Devansh Tripathi
Lecturer: Dr. Saiket Chatterjee

August 17, 2024

Lecture 1: Theory of Groups and Rings

Definition 1. *Fibre of f over b: For a function $f : A \to B$, 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 $x = [a] \cap [b]$. 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 prove 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. *$A_i \bigcap A_j = \phi \quad \forall i, j \in I$ 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 a equivalence relation forms 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

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

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 a 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

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

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 $A_i, i \in I$.

$\square$

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 $a_1, a_2, \ldots a_n$.
For the case when $A = \{a_1, a_2, \ldots a_{n+1}\}$, we already have m as the minimal element for $\{a_1, a_2, \ldots a_n\}$ 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, $m_1 = m_2$. $\square$

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 $d = gdc(a,b)$ and $l = lcm(a,b)$ then $dl = ab$.*

Definition 6. *The Division Algorithm: If $a, b \in \mathbb{Z} \backslash \{0\}$, 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 $a, b \in \mathbb{Z} \backslash \{0\}$, we can use this algorithm to find the gcd of these two number in the following way:*

$$a = q_0 b + r_0$$
$$b = q_1 r_0 + r_1$$
$$r_0 = q_2 r_1 + r_2$$
$$\vdots$$
$$r_{n-2} = q_{n+1} r_{n-1} + r_n$$
$$r_{n-1} = q_{n+2} r_n$$

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

$\mathbb{Z}$-linear combination of a and b: For $a, b \in \mathbb{Z} \backslash \{0\}$, 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 $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$, such that*

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

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 thatn 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 divides 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. $\qquad\square$

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

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

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

The function ϕ 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

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

Theorem 2. *If n is composite then there are integers a and b such that $n \mid ab$ 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 $n_i's \ge 1 \,\forall i \in \mathbb{N}$. We have to prove the existence of the integers a, b such that $n \mid ab$ but $n \nmid a$ or $n \nmid b$.
We can constuct 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. $\qquad\square$

Theorem 3. *If p is a prime then $\sqrt{p}$ is not an 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. $\qquad\square$

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 postive 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 mod n) if aRb.
The equivalence class of a is denoted by $\bar{a}$ and called *congruent class or residue class of a* mod n.

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

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 mod n of some integer a is refered to as *reducing a* mod n.

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

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

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 classess 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 $\bar{b}_1 = \bar{b}_2$, them $\overline{a_1 + a_1} = \overline{b_1 + b_2}$ and $\overline{a_1 a_1} = \overline{b_1 b_2}$, i.e. if*

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

then

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

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 $a_1 a_2 \equiv b_1 b_2 \pmod{n}$. $\qquad\square$

Definition 9. *A subset residue classes of $\mathbb{Z}/n\mathbb{Z}$ with multiplicative inverse lies in $\mathbb{Z}/n\mathbb{Z}$ itself:*
$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a}.\bar{c} = 1\}$$

Proposition 2. *Any representative $\bar{a}$ 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 $ax = 1 \pmod{n} \implies \overline{ax} = \bar{1}$ 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 $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

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

Theorem 5. *If $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a}.\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. Since, $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, there exists $\bar{a}'$ and $\bar{b}'$ such that $\bar{a}.\bar{a}' = \bar{1}$ and $\bar{b}.\bar{b}' = \bar{1}$. If we multiply both the equations then $\bar{a}.\bar{a}'.\bar{b}.\bar{b}' = \bar{1}$, Assume $\bar{a}.\bar{b} = \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ then we get $\bar{c}.\bar{a}'.\bar{b}' = \bar{1}$. Hence, there exist $\bar{c}' = \bar{a}'.\bar{b}'$ such that $\bar{c}.\bar{c}' = \bar{1}$. Therefore $\bar{a}.\bar{b} \in \mathbb{Z}/\mathbb{Z}$. $\qquad\square$

Lecture 3

Definition 10. *Binary operation: A binary operation $*$ on a set G is a function $* : G \times G \to G$. For any $a, b \in G$, we can write $a * b$ for $*(a, b)$.*

If $*$ is an binary operation on G and H is a subset of G. If restriction of $*$ on H is a binary operation on H i.e. $a, b \in H \implies a * b \in H$ then H is closed under $*$.

If $*$ is associative (or commutative) on G then it will be associative (or commutative) on H also.

Definition 11. *Group: A group is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying following axioms. G should be closed under the binary operation.*

1. *$(a * b) * c = a * (b * c), \forall a, b, c \in G$ i.e. $*$ is associative.*

2. *There exists an element e in G, called identity of G, such that for all $a \in G$ we have $a * e = e * a = a$.*

3. *for each $a \in G$ there is an element a^{-1} of G, called an inverse of a, such that $a * a^{-1} = a^{-1} * a = e$.*

The group G is called an abelian (or communtative) if $a * b = b * a$ for all $a, b \in G$. G is called finite group if it is a finite set.

Example:

1. $(V, +)$ where V is a vector space and $+$ is vector addition, is an additive group since operation defined is $+$. It is abelian group since $+$ is commutative.

2. For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is a group under operation $+$ with $\bar{0}$ as identity and for $\bar{a}$ inverse is $\overline{-a}$, such that $\bar{a} + \overline{-a} = \bar{0}$. And we can prove that $+$ is an associative operation.

3. For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes $\bar{a}$ which have multiplicative inverses $\pmod{n}$ is an abelian group under multiplication of residue classes. We assume here that multiplication is well defined and associative. (We can prove that). Identity will be $\bar{1}$ and by the definition of $(\mathbb{Z}/n\mathbb{Z})^\times$ inverse exists in the set itself.

Definition 12. *Direct Product: If $(A, *)$ and $(B, @)$ are two groups, then $A \times B$ is called direct product, whose elements are those in the Cartesian product*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

and whose operations are defined component-wise

$$(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 @ b_2)$$

The new set $A \times B$ will also be a group.

It can be prove easily as A and B both contains the inverse and identity element.

Proposition 3. *If G is a group under the operation $*$, then*

1. *the identity element of G is unique.*

2. *for each $a \in G$, a^{-1} is uniquely determined.*

3. *$(a^{-1})^{-1} = a$ for all $a \in G$.*

4. *$(a * b)^{-1} = (b^{-1}) * (a^{-1})$*

5. *for any $a_1, a_2. \ldots a_n \in G$ the value of $a_1 * a_2. \cdots * a_n \in G$ is independent of how the expression is bracketed (generalised associativity).*

Proof. 1. Suppose for contradiction, there are two identities e_1, e_2 such that $e_1 \neq e_2$. Then $e_1.e_2 = e_2$ (if e_1 is identity) and $e_1.e_2 = e_1$ (if e_2 is identity). But the result of $e_1.e_2$ should be same as left hand side is same for both equations. Hence $e_1 = e_2$.

2. Assume there exists two inverse of a, say b, c. If e is the identity element then we have $a * b = e$ and $a * c = e$. Also,

$$c = c * e$$
$$c = c * (a * b)$$
$$c = (c * a) * b$$
$$c = e * b$$
$$c = b$$

3. For some $a \in G$ inverse will be $(a)^{-1} \in G$ such that $aa^{-1} = e$ (e is identity). Now, interchaning the position of the elements $a^{-1}a = e$, we have inverse of a^{-1} is $a \implies (a^{-1})^{-1} = a$

4. Assume $c = (a * b)^{-1}$. Since $c \in G$, using property of inverse we have

$$c * (a * b) = (a * b)^{-1}(a * b) = e$$
$$(c * a) * b = e$$

Right multiply b^{-1} on both sides

$$(c * a) * (b * b^{-1}) = e * b^{-1}$$
$$c * a = b^{-1}$$

Right multiply a^{-1}

$$c * (a * a^{-1}) = b^{-1} * a^{-1}$$
$$c = b^{-1} * a^{-1}$$

$\square$

Proposition 4. *Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.*

1. *if $au = av$, then $u = v$*

2. *if $ub = vb$, then $u = v$*

Proof. We can solve $ax = b$ by multiplying both sides on the left by a^{-1} to get $x = a^{-1}b$. The uniqueness of x follows from the uniqueness of the inverse. Similarly, for $ya = b$, multiplying a^{-1} from right we get $y = ba^{-1}$. For $au = av$, if we multiply a^{-1} from left we get $u = v$. Similarly, the right cancellation law holds. $\square$

Definition 13. *For a group G, consider an element x in G, we define the order of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. If no positive power of x is the identity then the order of x is infinite.*

Examples:

1. In the additive groups $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ every nonidentity element has infinite order.

2. In the multiplicative groups $\mathbb{R}\backslash\{0\}$ and $\mathbb{Q}\backslash\{0\}$, the element -1 has order 2 rest all non identity elements have infinite order.

Definition 14. *Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The multiplication table or group table of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.*

Ques. Prove that $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

Ans. Assume $c = (a_1 a_2 \ldots a_n)^{-1}$ then by definition of inverse we have

$$(a_1 a_2 \ldots a_n)c = e$$

Multiply both sides by a_1 on the left and use assiciativity

$$a_1^{-1}(a_1 a_2 \ldots a_n)c = a_1^{-1} e$$
$$(a_1^{-1} a_1)(a_2 \ldots a_n)c = a_1^{-1} e$$
$$(e\, a_2 \ldots a_n)c = a_1^{-1} e$$

Keep doing the left multiplication, finally we will get

$$c = (a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1})$$

Remark. *Let x be an element in G and $|x| = n$ then $x^{-1} = x^{n-1}$.*
Also, x and x^{-1} have same order.

Dihedral Groups *Rigid motions:* A rigid motion is the distance preserving transformation, such as rotation, a reflection and a translation, and it is also called an *isometry.* A point in a plane can be uniquely identified by its distance from three noncollinear points.

A dihedral group is denoted by D_{2n}. (We follow this notation, some other books may follow D_n). Size of D_{2n} is $2n$. Order of D_{2n} is $2n$.

There are n rotations in D_{2n} given by $1, r, r^2, \ldots, r^{n-1}$ since rotation has order n.

The n reflections in D_{2n} are given by $s, rs, r^2 s, \ldots r^{n-1}s$. All non rotations are relection in D_{2n}. Order of reflections is 2 since $s^2 = 1$.

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$

In a general setting, we will use r to be the rotation by $\frac{2\pi}{n}$, where n is the number of sides in the regular polygon and s be the reflection along the line passing through the vertex 1 and the origin.

1. $1, r, r^2, \ldots, r^{n-1}$ are distinct and order of r is n.

2. Order of s is 2 i.e. $s = s^{-1}$.

3. $r^i \neq s$ for all $i \in \mathbb{N}$.

4. $sr^i \neq sr^j$ for all $0 \leq i, j \leq n - 1$ with $i \neq j$ i.e. each element can be written uniquely in the form of $s^k r^i$ for some $k = 0$ *or* 1 and $0 \leq i \leq n - 1$.

5. $rs = sr^{-1}$, hence D_{2n} is non-abelian group.

6. $r^i s = sr^{-i}$ for all $0 \leq i \leq n$ (generalised).

Generators A subset S of G is called a generator of G if all the elements of G can be written as a finite product of elements of S and their inverses. Then $G = \langle S \rangle$.

Example:

1. 1 is the generator for additive group $\mathbb{Z}$ of integers since every element of $\mathbb{Z}$ is the finite summation of $+1's$ and $-1's$ (its inverse).

2. $D_{2n} = \langle r, s \rangle$.

Relations   Any equations in a general group G that the generator satisfy are called relations.

Example: For D_{2n}, the relations are $r^n = s^2 = 1$ and $r^i s = s r^{-i}$.

Any other relation that the elements of the group satisfy can be derived by these three relations. In general, if the group G is generated by the some subset S and there is some collection of relations, say $R_1, R_2, \ldots, R_m$, such that any relation among the elements of S can be deduced from these relations then, the *presentation* of G is defined as

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle$$

Ques.   Assume H is a nonempty subset og $(G, *)$ which is closed under binary operation on G and is closed under inverses i.e. for all h and $k \in H$, hk and $h^{-2} \in H$. Prove that H is a group under the operation $*$ restricted to H, called subgroup of G.

Ans.   For a group, three axioms should be followed:

1. Assiciativity.

2. Existence of identity.

3. Existence of inverse.

Since, $H \subseteq G$ and associativity is there for all elements of G, in particular it will be followed for the elements of H also.

H is closed under inverse means for some $h \in H \; \exists \; h^{-1} \in H$ such that $h * h^{-1} = e$ and H is also closed under binary operation hence the identity will lie in H. Existence of inverse is obvious since H is closed under inverses.

Ques.   Prove that if x is an element of the group G then the set $A = \{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (called cyclic subgroup of G generated by x).

Ans.   For some $i, j \in \mathbb{Z}$ and $i \neq j$, we have $x^i x^j = x^{i+j}$ since $i, j \in \mathbb{Z} \implies i+j \in \mathbb{Z}$ therefore $x^{i+j} \in A$. Hence, it is closed under binary operation. For existence of inverse, since $\mathbb{Z}$ are symmetric about 0 means for every $i \in \mathbb{Z} \; \exists \; -i \in \mathbb{Z}$ such that $i + (-i) = 0$. Hence, for every $x^i \in A$ we have $x^{-i} \in \mathbb{Z}$ such that $x^i x^{-i} = x^{i+(-i)} = x^0 = e$. Hence, inverse exists.

Remark.   *1. $A \times B$ is abelian iff A and B both are abelian.*

2. $A \times B$ forms a group.

Theorem 6. *Let G be an finite group with even order. Then G will have atleast an element of order 2.*

Proof. Since order of G is even and it should contains e(identity, by the definition). This means, there will be odd number of nonidentity elements. Also, every element of the G should have its inverse in G hence we pair up the elements and their inverses which will leave us with a single element without a pair. By the definition, it should have its inverse in G but G is left with a single element. This implies that element should have self-inverse i.e. $a^2 = 1$ (order is 2). $\qquad\qquad\square$

Ques. Prove that if x is an element of finite order of G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Ans. For $x \in G$ such that $x^n = e$(identity) and $x \neq e$ (for identity it is trivial), we have $x^1 = x \neq e$ as we assumed. For $x^2 \neq x$ or $x^2 \neq e$ since if $x^2 = x$ then x is identity and if $x^2 = e$ then order of x is 2 which is not possible as $2 < n$. Hence, x^2 is distinct. With the similar arguments, we can proceed till $n-1$ as $x^n = e$ and at each step we are showing that the element is not one of the previous elements. Hence, all the elements $1, x, x^2, \ldots, x^{n-1}$ are distinct. For $|x| \leq |G|$, $|G|$ must contain atleast n elements (all powers of x) and there can also be any another element say $y \in G$. Hence, $|x| \leq |G|$.

Another proof for above question can be: (easy one)

Proof. For any $a \in G$, suppose for contradiction that there exist $i, j \in \mathbb{Z}^+, 0 \leq i, j \leq n$ such that $a^i = a^j \implies a^i - a^j = e \implies a^{i-j} = e$. This means that $i - j$ is the order of a and $i - j < n$ but this is the contradiction to the fact that $a^n = e$. Hence, all elements are distinct. For $|x| \leq |G|$, its same as above. $\square$

Ques. Prove that D_{2n} can be generated by two elements s and sr, both of which have order 2.

Ans. It is simple to show that s and sr have order 2.

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$$

Now, we have s and sr already there and we can generate each power of r by $ssr = r$, $(ssr)^2 = r^2$ hence $(ssr)^{n-1} = r^{n-1}$. For generating sr^2, sr^3 etc elements we can use $s(ssr)^2 = sr^2$ hence $s(ssr)^{n-1} = sr^{n-1}$. This way we can generate all the elements of the group D_{2n} hence s and sr are the generators of this group.

Definition 15. *Isomorphism of S with S': Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An isomorphism of S with S' is a **one to one** function ϕ mapping S **onto** S' such that*

$$\phi(x * y) = \phi(x) *' \phi(y) \ \forall \ x, y \in S \tag{1}$$

*A function which is not one-to-one and onto and but satisfies the eqn(1) is called an **homomorphism**.*

Examples:

1. A set which is subset (even proper subset) of another set, there can exists *isomorphism* between them. For e.g. $\langle \mathbb{Z}, + \rangle$ is isomorphic to $\langle 2\mathbb{Z}, + \rangle$ even though the first set is proper subset of another (even if there is a difference in cardinality).
   Here, $2\mathbb{Z}$ means that the subgroup of $\mathbb{Z}$ generated by 2 (even integers).

Examples:

1. e^x is a isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$

2. Identity map is obvious isomorphism to a group itself. (but not the only one.)

3. Isomorphism of symmetric group depends on cardinality of the group. For two sets Δ, Ω, the symmetric group S_Δ, S_Ω are isomorphic to each other if and only if $|\Delta| = |\Omega|$.

If two groups G and H are isomorphic then

1. $|G| \cong |H|$

2. G is abelian if and only if H is abelian.

3. for all $x \in G$, $|x| = |\phi(x)|$ where ϕ is the bijection between them.

Definition 16. *Structural property: A property of a binary structure that has been shared by any other structure that is isomorphic to it. It does not depends upon the name of binary operation of the structure. Both the structures can have different binary operations still share some structural property.*

Examples of Structural properties: 1. Number of elements in some set S is the structural property of the $\langle S, * \rangle$.
2. Commutativity
3. $x * x = x$ for all $x \in S$.
4. Equation $a * x = b$ has a solution $x \in S$ for all $a, b \in S$.
We can also show that two structures are not isomorphic if one has some structure property that other does not have.

Remark. *If x is an element of finite order n in G then*

1. *If n is odd then no element is self inverse $\implies x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.*

2. *If $n = 2k$, is even, the $x^i = x^{-i}$ iff $i = k$.*

Ques. Prove that if x is an element of finite order n in G then any integral power of x will belong to this set $\{1, x, x^2, \ldots, x^{n-1}\}$.

Ans. Since $x^n = 1$ this means that all the integral power of x for the integers $\{1, 2, \ldots, n-1\}$ is already in the set and $x^n = 1$ is already in the set.
For any $m \in \mathbb{Z}$ such that $m > n$, we can use write m as $m = nq + r$ such that $0 \leq r < n$.

$$x^m = x^{nq+r}$$
$$= x^{nq}x^r$$
$$= (x^n)^q x^r$$
$$= x^r$$

Therefore, for any $m > n$, we can write it as x^r such that $0 \leq r < n$ and $x^r \in \{1, x, x^2, \ldots, x^{n-1}\}$.