Modern Algebra

Dr. Anuj Jakhar

Indian Institute of Technology Bhilai

anujjakhar@iitbhilai.ac.in

2022

Binary operation.

- A binary operation on a set S is a rule for combining pairs a, b of S to get another element of S (i.e., S is closed under the operation which means if $a, b \in S$ then $a * b \in S$.), i.e., it defines a map

$$f : S * S \to S,$$

  where $*$ is binary operation.
- Here, we shall use the symbol $a * b$ to denote $f(a, b)$.

Example.

- Let S be a set of integers. The operations $f : S * S \to S$ defined by $f(a, b) = a * b$, where $a * b = a + b - ab$, is a binary operation in S.
- **Note :** In this example if we take S to be the set of only positive integres then $*$ operation does not define a binary operation because composition of two positive integers a, b which is $a * b$, can be negative.

Associativity: A binary operation $*$ in S is said to be associative, if $a * (b * c) = (a * b) * c$, for any a, b and c in S.
Commutativity: A binary operation $*$ in S is said to be commutative, if $a * b = b * a$, for any $a \in S$ and $b \in S$.

Example.

In the above example, we can check that the operation $*$ is associative and commutative.

- Checking of commutativity of the $*$ operation :
  $a * b = a + b - ab$
  $b * a = b + a - ba$ which can be rewrite as $a + b - ab$.
  Thus, we can see that, $a * b = b * a$.
- Checking of Associativity :
  $(a * b) * c = (a + b - ab) * c = a + b - ab + c - (a + b - ab)c = a + b + c - ab - ac - bc + (ab)c$
  $a * (b * c) = a * (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - bc - ab - ac + a(bc)$.
  Thus, we can have, $(a * b) * c = a * (b * c)$.

Identity and Inverse

- Identity: Let S be a set with binary operation $*$. An element $e \in S$ is called, a neutral element or identity element, if $a * e = a = e * a$, for each $a \in S$.
- Inverse: Let S be a set with binary operation $*$ and unit element e. An element $a \in S$ is said to have an inverse with respect to $*$ if there exists another element $a' \in S$ such that $a * a' = e = a' * a$.

Example. Let S be the set of integers with addition binary operation. Then, for finding identity and inverses, we proceed by definition :

- for identity : let e be the identity element, then by definition : $a * e = a + e = a = e + a = e * a$, which implies $e = 0$.
- for inverse : let a' be the inverse, then by definition : $a * a' = a + a' = 0 \text{ (identity)} = a' + a = a' * a$. Thus we have, $a' = -a$.

Definition. A non-empty set G with a binary operation '$*$' is said to be a *group*[1] with respect to '$*$' if the following three conditions are satisfied for all a, b, c belonging to G:

(i) $a * (b * c) = (a * b) * c$ (associativity),

(ii) there exists an element $e \in G$, such that $a * e = a = e * a$ (existence of identity),

(iii) for every $a \in G$, there exists an element $a' \in G$ such that $a * a' = e = a' * a$ (existence of inverse).

Further G is called commutative/abelian[2] if $a * b = b * a$ for all $a, b \in G$.

[1] The abstract form of the definition of a group, which we use today, was built up slowly over the course of 19th century, with suggested definitions by Cayley, Kronecker, Weber, Burnside, and Pierpont. The axioms of associativity, identity element and inverse were first stated in their present form by Pierpont.

[2] The term abelian is derived from the name of Norwegian Mathematician Niels Henrik Abel (1802-1829) who showed the importance of such groups in the theory of equations.

Examples

Groups	Binary Operation
$(\mathbb{Z},+)$,$(\mathbb{Q},+)$,$(\mathbb{R},+)$,$(\mathbb{C},+)$	Addition
$(\mathbb{R}$-$\{0\},\cdot)$,$(\mathbb{C}$-$\{0\},\cdot)$	Multiplication
D_n(Dihedral group of 2n elements)	Composition
S_n(Permutation Group of n elements)	Composition
A_n(Alternating group of n elements)	Composition
C_n,$\mathbb{Z}_n$ (Cyclic group of order n, integers modulo n)	Multipli., Addition respectively

Order, Generator

- Order of a group: Number of elements in group G is called the order of the group. We use $|G|$ for the order of group.

Order, Generator

- Order of a group: Number of elements in group G is called the order of the group. We use $|G|$ for the order of group.
- Order of an element of a group: Let $a \in G$. Then order of a will be m if m is the least positive integer greater than one such that $a^m = e$, where e is identity element (Here a^m means m times binary operation of element a with itself).

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,
(I) Closure : if $a, b \in H$, then $ab \in H$.

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,
(I) Closure : if $a, b \in H$, then $ab \in H$.
(II) Identity : $e \in H$.

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,

(I) Closure : if $a, b \in H$, then $ab \in H$.

(II) Identity : $e \in H$.

(III) Inverse : if $a \in H$, then $a^{-1} \in H$.

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,
(I) Closure : if $a, b \in H$, then $ab \in H$.
(II) Identity : $e \in H$.
(III) Inverse : if $a \in H$, then $a^{-1} \in H$.

- $\{e\}$(identity group) and G(itself) are the trivial subgroups of G. Other subgroups (nontrivial subgroups) are the proper subgroups of G.

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,
(I) Closure : if $a, b \in H$, then $ab \in H$.
(II) Identity : $e \in H$.
(III) Inverse : if $a \in H$, then $a^{-1} \in H$.

- $\{e\}$(identity group) and G(itself) are the trivial subgroups of G. Other subgroups (nontrivial subgroups) are the proper subgroups of G.
- Example. All subgroups of the additive group of integers $\mathbb{Z}$ are in the form
  $a\mathbb{Z} = \{an | n \in \mathbb{Z}\}$ for some integer a.

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,
(I) Closure : if $a, b \in H$, then $ab \in H$.
(II) Identity : $e \in H$.
(III) Inverse : if $a \in H$, then $a^{-1} \in H$.

- $\{e\}$(identity group) and G(itself) are the trivial subgroups of G. Other subgroups (nontrivial subgroups) are the proper subgroups of G.
- Example. All subgroups of the additive group of integers $\mathbb{Z}$ are in the form
  $a\mathbb{Z} = \{an | n \in \mathbb{Z}\}$ for some integer a.
- A non-empty subset H of a group G is a subgroup iff whenever $a \in H, b \in H$, the product $ab^{-1} \in H$.

Subgroup.

Definition. A subgroup of a group G is a group H in G, with the same binary operation. In other words following holds,
(I) Closure : if $a, b \in H$, then $ab \in H$.
(II) Identity : $e \in H$.
(III) Inverse : if $a \in H$, then $a^{-1} \in H$.

- $\{e\}$(identity group) and G(itself) are the trivial subgroups of G. Other subgroups (nontrivial subgroups) are the proper subgroups of G.
- Example. All subgroups of the additive group of integers $\mathbb{Z}$ are in the form
  $a\mathbb{Z} = \{an | n \in \mathbb{Z}\}$ for some integer a.
- A non-empty subset H of a group G is a subgroup iff whenever $a \in H, b \in H$, the product $ab^{-1} \in H$.
- If H and K are subgroups of G, then $H \cap K$ is also a subgroup of G.

- Intersection of finite number of subgroups of G is a subgroup of G.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.
- Let a be a fixed element of G. Then, $N(a) = \{x \mid xa = ax\}$, is called the centraliser of a.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.
- Let a be a fixed element of G. Then, $N(a) = \{x \mid xa = ax\}$, is called the centraliser of a.
- For any subset $A \subset G$, $N(A) = \{x \mid xA = Ax\}$, is called the normaliser of A.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.
- Let a be a fixed element of G. Then, $N(a) = \{x \mid xa = ax\}$, is called the centraliser of a.
- For any subset $A \subset G$, $N(A) = \{x \mid xA = Ax\}$, is called the normaliser of A.
- Check that $N(A)$ is a subgroup of G.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.
- Let a be a fixed element of G. Then, $N(a) = \{x \mid xa = ax\}$, is called the centraliser of a.
- For any subset $A \subset G$, $N(A) = \{x \mid xA = Ax\}$, is called the normaliser of A.
- Check that $N(A)$ is a subgroup of G.
- Note that whenever A is singleton set $\{a\}$, then $N(A)$ is same as centraliser of a.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.
- Let a be a fixed element of G. Then, $N(a) = \{x \mid xa = ax\}$, is called the centraliser of a.
- For any subset $A \subset G$, $N(A) = \{x \mid xA = Ax\}$, is called the normaliser of A.
- Check that $N(A)$ is a subgroup of G.
- Note that whenever A is singleton set $\{a\}$, then $N(A)$ is same as centraliser of a.
- If H and K are two subgroups of G, then their product HK will be subgroup of G if and only if $HK = KH$.

- Intersection of finite number of subgroups of G is a subgroup of G.
- Let H be a finite subset of a group G such that $ab \in H$, whenever $a \in H$, $b \in H$. Then H is a subgroup of G.
- For any group G, the set $H = \{x \mid x \in G, xa = ax, \text{ for each } a \in G\}$, is a subgroup of G.
- The center $Z(G) = \{x \mid xa = ax \text{ for each } a \in G\}$ is a subgroup of G.
- Let a be a fixed element of G. Then, $N(a) = \{x \mid xa = ax\}$, is called the centraliser of a.
- For any subset $A \subset G$, $N(A) = \{x \mid xA = Ax\}$, is called the normaliser of A.
- Check that $N(A)$ is a subgroup of G.
- Note that whenever A is singleton set $\{a\}$, then $N(A)$ is same as centraliser of a.
- If H and K are two subgroups of G, then their product HK will be subgroup of G if and only if $HK = KH$.
- Let H and K be finite subgroups of G such that HK is also a subgroup. Then
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Dihedral group of order $2n$.

- Let D_n denotes n-polygon which has n sides of same length.
- If r denotes rotation by $2\pi/n$ degree, hence we have, $r^n = 1$ (identity).
- f denotes flipping about the x - axis, hence $f^2 = 1$ (identity).
- Then group D_n has $2n$ elements and the elemnets of D_n are :

$$D_n = \{1, r, r^2, \cdots, r^{n-1}, f, rf, r^2f, \cdots, r^{n-1}f\}.$$

- Here, observe that $fr = r^{n-1}f$, $f^2 = 1 = r^n$.

- Generator of a group:

- Generator of a group: An element b is called a generator of a group if all the elements of groups can be written as powers of b (Here b^n means n times binary operation of element b with itself)

- Generator of a group: An element b is called a generator of a group if all the elements of groups can be written as powers of b (Here b^n means n times binary operation of element b with itself)

or

In a group of order n, an element b is called generator of G if n is the least positive integer greater than 1 such that $b^n = e$ (identity element).

Cyclic group of order n.

A group C_n is called a cyclic group of order n if it has at least one generator (it can have more than one).

Cyclic group of order n.

A group C_n is called a cyclic group of order n if it has at least one generator (it can have more than one).

Examples.

- The group $\mathbb{Z}$ of integers is cyclic. 1 and -1 are generators of $\mathbb{Z}$.

Cyclic group of order n.

A group C_n is called a cyclic group of order n if it has at least one generator (it can have more than one).

Examples.

- The group $\mathbb{Z}$ of integers is cyclic. 1 and -1 are generators of $\mathbb{Z}$.
- The group $G = \{1, -1, \iota, -\iota\}$ is cyclic with ι and $-\iota$ as generators.

Cyclic group of order n.

A group C_n is called a cyclic group of order n if it has at least one generator (it can have more than one).

Examples.

- The group $\mathbb{Z}$ of integers is cyclic. 1 and -1 are generators of $\mathbb{Z}$.
- The group $G = \{1, -1, \iota, -\iota\}$ is cyclic with ι and $-\iota$ as generators.
- The trivial group $G = \{e\}$ is cyclic with generator e.

Cyclic group of order n.

A group C_n is called a cyclic group of order n if it has at least one generator (it can have more than one).

Examples.

- The group $\mathbb{Z}$ of integers is cyclic. 1 and -1 are generators of $\mathbb{Z}$.
- The group $G = \{1, -1, \iota, -\iota\}$ is cyclic with ι and $-\iota$ as generators.
- The trivial group $G = \{e\}$ is cyclic with generator e.
- Group $\mathbb{Z}_n$ of residue classes modulo n is cyclic with generator.

Lemma. Any subgroup of an infinite cyclic group is also an infinite cyclic group.

Cyclic group of order n.

A group C_n is called a cyclic group of order n if it has at least one generator (it can have more than one).

Examples.

- The group $\mathbb{Z}$ of integers is cyclic. 1 and -1 are generators of $\mathbb{Z}$.
- The group $G = \{1, -1, \iota, -\iota\}$ is cyclic with ι and $-\iota$ as generators.
- The trivial group $G = \{e\}$ is cyclic with generator e.
- Group $\mathbb{Z}_n$ of residue classes modulo n is cyclic with generator.

Lemma. Any subgroup of an infinite cyclic group is also an infinite cyclic group.

Corollary. An infinte cyclic group has infinitely many subgroups each of which is an infinite cyclic group.

Lemma. Every cyclic group is abelian but converse is not true.

Lemma. Every cyclic group is abelian but converse is not true.

Couterexample for the converse part. Klein 4 group (V_4).

Lemma. Every cyclic group is abelian but converse is not true.

Couterexample for the converse part. Klein 4 group (V_4).

Lemma. Any infinte cyclic group has exactly two generators.

Lemma. Every cyclic group is abelian but converse is not true.

Couterexample for the converse part. Klein 4 group (V_4).

Lemma. Any infinte cyclic group has exactly two generators.

Number of generators in a cyclic group of order n. In a cyclic group of order n, the number of generators are $\phi(n)$ (Euler phi function).

Lemma. Every cyclic group is abelian but converse is not true.

Couterexample for the converse part. Klein 4 group (V_4).

Lemma. Any infinte cyclic group has exactly two generators.

Number of generators in a cyclic group of order n. In a cyclic group of order n, the number of generators are $\phi(n)$ (Euler phi function).

Euler phi(ϕ) function. If $n = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_k^{r_k}$, where $p_1, p_2, p_3, \cdots, p_k$ are the prime factors of n. Then :

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Lemma. Every cyclic group is abelian but converse is not true.

Couterexample for the converse part. Klein 4 group (V_4).

Lemma. Any infinte cyclic group has exactly two generators.

Number of generators in a cyclic group of order n. In a cyclic group of order n, the number of generators are $\phi(n)$ (Euler phi function).

Euler phi(ϕ) function. If $n = p_1^{r_1} p_2^{r_2} p_3^{r_3} \cdots p_k^{r_k}$, where $p_1, p_2, p_3, \cdots, p_k$ are the prime factors of n. Then :

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Lemma. Let G be a finite cyclic group of order n. Then G has a unique cyclic subgroup of order d for every divisor d of n.

Permutation.

Definition.

- A permutation on a set X is a bijective map from a set to itself.
- A permutation π can be written as a composition of cycles, a cycle written as $(a_1 a_2 \cdots a_k)$: $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, $\cdots$, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$.

Permutation.

Definition.

- A permutation on a set X is a bijective map from a set to itself.
- A permutation π can be written as a composition of cycles, a cycle written as $(a_1 a_2 \cdots a_k)$: $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, $\cdots$, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$.

Permutation Group.

- Let we have n different numbers.

Permutation.

Definition.

- A permutation on a set X is a bijective map from a set to itself.
- A permutation π can be written as a composition of cycles, a cycle written as $(a_1 a_2 \cdots a_k)$: $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, $\cdots$, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$.

Permutation Group.

- Let we have n different numbers.
- Then all the possible permutations and combinations of these n numbers are possible $n!$.

Permutation.

Definition.

- A permutation on a set X is a bijective map from a set to itself.
- A permutation π can be written as a composition of cycles, a cycle written as $(a_1 a_2 \cdots a_k)$: $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, $\cdots$, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$.

Permutation Group.

- Let we have n different numbers.
- Then all the possible permutations and combinations of these n numbers are possible $n!$.
- If we say every such permutation and combination one element then these $n!$ elements makes a group under composition, where composition means that if we operate one element to another then it permute it and we get other element from $n!$ elements.

Permutation.

Definition.

- A permutation on a set X is a bijective map from a set to itself.
- A permutation π can be written as a composition of cycles, a cycle written as $(a_1 a_2 \cdots a_k)$: $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, $\cdots$, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$.

Permutation Group.

- Let we have n different numbers.
- Then all the possible permutations and combinations of these n numbers are possible $n!$.
- If we say every such permutation and combination one element then these $n!$ elements makes a group under composition, where composition means that if we operate one element to another then it permute it and we get other element from $n!$ elements.
- We denote this group by S_n or P_n which order is $n!$.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.

- Supose we have two elements $(2\ 5\ 3\ 7)*(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.

- Supose we have two elements (2 5 3 7)$*$(6 3 1 9) $=$ (7 2 5 3 1 9 6).
- We process from last element. In above example we started from last element (6 3 1 9) from number 6. $\pi(6) = 3$, now we see in left element (2 5 3 7) that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from (6 3 1 9) that $\pi(7) = 7$ (Since 7 is not written, means (7 7), 7 is permuting with itself) and then we see in left element (2 5 3 7) that $\pi(7) = 2$.

- Supose we have two elements $(2\ 5\ 3\ 7)*(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element (6 3 1 9) from number 6. $\pi(6) = 3$, now we see in left element (2 5 3 7) that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from (6 3 1 9) that $\pi(7) = 7$ (Since 7 is not written, means (7 7), 7 is permuting with itself) and then we see in left element (2 5 3 7) that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get (7 2 5 3 1 9).

---

1. $(a_1\ \cdots\ a_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.

- Supose we have two elements $(2\ 5\ 3\ 7)*(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means (7 7), 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get (7 2 5 3 1 9).

---

1. $(a_1\ \cdots\ a_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means $(7\ 7)$, 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get $(7\ 2\ 5\ 3\ 1\ 9)$.

---

1. $(a_1 \cdots \mathrm{a}_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.
3. Cycle $(a_1 a_2 \cdots a_k)$ can be rewritten as $(a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$, product of two number cycles.

- Supose we have two elements $(2\ 5\ 3\ 7){*}(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means $(7\ 7)$, 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get $(7\ 2\ 5\ 3\ 1\ 9)$.

1. $(a_1 \ \cdots \ a_k)$ called a cycle, where $a_1,\cdots,a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.
3. Cycle $(a_1 a_2 \cdots a_k)$ can be rewritten as $(a_1 a_2)(a_1 a_3)\cdots(a_1 a_k)$, product of two number cycles.
4. We break an element of prmutation group according to (3) and after that if number of cycles are even then element is called even cycle otherwise odd cycle.
5. Identity element 1 is always even cycle.

- Supose we have two elements $(2\ 5\ 3\ 7)*(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.

- Supose we have two elements $(2\ 5\ 3\ 7)*(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means $(7\ 7)$, 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.

- Supose we have two elements $(2\ 5\ 3\ 7){*}(6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means $(7\ 7)$, 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get $(7\ 2\ 5\ 3\ 1\ 9)$.

---

1. $(a_1\ \cdots\ a_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element (6 3 1 9) from number 6. $\pi(6) = 3$, now we see in left element (2 5 3 7) that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from (6 3 1 9) that $\pi(7) = 7$ (Since 7 is not written, means (7 7), 7 is permuting with itself) and then we see in left element (2 5 3 7) that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get (7 2 5 3 1 9).

---

1. $(a_1 \cdots a_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means (7 7), 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get $(7\ 2\ 5\ 3\ 1\ 9)$.

---

1. $(a_1\ \cdots\ \mathrm{a}_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.
3. Cycle $(a_1 a_2 \cdots a_k)$ can be rewritten as $(a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$, product of two number cycles.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means $(7\ 7)$, 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get $(7\ 2\ 5\ 3\ 1\ 9)$.

---

1. $(a_1 \ \cdots \ \mathrm{a}_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.
3. Cycle $(a_1 a_2 \cdots a_k)$ can be rewritten as $(a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$, product of two number cycles.
4. We break an element of permutation group according to (3) and after that if number of cycles are even then element is called even cycle otherwise odd cycle.

- Supose we have two elements $(2\ 5\ 3\ 7) * (6\ 3\ 1\ 9) = (7\ 2\ 5\ 3\ 1\ 9\ 6)$.
- We process from last element. In above example we started from last element $(6\ 3\ 1\ 9)$ from number 6. $\pi(6) = 3$, now we see in left element $(2\ 5\ 3\ 7)$ that $\pi(3) = 7$. So, first number of new element is 7.
- Now we see again from $(6\ 3\ 1\ 9)$ that $\pi(7) = 7$ (Since 7 is not written, means $(7\ 7)$, 7 is permuting with itself) and then we see in left element $(2\ 5\ 3\ 7)$ that $\pi(7) = 2$.
- So the next number after 7 is 2.
- After continuing this process we get $(7\ 2\ 5\ 3\ 1\ 9)$.

1. $(a_1 \cdots\ a_k)$ called a cycle, where $a_1, \cdots, a_k$ are natural numbers or every element of permutation group is called a cycle.
2. $m \in \mathbb{N}$ is called the order of a cycle $(a_1 a_2 \cdots a_k)$, if $(a_1 a_2 \cdots a_k)^m = 1$.
3. Cycle $(a_1 a_2 \cdots a_k)$ can be rewritten as $(a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$, product of two number cycles.
4. We break an element of permutation group according to (3) and after that if number of cycles are even then element is called even cycle otherwise odd cycle.
5. Identity element 1 is always even cycle.

Alternating group.

- From the group S_n, if we remove all the odd cycles, then the set of all even cycles made a group, which is called Alternating group A_n, which has order $\frac{n!}{2}$.

Alternating group.

- From the group S_n, if we remove all the odd cycles, then the set of all even cycles made a group, which is called Alternating group A_n, which has order $\frac{n!}{2}$.
- A_n is always subgroup of S_n.

Example.

- If n $= 3$, then $S_3 = \{1, (12), (13), (23), (123), (132)\}$, has six (3!) elements.

Alternating group.

- From the group S_n, if we remove all the odd cycles, then the set of all even cycles made a group, which is called Alternating group A_n, which has order $\frac{n!}{2}$.
- A_n is always subgroup of S_n.

Example.

- If n $=3$, then $S_3 = \{1, (12), (13), (23), (123), (132)\}$, has six (3!) elements.
- Here, elements (1 2), (2 3), (13) have order 2 and (1 2 3), (1 3 2) have order 3. (1 2 3) and (1 3 2) are the inverses of each other. (1 2),(1 3) and (2 3) are the inverses of itself.

Alternating group.

- From the group S_n, if we remove all the odd cycles, then the set of all even cycles made a group, which is called Alternating group A_n, which has order $\frac{n!}{2}$.
- A_n is always subgroup of S_n.

Example.

- If n $= 3$, then $S_3 = \{1, (12), (13), (23), (123), (132)\}$, has six (3!) elements.
- Here, elements (1 2), (2 3), (13) have order 2 and (1 2 3), (1 3 2) have order 3. (1 2 3) and (1 3 2) are the inverses of each other. (1 2),(1 3) and (2 3) are the inverses of itself.
- $A_3 = \{1, (123), (132)\}$, has three $(\frac{3!}{2})$ elements, is a subgroup of S_3.

Alternating group.

- From the group S_n, if we remove all the odd cycles, then the set of all even cycles made a group, which is called Alternating group A_n, which has order $\frac{n!}{2}$.
- A_n is always subgroup of S_n.

Example.

- If n $= 3$, then $S_3 = \{1, (12), (13), (23), (123), (132)\}$, has six (3!) elements.
- Here, elements (1 2), (2 3), (13) have order 2 and (1 2 3), (1 3 2) have order 3. (1 2 3) and (1 3 2) are the inverses of each other. (1 2),(1 3) and (2 3) are the inverses of itself.
- $A_3 = \{1, (123), (132)\}$, has three $(\frac{3!}{2})$ elements, is a subgroup of S_3.
- Check that A_3 is abelian group but S_3 is not, because A_3 has prime order. Hence, A_3 is cyclic. In S_3, we can check that (1 2)(1 2 3) $=$ (3 2) and (1 2 3)(1 2) $=$ (3 1), which do not commute.

Cosets

Let G be a group and H be a subgroup of G. For any $a \in G$, the set Ha is called a right coset of H in G. Similarly aH is called a left coset of H in G.

Cosets

Let G be a group and H be a subgroup of G. For any $a \in G$, the set Ha is called a right coset of H in G. Similarly aH is called a left coset of H in G.

Lemma. Let G be a group and H be a subgroup of G. Then G is the union of all left cosets of H in G and any two distinct left cosets of H in G are disjoint.

Cosets

Let G be a group and H be a subgroup of G. For any $a \in G$, the set Ha is called a right coset of H in G. Similarly aH is called a left coset of H in G.

Lemma. Let G be a group and H be a subgroup of G. Then G is the union of all left cosets of H in G and any two distinct left cosets of H in G are disjoint.

Lemma. Any two left cosets of H in G have the same (finite or infinte) number of elements.

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group.

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group. Converse is false (A_4 does not have subgroup of order 6).

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group. Converse is false (A_4 does not have subgroup of order 6).

Corollary. The number of distinct left cosets of H in G is equal to $|G|/|H|$.

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group. Converse is false (A_4 does not have subgroup of order 6).

Corollary. The number of distinct left cosets of H in G is equal to $|G|/|H|$.

Definition. Let G be a group and H be a subgroup of G. Then the number (finite or infinte) of distinct left cosets of H in G are called the index of H in G, denoted by $[G : H]$.

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group. Converse is false (A_4 does not have subgroup of order 6).

Corollary. The number of distinct left cosets of H in G is equal to $|G|/|H|$.

Definition. Let G be a group and H be a subgroup of G. Then the number (finite or infinte) of distinct left cosets of H in G are called the index of H in G, denoted by $[G : H]$.

Lemma. Let G be a group, H be subgroup of G. Then the number of left cosets of H in G is the same as number of right cosets of H in G.

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group. Converse is false (A_4 does not have subgroup of order 6).

Corollary. The number of distinct left cosets of H in G is equal to $|G|/|H|$.

Definition. Let G be a group and H be a subgroup of G. Then the number (finite or infinte) of distinct left cosets of H in G are called the index of H in G, denoted by $[G : H]$.

Lemma. Let G be a group, H be subgroup of G. Then the number of left cosets of H in G is the same as number of right cosets of H in G.

Corollary. Let G be a finite group of order n, and $a \in G$. Then $|a|$ divides $|G|$, and in particular $a^n = e$.

Lagrange's theorem

Let G be a finite group and H be a subgroup of G. Then the order of the subgroup divides the order of the group. Converse is false (A_4 does not have subgroup of order 6).

Corollary. The number of distinct left cosets of H in G is equal to $|G|/|H|$.

Definition. Let G be a group and H be a subgroup of G. Then the number (finite or infinte) of distinct left cosets of H in G are called the index of H in G, denoted by $[G : H]$.

Lemma. Let G be a group, H be subgroup of G. Then the number of left cosets of H in G is the same as number of right cosets of H in G.

Corollary. Let G be a finite group of order n, and $a \in G$. Then $|a|$ divides $|G|$, and in particular $a^n = e$.

Corollary. Every group of prime order is cyclic.

Normal Subgroup.

Definition. A subgroup H of G is called normal subgroup if for all $a \in H$ and $g \in G$, $gag^{-1} \in H$.

Normal Subgroup.

Definition. A subgroup H of G is called normal subgroup if for all $a \in H$ and $g \in G$, $gag^{-1} \in H$.

Lemma. A subgroup H of G is called normal subgroup iff $g \cdot H = H \cdot g$ for all $g \in G$.

Normal Subgroup.

Definition. A subgroup H of G is called normal subgroup if for all $a \in H$ and $g \in G$, $gag^{-1} \in H$.

Lemma. A subgroup H of G is called normal subgroup iff $g \cdot H = H \cdot g$ for all $g \in G$.

Note. If $g \in H$, then $g \cdot H = H = H \cdot g$, by the definition of subgroup.

Normal Subgroup.

Definition. A subgroup H of G is called normal subgroup if for all $a \in H$ and $g \in G$, $gag^{-1} \in H$.

Lemma. A subgroup H of G is called normal subgroup iff $g \cdot H = H \cdot g$ for all $g \in G$.

Note. If $g \in H$, then $g \cdot H = H = H \cdot g$, by the definition of subgroup.

Example.

- A_3 is normal subgroup of S_3.

Normal Subgroup.

Definition. A subgroup H of G is called normal subgroup if for all $a \in H$ and $g \in G$, $gag^{-1} \in H$.

Lemma. A subgroup H of G is called normal subgroup iff $g \cdot H = H \cdot g$ for all $g \in G$.

Note. If $g \in H$, then $g \cdot H = H = H \cdot g$, by the definition of subgroup.

Example.

- A_3 is normal subgroup of S_3.
- Here $H = A_3$.
- By above note, we see that $1 \cdot A_3 = (1\ 2\ 3) \cdot A_3 = (132) \cdot A_3 = H$.
- Now if $g = (12)$, then $(12) \cdot H = (12) \cdot \{1, (123), (132)\} = \{(12), (32), (31)\} = \{1, (123), (132)\} \cdot (12) = H \cdot (12)$.

Normal Subgroup.

Definition. A subgroup H of G is called normal subgroup if for all $a \in H$ and $g \in G$, $gag^{-1} \in H$.

Lemma. A subgroup H of G is called normal subgroup iff $g \cdot H = H \cdot g$ for all $g \in G$.

Note. If $g \in H$, then $g \cdot H = H = H \cdot g$, by the definition of subgroup.

Example.

- A_3 is normal subgroup of S_3.
- Here $H = A_3$.
- By above note, we see that $1 \cdot A_3 = (1\ 2\ 3) \cdot A_3 = (132) \cdot A_3 = H$.
- Now if $g = (12)$, then $(12) \cdot H = (12) \cdot \{1, (123), (132)\} = \{(12), (32), (31)\} = \{1, (123), (132)\} \cdot (12) = H \cdot (12)$.
- Similarly, we can check for other elements. We get that A_3 is normal in S_3.

Normal Subgroup.

- Every subgroup of an abelian group is normal subgroup.

Normal Subgroup.

- Every subgroup of an abelian group is normal subgroup.
- Center of a group G is a normal subgroup of G.

Normal Subgroup.

- Every subgroup of an abelian group is normal subgroup.
- Center of a group G is a normal subgroup of G.

Lemma. If H is a subgroup of index 2 in G, then H is normal in G.

Normal Subgroup.

- Every subgroup of an abelian group is normal subgroup.
- Center of a group G is a normal subgroup of G.

Lemma. If H is a subgroup of index 2 in G, then H is normal in G.

Corollary. A_n is a normal subgroup of S_n and C_n is normal subgroup of D_n.

Normal Subgroup.

- Every subgroup of an abelian group is normal subgroup.
- Center of a group G is a normal subgroup of G.

Lemma. If H is a subgroup of index 2 in G, then H is normal in G.

Corollary. A_n is a normal subgroup of S_n and C_n is normal subgroup of D_n.

Simple Group. G is called a simple group if its only normal subgroups are G and $\{e\}$.

Normal Subgroup.

- Every subgroup of an abelian group is normal subgroup.
- Center of a group G is a normal subgroup of G.

Lemma. If H is a subgroup of index 2 in G, then H is normal in G.

Corollary. A_n is a normal subgroup of S_n and C_n is normal subgroup of D_n.

Simple Group. G is called a simple group if its only normal subgroups are G and $\{e\}$.

Example. A cyclic group of prime order is a simple group.

Quotient Groups

Definition. Let H be a normal subgroup of G. Then the set of left (right) cosets of H in G forms a group for the operation $(aH) * (bH) = abH$. We denote it by G/H and we say it the quotient group of G by H.

Quotient Groups

Definition. Let H be a normal subgroup of G. Then the set of left (right) cosets of H in G forms a group for the operation $(aH) * (bH) = abH$. We denote it by G/H and we say it the quotient group of G by H.

Examples.

- $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Then the quotient group G/H is the group $\mathbb{Z}$ of residue classes of modulo n.

Quotient Groups

Definition. Let H be a normal subgroup of G. Then the set of left (right) cosets of H in G forms a group for the operation $(aH) * (bH) = abH$. We denote it by G/H and we say it the quotient group of G by H.

Examples.

- $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Then the quotient group G/H is the group $\mathbb{Z}$ of residue classes of modulo n.
- If $G = S_3$, $H = A_3$, then $G/H = \{H, (12)H\}$, which is a cyclic group of order 2.

Quotient Groups

Definition. Let H be a normal subgroup of G. Then the set of left (right) cosets of H in G forms a group for the operation $(aH) * (bH) = abH$. We denote it by G/H and we say it the quotient group of G by H.

Examples.

- $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Then the quotient group G/H is the group $\mathbb{Z}$ of residue classes of modulo n.
- If $G = S_3$, $H = A_3$, then $G/H = \{H, (12)H\}$, which is a cyclic group of order 2.

G/Z Theorem. Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is abelian.

Homomorphism.

A homomorphism from a group G (with binary operation $*$) to a group G' (having binary operation $*'$) is a function f such that for all $a, b \in G$,

$$f : G \to G'$$

$$f(a * b) = f(a) *' f(b).$$

Homomorphism.

A homomorphism from a group G (with binary operation $*$) to a group G' (having binary operation $*'$) is a function f such that for all $a, b \in G$,

$$f : G \to G'$$

$$f(a * b) = f(a) *' f(b).$$

Example. Let $G = \mathbb{Z}$ and $G' = \{1, -1\}$ the multiplicative group. The mapping $\theta : G \to G'$ defined by $\theta(n) = 1$ if n is even and $\theta(n) = -1$ if n is odd is a group homomorphism, as $\theta(m + n) = \theta(m)\theta(n)$ for all $m, n \in \mathbb{Z}$.

Homomorphism.

A homomorphism from a group G (with binary operation $*$) to a group G' (having binary operation $*'$) is a function f such that for all $a, b \in G$,

$$f : G \to G'$$

$$f(a * b) = f(a) *' f(b).$$

Example. Let $G = \mathbb{Z}$ and $G' = \{1, -1\}$ the multiplicative group. The mapping $\theta : G \to G'$ defined by $\theta(n) = 1$ if n is even and $\theta(n) = -1$ if n is odd is a group homomorphism, as $\theta(m + n) = \theta(m)\theta(n)$ for all $m, n \in \mathbb{Z}$.

Let $f : G \to G'$ be a homomorphism of G onto G'. If G is abelian, then G' is abelian.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where e}_{G'} \text{ is the identity of G'}\}$$

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where } \text{e}_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{\text{x} \in \text{G'} \mid \text{x} = \text{f(a), for some a in G.}\}$$

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where e}_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{\text{x} \in \text{G'} \mid \text{x} = \text{f(a), for some a in G.}\}$$

Remark 1. Let $f : G \to G'$ be a homomorphism. Then

1. $|G| = |Ker(f)| \cdot |Im(f)|$.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where } \text{e}_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{\text{x} \in \text{G'} \mid \text{x} = \text{f(a), for some a in G.}\}$$

Remark 1. Let $f : G \to G'$ be a homomorphism. Then

1. $|G| = |Ker(f)| \cdot |Im(f)|$.
2. Ker(f) is always a normal subgroup of G.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where e}_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{\text{x} \in \text{G'} \mid \text{x} = \text{f(a), for some a in G.}\}$$

Remark 1. Let $f : G \to G'$ be a homomorphism. Then

1. $|G| = |Ker(f)| \cdot |Im(f)|$.
2. Ker(f) is always a normal subgroup of G.
3. Im(f) is always a subgroup of G'.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where e}_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{\text{x} \in \text{G'} \mid \text{x} = \text{f(a), for some a in G.}\}$$

Remark 1. Let $f : G \to G'$ be a homomorphism. Then

1. $|G| = |Ker(f)| \cdot |Im(f)|$.
2. Ker(f) is always a normal subgroup of G.
3. Im(f) is always a subgroup of G'.
4. $f(e) = e'$, where e and e' are the identity elements of G and G' respectively.
5. If $a \in G$, then $f(a^{-1}) = (f(a))^{-1}$, $|f(a)|$ divides $|a|$.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{\text{a} \in \text{G} \mid \text{f(a)} = \text{e}_{G'}, \text{ where e}_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{\text{x} \in \text{G'} \mid \text{x} = \text{f(a), for some a in G.}\}$$

Remark 1. Let $f : G \to G'$ be a homomorphism. Then

1. $|G| = |Ker(f)| \cdot |Im(f)|$.
2. Ker(f) is always a normal subgroup of G.
3. Im(f) is always a subgroup of G'.
4. $f(e) = e'$, where e and e' are the identity elements of G and G' respectively.
5. If $a \in G$, then $f(a^{-1}) = (f(a))^{-1}$, $|f(a)|$ divides $|a|$.
6. f is one-one mapping iff Ker(f) $= \{e\}$.

Kernel of f. The kernal of f is the set of elements in G which goes to the identity of G' under the map f.

$$Ker(f) = \{a \in G \mid f(a) = e_{G'}, \text{ where } e_{G'} \text{ is the identity of G'}\}$$

Image of f. The image of f is the subset of G' :

$$Im(f) = \{x \in G' \mid x = f(a), \text{ for some a in G.}\}$$

Remark 1. Let $f : G \to G'$ be a homomorphism. Then

1. $|G| = |Ker(f)| \cdot |Im(f)|$.
2. Ker(f) is always a normal subgroup of G.
3. Im(f) is always a subgroup of G'.
4. $f(e) = e'$, where e and e' are the identity elements of G and G' respectively.
5. If $a \in G$, then $f(a^{-1}) = (f(a))^{-1}$, $|f(a)|$ divides $|a|$.
6. f is one-one mapping iff Ker(f) $= \{e\}$.
7. If G is cyclic, then G' will be cyclic.
8. If H and K are two normal subgroups of G, then their product HK will be always normal subgroup.

Remark 2. Let $f : G \to G'$ be a homomorphism and H be a subgroup of G. Then

1. If H is cyclic, then $f(H)$ is cyclic.

Remark 2. Let $f : G \to G'$ be a homomorphism and H be a subgroup of G. Then

1. If H is cyclic, then $f(H)$ is cyclic.
2. If H is abelian, then $f(H)$ is abelian.

Remark 2. Let $f : G \to G'$ be a homomorphism and H be a subgroup of G. Then

1. If H is cyclic, then $f(H)$ is cyclic.
2. If H is abelian, then $f(H)$ is abelian.
3. If H is normal in G, then $f(H)$ is normal in $f(G)$.

Exercise. Find all homomorphisms from C_{12} to C_{30}.

Remark 2. Let $f : G \to G'$ be a homomorphism and H be a subgroup of G. Then

1. If H is cyclic, then $f(H)$ is cyclic.
2. If H is abelian, then $f(H)$ is abelian.
3. If H is normal in G, then $f(H)$ is normal in $f(G)$.

Exercise. Find all homomorphisms from C_{12} to C_{30}.

Isomorphism. Let G and G' be two groups. G is said to be isomporphic to G' if the homomorphism between G and G' is also one-one and onto (bijective).

Remark 2. Let $f : G \to G'$ be a homomorphism and H be a subgroup of G. Then

1. If H is cyclic, then $f(H)$ is cyclic.
2. If H is abelian, then $f(H)$ is abelian.
3. If H is normal in G, then $f(H)$ is normal in $f(G)$.

Exercise. Find all homomorphisms from C_{12} to C_{30}.

Isomorphism. Let G and G' be two groups. G is said to be isomporphic to G' if the homomorphism between G and G' is also one-one and onto (bijective).

Theorem (First isomorphism theorem). Let $f : G \to G'$ be a surjective homomorphism with kernel K, Then

$$\frac{G}{K} \cong G'.$$

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Lemma. Any infinite cyclic group is isomorphic to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Lemma. Any infinite cyclic group is isomorphic to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Corollary. 1. Any two cyclic groups of the same order are isomorphic.

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Lemma. Any infinite cyclic group is isomorphic to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Corollary. 1. Any two cyclic groups of the same order are isomorphic.
2. For each prime p, there exists only one group (up to isomorphism) of order p, namely, the cyclic group of order p.

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Lemma. Any infinite cyclic group is isomorphic to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Corollary. 1. Any two cyclic groups of the same order are isomorphic.
2. For each prime p, there exists only one group (up to isomorphism) of order p, namely, the cyclic group of order p.

Theorem (Cayley's theorem). Every group is isomorphic to a group of permutations.

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Lemma. Any infinite cyclic group is isomorphic to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Corollary. 1. Any two cyclic groups of the same order are isomorphic.
2. For each prime p, there exists only one group (up to isomorphism) of order p, namely, the cyclic group of order p.

Theorem (Cayley's theorem). Every group is isomorphic to a group of permutations.

Automorphism. An isomorphism of G onto itself is called an automorphism of G.

Example. $U(10) \cong U(5)$ but $U(10) \ncong U(12)$.

Lemma. Any infinite cyclic group is isomorphic to $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Corollary. 1. Any two cyclic groups of the same order are isomorphic.
2. For each prime p, there exists only one group (up to isomorphism) of order p, namely, the cyclic group of order p.

Theorem (Cayley's theorem). Every group is isomorphic to a group of permutations.

Automorphism. An isomorphism of G onto itself is called an automorphism of G.

Lemma. 1. If G be infinte cycic group, then G has just one non-trivial automorphism.
2. If G is finite cyclic group, then G has $\phi(n)$ (Euler function) automorphisms.

Conjugate Classes.

Definition. Let G be a group, $a \in G$ and $b \in G$. Then b is said to be conjugate to a, if $b = xax^{-1}$ for some $x \in G$.

Conjugate Classes.

Definition. Let G be a group, $a \in G$ and $b \in G$. Then b is said to be conjugate to a, if $b = xax^{-1}$ for some $x \in G$.

Lemma. Let G be a group, and $\sim$ the relation in G given by $b \sim a$ if and only if b is conjugate to a. Then $\sim$ is an equivalence relation in G.[Hint: Reflexive, Symmetry and transitive.]

Conjugate Classes.

Definition. Let G be a group, $a \in G$ and $b \in G$. Then b is said to be conjugate to a, if $b = xax^{-1}$ for some $x \in G$.

Lemma. Let G be a group, and $\sim$ the relation in G given by $b \sim a$ if and only if b is conjugate to a. Then $\sim$ is an equivalence relation in G.[Hint: Reflexive, Symmetry and transitive.]

Definition. The equivalence classes under the relation $b \sim a$ iff $b = xax^{-1}$ for some $x \in G$, are called conjugate classes.

Conjugate Classes.

Definition. Let G be a group, $a \in G$ and $b \in G$. Then b is said to be conjugate to a, if $b = xax^{-1}$ for some $x \in G$.

Lemma. Let G be a group, and $\sim$ the relation in G given by $b \sim a$ if and only if b is conjugate to a. Then $\sim$ is an equivalence relation in G.[Hint: Reflexive, Symmetry and transitive.]

Definition. The equivalence classes under the relation $b \sim a$ iff $b = xax^{-1}$ for some $x \in G$, are called conjugate classes.

Notation. We denote $C(a) = \{g \cdot a \cdot g^{-1} | \text{for all } g \in G\}$, the conjugate class containing a.

Conjugate Classes.

Definition. Let G be a group, $a \in G$ and $b \in G$. Then b is said to be conjugate to a, if $b = xax^{-1}$ for some $x \in G$.

Lemma. Let G be a group, and $\sim$ the relation in G given by $b \sim a$ if and only if b is conjugate to a. Then $\sim$ is an equivalence relation in G.[Hint: Reflexive, Symmetry and transitive.]

Definition. The equivalence classes under the relation $b \sim a$ iff $b = xax^{-1}$ for some $x \in G$, are called conjugate classes.

Notation. We denote $C(a) = \{g \cdot a \cdot g^{-1} | \text{for all } g \in G\}$, the conjugate class containing a.

Lemma. Let G be a group. Then any two distinct conjugate classes have no common in common and G is the union (disjoint) of all its conjugate classes.

Lemma. Let G be a group and $a \in G$. Then $C(a) = \{a\}$ iff $a \in Z(G)$.

Lemma. Let G be a group and $a \in G$. Then $C(a) = \{a\}$ iff $a \in Z(G)$.

Lemma. Let G be a group and $a \in G$. Then the number (finite or infinite) of elements in the conjugate class $C(a)$ is equal to the index of the normaliser $N(a)$ of a in G.

Lemma. Let G be a group and $a \in G$. Then $C(a) = \{a\}$ iff $a \in Z(G)$.

Lemma. Let G be a group and $a \in G$. Then the number (finite or infinite) of elements in the conjugate class $C(a)$ is equal to the index of the normaliser $N(a)$ of a in G.

Class equation. Let G be a finite group. Then

$$|G| = \sum_{x \in G} |\text{ conjugacy class of } x| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|,$$

where the summation runs over the set of representatives of distinct nontrivial conjugate classes.

Lemma. Let G be a group and $a \in G$. Then $C(a) = \{a\}$ iff $a \in Z(G)$.

Lemma. Let G be a group and $a \in G$. Then the number (finite or infinite) of elements in the conjugate class $C(a)$ is equal to the index of the normaliser $N(a)$ of a in G.

Class equation. Let G be a finite group. Then

$$|G| = \sum_{x \in G} |\text{ conjugacy class of } x| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|,$$

where the summation runs over the set of representatives of distinct nontrivial conjugate classes.

Corollary. Any group of order p^n, with p prime number, has nontrivial center.

Lemma. Let G be a group and $a \in G$. Then $C(a) = \{a\}$ iff $a \in Z(G)$.

Lemma. Let G be a group and $a \in G$. Then the number (finite or infinite) of elements in the conjugate class $C(a)$ is equal to the index of the normaliser $N(a)$ of a in G.

Class equation. Let G be a finite group. Then

$$|G| = \sum_{x \in G} |\text{ conjugacy class of } x| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|,$$

where the summation runs over the set of representatives of distinct nontrivial conjugate classes.

Corollary. Any group of order p^n, with p prime number, has nontrivial center.

Corollary. Every group of order p^2, with p prime, is abelian.

Lemma. Let G be a group and $a \in G$. Then $C(a) = \{a\}$ iff $a \in Z(G)$.

Lemma. Let G be a group and $a \in G$. Then the number (finite or infinite) of elements in the conjugate class $C(a)$ is equal to the index of the normaliser $N(a)$ of a in G.

Class equation. Let G be a finite group. Then

$$|G| = \sum_{x \in G} |\text{ conjugacy class of } x| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|,$$

where the summation runs over the set of representatives of distinct nontrivial conjugate classes.

Corollary. Any group of order p^n, with p prime number, has nontrivial center.

Corollary. Every group of order p^2, with p prime, is abelian.

Theorem (Cauchy). If $|G| = n$ and $p|n$, with p prime, then G has an element of order p. (Exercise !)

Group action.

A group action of G on a set S is a map $G \times S \to S$ such that :
[1.] $e_G \cdot s = s$ for all $s \in S$, where e_G is the identity element of G.
[2.] $(g \cdot h) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$, $s \in S$.
S is called a G - set.

Group action.

A group action of G on a set S is a map $G \times S \to S$ such that :
[1.] $e_G \cdot s = s$ for all $s \in S$, where e_G is the identity element of G.
[2.] $(g \cdot h) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$, $s \in S$.
S is called a G - set.

Example. Take $S = G$ and define map $g \cdot h = ghg^{-1}$. Then this map is a group action of G on G.

Group action.

A group action of G on a set S is a map $G \times S \to S$ such that :
[1.] $e_G \cdot s = s$ for all $s \in S$, where e_G is the identity element of G.
[2.] $(g \cdot h) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$, $s \in S$.
S is called a G - set.

Example. Take $S = G$ and define map $g \cdot h = ghg^{-1}$. Then this map is a group action of G on G.

Orbit of a group. The orbit of $s \in S$ is defined to be the set of elements in S that s can be sent to by elements in G:

$$Os = \{s' | s' = g \cdot s \text{ for some g} \in G\}$$

Group action.

A group action of G on a set S is a map $G \times S \to S$ such that :
[1.] $e_G \cdot s = s$ for all $s \in S$, where e_G is the identity element of G.
[2.] $(g \cdot h) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$, $s \in S$.
S is called a G - set.

Example. Take $S = G$ and define map $g \cdot h = ghg^{-1}$. Then this map is a group action of G on G.

Orbit of a group. The orbit of $s \in S$ is defined to be the set of elements in S that s can be sent to by elements in G:

$$Os = \{s' | s' = g \cdot s \text{ for some g} \in G\}$$

Stabilizer of group. The stabilizer of is the subgroup of elements of G that leave s fixed:

$$S_G(s) = \{g \in G | g \cdot s = s\}$$

Group action.

A group action of G on a set S is a map $G \times S \to S$ such that :
[1.] $e_G \cdot s = s$ for all $s \in S$, where e_G is the identity element of G.
[2.] $(g \cdot h) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$, $s \in S$.
S is called a G - set.

Example. Take $S = G$ and define map $g \cdot h = ghg^{-1}$. Then this map is a group action of G on G.

Orbit of a group. The orbit of $s \in S$ is defined to be the set of elements in S that s can be sent to by elements in G:

$$Os = \{s' | s' = g \cdot s \text{ for some g} \in G\}$$

Stabilizer of group. The stabilizer of is the subgroup of elements of G that leave s fixed:

$$S_G(s) = \{g \in G | g \cdot s = s\}$$

Remark. $|G| = |S_G(s)| \cdot |Os|$ for $s \in S$, and G be group.

Direct Products

Definition. Let G be a group, H and K normal subroups of G such that $G = HK$ and $H \cap K = \{e\}$. Then G is called the direct product of H and K.

Direct Products

Definition. Let G be a group, H and K normal subroups of G such that $G = HK$ and $H \cap K = \{e\}$. Then G is called the direct product of H and K.

Examples.

1. Let G be a cyclic group of order 6 generated by a. Let $H = \{e, a, a^2\}$ and $K = \{e, a^3\}$ be subgroups of order 3 and 2 respectively. Clearly, $G = HK$, $H \cap K = \{e\}$ and H and K are normal in G. Hence, $G = H \times K$.

Direct Products

Definition. Let G be a group, H and K normal subroups of G such that $G = HK$ and $H \cap K = \{e\}$. Then G is called the direct product of H and K.

Examples.

1. Let G be a cyclic group of order 6 generated by a. Let $H = \{e, a, a^2\}$ and $K = \{e, a^3\}$ be subgroups of order 3 and 2 respectively. Clearly, $G = HK$, $H \cap K = \{e\}$ and H and K are normal in G. Hence, $G = H \times K$.
2. Let $G = \{e, a, b, c\}$ be Klein 4 group. Let $H = \{e, a\}$ and $K = \{e, b\}$. Then $G = HK$, $H \cap K = \{e\}$ and H and K are normal in G. Hence, $G = H \times K$. Thus G is a direct product of two cyclic groups, each of order 2.

Sylow Theorems.

First Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then G has a subgroup of order p^r. This subgroup is called Sylow p-subgroup of order p^r.

Sylow Theorems.

First Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then G has a subgroup of order p^r. This subgroup is called Sylow p-subgroup of order p^r.

Second Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then all Sylow p-subgroups are conjugate to each other.

Sylow Theorems.

First Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then G has a subgroup of order p^r. This subgroup is called Sylow p-subgroup of order p^r.

Second Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then all Sylow p-subgroups are conjugate to each other.

Third Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Let n_p denote the number of Sylow p-subgroups of G. Then :

(1) n_p divides $|G|$.

(2) $n_p = 1 + k \cdot p$ for $k \in \mathbb{N} \cup \{0\}$.

Sylow Theorems.

First Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then G has a subgroup of order p^r. This subgroup is called Sylow p-subgroup of order p^r.

Second Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Then all Sylow p-subgroups are conjugate to each other.

Third Theorem. Let G be a finite group with $|G| = \mathrm{p}^r \cdot m$ and $p \nmid m$; where p is a prime number. Let n_p denote the number of Sylow p-subgroups of G. Then :
(1) n_p divides $|G|$.
(2) $n_p = 1 + k \cdot p$ for $k \in \mathbb{N} \cup \{0\}$.

Corollary of Second Theorem. A Sylow p-subgroup is normal subgroup of G if and only if it is unique.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.
- Now assume that $p^k \nmid |H|$ for all proper subgroups H of G.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.
- Now assume that $p^k \nmid |H|$ for all proper subgroups H of G.
- Consider the class equation $|G| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|$ where $N(a) \neq G$.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.
- Now assume that $p^k \nmid |H|$ for all proper subgroups H of G.
- Consider the class equation $|G| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|$ where $N(a) \neq G$.
- Since p^k does not divide $|N(a)|$, for each term in the summation we have p divides $|G : N(a)|$.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.
- Now assume that $p^k \nmid |H|$ for all proper subgroups H of G.
- Consider the class equation $|G| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|$ where $N(a) \neq G$.
- Since p^k does not divide $|N(a)|$, for each term in the summation we have p divides $|G : N(a)|$.
- Hence p divides $|Z(G)|$. So by Cauchy theorem, $Z(G)$ has an element a of order p.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.
- Now assume that $p^k \nmid |H|$ for all proper subgroups H of G.
- Consider the class equation $|G| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|$ where $N(a) \neq G$.
- Since p^k does not divide $|N(a)|$, for each term in the summation we have p divides $|G : N(a)|$.
- Hence p divides $|Z(G)|$. So by Cauchy theorem, $Z(G)$ has an element a of order p.
- By induction, the quotient group $G/\langle a\rangle$ has a subgroup $K/\langle a\rangle$ of order p^{k-1}.

Proof of Sylow's First Theorem

- The proof is by induction on n. The theorem is clearly true for $n = 2$.
- Assume the theorem is true for all subgroups of order $< n$.
- If G has a proper subgroup H with p^k divides $|H|$, then by induction H will have a subgroup of order p^k which is also a subgroup of G.
- Now assume that $p^k \nmid |H|$ for all proper subgroups H of G.
- Consider the class equation $|G| = |Z(G)| + \sum_{|G:N(a)|>1} |G : N(a)|$ where $N(a) \neq G$.
- Since p^k does not divide $|N(a)|$, for each term in the summation we have p divides $|G : N(a)|$.
- Hence p divides $|Z(G)|$. So by Cauchy theorem, $Z(G)$ has an element a of order p.
- By induction, the quotient group $G/\langle a \rangle$ has a subgroup $K/\langle a \rangle$ of order p^{k-1}.
- Then K is the required subgroup of G of order p^k.

Example.

- Let $|G| = 147 = 7^2 \cdot 3$.

Example.

- Let $|G| = 147 = 7^2{\cdot}3$.
- By first Sylow theorem, G has subgroup of order 49 and 3.

Example.

- Let $|G| = 147 = 7^2 \cdot 3$.
- By first Sylow theorem, G has subgroup of order 49 and 3.
- Now we will see that subgroup of order 49 is normal in G by Sylow third theorem.

Example.

- Let $|G| = 147 = 7^2 \cdot 3$.
- By first Sylow theorem, G has subgroup of order 49 and 3.
- Now we will see that subgroup of order 49 is normal in G by Sylow third theorem.
- The Sylow 7-subgroup are $1 + 7 \cdot k$ which divides 3.
- So, possible value of k is only 0.

Example.

- Let $|G| = 147 = 7^2 \cdot 3$.
- By first Sylow theorem, G has subgroup of order 49 and 3.
- Now we will see that subgroup of order 49 is normal in G by Sylow third theorem.
- The Sylow 7-subgroup are $1 + 7 \cdot k$ which divides 3.
- So, possible value of k is only 0.
- Hence the Sylow 7-subgroup is only one. Hence, Sylow 7-subgroup of order 49 is normal.

Example.

- Let $|G| = 147 = 7^2 \cdot 3$.
- By first Sylow theorem, G has subgroup of order 49 and 3.
- Now we will see that subgroup of order 49 is normal in G by Sylow third theorem.
- The Sylow 7-subgroup are $1 + 7 \cdot k$ which divides 3.
- So, possible value of k is only 0.
- Hence the Sylow 7-subgroup is only one. Hence, Sylow 7-subgroup of order 49 is normal.

Lemma. Let G be a group of order pq, where p and q are primes, $p < q$. Then following hold.

- G has a unique Sylow q-subgroup.

Example.

- Let $|G| = 147 = 7^2 \cdot 3$.
- By first Sylow theorem, G has subgroup of order 49 and 3.
- Now we will see that subgroup of order 49 is normal in G by Sylow third theorem.
- The Sylow 7-subgroup are $1 + 7 \cdot k$ which divides 3.
- So, possible value of k is only 0.
- Hence the Sylow 7-subgroup is only one. Hence, Sylow 7-subgroup of order 49 is normal.

Lemma. Let G be a group of order pq, where p and q are primes, $p < q$. Then following hold.

- G has a unique Sylow q-subgroup.
- If $p \nmid (q-1)$, then G has a unique Sylow p-subgroup, and G is cyclic of order pq.

Proof of the Lemma.

- Let Q be a Sylow q-subgroup of G. The umber of Sylow q-subgroups is equal to $1 + tq$ $(t \geq 0)$ and this must divide the index p of Q in G. Since $q > p$, $t = 0$, i.e., Q is unique.

Proof of the Lemma.

- Let Q be a Sylow q-subgroup of G. The umber of Sylow q-subgroups is equal to $1 + tq$ $(t \geq 0)$ and this must divide the index p of Q in G. Since $q > p$, $t = 0$, i.e., Q is unique.
- Let P be a Sylow p-subgroup. The number of Sylow p-subgroups is equal to $1 + sp$ $(s \geq 0)$ and this must divide the index q of P in G. If $s > 0$, the fact that $1 + sp$ divides q implies that p divides $q - 1$. Hence $s = 0$ and P is unique.

Proof of the Lemma.

- Let Q be a Sylow q-subgroup of G. The umber of Sylow q-subgroups is equal to $1 + tq$ $(t \geq 0)$ and this must divide the index p of Q in G. Since $q > p$, $t = 0$, i.e., Q is unique.
- Let P be a Sylow p-subgroup. The number of Sylow p-subgroups is equal to $1 + sp$ $(s \geq 0)$ and this must divide the index q of P in G. If $s > 0$, the fact that $1 + sp$ divides q implies that p divides $q - 1$. Hence $s = 0$ and P is unique.

  Choose a unique p-Sylow subgroup P and a unique q-Sylow subgroup Q. Then $G = PQ$ and G is a direct product of cyclic subgroups P and Q of relatively prime orders. Hence G is cyclic.

Proof of the Lemma.

- Let Q be a Sylow q-subgroup of G. The umber of Sylow q-subgroups is equal to $1 + tq$ $(t \geq 0)$ and this must divide the index p of Q in G. Since $q > p$, $t = 0$, i.e., Q is unique.
- Let P be a Sylow p-subgroup. The number of Sylow p-subgroups is equal to $1 + sp$ $(s \geq 0)$ and this must divide the index q of P in G. If $s > 0$, the fact that $1 + sp$ divides q implies that p divides $q - 1$. Hence $s = 0$ and P is unique.
  Choose a unique p-Sylow subgroup P and a unique q-Sylow subgroup Q. Then $G = PQ$ and G is a direct product of cyclic subgroups P and Q of relatively prime orders. Hence G is cyclic.

Corollary. An abelian group is simple if and only if its order is prime.

Ring.

Definition. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if

(i) $(R, +)$ is a commutative group,

Ring.

Definition. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if

(i) $(R, +)$ is a commutative group,

(ii) Multiplication is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for every $a, b, c \in R$,

Ring.

Definition. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if

(i) $(R, +)$ is a commutative group,

(ii) Multiplication is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for every $a, b, c \in R$,

(iii) Distributive laws hold: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for every $a, b, c \in R$.

Ring.

Definition. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if

(i) $(R, +)$ is a commutative group,

(ii) Multiplication is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for every $a, b, c \in R$,

(iii) Distributive laws hold: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for every $a, b, c \in R$.

Definition. R is called a ring with unit element if there exists an element $e \in R$ such that $ae = a = ea$ for all $a \in R$.

Ring.

Definition. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if

(i) $(R, +)$ is a commutative group,

(ii) Multiplication is associative, i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for every $a, b, c \in R$,

(iii) Distributive laws hold: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for every $a, b, c \in R$.

Definition. R is called a ring with unit element if there exists an element $e \in R$ such that $ae = a = ea$ for all $a \in R$.

Definition. R is said to be a commutative ring if $ab = ba$ for all $a \in R$ and $b \in R$.

Examples.

(i) $R = \mathbb{Z}$, the ring of integers, is a ring for the usual addition and multiplication. It has 1 as unit element, and is commutative.

Examples.

(i) $R = \mathbb{Z}$, the ring of integers, is a ring for the usual addition and multiplication. It has 1 as unit element, and is commutative.

(ii) $R = 2\mathbb{Z}$, the ring of even integers, is a ring for the usual addition and multiplication. It has no unit element, but is commutative.

Examples.

(i) $R = \mathbb{Z}$, the ring of integers, is a ring for the usual addition and multiplication. It has 1 as unit element, and is commutative.

(ii) $R = 2\mathbb{Z}$, the ring of even integers, is a ring for the usual addition and multiplication. It has no unit element, but is commutative.

(iii) Consider $R = \mathbb{Z}_n$, the additive abelian group of residue classes modulo n. It is a commutative ring with $\bar{1}$ as unit element.

Examples.

(i) $R = \mathbb{Z}$, the ring of integers, is a ring for the usual addition and multiplication. It has 1 as unit element, and is commutative.

(ii) $R = 2\mathbb{Z}$, the ring of even integers, is a ring for the usual addition and multiplication. It has no unit element, but is commutative.

(iii) Consider $R = \mathbb{Z}_n$, the additive abelian group of residue classes modulo n. It is a commutative ring with $\bar{1}$ as unit element.

(iv) Let R be the set of all 2×2 matrices with real entries. Then under usual addition and multiplication of matrices, R is a ring with identity element as identity matrix. It is non-commutative.

Examples.

(i) $R = \mathbb{Z}$, the ring of integers, is a ring for the usual addition and multiplication. It has 1 as unit element, and is commutative.

(ii) $R = 2\mathbb{Z}$, the ring of even integers, is a ring for the usual addition and multiplication. It has no unit element, but is commutative.

(iii) Consider $R = \mathbb{Z}_n$, the additive abelian group of residue classes modulo n. It is a commutative ring with $\bar{1}$ as unit element.

(iv) Let R be the set of all 2×2 matrices with real entries. Then under usual addition and multiplication of matrices, R is a ring with identity element as identity matrix. It is non-commutative.

(v) $R = \{a + \sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a ring for the usual addition and multiplication of complex numbers. It is a commutative ring with unit element $1 = 1 + 0\sqrt{5}$.

Integral domain.

Definition. Let R be a ring and $a \in R, b \in R$, both being non-zero. Then a is called a (left) zero divisor if $ab = 0$. We also say that b is a (right) zero divisor.

Integral domain.

Definition. Let R be a ring and $a \in R, b \in R$, both being non-zero. Then a is called a (left) zero divisor if $ab = 0$. We also say that b is a (right) zero divisor.

Note. A zero divisor is a non-zero element (by definition).

Integral domain.

Definition. Let R be a ring and $a \in R, b \in R$, both being non-zero. Then a is called a (left) zero divisor if $ab = 0$. We also say that b is a (right) zero divisor.

Note. A zero divisor is a non-zero element (by definition).

Definition. A commutative ring which has no zero divisors is called an integral domain.

Integral domain.

Definition. Let R be a ring and $a \in R, b \in R$, both being non-zero. Then a is called a (left) zero divisor if $ab = 0$. We also say that b is a (right) zero divisor.

Note. A zero divisor is a non-zero element (by definition).

Definition. A commutative ring which has no zero divisors is called an integral domain.

Examples.

- The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains.
- $\mathbb{Z}_5$, the ring of residue classes modulo 5, is an integral domain.

Integral domain.

Definition. Let R be a ring and $a \in R, b \in R$, both being non-zero. Then a is called a (left) zero divisor if $ab = 0$. We also say that b is a (right) zero divisor.

Note. A zero divisor is a non-zero element (by definition).

Definition. A commutative ring which has no zero divisors is called an integral domain.

Examples.

- The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains.
- $\mathbb{Z}_5$, the ring of residue classes modulo 5, is an integral domain.
- $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

Integral domain.

Definition. Let R be a ring and $a \in R, b \in R$, both being non-zero. Then a is called a (left) zero divisor if $ab = 0$. We also say that b is a (right) zero divisor.

Note. A zero divisor is a non-zero element (by definition).

Definition. A commutative ring which has no zero divisors is called an integral domain.

Examples.

- The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains.
- $\mathbb{Z}_5$, the ring of residue classes modulo 5, is an integral domain.
- $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is an integral domain.
- $\mathbb{Z}_4$ is not an integral domain, as $\bar{2} \cdot \bar{2} = \bar{0}$ in $\mathbb{Z}_4$.

Field.

Definition. A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

Field.

Definition. A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

Field.

Definition. A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.
- $R = \mathbb{Z}_p$ is a field.

Field.

Definition. A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.
- $R = \mathbb{Z}_p$ is a field.
- $\mathbb{Z}_n$ is not a field if n is not prime.

Definition. Let R be a ring. The characteristic of R is the smallest positive integer n, if it exists, such that $na = 0$ for all $a \in R$. If no such integer exists, then the characteristic of R is said to be zero.

Field.

Definition. A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.
- $R = \mathbb{Z}_p$ is a field.
- $\mathbb{Z}_n$ is not a field if n is not prime.

Definition. Let R be a ring. The characteristic of R is the smallest positive integer n, if it exists, such that $na = 0$ for all $a \in R$. If no such integer exists, then the characteristic of R is said to be zero.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic *zero*.

Field.

Definition. A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a field.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.
- $R = \mathbb{Z}_p$ is a field.
- $\mathbb{Z}_n$ is not a field if n is not prime.

Definition. Let R be a ring. The characteristic of R is the smallest positive integer n, if it exists, such that $na = 0$ for all $a \in R$. If no such integer exists, then the characteristic of R is said to be zero.

Examples.

- The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic *zero*.
- $R = \mathbb{Z}_p$ has characteristic p.

Homomorphism.

Definition. Let R and R' be two rings. A mapping $f : R \to R'$ is a homomorphism if it satisfies (i) $f(a+b) = f(a) + f(b)$, $a, b \in R$ (ii) $f(ab) = f(a)f(b), a, b \in R$.

Homomorphism.

Definition. Let R and R' be two rings. A mapping $f : R \to R'$ is a homomorphism if it satisfies (i) $f(a+b) = f(a) + f(b)$, $a, b \in R$ (ii) $f(ab) = f(a)f(b), a, b \in R$.

Note. If R and R' have unit elements e and e' respectively, we stipulate further that $f(e) = e'$.

Homomorphism.

Definition. Let R and R' be two rings. A mapping $f : R \to R'$ is a homomorphism if it satisfies (i) $f(a+b) = f(a) + f(b)$, $a, b \in R$ (ii) $f(ab) = f(a)f(b), a, b \in R$.

Note. If R and R' have unit elements e and e' respectively, we stipulate further that $f(e) = e'$.

Examples.

- Let $R = \mathbb{Z}$ and $R' = Z_n$. The mapping $f : R \to R'$ given by $f(i) = \bar{i}$, is a ring homomorphism, because $f(i+j) = \overline{i+j} = \bar{i} + \bar{j} = f(i) + f(j)$ and $f(ij) = \bar{ij} = \bar{i}\bar{j} = f(i)f(j)$.. Moreover $f(1) = \bar{1}$.

Homomorphism.

Definition. Let R and R' be two rings. A mapping $f : R \to R'$ is a homomorphism if it satisfies (i) $f(a+b) = f(a) + f(b)$, $a, b \in R$ (ii) $f(ab) = f(a)f(b), a, b \in R$.

Note. If R and R' have unit elements e and e' respectively, we stipulate further that $f(e) = e'$.

Examples.

- Let $R = \mathbb{Z}$ and $R' = Z_n$. The mapping $f : R \to R'$ given by $f(i) = \bar{i}$, is a ring homomorphism, because $f(i+j) = \overline{i+j} = \bar{i} + \bar{j} = f(i) + f(j)$ and $f(ij) = \overline{ij} = \overline{ij} = f(i)f(j)$.. Moreover $f(1) = \bar{1}$.
- If $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ and $f : R \to R'$ is defined by $f(a + b\sqrt{-5}) = a - b\sqrt{-5}$, then f is a ring homomorphism.

Kernel of f. Let $f : R \to R'$ be a homomorphism of rings. Then the kernel of $f = \{a \in R \mid f(a) = 0\}$.

Kernel of f. Let $f : R \to R'$ be a homomorphism of rings. Then the kernel of $f = \{a \in R \mid f(a) = 0\}$.

Lemma. Let $f : R \to R'$ be a homomorphism of rings. Then f is one-one mapping iff $\text{Ker}(f) = 0$.

Kernel of f. Let $f : R \to R'$ be a homomorphism of rings. Then the kernel of $f = \{a \in R \mid f(a) = 0\}$.

Lemma. Let $f : R \to R'$ be a homomorphism of rings. Then f is one-one mapping iff $\text{Ker}(f) = 0$.

Definition. Let R be a ring and $S \subset R$. S be called a subring of R if (i) S is a subgroup of the abelian group R, i.e., $a - b \in S$ whenever $a \in S$ and $b \in S$, (ii) S is closed for multiplication, i.e., $ab \in S$ whenever $a \in S$ and $b \in S$.

Kernel of f. Let $f : R \to R'$ be a homomorphism of rings. Then the kernel of $f = \{a \in R \mid f(a) = 0\}$.

Lemma. Let $f : R \to R'$ be a homomorphism of rings. Then f is one-one mapping iff $\mathrm{Ker}(f) = 0$.

Definition. Let R be a ring and $S \subset R$. S be called a subring of R if (i) S is a subgroup of the abelian group R, i.e., $a - b \in S$ whenever $a \in S$ and $b \in S$, (ii) S is closed for multiplication, i.e., $ab \in S$ whenever $a \in S$ and $b \in S$.

Example. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

Kernel of f. Let $f : R \to R'$ be a homomorphism of rings. Then the kernel of $f = \{a \in R \mid f(a) = 0\}$.

Lemma. Let $f : R \to R'$ be a homomorphism of rings. Then f is one-one mapping iff $\text{Ker}(f) = 0$.

Definition. Let R be a ring and $S \subset R$. S be called a subring of R if (i) S is a subgroup of the abelian group R, i.e., $a - b \in S$ whenever $a \in S$ and $b \in S$, (ii) S is closed for multiplication, i.e., $ab \in S$ whenever $a \in S$ and $b \in S$.

Example. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

Lemma. Let $f : R \to R'$ be a homomorphism of rings. Then $\text{Ker}(f)$ is a subring of R and $f(R) = \{f(a) \mid a \in R\}$ is a subring of R'.

Isomorphism

Definition. Let R and R' be rings. A mapping $f : R \to R'$ is called an isomorphism if (i) f is a homomorphism, (ii) f is one-one and onto.

Isomorphism

Definition. Let R and R' be rings. A mapping $f : R \to R'$ is called an isomorphism if (i) f is a homomorphism, (ii) f is one-one and onto.

Examples.

- Let $f : \mathbb{C} \to \mathbb{C}$ be a map given by $f(z) = \bar{z}$, where $\bar{z}$ is the complex conjugate of z. Then f is ring isomorphism.

Isomorphism

Definition. Let R and R' be rings. A mapping $f : R \to R'$ is called an isomorphism if (i) f is a homomorphism, (ii) f is one-one and onto.

Examples.

- Let $f : \mathbb{C} \to \mathbb{C}$ be a map given by $f(z) = \bar{z}$, where $\bar{z}$ is the complex conjugate of z. Then f is ring isomorphism.
- The only isomorphism of $\mathbb{Q}$ onto $\mathbb{Q}$ is the identity mapping $I_{\mathbb{Q}}$. [Hint: Prove $f(n) = n$ for all $n \in \mathbb{Z}$ and then show that $bf(a/b) = a$.]
- Rings $\mathbb{Z}$ and $2\mathbb{Z}$ are not isomorphic.

Ideals.

Definition. Let R be a ring and $I \subset R$. Then I is called an ideal if

Ideals.

Definition. Let R be a ring and $I \subset R$. Then I is called an ideal if

- I is an additive subgroup of R, i.e., $a - b \in I$ whenever $a \in I$ and $b \in I$.

Ideals.

Definition. Let R be a ring and $I \subset R$. Then I is called an ideal if

- I is an additive subgroup of R, i.e., $a - b \in I$ whenever $a \in I$ and $b \in I$.
- For any $a \in I$, $x \in R$ we have both $xa \in I$ and $ax \in I$.

Note. It is clear by definition that every ideal is a subring but a subring may not be ideal. For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not an ideal.

Ideals.

Definition. Let R be a ring and $I \subset R$. Then I is called an ideal if

- I is an additive subgroup of R, i.e., $a - b \in I$ whenever $a \in I$ and $b \in I$.
- For any $a \in I$, $x \in R$ we have both $xa \in I$ and $ax \in I$.

Note. It is clear by definition that every ideal is a subring but a subring may not be ideal. For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not an ideal.

Definition. For any ring, $\{0\}$ and R are ideals in R. These are called improper ideals and any other ideal is called a proper ideal.

Ideals.

Definition. Let R be a ring and $I \subset R$. Then I is called an ideal if

- I is an additive subgroup of R, i.e., $a - b \in I$ whenever $a \in I$ and $b \in I$.
- For any $a \in I$, $x \in R$ we have both $xa \in I$ and $ax \in I$.

Note. It is clear by definition that every ideal is a subring but a subring may not be ideal. For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not an ideal.

Definition. For any ring, $\{0\}$ and R are ideals in R. These are called improper ideals and any other ideal is called a proper ideal.

Examples.

- $I = m\mathbb{Z}$, $m \geq 0$, is an ideal of $\mathbb{Z}$.
- $I = \{\bar{0}, \bar{3}\}$ is an ideal of $\mathbb{Z}_6$.

Lemma. Let $f : R \to R'$ be a homomorphism of R in R'. Then $K = \text{Ker}(f)$ is an ideal in R.

Lemma. Let $f : R \to R'$ be a homomorphism of R in R'. Then $K = \text{Ker}(f)$ is an ideal in R.

Definition. A ring R with nontrivial multiplication is called a simple ring if it has no proper ideals.

Lemma. Let $f : R \to R'$ be a homomorphism of R in R'. Then $K = \text{Ker}(f)$ is an ideal in R.

Definition. A ring R with nontrivial multiplication is called a simple ring if it has no proper ideals.

Lemma. Any field is a simple ring. Conversely, let R be a commutative ring with identity which is a simple ring, then R is a field.

Lemma. Let $f : R \to R'$ be a homomorphism of R in R'. Then $K = \text{Ker}(f)$ is an ideal in R.

Definition. A ring R with nontrivial multiplication is called a simple ring if it has no proper ideals.

Lemma. Any field is a simple ring. Conversely, let R be a commutative ring with identity which is a simple ring, then R is a field.

Definitions. Let R be a ring and $I \subset R$. I is called a left (right) ideal of R if (i) I is an abelian subgroup of R, i.e., $a - b \in I$ whenever $a, b \in I$, (ii) For each $a \in I$ and $x \in R$, $xa \in I$ (respectively $ax \in I$).

Lemma. Let $f : R \to R'$ be a homomorphism of R in R'. Then $K = \text{Ker}(f)$ is an ideal in R.

Definition. A ring R with nontrivial multiplication is called a simple ring if it has no proper ideals.

Lemma. Any field is a simple ring. Conversely, let R be a commutative ring with identity which is a simple ring, then R is a field.

Definitions. Let R be a ring and $I \subset R$. I is called a left (right) ideal of R if (i) I is an abelian subgroup of R, i.e., $a - b \in I$ whenever $a, b \in I$, (ii) For each $a \in I$ and $x \in R$, $xa \in I$ (respectively $ax \in I$).

Note. Any ideal (two-sided) is both left and right ideal, and in a commutative ring any left (right) ideal is an ideal.

Definition. Let I and J be ideals in R. We define the sum and product as

$$I + J = \{a + b \mid a \in I, b \in I\}; \; IJ = \{\sum_{i=1}^{m} a_i b_i \mid a_i \in I, b_i \in J, m \text{ arbitrary}\}.$$

Definition. Let I and J be ideals in R. We define the sum and product as

$$I + J = \{a + b \mid a \in I, b \in I\}; IJ = \{\sum_{i=1}^{m} a_i b_i \mid a_i \in I, b_i \in J, m \text{ arbitrary}\}.$$

Lemma. For any ideals I and J, the sum $I + J$ and the product IJ are ideals in R.

Quotient ring. Let R be a ring and I be an ideal in R. The ring R/I with addition and multiplication defined as

$(a + I) + (b + I) = (a + b) + I,\ (a + I)(b + I) = ab + I$

is called the quotient ring of R by the ideal I.

Definition. Let I and J be ideals in R. We define the sum and product as

$$I + J = \{a + b \mid a \in I, b \in I\}; IJ = \{\sum_{i=1}^{m} a_i b_i \mid a_i \in I, b_i \in J, m \text{ arbitrary}\}.$$

Lemma. For any ideals I and J, the sum $I + J$ and the product IJ are ideals in R.

Quotient ring. Let R be a ring and I be an ideal in R. The ring R/I with addition and multiplication defined as

$(a + I) + (b + I) = (a + b) + I, \; (a + I)(b + I) = ab + I$

is called the quotient ring of R by the ideal I.

Examples.

- Let $R = \mathbb{Z}$, $I = n\mathbb{Z}, n > 0$, then the quotient ring R/I is the ring $\mathbb{Z}_n$ of residue classes modulo n.

Definition. Let I and J be ideals in R. We define the sum and product as

$$I+J=\{a+b \mid a\in I, b\in I\};\ IJ=\{\sum_{i=1}^{m} a_i b_i \mid a_i\in I, b_i\in J, m \text{ arbitrary}\}.$$

Lemma. For any ideals I and J, the sum $I+J$ and the product IJ are ideals in R.

Quotient ring. Let R be a ring and I be an ideal in R. The ring R/I with addition and multiplication defined as

$(a+I)+(b+I)=(a+b)+I,\ (a+I)(b+I)=ab+I$

is called the quotient ring of R by the ideal I.

Examples.

- Let $R=\mathbb{Z}$, $I=n\mathbb{Z}, n>0$, then the quotient ring R/I is the ring $\mathbb{Z}_n$ of residue classes modulo n.
- Let $R=\mathbb{Z}_6$ and $I=\{\bar{0},\bar{2},\bar{4}\}$. Then R/I is a ring with two elements $\bar{0}+I$ and $\bar{1}+I$.

Definition. Let I and J be ideals in R. We define the sum and product as

$$I+J=\{a+b \mid a\in I, b\in I\};\ IJ=\{\sum_{i=1}^{m} a_i b_i \mid a_i\in I, b_i\in J, m \text{ arbitrary}\}.$$

Lemma. For any ideals I and J, the sum $I+J$ and the product IJ are ideals in R.

Quotient ring. Let R be a ring and I be an ideal in R. The ring R/I with addition and multiplication defined as

$(a+I)+(b+I)=(a+b)+I,\ (a+I)(b+I)=ab+I$

is called the quotient ring of R by the ideal I.

Examples.

- Let $R=\mathbb{Z}$, $I=n\mathbb{Z}, n>0$, then the quotient ring R/I is the ring $\mathbb{Z}_n$ of residue classes modulo n.
- Let $R=\mathbb{Z}_6$ and $I=\{\bar{0},\bar{2},\bar{4}\}$. Then R/I is a ring with two elements $\bar{0}+I$ and $\bar{1}+I$.
- For any ring R, $R/I=R$ when $I=0$. Similarly R/R is the zero ring.

First Isomorphism Theorem. Let $f : R \to R'$ be a homomorphism of R onto R' and $I = \text{Ker}(f)$. Then I is an ideal in R, and $R/I \cong R'$.

First Isomorphism Theorem. Let $f : R \to R'$ be a homomorphism of R onto R' and $I =$Ker(f). Then I is an ideal in R, and $R/I \cong R'$.

Prime ideal. An ideal P in a ring R is said to be a prime ideal if whenever $ab \in P$, then either $a \in P$ or $b \in P$, $P \neq R$.

First Isomorphism Theorem. Let $f : R \to R'$ be a homomorphism of R onto R' and $I =$Ker(f). Then I is an ideal in R, and $R/I \cong R'$.

Prime ideal. An ideal P in a ring R is said to be a prime ideal if whenever $ab \in P$, then either $a \in P$ or $b \in P$, $P \neq R$.

Examples.

- Let $R = \mathbb{Z}$, $I = p\mathbb{Z}$ with p prime, then I is a prime ideal because if $ab \in I$, then $ab = pk$ for some $k \in \mathbb{Z}$, i.e., p divides ab. Since p is prime, we have p divides a or p divides b, i.e., $a \in p\mathbb{Z}$ or $b \in \mathbb{Z}$.

First Isomorphism Theorem. Let $f : R \to R'$ be a homomorphism of R onto R' and $I = \text{Ker}(f)$. Then I is an ideal in R, and $R/I \cong R'$.

Prime ideal. An ideal P in a ring R is said to be a prime ideal if whenever $ab \in P$, then either $a \in P$ or $b \in P$, $P \neq R$.

Examples.

- Let $R = \mathbb{Z}$, $I = p\mathbb{Z}$ with p prime, then I is a prime ideal because if $ab \in I$, then $ab = pk$ for some $k \in \mathbb{Z}$, i.e., p divides ab. Since p is prime, we have p divides a or p divides b, i.e., $a \in p\mathbb{Z}$ or $b \in \mathbb{Z}$.
- If R is an integral domain, $P = \{0\}$ is a prime ideal in R for if $ab \in P = \{0\}$, then $ab = 0$. This implies that $a = 0$ or $b = 0$, i.e., $a \in P$ or $b \in P$.

Lemma. P is a prime ideal of $\mathbb{Z}$ if and only if either $P = 0$ or $P = p\mathbb{Z}$ for some prime p.

Lemma. An ideal P in R is a prime ideal if and only if R/P is an integral domain.

Proof.

- Suppose P is a prime ideal, and let $\bar{a}\bar{b} = \bar{0}$ in R/P, i.e., $(a+P)(b+P) = P$. Then $ab + P = P$, i.e., $ab \in P$. Since P is a prime ideal, $a \in P$ or $b \in P$, i.e., $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Hence R/P is an integral domain.
- Conversely, let R/P be an integral domain and let $ab \in P$. Then

$$ab + P = P, \text{ i.e., } (a+P)(b+P) = P, \text{ i.e., } \bar{a}\bar{b} = \bar{0}.$$

Since R/P is an integral domain, we have $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, i.e., $a \in P$ or $b \in P$, showing that P is a prime ideal.

Maximal ideal. An ideal M in a ring R is said to be a maximal ideal if $M \neq R$, and if for any ideal I of R such that $M \subset I \subset R$, we have $I = M$ or $I = R$.

Examples.

- Let $R = \mathbb{Z}$, $M = p\mathbb{Z}$ with p prime, then M is a maximal ideal of R. Let I be any ideal containing M. Then $I = m\mathbb{Z}$ and since $M \subset I$, $p \in I$, i.e., $p = mk$ for some k. This implies that m divides p, and since p is prime $m = 1$ or $m = p$, i.e., $I = R$ or $I = M$. Thus M is maximal.
- If R is a field, then $M = \{0\}$ is a maximal ideal in R because the only ideals in R are $\{0\}$ and R. Hence no ideal of R except R properly contains $\{0\}$.

Exercise. M is maximal ideal of $\mathbb{Z}$ if and only if $M = p\mathbb{Z}$ for some prime p.

Lemma. Let R be a commutative ring with identity. An ideal M is a maximal ideal if and only if R/M is a field.

Proof.

- R/M is a commutative ring with 1. We know that R/M is field iff it has no proper ideals. Assume that R/M is field and let $M \subset J$ be any ideal. Then J/M is an ideal of R/M. Since R/M is field, we have $J/M = R/M$ or $\{\bar{0}\}$, i.e., $J = R$ or $J = J = M$. Hence M is a maximal ideal of R.
- Conversely, let M is maximal ideal and $\bar{J}$be any ideal of R/M. Then $\bar{J} = J/M$ where J is an ideal containing M. Since M is maximal, we have $J = M$ or $J = R$. Hence R/M is a field.

Corollary. Let R be a commutative ring with 1. Then every maximal idea in R is prime ideal. Converse is not true.

Proof. M is maximal, then R/M is field and hence an integral domain. So M is prime ideal. Converse example: $R = \mathbb{Z}$, $I = 0$.

Chinese Remainder Theorem.

Theorem. Let $I_1, \ldots, I_m$ be ideals of a commutative ring R with identity such that $I_i + I_j = R$ for $i \neq j, 1 \leq i, j \leq m$. Then given $x_1, \ldots, x_m$ in R, there exists $x \in R$ such that $x \equiv x_j \pmod{I_j}$ for $1 \leq j \leq m$.

Proof.

- Observe that given two ideals A and B of R with $A + B = R$, there exists y belonging to R such that $y \equiv 1 \pmod{A}$ and $y \equiv 0 \pmod{B}$, because on writing 1 as $a + b$ with $a \in A$ and $b \in B$, it is clear that $y = b$ works.

Proof Contd..

- Fix any j, $1 \le j \le m$ and set $I_j^* = \prod_{i=1, i\neq j}^{m} I_i$.
- By hypothesis, $I_i + I_j = R$ if $i \neq j$. This shows that $\prod_{i=1, i\neq j}^{m} (I_i + I_j) = R$.
- So the ideal $I_j^* + I_j$ which contains $\prod_{i=1, i\neq j}^{m} (I_i + I_j)$ equals R.
- In view of what has been said in the above paragraph, there exists $y_j \in R$ such that $y_j \equiv 1 \pmod{I_j}$, $y_j \equiv 0 \pmod{I_j^*}$, $1 \le j \le m$.
- Take $x = x_1 y_1 + \ldots + x_m y_m$. Then $x \equiv x_j \pmod{I_j}$ for $1 \le j \le m$.

Corollary. Given distinct prime $p_1, p_2, \cdots, p_k$ and integers $a_1, a_2, \cdots, a_k$, there exists an integer a such that $a \equiv a_i$ (mod p_i), $1 \le i \le k$.

Factorisation.

Definition. Let $a \in R$ and $b \in R$, $a \neq 0$. a is said to divide b if there exists $c \in R$ such that $b = ac$.
We use notation $a|b$ to indicate that a divides b.

Example.

- In $R = \mathbb{Z}$, 3 divides 15.
- In $R = \mathbb{Z} + \iota\mathbb{Z} = \{a + \iota b \mid a, b \in \mathbb{Z}\}$, $(1 + 3\iota)$ divides 10 as $10 = (1 + 3\iota)(1 - 3\iota)$.

Lemma. Let a, b be non-zero elements of R. If $a|b$ and $b|a$, then $b = au$ for some unit u in R, and conversely.

Definition. Two non-zero elements a and b are said to be associates of each other if $a|b$ and $b|a$.

Note: In view of above lemma, two elements are said to be associates iff they differ by a unit, i.e., $b = au$, for some unit u in R.

Example.

- In $R = \mathbb{Z}$, 5 and -5 are associates as $-5 = (-1) \cdot 5$.
- In $R = \mathbb{Z} + \iota\mathbb{Z} = \{a + \iota b \mid a, b \in \mathbb{Z}\}$, $1 + \sqrt{2}\iota$ and $\sqrt{2} - \iota$ are associates as $\sqrt{2} - \iota = (-\iota)(1 + \sqrt{2}\iota)$ and $-\iota$ is a unit in R.

Definition. $a \in R$ is called an irreducible element if

(i) a is not a unit,

(ii) the only divisors of a are units and associates of a.

Example.

- In $R = \mathbb{Z}$, $n \in \mathbb{Z}$, $n > 1$. Then n is irreducible iff the only divisors of n are ± 1 (units) and $\pm n$ (associates of n). Thus n is a prime integer.
- In $R = \{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\}$. Then $1 + 2\sqrt{-5}$ is an irreducible element of R. Check that only units of R are ± 1.
  Suppose now that $1 + 2\sqrt{-5} = \alpha\beta$, $\alpha, \beta \in R$. Then $N(1 + 2\sqrt{-5}) = N(\alpha)N(\beta)$, i.e., $N(\alpha)N(\beta) = 21$. Hence $N(\alpha) = 1, 3, 7$ or 21. If $\alpha = a + \sqrt{-5}b$, then $N(\alpha) = a^2 + 5b^2$. Hence $N(\alpha) = 3$ or 7 is impossible. Hence either $N(\alpha) = 1$ or $N(\beta) = 1$. So, either α or β is unit, showing that $1 + 2\sqrt{-5}$ is irreducible.

Definition. Let $p \in R$ which is not a unit, p is called a prime element if it has the property that whenever $p|ab$, we have that $p|a$ or $p|b$.

Lemma. Every prime element is irreducible.

Proof (Sketch). Suppose p is prime, and let a be any divisor of p so that $p = ab$. Now $p|p(= ab)$. Since p is prime, $p|a$ or $p|b$. Let (wlog) that $p|a$. Since $a|p$, we have a is an associate pf p and b is unit.

Example. Let $R = \{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\}$. Then $1 + 2\sqrt{-5}$ is an irreducible element of R but it is not a prime element, because $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 21$, $1 + 2\sqrt{-5}$ divides $21 = 3 \cdot 7$, but it does not divide either 3 or 7 as $N(1 + 2\sqrt{-5}) = 21$ whereas $N(3) = 9$ and $N(7) = 49$, and 21 does not divide 9 or 49.

Lemma. An element $p \in R$ is prime iff the ideal $P = Rp = \{xp \mid x \in R\}$ is a prime ideal.

Proof. Suppose p is a prime element, and let $ab \in P$. Then $ab \in P$. Then $ab = cp$ for some $c \in R$, i.e., $p|ab$. Since P is a prime, $p|a$ or $p|b$, i.e., $a \in P$ or $b \in P$. Hence P is a prime ideal.
Conversely, let P be a prime ideal and let $p|ab$. Then $ab = cp \in P$ and since P is a prime ideal, $a \in P$ or $b \in P$, i.e., $p|a$ or $p|b$. Hence p is a prime element.

Definition. Let $a \in R$ and $b \in R$. An element $d \in R$ is called a greatest common divisor (gcd) of a and b if

- $d|a$ and $d|b$.
- whenever $d'|a$ and $d'|b$, then $d'|d$.

Example.

- In $R = \mathbb{Z}$, if $a = 9$ and $b = -48$, then $d = 3$ is a gcd of a, b.

- Let $R = \{a + \sqrt{-5}b \mid a, b \in \mathbb{Z}\}$. Let $\alpha = 1 + 2\sqrt{-5}$ and $\beta = 3$. Any common divisor of α and β must have a norm which divides $N(\alpha) = 21$ and $N(\beta) = 9$, i.e., it must have norm 1 or 3. Since no element can have norm 3, the gcd has the norm 1, i.e., it must be a unit. Since a unit always divides α and β, the gcd of α and β is a unit.

Definition. If $a, b \in R$, then a and b are said to be relatively prime if there gcd is a unit.

Euclidean Domain.

Definition. A Euclidean domain is a commutative integral domain R in which there exists an integer valued function d on the non-zero elements of R, satisfying the following conditions.

(i) $d(a) \geq 0$ for all non-zero $a \in R$.

(ii) $d(ab) \geq d(a)$, $a, b \in R$.

(iii) For $a, b \in R$, $b \neq 0$, there exists $q', r \in R$ such that $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.

Example.

- In $R = \mathbb{Z}$, if $d(a) = |a|$, then d satisfies all conditions $(i), (ii)$ and (iii). Conditions (iii) is the usual division algorithm property in $\mathbb{Z}$.
- Let $R = \mathbb{Z} + \iota\mathbb{Z} = \{m + \iota n \mid m, n \in \mathbb{Z}\}$ be the ring of Gaussian integers. If $a \in R$, $a = m + \iota n$, define $d(a) = |a|^2 = m^2 + n^2$. Then check that R is a Euclidean domain.

Lemma. Let R be a Euclidean domain. Every ideal I of R is of the form $I = Ra$ for some $a \in R$.

Proof. If $I = 0$, then we can take $a = 0$.

- If $I \neq 0$, then choose $a \in I$, $a \neq 0$ such that $d(a)$ has a least value.
- We shall show that $I = Ra$.
- Clearly since $a \in I$, $Ra \subset I$.
- Now if $b \in I$, then by condition (iii) of definition, there exist $q, r \in R$ such that $b = aq + r$, either $r = 0$ or $d(r) < d(a)$.
- Now $r = b - aq \in I$ as $a, b \in I$ and I is an ideal.
- By the choice of a, $d(r) < d(a)$ is impossible and hence $r = 0$.
- This impies that $b = aq \in Ra$ proving that $I = Ra$.

Principal ideal domain.

Definition. An ideal I in a commutative ring R is called a principal ideal if there exists some $a \in R$ such that $I = Ra$.
We use the notation $\langle a \rangle$ to denote the ideal Ra.

Definition. An integral domain R is called principal ideal domain if every ideal in R is a principal ideal.

Remark. Every Euclidean domain is a principal ideal domain (in view of the last lemma).

- Hence, $\mathbb{Z}$ or $\mathbb{Z} + \iota\mathbb{Z}$ are examples of principal ideal domains.
- However a principal ideal domain need not be a Euclidean domain. For example: the ring of ll complex numbers of the form $\{a + \frac{b}{2}(1 + \sqrt{-19})\}, a, b \in \mathbb{Z}$ can be shown to be principal ideal domain but not a Euclidean domain.

Lemma. Let R be a principal ideal domain. Then every $a \in R$ which is not a unit can be expressed as a product of irreducible elements.

Proof. If $a \in R$ is irreducible, nothing to prove.

- Otherwise, $a = bc$, where b and c are proper divisors of a.
- If both b and c are irreducible, then $a = bc$ is the required decomposition.
- Otherwise if b (or c is irreducible,) we have $b = ef$, where e and f are proper divisors of b, etc.
- If we continue this process, after a finite number of steps, all the factors will be irreducible for, otherwise, there will be an infinite sequence of elements,

  $$a_0 = a, a_1 = b, a_2 = e, \cdots, a_n, \cdots$$

  such that each a_{n+1} is a proper divisor of a_n.
- We shal show that it is impossible.

- Suppose such a sequence exists.
- Let $I_n = Ra_n$, so that we have an increasing sequence of ideals, $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \cdots$.
- Since a_{n+1} is a proper divisor of a_n, $I_n \neq I_{n+1}$ for each n.
- Let $I = \cup_{k=0}^{\infty} I_k$.
- Then I is an ideal in R, because if $a, b \in I$, then $a \in I$, and $b \in I_s$, where either $I_r \subset I_s$ or $I_s \subset I_r$, so that $a - b \in I_r \cup I_s \subset I$, and $xa \in I_r \subset I$ for all $x \in R$.
- Since R is a principal ideal domain, $I = Rd$ for some $d \in R$.
- Now $d \in I_m$ for some m, so that $I = Rd \subset I_m \subset I_{m+1} \subset \cdots \subset I$, i.e., $I_m = I_{m+1} = I_{m+2} = \cdots = I$, which is a contradiction.
- This completes the proof.

Factorization domain.

Definition. An integral domain R is called a factorization domain if every domain $a \in R$, which is not a unit can be expressed as a product of irreducible elements.

Remark. Hence, using last two lemmas, Euclidean domains and principal ideal domains are factorization domains.

Definition. $a \in R$ is said to be expressible uniquely as a product of irreducible elements if whenever $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$, where p_i, q_j are irreducible then $m = n$, and each $p_i = u_i q_i$ where u_i is a unit in some order.

Remark. If $a \in R$ can be expressed as a product of irreducible elements, the expression need not be unique as the following example shows.

- $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Check that only units in R are ± 1, and that $1 + 2\sqrt{-5}$ is an irreducible element. Similarly we can show that 3 and 7 are irreducible elements. Then
$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.
The two factorizations of 21 as a product of irreducible elements, are distinct as $1 \pm 2\sqrt{-5}$ are not the associates of 3 and 7.

Definition. An integral domain R is called a unique factorization domain (ufd) if every $a \in R$ which is not a unit can be expressed uniquely as a product of irreducible elements.

Lemma. Let R be an integral domain in which:

- Every $a \in R$ which is a non-unit can be expressed as a product of irreducible elements.
- Every irreducible element is prime.

Then R is unique factorization domain (ufd).

Proof. It is sufficient to show that factorization is unique.

- Let $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$, p_i, q_j irreducible, and hence prime.
- Since $p_1 | a$ we have $p_1 | q_1 q_2 \cdots q_n$ and hence $p_1 | q_j$ for some j.
- Wlog, assume that $p_1 | q_1$. Since q_1 irreducible, and p_1 is not a unit, p_1 is an associate of q_1, i.e., $q_1 = u_1 p_1$, where u_1 is a unit.
- Thus $p_1 p_2 \cdots p_m = (u_1 p_1) q_2 \cdots q_n$.
- Since R is an integral domain we have $p_2 p_3 \cdots p_m = u_1 q_2 \cdots q_n$.
- Repeating the same arguments with p_2, and continuing the process, we must have either $m = n$ or a unit will be expressible as a product of irreducible elements, which is not possible.
- Hence $m = n$, and each $p_i = u_i q_i$ with u_i unit.

Corollary. If R is a Euclidean domain or principal ideal domain, then R is unique factorization domain.

Proof. It is sufficient to show that every irreducible element is prime.

- Let p be an irreducible element and let $p|ab$.
- Consider the $\gcd(p, a)$. It is either 1 or p.
- If $\gcd(p, a) = p$, then $p|a$.
- If $\gcd(p, a) = 1$, then $\lambda p + \mu a = 1$ for some $\lambda, \mu \in R$.
- Multiplying both sides by b, we have $\lambda pb + \mu ab = b$.
- Since $p|ab$, it follows that p divides b. Hence p is a prime.

Remark. A unique factorization domain need not be principal ideal domain. For example: Every principal ideal domain is a unique factorization domain (UFD).

The converse does not hold since for any UFD K, the ring $K[X, Y]$ of polynomials in 2 variables is a UFD but is not a PID. (To prove this, look at the ideal generated by $\langle X, Y \rangle$. It is not the whole ring since it contains no polynomials of degree 0, but it cannot be generated by any one single element.)

Polynomial Rings.

Definition. A polynomial in x with coefficients from R is an expression of the type $f(x) = a_0 + a_1x + \cdots + a_nx^n, a_i \in R, n \geq 0.$

Definition. Two polynomials $f(x) = a_0 + a_1x + \cdots + a_nx^n$, and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, $a_n, b_m \neq 0$ will be equal iff $m = n$ and $a_i = b_i$ for all i.

Examples.

- $f(x) = x^3 + \iota x^2 - x + 5 + 7\iota$ is a polynomial with coefficients from the ring of Gaussian integers.
- If $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, then $f(x) = (1 + \sqrt{5})x^3 - x^2 + (7 + 8\sqrt{-5})x + 9$ is a polynomial with coefficients from R.

Definition. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ be two polynomials over R. Their sum $f+g$ and their product fg are defined as follows:

$$(f+g)(x) = (a_0+b_0) + (a_1+b_1)x + \cdots +$$

and

$$(fg)(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n},$$

where $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_1$.

Remark. The set $R[x]$ of all polynomials over R forms a ring for the operation of $+$ and $\cdot$. The zero polynomial is the identity (zero) element. The ring $R[x]$ is called the polynomial ring in x over R.

Lemma. If R is a commutative ring with unit element, so is $R[x]$.

Proof.

- Let $f(x) \in R[x]$ and $g(x) \in R[x]$ where $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$.
- Then $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{m+n}$.
- Since R is commutative, check that $fg = gf$.
- It shows that $R[x]$ is commutative.
- Let 1 be the unit element of R.
- Consider the polynomial $1 = 1 + 0x + 0x^2 + \cdots$.
- Then for any $f(x) = a_0 + a_1x + \cdots + a_nx^n$, check that $1f(x) = f(x)1 = f(x)$.
- Thus 1 acts as the unit element of $R[x]$.

Lemma. If R is an integral domain, then $R[x]$ is also an integral domain.

Proof.

- Consider $f(x) \in R[x]$ and $g(x) \in R[x]$ both non-zero.
- At least one coefficient of $f(x)$ and $g(x)$ is non-zero.
- Let a_n be the highest non-zero coefficient of $f(x)$ and let b_m be the highest non-zero coefficient of $g(x)$.
- Then $f(x) = a_0 + a_1x + \cdots + a_nx^n, a_n \neq 0$,
  $g(x) = b_0 + b_1x + \cdots + b_mx^m, b_m \neq 0$.
- Now $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{m+n}$.
- Since R is an integral domain, we have $a_nb_m \neq 0$.
- Thus $fg \neq 0$ showing that $R[x]$ is an integral domain.

Corollary. If F is a field, $F[x]$ is an integral domain with unit element.

Definition. Let $f(x) \in R[x]$, $f(x) \neq 0$. Then the largest n such that the coefficient of x^n in $f(x)$ is non-zero is called the degree of $f(x)$. We shall use the notation $\deg f$ for the degree of $f(x)$. If $\deg f = 0$, then f is called constant polynomial.

Lemma. Let R be any commutative ring, $f(x), g(x) \in R[x]$. Then $\deg fg \leq \deg f + \deg g$ and equality holds when R is an integral domain.

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n, a_n \neq 0$, so that $\deg f = n$, and let $g(x) = b_0 + b_1x + \cdots + b_mx^m, b_m \neq 0$ with $\deg g = m$.

- Then $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{m+n}$.
- Thus $\deg fg \leq m + n = \deg f + \deg g$.
- If R is an integral domain, then $a_nb_m \neq 0$, so that $\deg fg = m + n = \deg f + \deg g$.

Corollary. If F is a field, $\deg fg = \deg f + \deg g$ and in particular $\deg fg \geq \deg f$, as $\deg g \geq 0$.

Lemma. If F is a field, then $F[x]$ is a Euclidean domain.

Sketch of Proof. Note that $F[x]$ is an integral domain.

- For any $f(x) \in F[x]$, $f \neq 0$, define $d(f) = \deg f$.
- Then $d(f)$ is a non-negative integer satisfying $d(fg) \geq d(f)$ by the above corollary
- Now verify division algorithm.
- Let $f(x) \in F[x]$ and $g(x) \in F[x]$, $g(x) \neq 0$.
- If $\deg f < \deg g$, then $f = 0 \cdot g + f$ with $d(f) < d(g)$, i.e., the division algorithm is true.
- So we can assume that $\deg f \geq \deg g$ and use induction on $\deg f = n$.
- If $n = 0$, then $m = \deg g = 0$ and we are done. Otherwise let it is true for all polynomials f, g with $\deg f < n$ and $\deg f \geq \deg g$.
- Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n, a_n \neq 0$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m, b_m \neq 0$ with $m \leq n$.

Proof Contd...

- Let $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ which has degree $n-1$ and apply induction for $h(x)$, we can write $h(x) = q(x)g(x) + r(x)$ with $r(x) = 0$ or $d(r) < d(g)$.
- Substituting for $h(x)$, we get $f(x) = q_1(x)g(x) + r(x)$, where $q_1(x) = a_n b_m^{-1} x^{n-m} + q(x)$ and either $r = 0$ or $d(r) < d(g)$.

Corollary. If F is a field, $F[x]$ is a PID, UFD.

Corollary. If F is a field, any two $f, g \in F[x]$ have a gcd $d(x)$ which can be expressed in the form $d(x) = \lambda(x)f(x) + \mu(x)g(x), \lambda(x), \mu(x) \in F[x]$. Moreover gcd of two elements can be obtained by the division algorithm process.

Example. Let $f(x) = x^4 + x^3 - 3x^2 - x + 2$ and $g(x) = x^4 + x^3 - x^2 + x - 2$ have gcd $x^2 + x - 2$.

Definition. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Then α be a root of $f(x)$ if $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

Remark. If R is a field, then $R[x]$ is UFD. Hence, every $f(x) \in R[x]$ which is not constant can be expressed uniquely as a product of irreducible polynomials. This result is true more generally, when R is UFD.

We now provide a famous irreducibility criterion which provides sufficient conditions for the irreducibility of polynomials with coefficients in a UFD.

Eisenstein's criterion. Let R be a UFD and $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, $a_n \neq 0$. Suppose there exists an irreducible element $p \in R$ such that

- $p | a_i$ for $0 \leq i \leq n-1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $R[x]$.

Proof.

- Suppose $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ where $\deg g < n$ and $\deg h < n$.
- Let $g(x) = b_0 + b_1 x + \cdots + b_r x^r, b_r \neq 0, r < n$.
- Let $h(x) = c_0 + c_1 x + \cdots + c_s x^s, c_s \neq 0, s < n$.
- Since $f(x) = g(x)h(x)$, we have $a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i$.
- Since $p | a_0$, we have $p | b_0$ or $p | c_0$ but not both as $p_2 \nmid a_0$.
- Wlog, let $p | b_0$ and $p \nmid c_0$.
- Since $p \nmid a_n$, $p \nmid b_i$ for some i, $1 \leq i \leq r < n$.
- Choose least i such that $p \nmid b_i$, i.e., $p \nmid b_i$ and $p | b_j$ for $0 \leq j \leq i - 1$.
- Consider $a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_1 c_{i-1} + b_0 c_i$.
- Since $i < n$, we have $p | a_i$. Also, $p | b_0, \cdots, p | b_{i-1}$.
- Hence $p | b_i c_0$, and this is a contradiction because $p \nmid b_i$ and $p \nmid c_0$.
- Therefore, $f(x)$ is irreducible in $R[x]$.

Definition. Let R be a UFD and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Then the gcd of the coefficients $a_0, a_1, \cdots, a_n$ is called the content of $f(x)$. We shall denote it by $c(f)$.

Definition. Let R be a UFD. Then $f(x)$ is called a primitive polynomial, if $c(f) = 1$.

Lemma. Let R be a UFD. Then the product of two primitive polynomials over R is also a primitive.

Gauss Lemma. Let R be a UFD and F the quotient field of R. Let $f(x) \in R[x]$ be irreducible in $R[x]$. Then $f(x)$ is also irreducible in $F[x]$.

Proof.

- Let $f(x) = a_0 + a_1x + \cdots + a_rx^r$ and $g(x) = b_0 + b_1x + \cdots + b_sx^s$ be primitive polynomials and let $h(x) = f(x)g(x) = c_0 + c_1x + \cdots + c_{r+s}x^{r+s}$.
- Suppose $h(x)$ is not primitive and that the $c_0, c_1, \cdots, c_{r+s}$ have a common irreducible factor p.
- Since $f(x)$ is primitive, p can not divide all the a_i's.
- We choose i such that $p \nmid a_i$ but $p|a_{i-1}$, $p|a_{i-2}$, $\cdots, p|a_0$, $0 \leq i \leq r$.
- Similarly we choose j such that $p \nmid b_j$, but $p|b_{j-1}, \cdots, p|b_0$, $0 \leq j \leq s$.
- Now $c_{i+j} = a_ib_j + \sum\limits_{k+\ell=i+j, k\neq i, \ell\neq j} a_kb_\ell$.
- Since $p|c_{i+j}$ and p divides $\sum\limits_{k+\ell=i+j, k\neq i, \ell\neq j} a_kb_\ell$, we have $p|a_ib_j$.
- This is a contradiction as $p \nmid a_i$ and $p \nmid b_j$.
- This proves that $h(x)$ is primitive.

Proof.

- If possible, let $f(x)$ is reducible in $F[x]$.
- Then $f(x) = g(x)h(x)$ with $\deg g < \deg f$ and $\deg h < \deg f$.
- We can write $g(x) = (a/b)g_1(x)$ and $h(x) = (c/d)h_1(x)$, where $a, b, c, d \in R$ and $g_1(x), h_1(x) \in R[x]$ both being primitive.
- Then $f(x) = \frac{ac}{bd}g_1(x)h_1(x)$ and $g_1(x)h_1(x)$ is primitive.
- Since $f(x) \in R[x]$ is irreducible, and $c(f)$ divides f, $c(f) = 1$, i.e., f is primitive.
- Now $bdf(x) = acg_1(x)h_1(x)$, and comparing the contents on both sides, we have $bd = ac$.
- Hence $g_1(x)h_1(x)$ where $g_1(x), h_1(x) \in R[x]$ and $\deg g_1 = \deg g < degf$, $\deg h_1 = \deg h < \deg f$.
- This contradicts the assumption that $f(x) \in R[x]$ is irreducible.
- Hence $f(x)$ is irreducible in $F[x]$.

Corollary. If $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Z}$, then it is reducible over $\mathbb{Z}$.

Remark. $f(x) \in F[x]$ is irreducible iff $f(x+a)$ is irreducible for $a \in F$. [Hint: If $f(x) = g(x)h(x)$, then $f(x+a) = g(x+a)h(x+a)$. And $f(x+a) = G(x)H(x)$, then $f(x) = G(x-a)H(x-a)$.]

Mod p irreducibility test. Let p be a prime number and suppose $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof.

- If $f(x)$ is irreducible over $\mathbb{Q}$, then $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$, and both $g(x)$ and $h(x)$ have degree less than that of $f(x)$.
- Let $\bar{f}(x)$, $\bar{g}(x)$, and $\bar{h}(x)$ be the polynomials obtained from $f(x), g(x)$ and $h(x)$ by reducing all the coefficients modulo p.
- Since $\deg f(x) = \deg \bar{f}(x)$, we have $\deg \bar{g}(x) \leq \deg g(x) < \deg \bar{f}(x)$ and $\deg \bar{h}(x) \leq \deg h(x) < \deg \bar{f}(x)$.
- But, $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, and this contradicts our assumption that $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$.
- This completes the proof.

Examples.

- If p is a prime number then $f(x) = 1 + x + x^2 + \cdots + x^{p-1} \in \mathbb{Q}[x]$ is irreducible.
  Hint: Check $f(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + p$.
  This it is irreducible by Eisenstein's criterion (w.r.t. p) over $\mathbb{Z}$. By Gauss lemma, it is irreducible in $\mathbb{Q}[x]$. Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.
- Let $f(x) = 5x^7 + 36x^3 - 12$. Then $f(x)$ is irreducible by Eisenstein criterion with $p = 3$.
- The polynomial $f(x) = x^3 + px + p^2$ with p prime, is irreducible over $\mathbb{Q}$ as it can not have a linear factor. [Hint: If $f(x)$ has a rational root, then it will be of form $\frac{r}{s}$ with $\gcd(r,s) = 1$. Hence check that r divides last coefficient and s divides leading coefficent.]
- If $p \neq 2$ a prime number and a, b positive integers, then $f(x) = x^3 + p^a x^2 + p^b$ is irreducible over $\mathbb{Q}$, as modulo 2 it reduces to $x^3 + x^2 + 1$, which is irreducible modulo 2. Hence $f(x)$ is irreducible over $\mathbb{Q}$ by Mod test.