

# MATH 3021: Algebra I

Joe Tran

August 30, 2023



# Preface



# Contents

<b>1</b>	<b>September 6, 2023</b>	<b>7</b>
1.1	Integers . . . . .	8
1.2	Fundamental Properties of Integers . . . . .	9
<b>2</b>	<b>September 8, 2023</b>	<b>11</b>
2.1	Fundamental Properties of Integers . . . . .	11
2.2	Greatest Common Divisor . . . . .	12
<b>3</b>	<b>September 11, 2023</b>	<b>17</b>
3.1	Mathematical Induction . . . . .	17
3.2	Unique Factorization . . . . .	19
<b>4</b>	<b>September 13, 2023</b>	<b>21</b>
4.1	Equivalence Relations . . . . .	23
4.2	Congruence . . . . .	23
4.3	Functions . . . . .	26
<b>5</b>	<b>September 15, 2023</b>	<b>27</b>
5.1	Functions . . . . .	27
<b>6</b>	<b>September 18, 2023</b>	<b>31</b>
6.1	Groups . . . . .	32
<b>7</b>	<b>September 20, 2023</b>	<b>35</b>
7.1	Cayley Tables of Finite Groups . . . . .	38
<b>8</b>	<b>September 22, 2023</b>	<b>39</b>
8.1	Cayley Tables of Finite Groups . . . . .	39
8.2	Some Group Notations . . . . .	41
8.3	Subgroups . . . . .	43

6

*CONTENTS*

9 September 25, 2023

45

# Lecture 1

## September 6, 2023

Your final grade for this class will be based on the following components.

1. 4 Homework Assignments on Crowdmark (30%)
2. Midterm (30%)
3. Final Exam (40%)

What is algebra? Studies operations between objects in sets such as

- Addition on numbers
- Multiplication between numbers
- Matrix multiplication
- Addition modulo  $n$
- and others...

A set  $G$  is called a *group* if it is enclosed with an operation that satisfies certain properties. Groups are the subject of MATH 3021.

**Prerequisites.** A proof-based course (i.e. MATH 1200 or similar). It is very important to be fluent in proof methods (contradiction, induction, etc.)

**Textbook.** Undergraduate Algebra, by S. Lang

Before groups, we will review the properties of integers and functions.

## 1.1 Integers

**Definition 1.1.1.** A *set* is an unordered collection of objects.

**Example 1.1.2.** The following are examples of sets.

- Empty set:  $\emptyset$
- Set of integers  $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$
- Set of natural numbers  $\mathbb{N} = \{1, 2, 3, \dots\}$
- Set of rational numbers  $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N} \right\}$
- Set of real numbers  $\mathbb{R}$
- Set of points in the plane  $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$
- Set of complex numbers  $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$

**Notation 1.1.3.** If  $A$  is a set and  $x$  is a member of  $A$ , we write  $x \in A$ . Otherwise, we write  $x \notin A$ .

**Notation 1.1.4.** For  $A, B$  we write  $A \subseteq B$  if every element in  $A$  is also a element of  $B$ .

**Example 1.1.5.**  $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

*Remark 1.1.6.* It is possible that  $A = B$ , i.e.  $A \subseteq A$

**Notation 1.1.7.** If  $A \subseteq B$  and  $A \neq B$ , then we write  $A \subsetneq B$ .

*Remark 1.1.8.* For sets  $A$  and  $B$ , whenever  $A \subseteq B$  and  $B \subseteq A$ , then  $A = B$ .

**Notation 1.1.9.** For  $A$  and  $B$ , we write

- $A \cup B$  for the union of the two sets.
- $A \cap B$  for the intersection of the two sets.
- $A \setminus B$  for the difference of  $A$  from  $B$
- $A \times B = \{(a, b) : a \in A, b \in B\}$  for the Cartesian product of the two sets.

**Notation 1.1.10.** For a finite set  $A$  we denote  $|A|$  for the number of elements in  $A$  (or the cardinality of  $A$ ). If  $A$  is infinite, then  $|A| = \infty$ .



## 1.2 Fundamental Properties of Integers

**Definition 1.2.1.** Let  $A \subseteq \mathbb{R}$  be a nonempty set and  $x \in \mathbb{R}$ . We call  $x$  a *lower bound* for  $A$  if for all  $y \in A$ ,  $x \leq y$ .

**Definition 1.2.2.** Let  $A \subseteq \mathbb{R}$  and  $x \in \mathbb{R}$ . We call  $x$  a *minimum* of  $A$  and write  $x = \min(A)$  if

- $x$  is a lower bound of  $A$
- $x \in A$ .

**Example 1.2.3.** If  $A = [0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ , then  $\min(A) = 0$ . If  $B = (0, 1)$ , then  $B$  has no minimum.

**Exercise.** If  $A \subseteq \mathbb{R}$  has a minimum, then it is unique.

**Solution.** To show the uniqueness of the minimum, suppose  $x$  and  $x'$  are minima of  $A$ . Then we have that  $x, x' \in A$ . Furthermore, for  $x$ , we have  $x \leq x'$  and we also have that  $x' \leq x$ . As  $\leq$  is antisymmetric, it follows that  $x = x'$ . That is, a minimum of  $A$  is unique if it exists.

**Theorem 1.2.4** (The Well Ordering Principle). *Every nonempty subset  $A$  of  $\mathbb{N}$  has a minimum.*

**Theorem 1.2.5** (Euclidean Algorithm). *Let  $n \in \mathbb{Z}$  and  $m \in \mathbb{N}$ . Then there exists a unique  $q, r \in \mathbb{Z}$  with  $0 \leq r < m$  and  $n = qm + r$ .*

*Proof.* For simplicity, we only treat the case for when  $n > 0$ . Define  $S = \{k \in \mathbb{N} : km > n\}$ . We show that  $S \neq \emptyset$ . Indeed, note that  $k = n + 1 \in S$  because  $km = (n + 1)m > n$ . By the Well Ordering Principle (Theorem 1.2.4), there exists a  $k_0 = \min(S)$ . Define  $q = k_0 - 1$ , and  $r = n - qm$ . Then  $n = qm + r$ . We need to show that  $0 \leq r < m$ .

**Claim 1.2.6.**  $0 \leq r < m$ .

Because  $q = k_0 - 1 < k_0$ , then  $q \notin S$  and so  $qm \leq n$  which implies that  $r = n - qm \geq 0$ .

Next, show that  $r < m$ . Towards contradiction, we assume that  $r \geq m$ . Then this implies that  $m \leq n - qm = r$  and so  $(1 + q)m \leq n$ , which implies that  $k_0 m \leq n$  and so  $k_0 \notin S$ , which is a contradiction, and so  $r < m$ , as required.  $\square$

**Exercise.** Prove that  $q$  and  $r$  are unique.

**Solution.** Suppose that  $q$  and  $r$  are not unique. Then let  $q, q', r, r' \in \mathbb{Z}$  be such that  $0 \leq r < m$  and  $0 \leq r' \leq m$  and  $n = qm + r$  and  $n = q'm + r'$ . Furthermore, assume that  $0 \leq r \leq r' < m$ . Then  $0 < r - r' < b$  and the expressions for  $n$  implies that

$$0 \leq (q - q')m = r' - r < b$$

which is absurd. Therefore,  $r = r'$  and  $q = q'$  as required.

## Lecture 2

September 8, 2023

### 2.1 Fundamental Properties of Integers

Recall the following definitions and theorems.

**Definition 2.1.1.** Let  $A \subseteq \mathbb{R}$  be a nonempty set and  $x \in \mathbb{R}$ . We call  $x$  a lower bound for  $A$  if for all  $y \in A$ ,  $x \leq y$ .

**Definition 2.1.2.** Let  $A \subseteq \mathbb{R}$  be a nonempty set and  $x \in \mathbb{R}$ . We call  $x$  a minimum of  $A$  if both of the following conditions hold.

- $x$  is a lower bound of  $A$
- $x \in A$

We then write  $x = \min(A)$ .

*Remark 2.1.3.* Not all nonempty sets of  $\mathbb{R}$  have a minimum.

**Theorem 2.1.4** (Well Ordering Principle). *Every nonempty subset of  $\mathbb{N}$  admits a minimum.*

**Definition 2.1.5.** Let  $A \subseteq \mathbb{R}$  and  $x \in \mathbb{R}$ . We call  $x$  an upper bound of  $A$  if for all  $y \in A$ ,  $y \leq x$ .

**Definition 2.1.6.** Let  $A \subseteq \mathbb{R}$  and  $x \in \mathbb{R}$ . We call  $x$  a maximum of  $A$  if

- $x$  is an upper bound of  $A$
- $x \in A$

We then write  $x = \max(A)$

**Example 2.1.7.** If  $A = \{n \in \mathbb{Z} : n < 0\}$ , then  $\max(A) = -1$ .

*Remark 2.1.8.* Some subsets of  $\mathbb{N}$  have  $m$  maxima.

**Example 2.1.9.**  $A = \mathbb{N}$  or  $A =$  positive even numbers have  $m$  maxima.

**Theorem 2.1.10.** If  $A \subseteq \mathbb{Z}$  and  $A \neq \emptyset$

(i) If  $A$  has an upper bound, then  $A$  has a maximum.

(ii) If  $A$  has a lower bound, then  $A$  has a minimum.

## 2.2 Greatest Common Divisor

**Definition 2.2.1.** Let  $d, n \in \mathbb{Z} \setminus \{0\}$ . We say that  $d$  divides  $n$  and write  $d \mid n$  if there exists a  $q \in \mathbb{Z}$  such that  $n = qd$ .

**Example 2.2.2.**  $3 \mid 12$  since  $12 = 4 \cdot 3$ .

**Exercise.** If  $n, d \in \mathbb{Z} \setminus \{0\}$  such that  $d \mid n$ , then  $1 \leq |d| \leq |n|$ .

**Solution.** Since  $d \mid n$ , there exists a  $q \in \mathbb{Z}$  such that  $n = qd$ , and so since  $n \neq 0$ , then  $q \neq 0$ , and so  $|n| = |qd| = |q||d|$ , where  $|q| \geq 1$ , and so  $|n| \geq 1 \cdot |d| = |d|$ . Furthermore, since  $|d| \geq 0$ , we have that  $|d| \geq 1$ , and therefore,  $1 \leq |d| \leq |n|$ , as required.

**Definition 2.2.3.** Let  $m, n \in \mathbb{Z} \setminus \{0\}$ . We define the *greatest common divisor* of  $m$  and  $n$  to be

$$\gcd(m, n) = \max\{d \in \mathbb{N} : d \mid m \text{ and } d \mid n\}$$

*Remark 2.2.4.* Note that  $1 \in \{d \in \mathbb{N} : d \mid m \text{ and } d \mid n\}$ . It has an upper bound, i.e.  $|m|$ . Therefore, by Theorem 2.1.10, the maximum of it exists.

**Definition 2.2.5.** A subset  $J \subseteq \mathbb{Z}$  is called an ideal if it satisfies all following conditions:

- $0 \in J$
- For all  $n \in J$  and for all  $m \in \mathbb{Z}$ ,  $mn \in J$  (it contains all multiples of its elements).
- For all  $m, n \in J$ ,  $m + n \in J$  (it contains all sums of its elements).

**Example 2.2.6.** The following are examples are ideals.

- $J = \mathbb{Z}$  is an ideal.
- $J = \{0\}$  is an ideal.
- $J = \{n, k \in \mathbb{Z} : n = 2k\}$

**Example 2.2.7.** Suppose  $m_1, m_2, \dots, m_r \in \mathbb{Z}$ . Consider the set given by

$$J = \left\{ \sum_{i=1}^r x_i m_i : x_i \in \mathbb{Z}, 1 \leq i \leq r \right\}$$

Then  $J$  is an ideal and we say that it is *generated* by  $m_1, m_2, \dots, m_r$ . To see that  $J$  is an ideal, first note that if we consider for each  $1 \leq i \leq r$ ,  $x_i = 0$ , then  $0 \in J$ .

Next, take  $n \in J$  and  $m \in \mathbb{Z}$ . We need to show that  $mn \in J$ . Since  $n \in J$ , for each  $1 \leq i \leq r$ , there exists  $x_i \in \mathbb{Z}$  such that

$$n = \sum_{i=1}^r x_i m_i$$

So

$$mn = m \sum_{i=1}^r x_i m_i = \sum_{i=1}^r x_i m_i m \in J$$

Finally, take  $m = \sum_{i=1}^r x_i m_i \in J$  and  $n = \sum_{i=1}^r y_i m_i \in J$ . Then

$$m + n = \sum_{i=1}^r x_i m_i + \sum_{i=1}^r y_i m_i = \left( \sum_{i=1}^r m_i (x_i + y_i) \right) \in J$$

Therefore,  $J$  is an ideal.

**Theorem 2.2.8.** Let  $J$  be a nonzero ideal (i.e.  $J \neq \{0\}$ ). Then there exists an  $m_0 \in \mathbb{Z}$  that generates  $J$ , i.e.  $J = \{xm_0 : x \in \mathbb{Z}\}$ . In fact, we may take  $m_0 = \min\{n \in J : n > 0\}$ .

*Proof.* We need to show that  $\{n \in J : n > 0\}$  is

- (i) Bounded below (1 is a lower bound)
- (ii) It is nonempty. We assumed there exists an  $n \in J \setminus \{0\}$ .
  - If  $n > 0$  then we are done.
  - If  $n < 0$ , then  $-1 \cdot n > 0$  and  $-1 \cdot n \in J$ .

Take  $m_0 = \min\{n \in J : n > 0\}$  (which exists). Take an arbitrary  $n \in J$ . We will use the Euclidean algorithm to write  $n = qm_0 + r$ , where  $0 \leq r < m_0$ .

**Claim 2.2.9.**  $r = 0$ . *If the claim is true, then  $n = qm_0$ , and so  $n = \{x \cdot m_0 : x \in \mathbb{Z}\}$ , which implies that  $J \subseteq \{x \cdot m_0 : x \in \mathbb{Z}\}$ .*

To show that the claim is true, assume that  $r \neq 0$ . Then  $0 < r < m_0$ . Since  $m_0 \in J$ , then  $-q \cdot m_0 \in J$ . Since  $n \in J$ , then  $n + (-q) \cdot m_0 \in J$  which implies that  $r \in J$ . This is absurd since  $m_0$  has to be the smallest positive number of  $J$  and  $r$  is even smaller.  $\square$

**Theorem 2.2.10.** *Let  $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$  and  $J$  be the ideal generated by then, i.e.  $J = \{x_1 m_1 + x_2 m_2 : x_1, x_2 \in \mathbb{Z}\}$ . Then  $\gcd(m_1, m_2)$  generates  $J$ .*

*Proof.* From Theorem 2.2.8, if we set  $m_0 = \min\{n \in J : n > 0\}$ , then  $m_0$  generates  $J$ . We will show that  $m_0 = \gcd(m_1, m_2)$ . Since  $m_0$  generates  $J$ , there exists  $x_1, x_2$  such that

$$m_1 = x_1 \cdot m_0 \Rightarrow m_0 \mid m_1$$

and

$$m_2 = x_2 \cdot m_0 \Rightarrow m_0 \mid m_2$$

Since  $m_0 \in \mathbb{N}$ ,  $1 \leq m_0 \leq \gcd(m_1, m_2)$ . We will now show that  $\gcd(m_1, m_2) \mid m_0$ . We have that

$$1 \leq |\gcd(m_1, m_2)| \leq |m_0| \Rightarrow 1 \leq \gcd(m_1, m_2) \leq m_0$$

which implies that  $\gcd(m_1, m_2) = m_0$ . Since  $m_0 \in J$ , there exists  $y_1, y_2 \in \mathbb{Z}$  such that

$$m_0 = y_1 m_1 + y_2 m_2 \tag{1}$$

Since  $\gcd(m_1, m_2) \mid m_1$  and  $\gcd(m_1, m_2) \mid m_2$ , there exists  $z_1, z_2 \in \mathbb{Z}$  such that

$$m_1 = z_1 \gcd(m_1, m_2) \quad m_2 = z_2 \gcd(m_1, m_2) \tag{2}$$

Substituting (2) to (1) gives us

$$\begin{aligned} m_0 &= y_1 z_1 \gcd(m_1, m_2) + y_2 z_2 \gcd(m_1, m_2) \\ &= (y_1 z_1 + y_2 z_2) \gcd(m_1, m_2) \end{aligned}$$

which implies that  $\gcd(m_1, m_2) \mid m_0$ , as required.  $\square$

**Corollary 2.2.11** (Bezout's Theorem). *If  $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$ , then there exists  $x_1, x_2 \in \mathbb{Z}$  such that  $\gcd(m_1, m_2) = x_1 m_1 + x_2 m_2$ .*

*Proof.* If  $J$  is an ideal generated by  $m_1$  and  $m_2$ , then  $\gcd(m_1, m_2) \in J$  by the previous theorem.  $\square$





## Lecture 3

September 11, 2023

Recall that in the previous lecture, we mentioned the following:

**Definition 3.0.1.** For  $m, n \in \mathbb{Z} \setminus \{0\}$ ,

$$\gcd(m, n) = \max\{d \in \mathbb{N} : d \mid m \text{ and } d \mid n\}$$

**Theorem 3.0.2** (Bezout's Theorem). *Let  $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$ . Then there exists  $x_1, x_2 \in \mathbb{Z}$  such that  $\gcd(m_1, m_2) = x_1m_1 + x_2m_2$ .*

*Remark 3.0.3.* A similar proof yields that for  $m_1, m_2, \dots, m_r \in \mathbb{Z} \setminus \{0\}$ , there exists  $x_1, x_2, \dots, x_r \in \mathbb{Z}$  such that

$$\gcd(m_1, m_2, \dots, m_r) = x_1m_1 + x_2m_2 + \dots + x_rm_r$$

Here,

$$\gcd(m_1, m_2, \dots, m_r) = \max\{d \in \mathbb{N} : d \mid m_1, d \mid m_2, \dots, d \mid m_r\}$$

**Theorem 3.0.4** (Well Ordering Principle). *Let  $A \subseteq \mathbb{N}$  be a nonempty set. Then  $A$  has a minimum.*

### 3.1 Mathematical Induction

**Theorem 3.1.1** (Principle of Mathematical Induction). *For all  $n \in \mathbb{N}$ , let  $A(n)$  be an assertion (i.e. a statement that is either true or false). Assume that we can prove the following*

(i)  $A(1)$  is true.

(ii) Whenever  $n \in \mathbb{N}$  is such that  $A(n)$  is true, then  $A(n+1)$  must be true as well.

Then  $A(n)$  is true for all  $n \in \mathbb{N}$ .

**Example 3.1.2.** Suppose  $A(n)$  is the assertion that “ $n \leq 2^n$ ” for all  $n \in \mathbb{N}$ . We could see that  $A(1)$ ,  $A(2)$ ,  $A(3)$  is true, and may also be true for higher  $n$ .

*Proof.* Define  $S = \{n \in \mathbb{N} : A(n) \text{ is true}\}$ . We want to show  $S = \mathbb{N}$ . From (i),  $1 \in S$ . Define  $B = \mathbb{N} \setminus S$ . We will show that  $B = \emptyset$ , which then implies  $S = \mathbb{N}$ . For contradiction, let us assume that  $B \neq \emptyset$ . By the Well Ordering Principle (Theorem 3.0.4), there exists an  $m_0 = \min(B)$  since

- $1 \in S$  which implies  $m_0 \neq 1$  and so  $m_0 > 1$  or  $m_0 \geq 2$ .
- $m_0 - 1 < m_0 = \min(B)$  which implies that  $m_0 - 1 \geq 1$  and  $m_0 - 1 \notin B$  which implies that  $m_0 - 1 \in S$  and so  $A(m_0 - 1)$  is true.

By (ii),  $A(m_0 - 1)$  being true implies  $A(m_0 - 1 + 1) = A(m_0)$  is true and so  $m_0 \in S$ . But this is absurd, and so  $B = \emptyset$ .  $\square$

**Exercise.** Prove that for all  $n \in \mathbb{N}$ ,

$$\left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n}\right)^n = \frac{(n+1)^n}{n!}$$

**Solution.** For the base case  $n = 1$ , we have

$$\left(1 + \frac{1}{1}\right)^1 = 2$$

and

$$\frac{(1+1)^1}{1!} = 2$$

So the base case is true. Now assume that for all  $n \in \mathbb{N}$ ,

$$\left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n}\right)^n = \frac{(n+1)^n}{n!}$$

Then for  $n+1 \in \mathbb{N}$ , we have

$$\begin{aligned} \left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n+1}\right)^{n+1} &= \frac{(n+1)^n}{n!} \cdot \left(1 + \frac{1}{n+1}\right)^{n+1} \\ &= \frac{(n+1)^n}{n!} \left(\frac{n+2}{n+1}\right)^{n+1} \\ &= \frac{(n+2)^{n+1}}{(n+1)n!} = \frac{(n+2)^{n+1}}{(n+1)!} \end{aligned}$$

as desired.

**Theorem 3.1.3** (Strong Mathematical Induction). *For  $n \in \mathbb{N}$ , let  $A(n)$  be an assertion and assume that we can prove the following:*

- (i)  $A(1)$  is true
- (ii) If  $n \in \mathbb{N}$  is such that  $A(1), A(2), \dots, A(n)$  are all true, then  $A(n+1)$  must also be true as well.

*Then for all  $n \in \mathbb{N}$ ,  $A(n)$  is true.*

*Proof.* The proof is similar as Theorem 3.1.1. □

## 3.2 Unique Factorization

Recall that if  $p \in \mathbb{N}$  is such that  $p \geq 2$ , then  $p$  is called a *prime number* if its only divisors in  $\mathbb{N}$  are 1 and  $p$ .

**Example 3.2.1.** 2, 3, 5, 7, 11, ... are all prime numbers

**Theorem 3.2.2** (Prime Factorization). *Let  $n \in \mathbb{N}$  with  $n \geq 2$ . Then  $n$  can be written as a product of prime numbers*

$$n = p_1 \cdot p_2 \cdots p_r$$

*Remark 3.2.3.* (i) If  $n = p_1 \cdot p_2 \cdots p_r$ , then some of the primes may be repeated. For example,  $12 = 2 \cdot 2 \cdot 3$ .

(ii) If  $n = p$  is already prime, we consider this a trivial product of primes.

*Proof by Strong Induction.* For the base case  $n = 2$  is prime, so it is trivially a product of primes. Let  $n \in \mathbb{N}$  for  $n \geq 2$  be such that 2, 3, 4, ...,  $n$  can all be written as a product of primes. We want to show that  $n+1$  is a product of primes.

Case 1:  $n+1$  is already prime, so there is nothing that needs to be shown.

Case 2:  $n+1$  is not prime, then there exists a  $d \in \mathbb{N}$  such that  $d \neq 1$  and  $d \neq n+1$  such that  $d \mid n+1$ . Since  $1 \leq d \leq n+1$ , we have

$$1 < d < n+1 \tag{1}$$

Then there exists a  $q \in \mathbb{Z}$  such that  $n+1 = qd$ . Then  $q \in \mathbb{N}$  and  $q \mid n+1$  which implies that  $1 \leq q \leq n+1$ . From (1), we have

$$1 < q < n+1 \tag{2}$$

and so we have  $2 \leq d \leq n$  and  $2 \leq q \leq n$ . By the inductive hypothesis,  $d$  and  $q$  may be written as products of primes. Because  $n + 1 = qd$  is a product of primes.  $\square$

*Remark 3.2.4.* In  $n = p_1 \cdot p_2 \cdots p_r$  there may be repetitions. We may avoid these and write

$$n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$$

where  $p_1 < p_2 < \cdots < p_s$  are prime numbers and  $m_1, m_2, \dots, m_s \in \mathbb{N}$ .

**Example 3.2.5.**  $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1$ . Note that this representation is unique.

**Lemma 3.2.6.** Let  $n, m \in \mathbb{Z} \setminus \{0\}$  and  $p \in \mathbb{N}$  be a prime number. If  $p \mid nm$  then either  $p \mid n$  or  $p \mid m$ .

*Proof.* Let  $d = \gcd(n, p)$ . Since  $p$  is prime and  $d \mid p$ , then either  $d = 1$  or  $d = p$  (Note that there exists an  $x \in \mathbb{Z}$  such that  $n = xd$ )

Case 1: When  $d = p$ , then because  $d \mid n$ , we have  $p \mid n$ .

Case 2: When  $d = 1$ , then by Bezout's Theorem, there exists  $y, z \in \mathbb{Z}$  such that

$$1 = d = \gcd(n, p) = yn + zp$$

times  $m$  and so

$$m = ymn + zmp$$

Since  $p \mid mn$ , there exists  $w \in \mathbb{Z}$  such that  $mn = wp$ . and so

$$m = ywp + zmp = (yw + zm)p$$

Therefore  $p \mid m$  as desired.  $\square$

**Corollary 3.2.7.** If  $p \in \mathbb{N}$  is prime and  $n_1, n_2, \dots, n_r \in \mathbb{Z} \setminus \{0\}$ , then if  $p \mid n_1 \cdot n_2 \cdots n_r$ , then there exists  $1 \leq i \leq r$  such that  $p \mid n_i$ .

*Proof.* Exercise.  $\square$

**Proposition 3.2.8.** Let  $n \in \mathbb{N}$  be such that  $n \geq 2$ . If

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$$

and

$$n = q_1^{k_1} \cdot q_2^{k_2} \cdots q_s^{k_s}$$

with  $p_1 < p_2 < \cdots < p_r$ ,  $m_1, \dots, m_r \in \mathbb{N}$ ,  $q_1 < q_2 < \cdots < q_s$  and  $k_1, \dots, k_s \in \mathbb{N}$ , then  $r = s$  and for each  $1 \leq i \leq r$ ,  $p_i = q_i$  and  $m_i = k_i$ .

## Lecture 4

# September 13, 2023

Recall in the previous lecture we have mentioned the following:

**Theorem 4.0.1** (Prime Factorization). *Let  $n \in \mathbb{N}$  with  $n \geq 2$ . Then  $n$  can be written as a product of prime numbers*

$$n = p_1 \cdot p_2 \cdots p_r$$

*Remark 4.0.2.* In  $n = p_1 \cdot p_2 \cdots p_r$  there may be repetitions. We may avoid these and write

$$n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$$

where  $p_1 < p_2 < \cdots < p_s$  are prime numbers and  $m_1, m_2, \dots, m_s \in \mathbb{N}$ . This representation is unique, as we will prove.

**Lemma 4.0.3.** *Let  $n, m \in \mathbb{Z} \setminus \{0\}$  and  $p \in \mathbb{N}$  be a prime number. If  $p \mid nm$  then either  $p \mid n$  or  $p \mid m$ .*

**Proposition 4.0.4.** *Let  $n \in \mathbb{N}$  be such that  $n \geq 2$ . If*

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$$

*and*

$$n = q_1^{k_1} \cdot q_2^{k_2} \cdots q_s^{k_s}$$

*with  $p_1 < p_2 < \cdots < p_r$ ,  $m_1, \dots, m_r \in \mathbb{N}$ ,  $q_1 < q_2 < \cdots < q_s$  and  $k_1, \dots, k_s \in \mathbb{N}$ , then  $r = s$  and for each  $1 \leq i \leq r$ ,  $p_i = q_i$  and  $m_i = k_i$ . Therefore, the prime decomposition of  $n$  is unique.*

*Remark 4.0.5.* The existence and uniqueness of the prime decomposition of all  $n \in \mathbb{N}$  with  $n \geq 2$  is called the Fundamental Theorem of Arithmetic.

*Proof of Proposition 4.0.4.* We will prove Proposition 4.0.4 in two steps.

**Claim 4.0.6.** *If  $n \in \mathbb{N}$  with  $n \geq 2$  is such that*

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r} = q_1^{k_1} \cdot q_2^{k_2} \cdots q_s^{k_s}$$

*then*

$$\{p_1, p_2, \dots, p_r\} = \{q_1, q_2, \dots, q_s\}$$

*In particular,  $r = s$ .*

Let  $A = \{p_1, p_2, \dots, p_r\}$  and  $B = \{q_1, q_2, \dots, q_s\}$ . We show that  $A \subseteq B$ . Take  $p_i \in A$ . Since

$$n = p_1^{m_1} \cdots p_i^{m_i} \cdots p_r^{m_r} = p_i p_1^{m_1} \cdots p_i^{m_i-1} \cdots p_r^{m_r} = p_i q$$

then

$$p_i \mid n = \underbrace{q_1 \cdots q_1}_{k_1 \text{ times}} \cdot \underbrace{q_2 \cdots q_2}_{k_2 \text{ times}} \cdots \underbrace{q_s \cdots q_s}_{k_s \text{ times}}$$

By Lemma 4.0.3, there exists  $1 \leq j \leq s$  such that  $p_i \mid q_j$ . Since  $q_j$  is prime, then  $p_i = 1$  or  $p_i = q_j$ . Since  $p_i$  is prime,  $p_i \neq 1$  which implies that  $p_i = q_j \in B$ , and therefore  $A \subseteq B$ . Similarly, we would also have to show that  $B \subseteq A$ , and so  $A = B$ .

**Claim 4.0.7.** *If  $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r} = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$  then for each  $1 \leq i \leq r$ ,  $m_i = k_i$ .*

Take  $1 \leq i \leq r$ , we show  $m_i \leq k_i$ . Assume otherwise that  $m_i > k_i$ . Consider

$$\begin{aligned} n' &= \frac{n}{p_i^{k_i}} = \frac{p_1^{m_1} \cdots p_i^{m_i} \cdots p_r^{m_r}}{p_i^{k_i}} \\ &= p_1^{m_1} \cdots p_i^{m_i-k_i} \cdots p_r^{m_r} \in \mathbb{N} \end{aligned}$$

(since  $m_i - k_i > 0$ ). Also,

$$n' = \frac{p_1^{k_1} \cdots p_i^{k_1} \cdots p_r^{k_r}}{p_i^{k_i}} = p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_r^{k_r}$$

So  $n' = p_1^{m_1} \cdots p_i^{m_i-k_i} \cdots p_r^{m_r} = p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_r^{k_r}$ . Then by Claim 4.0.6, we have that

$$\{p_1, p_2, \dots, p_{i-1}, p_i, p_{i+1}, \dots, p_r\} = \{p_1, p_2, \dots, p_{i-1}, p_{i+1}, \dots, p_r\}$$

which is absurd because  $p_i$  is missing in the second set. Therefore,  $m_i \leq k_i$ . Similarly, it can be shown that  $k_i \leq m_i$ , and which implies that  $m_i = k_i$  as required.  $\square$

## 4.1 Equivalence Relations

**Definition 4.1.1.** Let  $X$  be a nonempty set. A binary relation  $\sim$  on  $X$  is called an *equivalence relation* if the following hold:

- (i) (Reflexivity) For all  $x \in X$ ,  $x \sim x$
- (ii) (Symmetry) For all  $x, y \in X$ , if  $x \sim y$ , then  $y \sim x$ .
- (iii) (Transitivity) For all  $x, y, z \in X$ , if  $x \sim y$  and  $y \sim z$ , then  $x \sim z$ .

**Example 4.1.2.** The following are examples of an equivalence relation.

- For all nonempty sets  $X$ ,  $=$  is an equivalence relation.
- Define  $\sim$  on  $\mathbb{R}$  given by  $x \sim y$  whenever  $x - y \in \mathbb{Q}$  (Verify that this is an equivalence relation).

**Definition 4.1.3.** Let  $X$  be a nonempty set and let  $\sim$  be an equivalence relation on  $X$ . For all  $x \in X$ , the *equivalence class of  $x$*  is the set  $[x] = \{y : y \sim x\}$ .

**Proposition 4.1.4.** If  $X$  is a nonempty set and  $\sim$  is an equivalence relation on  $X$ , then for all  $x, y \in X$ , exactly one of the following holds:

- (i)  $[x] = [y]$
- (ii)  $[x] \cap [y] = \emptyset$ .

*Proof.* Exercise. □

**Corollary 4.1.5.** The equivalence classes form a partition of  $X$ .

## 4.2 Congruence

**Definition 4.2.1.** Let  $n \in \mathbb{N}$  and  $x, y \in \mathbb{Z}$ . We say that  $x$  is congruent to  $y$  modulo  $n$  and write

$$x \equiv y \pmod{n}$$

if  $n \mid x - y$ .

**Exercise.** For given  $n \in \mathbb{N}$ , congruence mod  $n$  defines an equivalence relation on  $\mathbb{Z}$ .

**Solution.** Let  $x, y, z \in \mathbb{Z}$  be arbitrary. To show that  $\equiv \bmod n$  defines an equivalence relation, we need to verify the three properties that define an equivalence relation.

To show that (i) is true, note that  $x \equiv x \bmod n$  implies that  $n \mid x - x$ , or  $n \mid 0$ , which implies that there exists an integer  $k \in \mathbb{Z}$  such that

$$0 = kn$$

In particular, we can choose  $k = 0$  and the result will hold.

To show that (ii) is true, note that  $x \equiv y \bmod n$  implies that  $n \mid x - y$ , which implies that there exists an integer  $k \in \mathbb{Z}$  such that

$$x - y = kn$$

By multiplying both sides by  $-1$ , we have that

$$y - x = -kn$$

where  $-k \in \mathbb{Z}$ . This implies that  $n \mid y - x$ , which also implies that  $y \equiv x \bmod n$ , as required.

To show that (iii) is true, note that  $x \equiv y \bmod n$  implies that  $n \mid x - y$ , which implies that there exists an integer  $k_1 \in \mathbb{Z}$  such that

$$x - y = k_1n$$

Similarly, note that  $y \equiv z \bmod n$  implies that  $n \mid y - z$  which implies that there exists an integer  $k_2 \in \mathbb{Z}$  such that

$$y - z = k_2n$$

Add the two equations together so that

$$x - y + y - z = x - z = k_1n - k_2n = (k_1 - k_2)n$$

Note that  $k_1 - k_2 \in \mathbb{Z}$ , and so this implies that  $n \mid x - z$ , which implies that  $x \equiv z \bmod n$  as required.

Since the congruence modulo  $n$  satisfies the three properties of an equivalence relation, the congruence modulo  $n$  is an equivalence relation.

**Exercise.** For given  $n \in \mathbb{N}$ , show that for all  $x \in \mathbb{Z}$ ,  $x \equiv r \bmod n$  where  $r$  is the remainder of  $x$  divided by  $n$ , i.e.  $x = qn + r$  where  $0 \leq r < n$ . In



particular, the equivalence of congruence modulo  $n$  are

$$\begin{aligned} [0] &= \{k \in \mathbb{Z} : kn\} \\ [1] &= \{k \in \mathbb{Z} : kn + 1\} \\ [2] &= \{k \in \mathbb{Z} : kn + 2\} \\ &\vdots \\ [n-1] &= \{k \in \mathbb{Z} : kn + (n-1)\} \end{aligned}$$

**Solution.** Let  $x = qn + r$ , by the Euclidean algorithm. Then we can rearrange the equation so that

$$x - r = qn$$

where  $q \in \mathbb{Z}$ ,  $n \in \mathbb{N}$  and  $0 \leq r < n$ . Then this implies that  $n \mid x - r$ , which also implies that  $x \equiv r \pmod{n}$ , as required.

**Proposition 4.2.2.** *Let  $n \in \mathbb{N}$  and let  $x, y, z, w \in \mathbb{Z}$  be such that  $x \equiv y \pmod{n}$  and  $z \equiv w \pmod{n}$ . Then*

$$x + z \equiv y + w \pmod{n} \quad xz \equiv yw \pmod{n}$$

*Proof.* First, since  $x \equiv y \pmod{n}$ , then this implies that  $n \mid x - y$ , which implies that there exists an  $k_1 \in \mathbb{Z}$  such that

$$x - y = k_1 n \tag{1}$$

Similarly, since  $z \equiv w \pmod{n}$ , then this implies that  $n \mid z - w$  which implies that there exists a  $k_2 \in \mathbb{Z}$  such that

$$z - w = k_2 n \tag{2}$$

By adding (1) and (2), we obtain

$$(x - y) + (z - w) = k_1 n + k_2 n \Rightarrow (x + z) - (y + w) = n(k_1 + k_2)$$

Note that  $k_1 + k_2 \in \mathbb{Z}$ , which implies that  $n \mid (x + z) - (y + w)$ , which implies that  $x + z \equiv y + w \pmod{n}$ . Hence, the first result holds.

To show the second result, take  $xz - yw = xz - yz + yz - yw$  and so  $(x - y)z + (z - w)y$  which implies that  $k_1 n z + k_2 n y$ , or  $(k_1 z + k_2 y)n$  which implies that  $n \mid xz - yw$  as desired.  $\square$

### 4.3 Functions

**Definition 4.3.1** (Informal Definition of a Function). Let  $X, Y$  be two nonempty sets. A function from  $X$  to  $Y$  is a rule that assigns to every  $x \in X$ , a unique  $y \in Y$  which we denote by  $f(x)$ . We then write  $f : X \rightarrow Y$ . Here  $X$  is the domain of  $f$  and  $Y$  is the codomain of  $f$ .

**Definition 4.3.2.** Let  $X, Y$  be two nonempty sets and  $f : X \rightarrow Y$  be a function. The graph of  $f$  is the set

$$\text{gr}(f) = \{(x, y) : x \in X, y \in Y, y = f(x)\} \subseteq X \times Y$$

*Remark 4.3.3.* The graph of  $f$  has the following property: For all  $x \in X$ , there exists a unique  $y \in Y$  such that  $(x, y) \in \text{gr}(f)$ .

# Lecture 5

## September 15, 2023

### 5.1 Functions

**Example 5.1.1.** Let  $X$  be a nonempty set. Then

- $\text{id} : X \rightarrow X$  is a function (i.e. for all  $x \in X$ ,  $\text{id}(x) = x$ )
- For fixed  $x_0 \in X$ , define  $x \in X$  so that  $f(x) = x_0$ .

**Definition 5.1.2.** Let  $X, Y$  be nonempty sets,  $f : X \rightarrow Y$  be a function, and  $A \subseteq X$ . We define the *image of  $A$  under  $f$*  as follows:

$$f(A) = \{y \in Y : \exists x \in A : f(x) = y\} = \{f(x) : x \in A\}$$

In particular,  $f(X)$  is called the range of  $f$ .

*Remark 5.1.3.* The range and codomain may not be the same.

**Example 5.1.4.** Take  $f : \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = x^2$ . The codomain is  $\mathbb{R}$  while the range is  $[0, \infty)$ .

**Definition 5.1.5.** Let  $X, Y$  be nonempty sets and let  $f : X \rightarrow Y$  be a function.

- (i) If for all  $x_1 \neq x_2$ ,  $f(x_1) \neq f(x_2)$ , then we call  $f$  one-to-one, or injective.
- (ii) If for all  $y \in Y$  there exists  $x \in X$  such that  $f(x) = y$ , then we call  $f$  onto, or surjective.
- (iii) If  $f$  is one-to-one and onto, then we call it a bijection.

**Example 5.1.6.** Take  $f : \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = x + 1$ . This is a one-to-one and onto function, and therefore it is a bijection.

**Definition 5.1.7.** Let  $X, Y, Z$  be nonempty sets,  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be functions. The *composition of  $g$  with  $f$*  is the function  $g \circ f : X \rightarrow Z$  given by  $(g \circ f)(x) = g(f(x))$ .

*Remark 5.1.8.* Let  $X$  be a nonempty set.

$$X^X = \{\text{all functions } f : X \rightarrow X\}$$

The composition takes two functions  $f, g \in X^X$  and creates a new member  $g \circ f \in X^X$ . This means  $\circ$  is a type of operation chain to  $+$  or  $\cdot$  on  $\mathbb{R}$ .

*Remark 5.1.9.* Let  $X$  be a nonempty set and let  $f, g : X \rightarrow X$ . It is not always true that  $g \circ f = f \circ g$ .

**Example 5.1.10.** Take  $f, g : \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = x + 1$  and  $g(x) = x^2$ . Then  $(f \circ g)(1) = 2$  and  $(g \circ f)(1) = 4$ , so clearly,  $g \circ f \neq f \circ g$ .

**Proposition 5.1.11.** Let  $X, Y$  be nonempty sets and let  $f : X \rightarrow Y$  be a bijection. Then there exists some unique function  $f^{-1} : Y \rightarrow X$  such that

(i) For all  $x \in X$ ,  $(f^{-1} \circ f)(x) = x$ , i.e.  $f^{-1} \circ f = \text{id} : X \rightarrow X$ .

(ii) For all  $y \in Y$ ,  $(f \circ f^{-1})(y) = y$ , i.e.  $f \circ f^{-1} = \text{id} : Y \rightarrow Y$ .

Sometimes we call bijections *invertible functions* (because  $f^{-1}$  is called the *inverse of  $f$* .)

**Example 5.1.12.** •  $f : [0, \infty) \rightarrow [0, \infty)$  with  $f(x) = x^2$ . Then  $f^{-1}(x) = \sqrt{x}$

•  $f : \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = x^2$ . Then  $f$  is not invertible.

**Exercise.** Let  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be functions.

(i) If  $f$  and  $g$  are both one-to-one, then  $g \circ f : X \rightarrow Z$  is one-to-one.

(ii) If  $f$  and  $g$  are both onto, then  $g \circ f : X \rightarrow Z$  is onto.

(iii) If  $f$  and  $g$  are both invertible, then  $g \circ f : X \rightarrow Z$  is invertible.

**Solution.** To show that (i) is true, assume that  $f$  and  $g$  are both one-to-one functions. Since  $f$  is one-to-one, then for all  $x_1 \neq x_2$ , we have  $f(x_1) \neq f(x_2)$ . Similarly, since  $g$  is one-to-one, then for all  $y_1 \neq y_2$ , we have  $g(y_1) \neq g(y_2)$ . In particular, for all  $f(x_1) \neq f(x_2)$ , we obtain  $g(f(x_1)) \neq g(f(x_2))$ , which implies that  $g \circ f$  is one-to-one.

To show that (ii) is true, assume that  $f$  and  $g$  are both onto. Since  $f$  is onto, for all  $y \in Y$  then there exists an  $x \in X$  such that  $f(x) = y$ . Similarly, since  $g$  is onto, for all  $z \in Z$ , there exists a  $y \in Y$  such that  $g(y) = z$ . In particular, if  $y = f(x)$ , then this implies that  $g(f(x)) = z$ , implying that  $g \circ f$  is onto.

To show that (iii) is true, note that  $f$  and  $g$  have to be both one-to-one and onto, which we have shown above, and if  $f$  and  $g$  satisfy both (i) and (ii) from above, then  $g \circ f$  would also be a bijection.

**Definition 5.1.13.** Let  $f : X \rightarrow Y$  be a function and let  $B \subseteq Y$ . The inverse image of  $B$  under  $f$  is the set

$$f^{-1}(B) = \{x \in X : f(x) \in B\}$$

*Remark 5.1.14.* The inverse image is always well defined, regardless whether  $f$  has an inverse.

**Example 5.1.15.** Take  $f : \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = x^2$ . Note that  $f$  is not invertible.

- If  $B = (1, 4)$ , then  $f^{-1}(B) = (-2, -1) \cup (1, 2)$
- If  $B = (-1, 0)$ , then  $f^{-1}(B) = \emptyset$ .

**Definition 5.1.16.** Let  $X$  be a nonempty set. A function  $*$  :  $X \times X \rightarrow X$  is called a binary operation.

**Notation 5.1.17.** Instead of  $*(x, y)$ , we write  $x * y$ .

**Example 5.1.18.** •  $+$  :  $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , i.e.  $+(x, y) = x + y$ .

- $\cdot$  :  $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , i.e.  $\cdot(x, y) = x \cdot y$
- If  $\mathcal{M}_n(\mathbb{R})$  denotes the set of all  $n \times n$  matrices with real entries, then  $\cdot : \mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_n(\mathbb{R}) \rightarrow \mathcal{M}_n(\mathbb{R})$  given matrix multiplication, i.e. if  $A$  and  $B$  are  $n \times n$  matrices, then  $AB$  is an  $n \times n$  matrix.
- $\cdot$  :  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  with

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

- $\circ : X^X \times X^X \rightarrow X^X$ , i.e. for  $f, g : X \rightarrow X$ ,  $\circ(f, g) = f \circ g$ .
- $\mathbb{Q}^+ = \mathbb{Q} \setminus \{0\}$ ,  $\div : \mathbb{Q}^+ \times \mathbb{Q}^+ \rightarrow \mathbb{Q}^+$  with  $\div(x, y) = \frac{x}{y}$ .
- Division is *not* a binary operation on  $\mathbb{N}$  because it is not always true that  $\frac{n}{m} \in \mathbb{N}$  whenever  $n, m \in \mathbb{N}$ .

**Definition 5.1.19.** Let  $*$  be a binary operation on a set  $X$ .

- (i)  $*$  is called associative if for all  $x, y, z \in X$ ,

$$(x * y) * z = x * (y * z)$$

- (ii)  $*$  is called commutative if for all  $x, y \in X$ ,

$$x * y = y * x$$

**Example 5.1.20.** •  $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$  is both associative and commutative. For (i) if  $x, y, z \in \mathbb{R}$ , then

$$(x + y) + z = x + (y + z)$$

For (ii), if  $x, y \in \mathbb{R}$ , then  $x + y = y + x$ .

- $\div : \mathbb{Q}^+ \times \mathbb{Q}^+ \rightarrow \mathbb{Q}^+$  is neither associative nor commutative. For (i), take  $x, y, z \in \mathbb{Q}^+$ ,

$$(x \div y) \div z = \left(\frac{x}{y}\right) \div z = \frac{\frac{x}{y}}{z} = \frac{x}{yz}$$

and

$$x \div (y \div z) = x \div \left(\frac{y}{z}\right) = \frac{x}{\frac{y}{z}} = \frac{zx}{y}$$

Clearly,  $(x \div y) \div z \neq x \div (y \div z)$ .

- $\circ : X^X \times X^X \rightarrow X^X$  is associative but (usually) not commutative. We said that for  $X = \mathbb{R}$ ,  $\circ$  is not commutative.  $\circ$  is associative however! For functions  $f, g, h \in X^X$ , we have

$$\begin{aligned} (f \circ g) \circ h &= f \circ (g \circ h) \\ ((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) = f(g(h(x))) \\ (f \circ (g \circ h))(x) &= f((g \circ h)(x)) = f(g(h(x))) \end{aligned}$$

## Lecture 6

# September 18, 2023

Recall in the previous lecture, we have started to talk about binary operations:

**Definition 6.0.1.** Let  $X$  be a nonempty set. A function  $*$  :  $X \times X \rightarrow X$  is called a binary operation.

**Definition 6.0.2.** Let  $*$  be a binary operation on a set  $X$ .

- (i)  $*$  is called associative if for all  $x, y, z \in X$ ,

$$(x * y) * z = x * (y * z)$$

- (ii)  $*$  is called commutative if for all  $x, y \in X$ ,

$$x * y = y * x$$

**Example 6.0.3.** •  $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , i.e.  $+(x, y) = x + y$ .

•  $\cdot: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ , i.e.  $\cdot(x, y) = x \cdot y$

• If  $\mathcal{M}_n(\mathbb{R})$  denotes the set of all  $n \times n$  matrices with real entries, then  $\cdot: \mathcal{M}_n(\mathbb{R}) \times \mathcal{M}_n(\mathbb{R}) \rightarrow \mathcal{M}_n(\mathbb{R})$  given matrix multiplication, i.e. if  $A$  and  $B$  are  $n \times n$  matrices, then  $AB$  is an  $n \times n$  matrix.

•  $\cdot: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  with

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

•  $\circ: X^X \times X^X \rightarrow X^X$ , i.e. for  $f, g: X \rightarrow X$ ,  $\circ(f, g) = f \circ g$ .

•  $\mathbb{Q}^+ = \mathbb{Q} \setminus \{0\}$ ,  $\div: \mathbb{Q}^+ \times \mathbb{Q}^+ \rightarrow \mathbb{Q}^+$  with  $\div(x, y) = \frac{x}{y}$ .

• Division is *not* a binary operation on  $\mathbb{N}$  because it is not always true that  $\frac{n}{m} \in \mathbb{N}$  whenever  $n, m \in \mathbb{N}$ .

## 6.1 Groups

**Definition 6.1.1** (Group). A group is a pair  $(G, *)$  where  $G$  is a nonempty set and  $*$  is a binary operation on  $G$  that satisfies the following properties:

- (i)  $*$  is associative, i.e.  $(x * y) * z = x * (y * z)$ .
- (ii) There exists an element  $e \in G$  with the property that for all  $x \in G$ ,  $e * x = x * e = x$ . This  $e$  is called the *identity element* of  $(G, *)$ .
- (iii) For all  $x \in G$ , there exists an element  $x' \in G$  such that  $x * x' = x' * x = e$ . This  $x'$  is called the *inverse* of  $x$ .

**Example 6.1.2.** Take  $(\mathbb{Z}, +)$ . This is a group because (i)  $+$  is associative, i.e. take  $x, y, z \in \mathbb{Z}$ , we have

$$(x + y) + z = x + (y + z)$$

(ii) there exists a  $0 \in \mathbb{Z}$  with the property that for all  $x \in \mathbb{Z}$ ,  $0 + x = x + 0 = x$ , and (iii) for all  $x \in \mathbb{Z}$ , there exists a  $-x \in \mathbb{Z}$  such that  $x + (-x) = (-x) + x = 0$ . Therefore,  $(\mathbb{Z}, +)$  is a group.

**Example 6.1.3.** Let  $W = \{0, 1, 2, \dots\}$ . Then  $(W, +)$  is not a group. It satisfies (i) and (ii) but not (iii). For example, for  $x = 3$ , there is no such element  $x' \in W$  such that  $x + x' = x' + x = 0$ .

**Example 6.1.4.** The following are examples of groups:

- $(\mathbb{Q}, +)$  is a group.
- $(\mathbb{R}, +)$  is a group.
- $(\mathbb{C}, +)$  is a group.
- If  $n \in \mathbb{N}$  and  $\mathcal{M}_n(\mathbb{R})$  is all  $n \times n$  matrices with real entries, then  $(\mathcal{M}_n(\mathbb{R}), +)$  is a group, i.e. if  $A = [a_{ij}]$  and  $B = [b_{ij}]$ , then  $A + B = [a_{ij} + b_{ij}]$ .

**Remark 6.1.5.** • Groups in which the binary operations is a common form of addition are called *additive groups*. This is an informal concept.

- In additive groups, the identity element is typically denoted by 0 and it is called the *zero element*.
- The inverse of  $x$  in an additive group is usually denoted by  $-x$  and it can be called the *additive inverse* of  $x$ .



**Example 6.1.6.** Let  $n \in \mathbb{N}$  and consider the set

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

and consider the binary operation  $+_n$  such that for all  $x, y, z \in \mathbb{Z}_n$ , then  $x +_n y$  is the unique  $r \in \{0, 1, \dots, n-1\}$  such that  $x + y \equiv r \pmod{n}$ . Then  $(\mathbb{Z}_n, +_n)$  is a group. That is,

- (i)  $+_n$  is associative
- (ii) 0 is the zero element (identity element).
- (iii) For all  $x \in \mathbb{Z}_n$ , there exists a  $-x \in \mathbb{Z}_n$  such that  $x +_n (-x) = 0$ , i.e.  $x + (-x) \equiv 0 \pmod{n}$ . (In particular, for  $x \in \{1, \dots, n-1\}$ ,  $-x = n - x$  for  $x = 0$ ,  $-x = 0$ .)

*Remark 6.1.7.* In all of the above examples, the binary operation is commutative, i.e.  $x + y = y + x$ .

**Definition 6.1.8.** A group  $(G, *)$  in which  $*$  is commutative is called an *abelian* group.

**Notation 6.1.9.** Whenever we use the term “additive group” it will be assumed that it is abelian ( $+$  is always commutative).

*Remark 6.1.10.* Not all groups are abelian.

Next let us have a look at some multiplicative groups.

**Example 6.1.11.** Let  $\mathbb{Q}^+ = \{q \in \mathbb{Q} : q \neq 0\}$ . Then  $(\mathbb{Q}^+, \cdot)$  is a group.

- (i) Multiplication is associative, i.e. for all  $x, y, z \in \mathbb{Q}^+$ , we have  $(xy)z = x(yz)$ .
- (ii) There exists a  $1 \in \mathbb{Q}^+$  such that for all  $x \in \mathbb{Q}^+$ ,  $1x = x1 = x$ .
- (iii) For all  $x \in \mathbb{Q}^+$ , there exists  $x^{-1} \in \mathbb{Q}^+$  such that  $xx^{-1} = x^{-1}x = 1$ , i.e.  $x^{-1}$  is the inverse of  $x$ .

*Remark 6.1.12.* Groups in which the binary operation is a common form of multiplication are called multiplicative groups (this is informal).

- In multiplicative groups, the identity element is commonly called a unit element (sometimes but not always denoted by 1).
- We usually suppress the  $\cdot$  symbol, i.e. we write  $xy$  instead of  $x \cdot y$ .

**Example 6.1.13.**    •  $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$  with  $\cdot$  is a multiplicative group.

- $\mathbb{Q}^- = \{x \in \mathbb{Q} : x < 0\}$  with  $\cdot$  is not a binary operation on  $\mathbb{Q}^-$ .
- Take  $\{-1, 1\}$  with usual multiplication. This is a multiplicative group. Indeed, firstly, multiplication is a binary operation on  $\{-1, 1\}$ .
  - (i) Multiplication is associative
  - (ii)  $1 \in \{-1, 1\}$  is the identity element
  - (iii) For all  $x \in \{-1, 1\}$ , there exists  $x^{-1}$  such that  $xx^{-1} = x^{-1}x = 1$ .  
In particular,  $1^{-1} = 1$  and  $(-1)^{-1} = -1$ .

## Lecture 7

September 20, 2023

Recall in the previous lecture, we introduced the concept of groups.

**Definition 7.0.1** (Group). A group is a pair  $(G, *)$  where  $G$  is a nonempty set and  $*$  is a binary operation on  $G$  that satisfies the following properties:

- (i)  $*$  is associative, i.e.  $(x * y) * z = x * (y * z)$ .
- (ii) There exists an element  $e \in G$  with the property that for all  $x \in G$ ,  $e * x = x * e = x$ . This  $e$  is called the *identity element* of  $(G, *)$ .
- (iii) For all  $x \in G$ , there exists an element  $x' \in G$  such that  $x * x' = x' * x = e$ . This  $x'$  is called the *inverse* of  $x$ .

**Notation 7.0.2.** Whenever we use the term “additive group” it will be assumed that it is abelian ( $+$  is always commutative).

*Remark 7.0.3.* Not all groups are abelian.

**Example 7.0.4.**  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathcal{M}_n(\mathbb{R}), +)$  and  $(\mathbb{Z}_n, +_n)$  are all examples of groups that we had a look at in the previous lecture.

**Notation 7.0.5.** Groups in which the operation is a common form of multiplication, are called *multiplicative groups*.

**Example 7.0.6.**  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{Q}^+, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$  and  $(\{-1, 1\}, \cdot)$  are examples of multiplicative groups.

*Remark 7.0.7.* Not all multiplicative groups are abelian.

**Example 7.0.8.** Recall  $\mathcal{M}_2(\mathbb{R})$  denotes the set of all  $2 \times 2$  matrices with real entries. Consider matrix multiplication on  $\mathcal{M}_2(\mathbb{R})$ . This is not a group (not all elements have an inverse). Define  $\text{GL}_2(\mathbb{R})$  to be the set of all  $2 \times 2$  invertible matrices with real entries. This is a group.

- (i) For all  $A, B, C \in \text{GL}_2(\mathbb{R})$ , we have that  $(AB)C = A(BC)$  from linear algebra.
- (ii) There exists a  $2 \times 2$  identity matrix  $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \text{GL}_2(\mathbb{R})$  such that for all  $A \in \text{GL}_2(\mathbb{R})$ ,  $I_2 A = A I_2 = A$ .
- (iii) For all  $A \in \text{GL}_2(\mathbb{R})$ , there exists  $A^{-1} \in \text{GL}_2(\mathbb{R})$  such that  $AA^{-1} = A^{-1}A = I_2$ .

This multiplicative group is not abelian. Take  $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ , then these are in  $\text{GL}_2(\mathbb{R})$  but  $AB \neq BA$ .

**Example 7.0.9.** Let  $X$  be a nonempty set. Recall  $X^X$  denotes the set of all functions  $f : X \rightarrow X$ . Then  $\circ$  is a binary operation on  $X^X$ , which is associative. Also  $\text{id} : X \rightarrow X$  is an identity element for  $X^X$ . Unless  $|X| = 1$ ,  $X^X$  is not a group. Define

$$\text{Perm}(X) = \{f : X \rightarrow X, f \text{ is a bijection}\}$$

(which is called the permutation group of  $X$ ). Note that this may not be the standard notation.  $\text{Perm}(X)$  with  $\circ$  is a group.

**Proposition 7.0.10.** *If  $|X| \geq 3$ , then  $\text{Perm}(X)$  is not abelian.*

*Proof.* For exposition, assume  $|X| = 3$ , i.e.  $X = \{a, b, c\}$ . Take  $f, g : X \rightarrow X$  with

$$\begin{aligned} f(a) &= b & g(a) &= a \\ f(b) &= a & g(b) &= c \\ f(c) &= c & g(c) &= b \end{aligned}$$

Then  $(f \circ g)(a) = f(g(a)) = f(a) = b$  and  $(g \circ f)(a) = g(f(a)) = g(b) = c$ . So  $f \circ g \neq g \circ f$ .  $\square$

**Exercise.** Let  $|X| = n$ . Then  $|X^X| = n^n$  and  $|\text{Perm}(X)| = n!$ .

**Notation 7.0.11.** Henceforth, we avoid the  $*$  notation. For general groups we will use the multiplicative group notation. We will write:

*Let  $G$  be a group. Then  $G$  satisfies*

- (i) *For all  $x, y, z \in G$ ,  $(xy)z = x(yz)$*

- (ii) There exists a  $e \in G$  such that for all  $x \in G$ ,  $ex = xe = x$ .  
 (iii) For all  $x \in G$ , there exists a  $x^{-1} \in G$  such that  $xx^{-1} = x^{-1}x = e$ .

**Proposition 7.0.12.** *Let  $G$  be a group.*

- (i) Let  $a, b, c \in G$ .  
 (a) If  $ab = ac$ , then  $b = c$  (left cancellation law).  
 (b) If  $ba = ca$ , then  $b = c$  (right cancellation law).  
 (ii) The identity element is unique, i.e. if  $e' \in G$  such that for all  $x \in G$ ,  $e'x = xe' = x$ , then  $e = e'$ .  
 (iii) The inverse of  $x \in G$  is unique, i.e. if  $y \in G$  is such that  $xy = yx = e$ , then  $y = x^{-1}$ .  
 (iv) For all  $x, y \in G$ ,  $(xy)^{-1} = y^{-1}x^{-1}$ .

*Proof.* (ia) Assume that  $ab = ac$ . Multiply by  $a^{-1}$  on the left

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c && \text{(Associativity)} \\ eb &= ec \\ b &= c \end{aligned}$$

The proof for (ib) is similar.

(ii) Assume that  $e'$  has the above property. Apply it for  $x = e$ , so that  $e'e = ee' = e$ . Take the defining property of  $e$  and take  $x = e'$ . Then  $ee' = e'e = e'$ , so

$$\begin{cases} ee' = e \\ ee' = e' \end{cases} \Rightarrow e = e'$$

(iii) Assume that  $y$  has the above property, i.e.  $yx = xy = e$ . Then

$$\begin{cases} yx = xy = e \\ x^{-1}x = xx^{-1} = e \end{cases} \Rightarrow yx = x^{-1}x$$

and by the right cancellation law,  $y = x^{-1}$ . □

**Definition 7.0.13.** • A group with only one element is called a trivial group.

- A group  $G$  with finitely many elements is called a finite group and  $|G|$  is called the *order of  $G$* .
- If  $G$  is infinite, we say it has infinite order.

**Example 7.0.14.** •  $(\{1\}, \cdot)$  and  $(\{0\}, +)$  are trivial groups.

- $(\{1, -1\}, \cdot)$  has order 2.
- $(\mathbb{Z}_n, +_n)$  has order  $n$ .
- $(\mathbb{Q}^+, \cdot)$  and  $(\mathbb{Z}, +)$  are infinite groups.

## 7.1 Cayley Tables of Finite Groups

For a group of order  $n$ ,  $G = \{x_1, x_2, \dots, x_n\}$ , its Cayley table is an  $n \times n$  table where the  $(i, j)$  entry is  $x_i x_j$ . Typically,  $x_1 = e$ .

**Example 7.1.1.** Consider  $\{1, -1, i, -i\} \subseteq \mathbb{C}$  with multiplication, this is a group.

		C1	C2	C3	C4
		1	-1	$i$	$-i$
R1	1	1	-1	$i$	$-i$
R2	-1	-1	1	$-i$	$i$
R3	$i$	$i$	$-i$	-1	1
R4	$-i$	$-i$	$i$	1	-1

# Lecture 8

## September 22, 2023

### 8.1 Cayley Tables of Finite Groups

Recall in the previous lecture we have briefly introduced the Cayley table of finite groups.

**Definition 8.1.1.** If  $G = \{x_1, x_2, \dots, x_n\}$  is a group of order  $n$ , the Cayley table of  $G$  is an  $n \times n$  table where the  $(i, j)$  entry contains  $x_i x_j$ . Typically,  $x_1 = e$ .

**Example 8.1.2.** Consider  $\{1, -1, i, -i\} \subseteq \mathbb{C}$  with multiplication, this is a group.

		C1	C2	C3	C4
		1	-1	$i$	$-i$
R1	1	1	-1	$i$	$-i$
R2	-1	-1	1	$-i$	$i$
R3	$i$	$i$	$-i$	-1	1
R4	$-i$	$-i$	$i$	1	-1

**Proposition 8.1.3.** Let  $G$  be a group of order  $n \in \mathbb{N}$ .

- (i) Every row of the Cayley table of  $G$  contains every member of  $G$  exactly once.
- (ii) Every column of the Cayley table of  $G$  contains every member of  $G$  exactly once.
- (iii)  $G$  is commutative if and only if the Cayley table is symmetric, i.e. the  $(i, j)$  and  $(j, i)$  entries coincide.

*Proof.* (i) Fix a row  $i$ . Take  $1 \leq j_1 \leq j_2 \leq n$ . Assume the entries  $(i, j_1)$  and  $(i, j_2)$  are different. Assume not, i.e.  $x_i x_{j_1} = x_i x_{j_2}$ . By the left cancellation law,  $x_{j_1} = x_{j_2}$ . This is absurd (since  $G = \{x_1, x_2, \dots, x_n\}$  with  $|G| = n$  because there are  $n$  distinct members of  $G$  in the  $i$ th row and  $|G|$ — all must appear in the  $i$ th row). The proof for (ii) is similar, and (iii) is by definition.  $\square$

**Exercise.** Let  $G = \{e, a\}$ . How many different binary operations  $*$  can be defined on  $G$  such that  $(G, *)$  is a group with identity  $e$ ?

**Solution.** We try to draw the Cayley tables

		C1	C2
		$e$	$a$
R1	$e$	$e$	$a$
R2	$a$	$a$	$e$

The  $(2, 2)$  entry must be  $e$  for everything to appear once in each row and each column. Check that this indeed defines a group. There is exactly one such binary operation.

**Exercise.** Let  $G = \{e, a, b\}$ . How many binary operations can make  $G$  a group with identity  $e$ ?

**Solution.** Consider the following Cayley table.

		C1	C2	C3
		$e$	$a$	$b$
R1	$e$	$e$	$a$	$b$
R2	$a$	$a$	$e$	$b$
R3	$b$	$b$		

In this table, the  $(2, 3)$  and  $(2, 4)$  entries must be  $e$  and  $b$ , in some order.  $e$  then is not valid because then the third column has two  $b$ 's.

		C1	C2	C3
		$e$	$a$	$b$
R1	$e$	$e$	$a$	$b$
R2	$a$	$a$	$b$	$e$
R3	$b$	$b$	$e$	$a$

This is a group operation (check this). The conclusion is that, there is only one operation that can complete this. Furthermore, note that this group  $G$  is abelian.



**Exercise.** Let  $G = \{e, a, b, c\}$ . How many binary operations make this a group with identity  $e$ ? (There are 4, and they are all abelian)

*Remark 8.1.4.* In some sense, some of these four “the sense”. In reality, there are only 2.

## 8.2 Some Group Notations

Let  $G$  be a group and  $x_1, x_2, \dots, x_n \in G$ . Define

$$\prod_{i=1}^n x_i = x_1 x_2 \cdots x_n$$

Formally, this is defined by induction on  $n$ . For example,

$$\prod_{i=1}^1 x_i = x_1$$

and if  $\prod_{i=1}^k x_i$  has been defined, then

$$\prod_{i=1}^{k+1} x_i = \left( \prod_{i=1}^k x_i \right) x_{k+1}$$

*Remark 8.2.1.* If  $k \leq \ell \in \mathbb{N}$  and  $x_k, x_{k+1}, \dots, x_\ell \in G$ , we similarly define

$$\prod_{i=k}^{\ell} x_i = x_k x_{k+1} \cdots x_\ell$$

**Exercise.** Let  $G$  be a group and let  $x_1, x_2, \dots, x_n \in G$ , where  $n \in \mathbb{N}$  and  $1 \leq k \leq n$ . Then

$$\prod_{i=1}^n x_i = \left( \prod_{i=1}^k x_i \right) \left( \prod_{i=1}^n x_i \right)$$

Hint: Keep  $k$  fixed and use induction on  $n = k + 1, k + 2, \dots$

**Example 8.2.2.** Consider  $G = \{x_1, x_2, x_3, x_4\}$ . Then observe that

$$\begin{aligned} \prod_{i=1}^4 x_i &= x_1 x_2 x_3 x_4 \\ &= (x_1 x_2)(x_3 x_4) \\ &= x_1(x_2 x_3 x_4) \\ &= x_1((x_2 x_3)x_4) \end{aligned}$$

*Remark 8.2.3.* Note that the order of  $x_1, x_2, \dots, x_n$  matters, unless  $G$  is abelian.

**Exercise.** Let  $G$  be a group and let  $x_1, x_2, \dots, x_n \in G$ . Then

$$\left( \prod_{i=1}^n x_i \right)^{-1} = \prod_{i=1}^n y_i = \prod_{i=1}^n x_{n-i+1}^{-1}$$

where  $y_1 = x_n^{-1}$ ,  $y_2 = x_{n-1}^{-1}, \dots, y_n = x_1^{-1}$ .

**Notation 8.2.4.** Let  $G$  be a group and let  $x \in G$ .

- For  $n \in \mathbb{N}$ , define  $x^n = x \cdots x = \prod_{i=1}^n x$ .
- Define  $x^0 = e$
- For  $n \in \mathbb{N}$ , define  $x^{-n} = (x^n)^{-1}$ .

**Proposition 8.2.5.** Let  $G$  be a group.

- (i) For all  $x \in G$  and  $n \in \mathbb{Z}$ ,  $(x^{-1})^n = x^{-n}$
- (ii) For all  $x \in G$  and  $m, n \in \mathbb{Z}$ ,  $x^{n+m} = x^n x^m$ .
- (iii) For all  $x \in G$  and  $m, n \in \mathbb{Z}$ ,  $(x^m)^n = x^{mn}$ .

*Proof.* (i) Take the case  $n > 0$ . Then

$$x^{-n} = (x^n)^{-1} = \left( \prod_{i=1}^n x \right)^{-1} = \prod_{i=1}^n y_i = \prod_{i=1}^n x^{-1} = (x^{-1})^n$$

(ii) If  $n, m \geq 0$ , then this is easy (also if  $n, m \leq 0$ ). Consider the case when  $n > 0$  and  $m < 0$ . Then

$$x^n = \prod_{i=1}^n x$$

and if  $m = -k$  for some  $k > 0$ , then

$$x^m = \prod_{i=1}^k x^{-1}$$

Question: What is  $\left( \prod_{i=1}^n x \right) \left( \prod_{i=1}^k x^{-1} \right)$ ? Take further cases

Case 1: If  $n < k$ , then  $\left( \prod_{i=1}^n x \right) \left( \prod_{i=1}^k x^{-1} \right) = (x^{-1})^{k-n} = x^{n-k} = x^{n+m}$ .

Case 2: Similar for  $n \geq k$ .

(iii) Exercise. □

*Remark 8.2.6.* In additive groups  $(G, +)$ ,  $\prod$  becomes  $\sum$  and  $n$  in the exponent becomes  $n$  as a coefficient.

- We define  $\sum_{i=1}^n x_i = x_1 + x_2 + \cdots + x_n$ .
- Define  $nx = \sum_{i=1}^n x$
- Then
  - For all  $x \in G$ ,  $n \in \mathbb{Z}$ ,  $-(nx) = (-n)x$
  - For all  $x, y \in G$  and  $m, n \in \mathbb{Z}$ ,  $(n + m)x = nx + mx$
  - For all  $x, y \in G$  and  $m, n \in \mathbb{Z}$ ,  $n(mx) = (nm)x$ .

### 8.3 Subgroups

**Definition 8.3.1.** Let  $G$  be a group. A subset  $H$  of  $G$  is called a *subgroup* of  $G$  if it satisfies the following:

- (i)  $e \in H$
- (ii) For all  $x \in H$ ,  $x^{-1} \in H$ .
- (iii) For all  $x, y \in H$ ,  $xy \in H$ .

We then write  $H \leq G$ .

**Example 8.3.2.** • If  $G$  is a group, then  $G \leq G$ , which is called the *improper subgroup*.

- If  $G$  is a group, then  $H = \{e\}$  is the *trivial subgroup* of  $G$ .
- $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$ .
- $(\mathbb{Q}^+, \cdot) \leq (\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^+, \cdot)$
- $(\{-1, 1\}, \cdot) \leq (\{1, -1, i, -i\}, \cdot)$

*Remark 8.3.3.* A subgroup of a group is itself, a group.



## Lecture 9

September 25, 2023