

Devansh Tripathi  
Lecturer:

August 5, 2024

---

## Lecture 1: Theory of Groups and Rings

**Definition 1.** *Fibre of  $f$  over  $b$ :* For a function  $f : A \rightarrow B$ , the pre-image of  $b \in B$  is called the fibre of  $f$  over  $b$ .

**Definition 2.** *Equivalence class of  $a \in A$  is defined to be  $\{x \mid xRa\}$ . The elements of equivalence class of  $a \in A$  are said to be equivalent to  $a$  and any element of this class is called the representative of this class. They are denoted by  $[a]$ .*

**Lemma 1.** *Any two equivalence classes are either disjoint or equal.*

*Proof.* Suppose, we have two equivalence classes  $[a]$  and  $[b]$  such that  $[a] \neq [b]$ . We need to prove that  $[a] \cap [b] = \phi$ . Suppose for contradiction that  $\exists x$  such that  $x \in [a] \cap [b]$ . This means that  $xRa$  and  $xRb$ . Using symmetry of equivalence relation, we have  $aRx$  and  $xRb$  and by transitivity we can say  $aRb$ . Hence,  $[a] = [b]$  which is a contradiction.

We have proved that if they are not equal then they are disjoint. Other way can be proved with similar argument.  $\square$

**Definition 3.** *Partition of  $A$ :* A partition of  $A$  is any collection  $\{A_i \mid i \in I\}$  of non-empty subsets of  $A$  such that it follows:

1.  $\bigcup_{i \in I} A_i = A$ , and
2.  $A_i \cap A_j = \phi \quad \forall i, j \in I \text{ and } i \neq j$ .

**Remark.** *The notion of an equivalence relation on  $A$  and a partition of  $A$  are the same.*

For a set  $A$ , every equivalence relation on  $A$  induces the partition on set  $A$  using equivalence classes. In other words, every equivalence class associated with an equivalence relation forms a partition of  $A$ .

If  $R$  is the equivalence relation on  $A$  then the induced partition  $P$  will be

$$P = \{\{b \mid bRa, \forall b \in A\} \mid a \in A\}$$

Also, with the given partition  $P$ , we can define relation  $R$  as

$$R = \{bRa \mid \exists p_i \in P \text{ such that } a, b \in p_i \quad \forall i \in I\}$$

We can say a partition  $P$  is made up of equivalence classes  $p_i$ .

**Proposition 1.** *Let  $A$  be a nonempty set.*

1. *If  $R$  defines an equivalence relation on  $A$  then the set of equivalence classes of  $R$  forms a partition of  $A$ .*
2. *If  $\{A_i \mid i \in I\}$  is a partition of  $A$  then there is an equivalence relation on  $A$  whose equivalence classes are sets  $A_i, i \in I$ .*

---

*Proof.* 1. Suppose  $P$  is a set of equivalence classes of  $R$ , defined as

$$P = \{\{b \mid bRa, b \in A\} \mid a \in A\}$$

We need to prove that  $P$  defines partition of  $A$ . For some  $p_i \in P$ , it will be nonempty since it will have atleast  $a$  which is related to itself. Now, using lemma 1, we can say that  $p_i \cap p_j = \phi$  for some  $p_i, p_j \in P$  and  $i, j \in \mathbb{N}$  given that  $i \neq j$ .

Also, we know that every point of set  $A$  will be in some equivalence class (reflexivity so atleast in the equivalence of itself). If we take union of all those classes we will get  $A$  as each point has a atleast a equivalence class.

2. Given the collection of sets,  $Q = \{A_i \mid i \in I\}$  as a partition of  $A$ , we need to show that there exists an equivalence relation on  $A$  with equivalence classes as sets  $A_i, i \in I$ .

We can define relation  $R$  as

$$R = \{(a, b) \mid bRa \text{ and } \exists A_i \in Q \text{ such that } a, b \in A_i\}$$

It is reflexive (obvious), symmetric (obvious) and transitive ( $aRb$  such that  $a, b \in A_i$  and  $bRc$  such that  $b, c \in A_i \implies aRc$  such that  $a, c \in A_i$ ). Hence, it is a equivalence relation and the corresponding equivalence class for some  $i$  will be

$$q_i = \{b \mid bRa_i, \forall b \in A \text{ \& } a_i \in A\}$$

Since with the same arguments given in proof of part (1) that  $q_i, i \in I$  is nonempty, disjoint and exhausts the set  $A$ , we can say it forms the partition of  $A$  and since every equivalence relation induces a unique partition, we can also say that  $q_i, i \in I$  are precisely the sets  $A_i, i \in I$ . □

## Properties of Integers

**Property 1.** *Well Ordering of  $\mathbb{Z}$ : If  $A$  is any nonempty subset of  $\mathbb{Z}^+$ , there is some element  $m \in A$  such that  $m \leq a, \forall a \in A$ .  $m$  is called the minimum element of  $A$ .*

*Proof.* Proof for well ordering property of  $\mathbb{Z}$  i.e. existence and uniqueness of minimal element.

For a nonempty subset  $A$  of  $\mathbb{Z}^+$ , we can prove this by induction. Suppose  $A = \{a_1\}$  then  $a_1 \leq a_1$  hence  $a_1$  is the minimal element. Suppose there exists a minimal element  $m$  in the set  $A$  have  $n$  element  $a_1, a_2, \dots a_n$ .

For the case when  $A = \{a_1, a_2, \dots a_{n+1}\}$ , we already have  $m$  as the minimal element for  $\{a_1, a_2, \dots a_n\}$  hence there are three cases: if  $a_{n+1} = m$ ,  $a_{n+1} > m$  and  $a_{n+1} < m$  and in all three cases there exists a minimal element in set  $A$ .

For uniqueness of minimal element, suppose for contradiction there exists two minimal elements in set  $A$ , say  $m_1, m_2$  such that  $m_1 \neq m_2$ . Then there are two possibilities  $m_1 > m_2$  and  $m_1 < m_2$ . If  $m_1 > m_2$  then assume  $m_1$  to be the minimal element hence this case is not possible. Similarly,  $m_1 < m_2$  is also not possible assuming  $m_2$  be the minimal element. Hence, contradiction. Therefore,  $m_1 = m_2$ . □

**Definition 4.**  $a|b = a$  divides  $b$ .  $b = ac$  for some  $c \in \mathbb{Z}$ .

---

**Definition 5.** For some  $a, b \in \mathbb{Z}$ , denote  $d = \gcd(a, b)$  and  $l = \text{lcm}(a, b)$  then  $dl = ab$ .

**Definition 6.** The Division Algorithm: If  $a, b \in \mathbb{Z} \setminus \{0\}$ , then there exists a unique  $q, r \in \mathbb{Z}$  such that  $a = bq + r$  where  $0 \leq r \leq |b|$ . And  $q$  is called quotient and  $r$  is called remainder.

**Definition 7.** The Euclidean Algorithm: Suppose  $a, b \in \mathbb{Z} \setminus \{0\}$ , we can use this algorithm to find the gcd of these two number in the following way:

$$\begin{aligned} a &= q_0b + r_0 \\ b &= q_1r_0 + r_1 \\ r_0 &= q_2r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_{n+1}r_{n-1} + r_n \\ r_{n-1} &= q_{n+2}r_n \end{aligned}$$

where  $r_n$  is the gcd of  $(a, b)$ . Such an  $r_n$  exists because  $|b| > |r_0| > |r_1| \dots$  is a decreasing sequence of strictly positive integers hence it cannot go on to infinite elements.

$\mathbb{Z}$ -linear combination of  $a$  and  $b$ : For  $a, b \in \mathbb{Z} \setminus \{0\}$ , we have  $x, y \in \mathbb{Z}$  such that we can write  $\gcd(a, b)$  as linear combination of  $x, y$

$$\gcd(a, b) = ax + by$$

.

**Theorem 1.** Fundamental Theorem of Arithmetic: If  $n \in \mathbb{Z}$ ,  $n > 1$ , then  $n$  can be factored uniquely into the product of primes, i.e. there are distinct primes  $p_1, p_2, \dots, p_s$  and positive integers  $\alpha_1, \alpha_2, \dots, \alpha_s$ , such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

This factorization is unique in the sense that the set of  $p_i$ 's is unique and no other set of primes and the exponent can generate the same number.

*Proof.* We will use induction to prove the first part that every  $n > 1$  can be written as the product of primes.

For  $n = 2$  it is true as  $2 = 2^1$ . Suppose for all the numbers less than  $n$  can be written as the product of primes. Now, for  $n$  we can have two cases:

**Case: 1** If  $n$  is prime then it is obvious that it's true.

**Case: 2** If  $n$  is composite then  $n$  can be written as  $n = ab$  where  $0 < a, b < n$  by definition of composite numbers. And by our assumption for induction it is true that  $a, b$  can be written as product of primes as they are less than  $n$ . Hence,  $n = ab$  can also be a product of primes.

Now, about the uniqueness of the primes factors. Let's assume that there exists some primes  $q'_i$ s and the exponents  $\beta'_i$ s such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

Since  $p_1$  divides the left side, it should also divide the right side. Hence,  $p_1 | q_i$  for some  $i$ . But  $p_1$  and  $q_i$  are primes  $\implies p_1 = q_i$ . WLOG, we can choose  $i = 1 \implies p_1 = q_1$ .

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = p_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

Now, we can have  $\alpha_1 > \beta_1$  and we can cancel  $p_1^{\beta_1}$  from both sides.

$$p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = q_2^{\beta_2} \dots q_s^{\beta_s}$$

But observe that now  $p_1$  divides left side but not the right side. Hence  $\alpha_1 \not> \beta_1$ . Similar argument for  $\alpha_1 < \beta_1$ . Therefore,  $\alpha_1 = \beta_1$ .

Using induction we can show that both sides are equivalent. Hence, primes and their coefficients are unique.  $\square$

We can also define lcm and gcd using fundamental theorem of arithmetic as:

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots$$

$$\text{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots$$

**Definition 8.** Euler  $\phi$ - function: For  $n \in \mathbb{Z}^+$  let  $\phi(n)$  be the number of positive integers  $a \leq n$  with  $(a, n) = 1$ . For primes  $p$ ,  $\phi(p) = p - 1$ , and more generally,  $\forall a \geq 1$  we have

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$$

The function  $\phi$  is multiplicative in the sense that  $\phi(ab) = \phi(a)\phi(b)$  if  $(a, b) = 1$ . So for some  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$  we can write

$$\begin{aligned} \phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}) = \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \dots \phi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1} (p_1 - 1) p_2^{\alpha_2 - 1} (p_2 - 1) \dots p_s^{\alpha_s - 1} (p_s - 1) \end{aligned}$$

**Theorem 2.** If  $n$  is composite then there are integers  $a$  and  $b$  such that  $n | ab$  but  $n \nmid a$  or  $n \nmid b$ .

*Proof.* Since  $n$  is composite then  $n = x_1^{n_1} x_2^{n_2} \dots y_1^{n'_1} y_2^{n'_2} \dots$  where  $x, y$  are primes  $\in (0, n)$  and  $n'_i \geq 1 \forall i \in \mathbb{N}$ . We have to prove the existence of the integers  $a, b$  such that  $n | ab$  but  $n \nmid a$  or  $n \nmid b$ .

We can construct such integers given the prime factorization of  $n$ . If we define  $a = x_1^{n_1} x_2^{n_2} \dots$  and  $b = y_1^{n'_1} y_2^{n'_2} \dots$  then we have satisfied the needed conditions.  $\square$

**Theorem 3.** If  $p$  is a prime then  $\sqrt{p}$  is not a rational number.

*Proof.* Suppose for contradiction,  $\sqrt{p}$  is a rational number. Then there exist  $x, y$  such that  $\sqrt{p} = \frac{x}{y}$  and  $(x, y) = 1$ . Then  $p = (\frac{x}{y})^2$  but  $p$  is a prime hence the only factorization it has is  $p = p \times 1$  and factorization is unique by fundamental theorem of arithmetic. Hence contradiction,  $\sqrt{p}$  is an irrational number.  $\square$

---

**Ques.** If  $p$  is a prime then prove that there do not exist nonzero integers  $a$  and  $b$  such that  $a^2 = pb^2$ .

**Ans.** If  $a^2 = pb^2$  then  $a = \pm\sqrt{p}b$  and using theorem 3, we can say  $\sqrt{p}$  is an irrational number and the product of an irrational and an integer can never be an integer. Hence, there does not exist nonzero  $a, b \in \mathbb{Z}$  such that  $a^2 = pb^2$ .

---

## Lecture 2

**$\mathbb{Z}/n\mathbb{Z}$  : Integers modulo  $n$**  Let  $n$  be a fixed positive integer. Define a relation  $R$  on  $\mathbb{Z}$  as

$$aRb \text{ iff } n \mid (b - a)$$

$R$  is the equivalence relation as can be verified. We call  $a \equiv b \pmod{n}$ , (read as:  $a$  is congruent to  $b \pmod{n}$ ) if  $aRb$ .

The equivalence class of  $a$  is denoted by  $\bar{a}$  and called *congruent class or residue class of  $a \pmod{n}$* .

$$\begin{aligned} n \mid (b - a) &\implies b - a = nk \text{ for some } k \in \mathbb{Z} \\ &\implies b = a + kn \text{ and } b \in \bar{a} \end{aligned}$$

For example:  $\bar{0}$  = perfectly divisible by  $n$ . These residue classes partitions the  $\mathbb{Z}$ . The set of all these equivalence classes under this equivalence relation will be denoted by  $\mathbb{Z}/n\mathbb{Z}$ , called *integers modulo  $n$*  or *integer mod  $n$* .

The process of finding the equivalence class  $\pmod{n}$  of some integer  $a$  is referred to as *reducing  $a \pmod{n}$* .

Addition and multiplication for elements of  $\mathbb{Z}/n\mathbb{Z}$ :

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{and} \quad \bar{a} \cdot \bar{b} = \overline{ab}$$

This means that we can take any *representative* element from class  $\bar{a}$  and any *representative* element from class  $\bar{b}$  and then do usual addition (or multiplication) then find the class in which the result lies.

**For example:** If we take  $\mathbb{Z}/2\mathbb{Z}$ , then we have two classes  $\bar{0}, \bar{1}$  (it's 0 to  $n - 1$ ,  $n = 2$  here) then we can take 4 and 7 from  $\bar{0}$  and  $\bar{1}$  respectively.  $4 + 7 = 11$  and 11 lies in  $\bar{1}$  class hence  $\bar{0} + \bar{1} = \overline{4 + 7} = \bar{1}$ .

The result is well defined and does not depend upon the choice of representatives as shown by the theorem below.

**Theorem 4.** *The operation of addition and multiplication on  $\mathbb{Z}/n\mathbb{Z}$  defined above are well defined i.e. they do not depend on the choice of representative for the classes involved. More precisely, if  $a_1, a_2 \in \mathbb{Z}$  and  $b_1, b_2 \in \mathbb{Z}$  with  $\bar{a}_1 = \bar{b}_1$  and  $\bar{a}_2 = \bar{b}_2$ , then  $\overline{a_1 + a_2} = \overline{b_1 + b_2}$  and  $\overline{a_1 a_2} = \overline{b_1 b_2}$ , i.e. if*

$$a_1 \equiv b_1 \pmod{n} \quad \text{and} \quad a_2 \equiv b_2 \pmod{n}$$

then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n} \quad \text{and} \quad a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

---

*Proof.* Since  $a_1 \equiv b_1 \pmod{n}$  that means  $n \mid b_1 - a_1$  and  $b_1 = a_1 + nt$ . Similarly, for  $a_2$ , we have  $b_2 = a_2 + ns$ . On adding the equations, we get  $b_1 + b_2 = a_1 + a_2 + n(t + s)$  and  $b_1 b_2 = n(nst + a_1 t + a_2 s) + a_1 a_2$ . Hence,  $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$  and  $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ .  $\square$

**Definition 9.** A subset residue classes of  $\mathbb{Z}/n\mathbb{Z}$  with multiplicative inverse lies in  $\mathbb{Z}/n\mathbb{Z}$  itself:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = 1\}$$

**Proposition 2.** Any representative of  $\bar{a}$  is coprime to  $n$ .

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

If  $a$  is integer which is coprime to  $n$  then we can write  $ax + ny = 1$  using Euclidean algorithm for some  $x, y \in \mathbb{Z} \implies 1 - ax = ny$  that means  $ax = 1 \pmod{n} \implies \bar{a}\bar{x} = \bar{1}$  hence  $\bar{x}$  is the multiplicative inverse of  $\bar{a}$ . Efficient way of calculating multiplicative inverse.

**Ques.** Prove that the distinct equivalence classes in  $\mathbb{Z}/n\mathbb{Z}$  are precisely  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ .

**Ans.** Division algorithm says that for  $a, b \in \mathbb{Z} \setminus \{0\}$ , we have unique  $q, r \in \mathbb{Z} \setminus \{0\}$  such that  $b = aq + r$  where  $0 \leq r < |a|$ . Hence,  $r$  can only be  $0, 1, 2, \dots, n-1$  which corresponds to equivalence classes.