FEBRUARY 1 NOTES

1. Section 0: Sets and Induction

Most of this section was covered in Math 300. We will mention a few things now for consistency of notation.

Definition 1.1. A **set** is a collection of objects, called **elements** of the set.

If S is a set and x is an element of S, we write $x \in S$. If x is not an element of S, we write $x \notin S$.

Generally, sets are written using brackets to enclose elements: $S = \{1, 2, 3, 4\}$. If there is a clear pattern, we use $\dots$: $S = \{1, 2, \dots, 9, 10\}$ to represent the numbers from 1 to 10 or $S = \{1, 2, 3, \dots, \}$ to represent positive integers. We also use vertical lines to mean 'such that': $S = \{x \mid x \text{ is a positive integer } \}$ is read as 'S is the set of all x such that x is a positive integer.'

There are several sets that we will use frequently:

- $\emptyset$ denotes the *empty set* (the set with no elements)
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ denotes the *integers*
- $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, \quad b \neq 0\}$ denotes the **rational numbers**
- $\mathbb{R}$ denotes the *real numbers*
- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ denotes the *complex numbers*

We will sometimes use notation like $\mathbb{Z}^+$ or $\mathbb{Z}^{\geq 0}$ to indicate things like $\mathbb{Z}^+$ = positive integers or $\mathbb{Z}^{\geq 0}$ = nonnegative integers.

I will post a textbook with related content to Section 0 (essentially, a Math 300 review) if you need a refresher on proof basics, induction, etc.

2. Section 1: Binary Operations

Informally: a binary operation is a way to combine two elements of a given set to form a new element of the set. (Think: addition, multiplication, subtraction, ...)

Definition 2.1. Let S be a set. A **binary operation $\star$ on S** is a function that associates to each ordered pair (s_1, s_2) of elements in S an element $s_1 \star s_2 \in S$. In function notation, a binary operation is a function

$$\star : S \times S \to S$$

$$(s_1, s_2) \mapsto s_1 \star s_2.$$

Example 2.2.

1. Addition $+$ is a binary operation on $\mathbb{Z}$: if $a, b \in \mathbb{Z}$, $a \star b = a + b$ is an integer. Similarly, it is a binary operation on $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. Multiplication $\times$ is a binary operation on $\mathbb{Z}, \mathbb{Z}^+, \mathbb{Q}, \mathbb{Q}^+, \dots$: $a \star b = a \times b$.
3. Division $/$ is a binary operation on $\mathbb{Q}^+$, but **not** on $\mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}$. If $a, b \in \mathbb{Q}^+$, then $a \star b = a/b$ is defined for any pair of rational numbers a, b and produces a rational number. However, if $a, b \in \mathbb{Z}$, a/b is not necessarily in $\mathbb{Z}$, so division is not a binary operation on $\mathbb{Z}$. It also fails to be a binary operation on $\mathbb{Q}$ because a/b is *not defined* if $b = 0$.

In summary: a binary operation must (1) be defined for any two elements of the set, and (2) always produce an element of the set.

Definition 2.3. A binary operation $\star$ on a set S is **commutative** if, for every $s_1, s_2 \in S$,

$$s_1 \star s_2 = s_2 \star s_1.$$

It is **associative** if, for every $s_1, s_2, s_3 \in S$,

$$(s_1 \star s_2) \star s_3 = s_1 \star (s_2 \star s_3).$$

Exercise 2.4. Which of the previous binary operations are commutative? Which are associative?

If you are just reading this, try the exercise before looking at the answer.

Addition on $\mathbb{Z}$ is commutative and associative: $a + b = b + a$ and $(a + b) + c = a + (b + c)$ for any $a, b, c \in \mathbb{Z}$.

Multiplication on $\mathbb{Z}$ is commutative and associative: $a \times b = b \times a$ and $a \times (b \times c) = (a \times b) \times c$ for any $a, b, c \in \mathbb{Z}$.

Division on $\mathbb{Q}^+$ is *not* commutative. If $a = 1$ and $b = 2$, then $a/b = 1/2 \neq 2/1 = b/a$. It is **not** associative: if $a = 1, b = 2, c = 3$, $(a/b)/c = (1/2)/3 = 1/6$ but $a/(b/c) = 1/(2/3) = 3/2$, and these are not equal.

Definition 2.5. We define $M_{n \times m}(\mathbb{R})$ to be the set of all $n \times m$ matrices with real number entries. We define $M_n(\mathbb{R})$ to be the set of all $n \times n$ matrices.

Example 2.6. Multiplication $\times$ is a binary operation on $M_n(\mathbb{R})$ because, for any two $n \times n$ matrices A, B, AB is defined and results in an $n \times n$ matrix. Furthermore, for any three matrices $A, B, C \in M_n(\mathbb{R})$, $(AB)C = A(BC)$ so this is associative. But, there exist matrices A, B such that $AB \neq BA$, so it is not commutative.

If $n \neq m$, multiplication is not a binary operation on $M_{n \times m}(\mathbb{R})$ because the product of two matrices A, B in this set is not defined.

Definition 2.7. Let X be a set. The **power set** of X, denoted $\mathcal{P}(X)$, is the set of all subsets of X.

$$\mathcal{P}(X) = \{S \mid S \subset X\}.$$

Example 2.8. If $X = \{1, 2\}$, then $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Exercise 2.9. If $X = \{1, 2, 3\}$, find $\mathcal{P}(X)$.

Answer: $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Example 2.10. For any set X, the operation $\cup$ (union) is a binary operation on $\mathcal{P}(X)$. Given $A, B \in \mathcal{P}(X)$, A and B are subsets of X, so $A \cup B$ is a subset of X, and hence $A \cup B \in \mathcal{P}(X)$.

It is commutative and associative because $A \cup B = B \cup A$ and $(A \cup B) \cup C = A \cup (B \cup C)$.

We use a table to describe binary operations on finite sets. For example, if $S = \{a, b, c\}$, we can list the elements in the top row and left-most column of the table, and then we fill in the table with the element obtained by applying the binary operation of the element in the left column with the element in the top row:

$\star$	a	b	c
a	$a \star a$	$a \star b$	$a \star c$
b	$b \star a$	$b \star b$	$b \star c$
c	$c \star a$	$c \star b$	$c \star c$

Exercise 2.11. If $X = \{1, 2\}$ so $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, make a table for the binary operation $\cup$ on $\mathcal{P}(X)$.

Answer:

$\star$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1, 2\}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1, 2\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1, 2\}$	$\{1, 2\}$
$\{2\}$	$\{2\}$	$\{1, 2\}$	$\{2\}$	$\{1, 2\}$
$\{1, 2\}$	$\{1, 2\}$	$\{1, 2\}$	$\{1, 2\}$	$\{1, 2\}$