1 + i)^3$.

Polar form of $z = a + ib$ is

$$|z|(\cos \theta + i \sin \theta) = |z|e^{i\theta},$$

where $|z| = \sqrt{a^2 + b^2}$ is the absolute value of $z$ and $\theta$ is the argument or angle of $z$ so that $\cos \theta = a/|z|$ and $\sin \theta = b/|z|$.

Euler formula

If $z_1 = |z_1|e^{i\theta_1}$ and $z_2 = |z_2|e^{i\theta_2}$, then $z_1z_2 = |z_1| |z_2|e^{i(\theta_1 + \theta_2)}$.

Proof.

$$|z_1|(\cos \theta_1 + i \sin \theta_1)|z_2|(\cos \theta_2 + i \sin \theta_2)$$

$$= |z_1| |z_2|[\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)].$$

Example (1.7) Solve $z^4 = -16$.

Multiplication on the unit circle $U = \{z \in \mathbb{C} : |z| = 1\}$ is the same as (isomorphic to) $\mathbb{R}_{2\pi}$, i.e., $\mathbb{R}$ under addition modulo $2\pi$.

Multiplication on the set $U_n = \{z \in \mathbb{C} : z^n = 1\}$ of $n$th roots of unity is essentially the same as addition modulo $n$ on $\mathbb{Z}_n$.

Solve $x + 2\pi x + 2\pi x + 2\pi x = 0$ in $\mathbb{R}_{2\pi}$ and $z \cdot z \cdot z = 1$ in $U$.

Solve $x + 2\pi \frac{3\pi}{2} = \frac{3\pi}{2}$ in $\mathbb{R}_{2\pi}$.

Solve $x + 7x + 7x = 5$ in $\mathbb{Z}_7$.

Use the fact that $e^{i3\theta} = (\cos \theta + i \sin \theta)^3$ to show

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta, \text{ } \sin 3\theta = 3 \sin \theta - 4 \sin^3 \theta.$$
§2 Binary operations

An binary operation $\ast$ on a set $S$ is a rule assigning every pair of elements $a, b \in S$ a unique element $c = a \ast b$ in $S$.

[So, a binary operation is a function from $S \times S$ to $S$.]

Let $H \subseteq S$, and $\ast$ be an binary operation on $S$. We say that $H$ is closed under $\ast$ if for any $a, b \in H$ we also have $a \ast b \in H$. If this happens, $\ast$ becomes an induced binary operation on $H$.

Examples Number systems, matrices, polynomials, functions, sets, ....

Definitions A binary operation $\ast$ on $S$ is commutative if ... It is associative if ...

If $S$ is finite, one can construct operation (multiplication/addition) tables

§3 Isomorphic binary structures

Let $(S, \ast)$ and $(S', \ast')$ be binary structures. They are isomorphic if there is a bijective (one-one/onto) function $\phi : S \rightarrow S'$ such that

$$\phi(x \ast y) = \phi(x) \ast' \phi(y) \quad \text{for all } x, y \in S. \tag{1}$$

Q1: How to show two binary structures are isomorphic?

Construct an isomorphism. Define the function $\phi$, check one-one, onto, and (1).

Q2: How to show two binary structure are not isomorphic?

Find structural differences.

For example, one is commutative, but the other is not; certain equation involving the binary operation can be solved in one structure but not in the other.

Identity element and uniqueness

An element $e$ in $(S, \ast)$ is an identity if $s \ast e = e \ast s = s$ for every $s \in S$.

Proposition (3.13) There is at most one identity element in a binary structure, i.e., if identity exists, it is unique.

Proposition (3.14) An isomorphism on binary structures maps identity to identity.