# SETS AND BINARY OPERATIONS

## SET

Set is a well-defined collection of objects. A set is represented by capital letter and the elements by small letters.

### EXAMPLES

- $\mathbb{N}$ of natural numbers
- $\mathbb{Z}$ of integers
- $\mathbb{R}$ of real numbers

## BINARY OPERATION ON A SET

- A binary operation $*$ on a set A is a mapping from A×A in to A.
- For each (a, b) ∈ A×A we denote $*(\mathrm{a}, \mathrm{b}) = \mathrm{a} * \mathrm{b}$
- The number of binary operations on a set A of cardinality n is $n^{n^2}$.

## PROPERTIES

### COMMUTATIVE BINARY OPERATION

A binary operation $*$ on a set A is commutative if $\mathrm{a} * \mathrm{b} = \mathrm{b} * \mathrm{a}$, $\forall$ a, b $\in$ A. Total number of commutative binary operations on a set A of cardinality n is $n^{\frac{n(n+1)}{2}}$.

### ASSOCIATIVE BINARY OPERATION

A binary operation $*$ on a set A is associative if $\mathrm{a} * (\mathrm{b} * \mathrm{c}) = (\mathrm{a} * \mathrm{b}) * \mathrm{c}, \forall\, \mathrm{a}, \mathrm{b}, \mathrm{c} \in \mathrm{A}$.

### IDENTITY ELEMENT

An element e of a set A is said to be an identity element if $a * e = a = e * a$, $\forall\, a \in A$.

### INVERSE ELEMENT

a ∈ A is said to have an inverse in A if ∃ b ∈ A such that $a * b = e = b * a$, and we write $a^{-1} = b$.

## EXAMPLES FOR BINARY OPERATION

- Usual addition $'+'$ on the set $\mathbb{R}$
- Usual multiplication $'\cdot'$on the set $\mathbb{R}$

## ALGEBRAIC STRUCTURES

### QUASI GROUP

Quasi-group is a set $A \neq \phi$ with a binary operation on it.
**Example:** $(\mathbb{Z}, +)$, $(\mathbb{R}, -)$…etc

### SEMI GROUP

Semi group is a quasi-group with associative binary operation on it.

**Example:** $(\mathbb{N}, +)$

## MONOID

Monoid is a semi group having identity element

**Example:** $(\mathbb{N} \cup \{0\}, +)$, $(P(A), \cup)$, $(P(A), \cap)$,etc , where $P(A)$ is the power set of A.

## GROUP

Group is a monoid in which the inverse element exists for all elements.ie,

# GROUP THEORY

## GROUP

The set G together with a binary operation $*$ is said to be a group $(G, *)$ if it satisfies the following axioms.

- **Closure property:** if $x, y \in G \implies x * y \in G$.
- **Associativity:** For any $\mathrm{a, b, c} \in \mathrm{G}$, we have, $\mathrm{a} * (\mathrm{b} * \mathrm{c}) = (\mathrm{a} * \mathrm{b}) * \mathrm{c}$
- **Identity:** There exist an element $e \in G, such\ that\ for\ any\ a \in G, we\ have,\ \ a * e = a = e * a$
- **Inverse:** for any element $\mathrm{a} \in \mathrm{G}$, there exist $\mathrm{b} \in \mathrm{G}$ such that
$$a * b = e = b * a \quad and\ we\ denote\ b\ as\ a^{-1}$$

## EXAMPLES

- $\boldsymbol{M_n}(\mathbb{R})$ matrix addition
- $\boldsymbol{M_{m \times n}}(\mathbb{R})$ under matrix addition
- $\mathrm{F} = \{\mathrm{f} \mid \mathrm{f}: \mathbb{R} \to \mathbb{R}\}$ under function addition

## ABELIAN AND NON-ABELIAN GROUPS

A group G is said to be abelian if $a * b = b * a\ for\ all\ a, b \in G$ . otherwise G is non-abelian.

## CANCELLATION LAW

There are two types of cancellation laws

- Right cancellation law: $a * b = a * c \Leftrightarrow b = c\ \forall a, b, c \in G$.
- Left cancellation law: $a * c = b * c \Leftrightarrow a = b, \forall a, b, c \in G$.

## ORDER OF AN ELEMENT

If $(G,*)$be a group then, order of an element a in G is the least positive integer r such that

$a^r = e$ where e is the identity element of $(G,*)$. If no such least positive integer exists for an element a in G then we say that a has infinite order. We write o(a) to denote order of an element a.

## SUBGROUP

Let $(G,*)$be a group and a non-empty subset H of G is said to be a subgroup of G if H itself is a group under same binary compositions as that of G.

ENTRI

### EXAMPLE

- $(n\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$
- $(\mathbb{R},+)$is a subgroup of $(\mathbb{C},+)$

## COSETS

Let G be a group and $H \leq G$, then the subset $aH = \{ah: a \in G, h \in H\}$ of G is known as the left coset of H containing 'a' and similarly the subset $Ha = \{ha: a \in G , h \in H\}$ of G is known as the right coset of H containing 'a'.

- The number of left/right cosets of H in G is called the index of H in G, and is denoted by $[G: H]$.

## SOME IMPORTANT THEOREMS

### LAGRAGE'S THEOREM

Let g be a finite group, then $O(a)$ divides $|G|$ for all $a \in G$

### LAGRANGE'S THEOREM FOR FINITE ORDER GROUPS

Let G be a group of finite order, and $H \leq G$, then $|H|$ divides $|G|$.

### THEOREM

Let G be a group and $H, K \leq G$ such that $K \leq H \leq G$ and $[G: H], [H: K]$ are finite, then $[G: K] = [G: H][H: K]$.

## CYCLIC GROUPS

A group G is said to be cyclic group if $G =< a >$ for some $a \in G$, here a is called Generator for G

### EXAMPLE

Consider the group $(\mathbb{Z},+)$, it is clear that $< -1 >=< 1 >= \{n.1 | n \in \mathbb{Z}\} = \mathbb{Z}$.

### NOTE

- $(\mathbb{R},+)$, $(\mathbb{Q},+)$ has no generators.
- Cyclic groups are always are always abelian. But converse is not true.
  Example: $\mathrm{K}_4$ is abelian but not cyclic.
- Subgroups of cyclic groups are cyclic. Converse not true.
  Example: $(\mathbb{Z},+)$ is cyclic but $(\mathbb{Q},+)$ is not cyclic.

## GROUP HOMOMORPHISM

Let $(G,*)$, $(G',*')$ be two group structures, then a map $\phi: G \to G'$ is said to be a group homomorphism if $\emptyset(a * b) = \emptyset(a) *' \emptyset(b)$.

### PROPERTIES

suppose that $\emptyset: G \to G'$ is a group homomorphism then,

- $\phi(e) = e'$
- $\phi(a^{-1}) = \phi(a)^{-1}$
- $O(\phi(a))$ divides $O(a)$

- $H \leq G \Rightarrow \phi(H) \leq G'$
- $K \leq G' \Rightarrow \phi^{-1}(K) \leq G$
- $\ker(\phi) = \{x \in G: \phi(x) = e'\}$
- $\ker(\phi) \leq G$
- $\phi(G) \leq G'$
- $\phi$ is said to be a Monomorphism if it is injective.
- $\phi$ is said to be a Epimorphism if it is surjective**.**
- $\phi$ is said to be a Isomorphism if it is bijective. In this case we write $G \cong G'$
- $\phi$ is said to be a Automorphism on the group G if $\phi : G \to G$ is an isomorphism.

## NORMAL SUBGROUP

Let G be a group and $H \leq G$, then H is said to be normal in G (denoted by $H\Delta G$ or $H \trianglelefteq G$) if $gH = Hg, \forall g \in G$.

### NOTE

Let G, G' be two groups and $H \leq G$, then

- $\phi: G \to G'$ is a group homo$\Rightarrow$ker $(\phi) \trianglelefteq G$.
- $Z(G) \trianglelefteq G$
- $C(a) \trianglelefteq G, \forall a \in G$
- $[G:H] = 2 \Rightarrow H \trianglelefteq G$

## FIRST ISOMORPHISM THEOREM

Let $\phi: G \to G'$ be a group homomorphism with $\ker(\phi) = H$. let $\mu: G/H \to \phi(G)$ be a homomorphism defined by $\mu(gH) = \phi(g)$, then µ is an isomorphism.
i.e $G/H \cong \phi(G)$

- Equivalent necessary and sufficient conditions for $H \leq G$ to be normal in G
  (i) $ghg^{-1} \in H, \forall g \in G \;\&\; h \in H$
  (ii) $gHg^{-1} = H, \forall g \in G$
  (iii) $gH = Hg, \forall g \in G$

## FINITELY GENERATED GROUPS

Let G be a group, $a_i \in G, i \in I$ for some index set $I$, we know that the subgroup generated by $\{a_i | i \in I\}$ is the smallest subgroup containing $\{a_i | i \in I\}$ . If the referred subgroup is all of G, then G is said to be finitely generated by $\{a_i | i \in I\}$. In this case $a_i$s are the generators of G.

- Every cyclic group is finitely generated.

## MULTIPLICATIVE GROUP OF nth ROOT OF UNITY

The set of all $z \in \mathbb{C}$ such that $z^n = 1$ is given by $U_n = \{e^{\frac{i2\pi k}{n}} | k = 0,1, \dots, n-1\}$

**Properties**

- $|U_n| = n$.
- $U_n$ is cyclic.

- $(Un\,,.) \leq (\mathbb{C}^*,\ .)$
- Generators of $U_n$ are called the primitive n[th] roots of unity.

  $\{e^{\frac{i2\pi k}{n}} |(n,k) = 1\}$

### GROUP OF QUARTERNIONS

Consider the set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with the following operational properties.

$$i^2 = j^2 = k^2 = -1$$
$$ij = k = -ji,\ jk = i = -kj,\ ki = j = -ik$$

then $Q_8$ form a multiplicative group known as Group of quaternions.

**Note**

- $Q_8$ is not abelian.
- $O(\pm i) = O(\pm j) = O(\pm k) = 4$

### THE GROUP $GL(n, \mathbb{Z}_p)$

Let $A \in GL(n, \mathbb{Z}_p)$, then the number of choices of the entries in each row is given by

$$A \begin{bmatrix} * & * & \cdots & * \\ * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{bmatrix} \begin{matrix} \to p^n - 1\ choices \\ \to p^n - p\ choices \\ \vdots \\ \to p^n - p^{n-1}\ choices \end{matrix}$$

Thus,

- $$|GL(n, \mathbb{Z}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$$
  $$= p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1) \dots (p - 1)$$
- $|GL(2, \mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 3 \times 2 = 6$

# SYLOW THEOREMS

## P-GROUP

Let G be a group and p be a prime, then G is said to be a p-group if $o(a) = p^n, \forall a \in G$ and $n \in \mathbb{N}$.

- G is a p-group $\Leftrightarrow |G| = p^n\ for\ some\ n \in \mathbb{N}$.
- For every prime p there exist a p-group.
- A finite group G is a p-group if and only if O(G)=$p^n$.
- Every subgroup of a p-group is again a p-group.
- A non-p-group can have a p-subgroup.

### EXAMPLES

- $Q_8$ is a 2 group of finite order.
- $K_4 = \{e, a, b, c\}$ is a 2 group of finite order.

## FIRST SYLOW THEOREM

Let G be a group and p be a prime so that $|G| = p^n m, n \geq 1, p \nmid m$, then

1. $\exists\, H_k \leq G$ such that $|H_k| = p^k,\ \forall k |\, 1 \leq k \leq n.$
2. $H_{k-1} \trianglelefteq H_k$

### SECOND SYLOW THEOREM

Let G be a group and p be a prime so that $P_1 \,\&\, P_2$ are two Sylow-p subgroups of G, then $P_1 \,\&\, P_2$ are two conjugates to each other. i.e $\exists\, g \in G$ such that $gP_1 = P_2 g$, & $P_1 \cap P_2 = \{e\}$.

### THIRD SYLOW THEOREM

Let G be a group and p be prime so that $|G| = p^n m$, then $n_p$ divides $|G|$, where $n_p$ is the number of Sylow-p subgroups of G and also $n_p \equiv 1 (mod p)$.

### NOTES

- Since $n_p \equiv 1 (mod p)$ and $n_p | p^n m$ then $n_p$ must be a divisor of m.
- A sylow-p subgroup of G is normal in G$\Leftrightarrow n_p = 1$.
- Let G be a group and p be a prime so that $|G| = n$, n is composite, $p|n \,\&\, d = 1$ is the only divisor of n such that $d \equiv 1 (mod p)$,$\Rightarrow \nexists$ a simple group with order n.
- Let G be a group with $|G| = 2n$, where $n (> 1)$ is odd, then G cannot be simple.
- Let $G$ be a group and $p, q$ be a prime so that $|G| = pq, p < q$, then G is not simple $(here\ n_q = 1)$ also. $|G| = pqr, p < q < r \Rightarrow$G is not simple.
- Intersection of sylow-p with a sylow-q subgroup is trivial.
- $H, K \trianglelefteq G \Rightarrow HK \trianglelefteq G.$
- Let G be a group and p be a prime such that $|G| = p^3$, then G can be abelian (cyclic) and also non-abelian.

# RINGS AND IDEALS

### RING

A ring (R, +, ·) is a set together with '+' and '·' as binary operations so that the following axioms are satisfied,

1. (R, +) is abelian
2. (R, ·) is a semi group (holds associativity)
3. '+' is distributive(L/R) over '·'

**EXAMPLE**

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ $(\boldsymbol{M_n}(\mathbb{R}), +, \cdot)$, $(\mathbb{Z}_{\boldsymbol{n}}, +_{\boldsymbol{n}}, \times_{\boldsymbol{n}})$, $(\boldsymbol{n}\mathbb{Z}, +, \cdot)$...

### NOTES

- The requirements for $(\mathbb{R}^*, \cdot)$ to become abelian group:

1. Existence of identity (Unity 1)
2. Existence of inverse, those having inverse (here multiplicative inverse) are known as Units.

3. Commutativity (here R is said to be Commutative ring).

## CHARECTERISTIC OF A RING

The least positive integer n such that $na = 0, \forall a \in R$.

- If there is no such integer then $char = 0$.
- Char of the ring $(\mathbb{Z}_n, +_n, \times_n)$ is $n$.
- Finite product of rings are again rings.
- $Char(\mathbb{Z}_m \times \mathbb{Z}_n) = l.c.m\{m, n\}$.
- $Char(\mathbb{R}) = Char(\mathbb{Q}) = Char(\mathbb{Z}) = Char(\mathbb{Z} \times \mathbb{Z}_n) = 0$.
- Let F be a field, then $|F| = p^n \Rightarrow Char(F) = p$.
- $Char\ (\mathbb{R}) = 0\ or\ p$.
- Ring R is infinite $\Rightarrow Char(R) = 0$, converse need not be true. ({0})
- Let S, R be finite rings and S is a quotient ring of R $\Rightarrow char(s)|\ Char(R)$.

## SUBRINGS

Let R be a ring, $S \subset R$ is said to be a ring if

1. $\forall a, b \in S$
2. $ab \in S\ \forall a, b \in S$

### EXAMPLE

- Sub rings of $\mathbb{Z}$ are trivial and $n\mathbb{Z}$.
- $\mathbb{Z}[i] = \{a + ib\ |a, b \in \mathbb{Z}\}$(Gaussian integers) is a sub ring of $\mathbb{C}$.
- $\mathcal{F}$ cannot be a ring under function addition and function composition, since by taking $f(x) = sinx$, $g(x) = x$ and $h(x) = \sqrt{x}$, we are not able to conform the distributive laws.
- $\mathcal{S} = \{f \in \mathcal{F}\ |f(0) = 0\}$ form a sub ring of $\mathcal{F}$.

## IDEAL

### TWO SIDED IDEALS

Let R be a ring, A be a subring of R, then A is said to be a two sided ideal of R if $ar \in A, \forall a \in A, \& r \in R$.

- {0} is a trivial ideal.
- Let F be a field, then F has no trivial proper Ideals, only ideals of F are trivial and F itself.

## IDEAL TEST

Let $A \subset R$ (ring) is said to be an ideal of R if

1. $a - b \in A\,, \forall a, b \in A$
2. $ra \subset A\ \&\ Ar \subset A\quad \forall r \in R$.

- For a finite field F, the group ($F^*$, ·) is a cyclic group.

## PRINCIPAL IDEAL

Let R be a commutative ring with unity, $a \in R$, then the set,

$< a >= \{ra\ |r \in R\}$ is an ideal of R known as the Principal ideal of R generated by a

- The ring $n\mathbb{Z}$, $n > 1$ has no principal ideals.
- Ideals of R generated by $\mathbf{a_1}$ & $\mathbf{a_2}$
  $< a_1, a_2 >= \{r_1a_1 + r_2a_2|\ r_1, r_2 \in R\}$

### EXAMPLE

Consider $\mathbb{Z}[x]$, then the ideal $I$ of all polynomials with constant term even/zero,
$I =< x, 2 >= \{P_1(x)x + 2P_2(x) | P_1(x), P_2(x) \in \mathbb{Z}[x]\}$

### NOTE

- Let R be a ring with unity $1 \neq 0$ and $I$ is an ideal of R, containing unity 1, then $I = R$.
- For a field F, every ideal of F[x] are principal.

## PRIME IDEAL

An ideal A of R is said to be Prime if for $a, b \in R$ & $ab \in A \Rightarrow a \in A$ $or$ $b \in A$.

### EXAMPLE

From the ideals $n\mathbb{Z}$ $of$ $\mathbb{Z}$, prime ideals are $p\mathbb{Z}$**.**

## MAXIMAL IDEAL

Suppose A is a proper Ideal of R, then A is said to be Maximal ideal of R, if ∃ an ideal B such that $A \subseteq B \subseteq R \Rightarrow B = A$ $or$ $B = R$.

- Let R be a finite commutative ring with unity, A is a non-trivial ideal of R, then A is maximal ⇔ A is prime.

| Ring | Ideals |
|---|---|
| $\mathbb{R}$ | $\{0\}$, $\mathbb{R}$ |
| $\mathbb{Q}$ | $\{0\}$, $\mathbb{Q}$ |
| $\mathbb{Z}$ | n$\mathbb{Z}$, $\mathbb{Z}$ |
| $\mathbb{Z}_n$, n is composite | $\{0\}, < d > \ d|n, \mathbb{Z}_n$ |
| $\mathbb{Z}_p$ | $\{0\}$, $\mathbb{Z}_p$ |
| $\mathbb{Z} \times \mathbb{Z}$ | |
| $F[x]$ | |

- Maximal ideals in z[x] are of the form (r(x),p), where r(x) is an irreducible polynomial $Z_t$ where t is a prime in Z.
- $< p(x) >$ is a maximal ideal in F[x] $\Leftrightarrow < p(x) >$ is irr. Over F.
- Every maximal ideal in a commutative ring with unity is a prime ideal.

## FACTOR RING

Let R be a ring, A be an ideal of R, then the set of all additive cosets $\frac{R}{A} = \{r + A \,| r \in R\}$ form a ring with the binary operations defined by,
$(a + A) + (b + A) = (a + b) + A$ and (a+A) (b+A)=(ab)+A

### EXAMPLE

- $< 2 + i >$ is an ideal of $\mathbb{Z}[i]$.

# FIELDS

## FIELD

a field is a set together with two binary operations + and . on F such that (F, +) is an abelian group and $(F^*,\cdot)$ is where $F^* = F\backslash\{0\}$ is also an abelian group and distributive law holds.

- If all nonzero elements of $(R, +, \ \cdot)$ are units, then R is said to be Division Ring/Skew field (here, existence of unity trivially hold.)
- A non-commutative division ring is called a Strictly skew field.
- A Field is a commutative division ring.
- Let F be a field, then $|F| = p^n \Rightarrow Char(F) = p.$
- $Char\ (\mathbb{R}) = 0\ or\ p.$

## SUB FIELD

A non-empty subset S of F is said to be a sub field of F if

i. $a \in S, b \in S \Rightarrow a + b\ \in S, ab \in S$
ii. S is a field under the induced addition and multiplication compositions.

- Number of sub fields for F is d(n) (no. of divisors of n.ie, $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} \Rightarrow d(n) = (r_1 + 1)(r_2 + 1) \dots (r_k + 1)$)

## ZERO DEVISORS

Let R be a ring, $a \neq 0, b \neq 0 \in R$ such that $(ab = 0)$ then $a\ \&\ b$ are said to be zero devisors.

- Number of zero divisors in $\mathbb{Z}_n$ is $n - \phi(n) - 1$.
- $\mathbb{Z}_p$ has no zero divisors
- $M_n(\mathbb{R})$ is a ring having zero divisors.
  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
- $GL_n(\mathbb{R})$ is not a ring.
- Cancellation law holds in a ring R, if it has no zero divisors
  (since, if $a \neq 0, b \neq 0, \& \ ab = 0 \in R, a.0 = ab \Rightarrow b = 0$) i.e zero divisors are not units.

## INTEGRAL DOMAINS(ID)

An integral domain is a commutative ring with unity having no zero divisors.

### EXAMPLE

$(\mathbb{Z}, +,\cdot)$, $(\mathbb{Z}_p, +_p, \times_p)$

### PROPERTIES

- Every field is an integral domain.
- Every finite integral domain is a field.
- $(\mathbb{Z}_p, +_p, \times_p)$ is a field
- Order of finite field is $p^n$.
- Char of an integral domain is 0 or p($\mathbb{Z}_p$).
- product of two I.D s is not an I.D, that's why product fields (since (1,0)(0,1)=(0,0))

### FIELD OF QUOTIENTS OF AN ID

Let D be an I.D, take $F = \{\frac{p}{q} \,|\mathrm{p} \in \mathrm{D}, \mathrm{q}(\neq 0) \in \mathrm{D}\}$, then F is the smallest field containing D known as the quotient field of D.

- $\mathbb{Q}$ is the Q.F of $\mathbb{Z}$.

## EXTENSION FIELDS

### FIELD EXTENSION

A field extension of a field F is a pair $(K, \phi)$ where K is a field and $\phi$is a monomorphism of F in to K.

#### EXAMPLE

- Let $F = \mathbb{Q}$ $and$ $E = \mathbb{R}$ $or$ $E = \mathbb{C}$. Then E/F is an extension.
- Let E be any field and F be its prime subfield then, E/F is an extension.

### DEGREE OF A VECTOR SPACE OVER FIELD

The dimension of K as a vector space over F is called the degree of K over F and is written as [K:F] or $dim_F K$.

### FINITE/INFINITE EXTENSION

K is said to be a finite or infinite extension according as the degree of K over F is finite or infinite.

### RESULT

- If K is a finite field extension of F and L is a finite field extension of K, then L is a finite field extension of F and [L : F] = [L:K] [K : F]

### SIMPLE EXTENSION

Let K be an extension of the field F and if the field K is generated by a single element $\alpha$ over F, i.e,

K = F ( $\alpha$) then K is said to be a simple extension of F and the element $\alpha$is called the primitive element.

### ALGEBRAIC EXTENSION

An element a of K is said to be algebraic over F if a is a root of a non-zero polynomial f(x) in F(x). K is said to be an algebraic extension of F if every element of K is algebraic over F.

EXAMPLE

- $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it satisfies $x^2 - 2\ in\ \mathbb{Q}[x]$.

## NOTE

- Every field extension of prime degree is simple.
- Every finite extension of a field is an algebraic extension but converse is not true.
- An element a of K is algebraic over F if and only if [ F($\alpha$): F) is finite.

## MONIC POLYNOMIAL

A non-zero polynomial f(x) in F[x] is said to be a monic polynomial over F if the coefficient of highest power of x in f(x) is equal to 1, the unity of F.

## MINIMAL POLYNOMIAL

If any element a in K is algebraic over F then a monic polynomial of smallest degree over F satisfied by a is called the minimal polynomial of a over F. If the degree of the minimal polynomial of a is n, then a is said to be algebraic over F of degree n.

## SPLITTING FIELD

Let f(x) be any polynomial of degree $n \geq 1$ over a field F. Then a field extension E of F is called splitting field of f(x) if

i. f(x) can be factored in to n linear factors over E and
ii. there does not exist any proper subfield E' of E containing F such that f(x) if can be factored into n linear factors over E'.

equivalently, one can say that E is a splitting field of f(x) if E contains all roots of f(x) and

$E\ =\ F(a_1, a_2, \dots, a_n)$, the field generated by F and n roots $a_1, a_2, \dots, a_n$ of f(x) in E.

# RINGS OF POLYNOMIALS

## RING OF POLYNOMIAL

Let R be a commutative ring, then
$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in R, n \in \mathbb{N}\}$ forms a ring under polynomial addition and polynomial multiplication, known as the ring of polynomials.

- $f \in R[x] \Leftrightarrow f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_n \neq 0$
- $a_n = 1$, then $f(x)$ is said to be monic.
- $f(x) = 0$, then deg $(f(x))$ is not defined (since $\mathrm{a_n} \neq 0$)
- $f(x) = c$, then $\deg(f) = 0$

## NOTE

- $\deg(fg) = \deg(f) + \deg(g) \Leftrightarrow Ris\ an\ I.D$
- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
- D is an I.D $\Rightarrow D[x]$ is an I.D.
- F is a field $\Rightarrow F[x]$ is an I.D, ($x^{-1} \notin F[x]$)

## DIVISION ALGORITHM

Let F be a field, $f, g \in F[x]$, then $\exists$ unique polynomial $q(x), r(x) \in F(x)$ such that

$$f(x) = q(x)g(x) + r(x), \qquad r(x) = 0\ or\ \deg(r) < \deg(g)$$

## REMAINDER THEOREM

Let F be a field, $a \in F$, then $f(a)$ is the remainder when $f$ is divided by $x - a$.

## FACTOR THEOREM

Let F be a field, $a \in F$ such that $f(a) = 0$, then $x - a$ is a factor of $f$.

## CONTENT OF A POLYNOMIAL

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$, then $g.c.d\{a_i\}$ is known as the content of $f$.

- Content of a monic polynomial is 1.
- Polynomials with content 1 is known as primitive polynomials.
- The product of two primitive polynomials is primitive.

## REDUCIBLE AND IRREDUCIBLE POLYNOMIAL

Let $f(x) \in D[x]$, where D is an I.D and $f \neq 0$ or a unit in $D[x]$, then f is said to be Irreducible over D if, whenever $f(x)$ can be expressed as $f(x) = g(x)h(x)$, $g(x), h(x) \in D[x]$ then h or g is a unit in $D[x]$.

- $f(x) \in F[x]$, where F is a field and $f \neq c$ in F[x] then $f$ is said to be irreducible over $F$ if $f(x)$ cannot be expressed as $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$ with $\deg(g), \deg(h) < \deg(f)$

## EXAMPLE

- $x^2 + 4 \in \mathbb{Z}[x], 2x^2 + 4 = 2(x^2 + 2)$, neither 2 nor $x^2 + 2$ is a unit in $\mathbb{Z}[x]$, thus $2x^2 + 4$ is reducible over $\mathbb{Z}$.
- $2x^2 + 4 \in \mathbb{Q}[x]$, $2x^2 + 4 = 2(x^2 + 2)$ but $\deg(x^2 + 2) \nless \deg(2x^2 + 4)$ in $\mathbb{Q}$[x], thus $2x^2 + 4$ is irreducible over $\mathbb{Q}$.

## REDUCIBILITY TEST IN FIELDS

- $f \in F[x]$, $\deg(f) = 2\ or\ 3$, then $f$ is reducible over F$\Leftrightarrow f$ has a zero in F.
- $f \in \mathbb{R}[x]$, $\deg(f) \geq 3 \Rightarrow f$ is reducible over $\mathbb{R}$.
- $f \in \mathbb{Z}[x]$ and $f$ is reducible over $\mathbb{Q} \Rightarrow f$ is reducible over $\mathbb{Z}$.
- $f \in \mathbb{Z}[x]$ and $f$ is irreducible over $\mathbb{Z} \Rightarrow f$ is irreducible over $\mathbb{Q}$.

## mod p TEST

Let $f \neq c \in \mathbb{Z}[x]$, $f(x) = \bar{f}(x)$ in $\mathbb{Z}_\text{p}[x]$ & $\deg(f) = \deg(\bar{f})$, if $\bar{f}$ is irreducible over $\mathbb{Z}_p \Rightarrow f$ is irreducible over $\mathbb{Q}$.

### EINSTEIN'S CRITERION

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$, if $\exists$ a prime p such that $p \nmid a_n$, $p|a_{n-1}$, $p|a_{n-2}$,...$p|a_1$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

# GALOIS THEORY

## GALOIS EXTENSION

An extension K of F is called Galois extension if K/F is finite extension and F is fixed field of a group of automorphisms of K denoted by *Aut*(K).

## FUNDAMENTAL THEOREM OF GALOIS THEORY

Let K/F be a Galois extension and Gal(K/F) is a Galois group of K/F .i.e, the group of all F-automorphisms of K. Then

1) There is one-one correspondence between the set $A = E/F \subseteq E \subseteq K and$ $B = \{H/H\ subgroup\ of\ Gal(K/F)$.
2) If H is subgroup of $(K/F)$ in B corresponding to field E in A, then O(H)= [K : E] and $[Gal(K/F): H] = [E: F]$.
3) If $H_1, H_2 \in B$ corresponding to field $E_1, E_2 \in A$ respectively. Then $E_1, E_2$are conjugate under an automorphism $\sigma \in\ Gal(K/F)$ iff $\sigma^{-1}H_1\sigma = H_2$.
4) If H $\in B$ corresponds to E $\in A$, then E/F is a normal extension iff H is normal subgroup of Gal(K/F) and moreover, $Gal(E/F) \cong Gal(K/F)/H$.