Basic Algebraic Structures: An Introduction

Introduction

Understanding algebraic structures is like learning the rules of different "games" in mathematics. Each structure has specific rules that define how numbers or objects interact with each other. Let's explore these structures step by step, starting from familiar concepts.

1 Sets and Operations

A **set** is simply a collection of objects. For example:

$$\text{Set of integers: } \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

An **operation** is a rule that takes two elements from a set and combines them to produce another element in the same set. Common operations include addition $(+)$, subtraction $(-)$, and multiplication $(\cdot)$.

2 Groups

A **group** is a set with an operation that satisfies the following four rules:

1. **Closure:** If a, b are in the set, then $a \cdot b$ is also in the set.
2. **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in the set.
3. **Identity Element:** There is an element e such that $a \cdot e = a$ for all a.
4. **Inverse:** For every a, there exists b such that $a \cdot b = e$.

Example: The set of integers $\mathbb{Z}$ under addition is a group. The identity is 0, and the inverse of a is $-a$.

3 Rings

A **ring** is a set equipped with two operations, usually called addition $(+)$ and multiplication $(\cdot)$, that satisfy:

- **Addition forms a group:** The set with addition is a group.
- **Multiplication is associative:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Distributive laws:** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Example: The set of integers $\mathbb{Z}$ is a ring.

4 Fields

A **field** is a ring where:

- Multiplication also forms a group (excluding 0).
- Every nonzero element has a multiplicative inverse.

Example: The set of rational numbers $\mathbb{Q}$ is a field.

5 Polynomials

Polynomials are expressions like $p(x) = 2x^2 + 3x + 1$. The set of all polynomials with coefficients from a field (e.g., $\mathbb{Q}[x]$) forms a ring. Operations like addition and multiplication follow the same rules as numbers.

6 $\mathbb{Z}/n\mathbb{Z}$ (Integers Modulo n)

The set $\mathbb{Z}/n\mathbb{Z}$ consists of integers $0, 1, \ldots, n-1$, where addition and multiplication "wrap around" after n.

6.1 Case 1: n is Prime

If n is a prime number, $\mathbb{Z}/n\mathbb{Z}$ is a **field**. This means:

- Addition and multiplication are well-defined.
- Every nonzero element has a multiplicative inverse.

Example: In $\mathbb{Z}/5\mathbb{Z}$:

$$4 + 3 \equiv 2 \pmod{5}, \quad 3 \cdot 4 \equiv 2 \pmod{5}.$$

The inverse of 3 (mod 5) is 2, since $3 \cdot 2 \equiv 1 \pmod{5}$.

6.2 Case 2: n is Composite

If n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is **not a field**, because some elements do not have inverses. For instance, in $\mathbb{Z}/6\mathbb{Z}$:

$$2 \cdot 3 \equiv 0 \pmod{6},$$

so 2 has no inverse.

$\mathbb{Z}/n\mathbb{Z}$ is still a **ring** in this case, but not all the properties of a field hold.

7 Matrices

A **matrix** is a rectangular array of numbers. For example:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

Matrices can be added and multiplied under specific rules.

7.1 Matrix Properties

- **Addition:** Matrices of the same dimensions can be added element by element.
- **Multiplication:** The product of two matrices A and B is defined if the number of columns in A equals the number of rows in B.
- **Determinant:** A square matrix has an inverse if and only if its determinant is nonzero.

The set of $n \times n$ matrices with entries from a field forms a **ring**, but not a field since not all matrices have inverses.

8 Preparing for Vector Spaces

To study vector spaces, we need to understand fields because vectors are defined over fields. In vector spaces:

- Scalars come from a field (e.g., $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$).
- Operations like addition and scalar multiplication must follow the rules of the field.

8.1 Connecting to Algebraic Structures

- Fields provide the framework for scalar multiplication.
- Understanding $\mathbb{Z}/n\mathbb{Z}$ helps with modular arithmetic, which is useful in computer science and cryptography.
- Matrix operations link directly to transformations in vector spaces.

By mastering these structures, you are ready to dive into the study of vector spaces, which combine algebraic and geometric ideas. Understanding $\mathbb{Z}/n\mathbb{Z}$, especially when n is prime, will help you see how fields work in abstract settings, paving the way to more advanced topics.