MODERN ALGEBRA

M A Rawoof Shaik (IFoS 30 + CSE 309) 2021

→ $(G, *)$ is algebraic structure : $*$ is b.o.
→ If $(G, *)$ satisfies
(i) closure property ⇒ k.a. groupoid
(ii) (i) and associativity ⇒ k.a. demi group
(iii) (i)(ii), & identity property ⇒ k.a. monoid.
(iv) (i)-(iii) & inverse property ⇒ k.a. group
(v) (i)-(iv) & commutativity ⇒ k.a abelian group.
→ In a group G, LCL & RCL hold.
→ In identity & inverse property, it is enough to show only left (or right) identity or inverse.
→ In a composition table,
(i) all entries ∈ G ⇒ closure satisfied ✓
(ii) any row coincides top row ⇒ identity ✓
(iii) every row & column contains e ⇒ inverse ✓
(iv) rows-columns interchangeable ⇒ commutative ✓
→ Klein 4 group ⇒ order = 4 & each elt is inverse of itself. eg. $(\{1,3,5,7\}, \times_8)$
→ Quaternion group = $\{\pm 1, \pm i, \pm j, \pm k\}$
→ Congruence modulo : $a \equiv b \pmod m \Leftrightarrow$ $a-b$ divided by m gives $r = 0 \Leftrightarrow$ $b \equiv a \pmod m \Rightarrow a +_m c = b +_m c$.
→ Equivalence = reflexive + symmetric + transitive. $\equiv \pmod m$ is an eqv relation.
→ $\bar{a} = [a] = \{x \in G / x \equiv a \pmod m\}$
→ $\bar{a} + \bar{b} = \overline{a+b}$; $a \times_p b = ab \pmod p$
→ If p is prime s.t. $p \mid ab$, then $p \mid a$ or $p \mid b$.
→ $G = \{1, 2, \ldots, p-1\}$ is an abelian group of order $p-1$ wrt to $\times_p$. If p is composite ⇒ NOT a group.
→ Law of Integral Exponents : $(G, \cdot)$ be a group. Then $a, aa, aaa, \ldots \in G$ by closure.
$(G, +) \Rightarrow a, 2a, \ldots, na, \ldots \in G$ by closure.
→ $(ab)^n = a^n b^n$ when G is abelian : $n \in N$
→ If p, n are relatively prime, ∃ 2 integers x, y s.t. $px + ny = 1$.

→ Let $(G, *)$ be a group. Let $a \in G$. If ∃ a least +ve integer n s.t. $a^n = e \Rightarrow O(a) = n$.
→ If ∃ a +ve int 'n' s.t. $a^n = e \Rightarrow O(a) \leq n$.
→ If ∄ no 'n' s.t. $a^n = e \Rightarrow O(a) = 0$ or ∞.
→ $O(e) = 1$; $O(a) = O(a^{-1})$; $O(a) \leq O(G)$ where G is finite.
→ $O(a) = O(b^{-1}ab)$: $O(ab) = O(ba)$
→ Div Algo Prop : $a = bq + r$: $0 \leq r < |b|$
→ All groups of order ≤ 4 are commutative.
→ $O(a) = n \Rightarrow O(a^k) = \frac{n}{\gcd(n,k)}$.
→ A perm $f : G \to G$ is a bijective function.
→ $O(S_n \text{ or } P_n) = n!$: degree = n (# of symbols)
→ S_n is finite group : $n \leq 2 \Rightarrow$ abelian ; $n \geq 3 \Rightarrow$ non-abelian
→ Orbit of 'a' under f : If ∃ a smallest +ve integer l s.t. $f^l(a) = a$, then $\{a, f(a), f^2(a), \ldots, f^{l-1}(a)\}$ is called the orbit of a under f.
→ $f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_k & a_{k+1} & \ldots & a_n \\ a_2 & a_3 & a_4 & \ldots & a_1 & a_{k+1} & \ldots & a_n \end{pmatrix}$ is a cyclic perm of length k & degree n.
→ A cycle of length 2 = transposition
→ f, g are disjoint cycles ⇒ $fg = gf$.
→ $f = (a, b\ c\ d) \Leftrightarrow f^{-1} = (d\ c\ b\ a)$
→ Order of a cyclic perm = length of the perm
→ Every cycle can be expressed as a product of transpositions in many ways-
$f = (a_1 a_2 \ldots a_n) = (a_1 a_n)(a_1 a_{n-1}) \ldots (a_1 a_3)(a_1 a_2)$
→ A perm expressed as a product of perm even (odd) # of transpositions is k.a. even (odd).
→ Cycle of length 'n' can be expressed as a product of $(n-1)$ transpositions.
→ If f is a product of disjoint cycles of length $m_1, m_2, \ldots, m_k$, then $O(f) = \text{LCM}[m_1, m_2, \ldots, m_k]$
→ $(fg)^{-1} = g^{-1}f^{-1}$; A_n - Alternating set of perms of degree n - all even perms

→ A Non empty subset of G_1 is called Complex of G_1.
→ $(MN)P = M(NP)$; $M^{-1} = \{m^{-1} \in G_1 / m \in M\}$
→ $MN = \{mn \in G_1 / m \in H, n \in N\}$; $(MN)^{-1} = N^{-1}M^{-1}$
→ $H \leq G_1$ if H is a group wrt b-o defd. in G_1.
→ $H \leq G_1 \Rightarrow H^{-1} = H$; $H \leq G_1 \Rightarrow HH = H$ (CONVERSE NOT TRUE)
→ Let $H \subseteq G_1$. $H \leq G_1 \Leftrightarrow$ (i) $a, b \in H \Rightarrow ab \in H$ (ii) $a \in H \Rightarrow a^{-1} \in H$. [FAILURE CHECK]
→ $H \leq G_1 \Leftrightarrow a \in H, b \in H \Rightarrow ab^{-1} \in H$ [SUCCESS CHECK]
→* $H \leq G_1 \Leftrightarrow HH^{-1} = H$ { → $a = x^{-1}ax \ \forall x \in G_1$, then a is called self conjugate elt of G_1 }
→ Let $H \leq G_1, K \leq G_1$. $HK \leq G_1 \Leftrightarrow HK = KH$
→ Normaliser, $N(a) = \{x \in G_1 / xa = ax\}$
→ Center, $Z = \{z \in G_1 / zx = xz \ \forall x \in G_1\}$
→ $H \leq G_1$, $a \in G_1$. Left coset $aH = \{ah / h \in H\}$
→ G_1 is abelian $\Rightarrow aH = Ha$; $a \in H \Rightarrow aH = H = Ha$
→ $a, b \in G_1$. $aH = bH \Leftrightarrow a^{-1}b \in H$; $Ha = Hb \Leftrightarrow ab^{-1} \in H$
→ $a, b \in G_1$. $a \in bH \Leftrightarrow aH = bH$; $a \in Hb \Leftrightarrow Ha = Hb$
→ Any 2 left (right) cosets are either disjoint or identical. G_1 = union of all left (right) cosets of H in G_1.
→ $a, b \in G_1$. $b^{-1}a \in H \Rightarrow a \equiv b \pmod H$
→ $\bar{a} = \{x \in G_1 / x \equiv a \pmod H\} = aH$.
→ Index of $H = [G_1 : H] = i_{G_1}(H)$ = # of distinct left (right) cosets $= \frac{O(G_1)}{O(H)}$ aka Lagrange Thm
→ $O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$.
→ For every group, there must exist cyclic subgroups generated by elts. of the group.
→ cyclic $G_1 \Rightarrow$ abelian G_1; $G_1 = \langle a \rangle \Rightarrow G_1 = \langle a^{-1} \rangle$
→ Every subgroup of a cyclic group is cyclic.
→ $O(G_1)$ = prime $\Rightarrow$ it is cyclic and # of generators $= p - 1$ ∴ $O(G_1) = 5 \Rightarrow G_1$ is abelian.
∴ every G_1 of order < 6 is abelian.
→ $G_1 = \langle a \rangle \Leftrightarrow O(G_1) = O(a)$
→ $O(G_1)$ = prime $\Rightarrow$ no proper subgroups for G_1
$O(G_1)$ = composite $\Rightarrow$ atleast 1 proper subgroup.
→ G_1 is union of mutually disjoint conjugate classes.

→ Let $G_1 = \langle a \rangle : o(a) = n$. $G_1 = \langle a^m \rangle \Leftrightarrow gcd(m, n) = 1$. (relatively prime)
→ Euler ϕ function: $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots$ where $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. $\phi(n)$ is the # of +ve integers $< n$ and rel. prime to n ∴ $\phi(n)$ = # of generators of cyclic group of order 'n'.
→ U_n denotes group of integers relatively prime to n under multiplication modulo n.
→ $a \in G_1$. $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^k \rangle : k = lcm(m,n)$
→ $H \leq G_1$ is $H \trianglelefteq G_1$, if $\forall x \in G_1, \forall h \in H$, $xhx^{-1} \in H$
→ $H \trianglelefteq G_1 \Leftrightarrow xHx^{-1} \subseteq H \ \forall x \in G_1$ & $xHx^{-1} = H$
→ A group having no proper normal subgroups is called a simple group. Eg. G_1s of prime order
→ $H \trianglelefteq G_1 \Leftrightarrow gH = Hg \ \forall g \in G_1$ {i.e. every left coset = right coset}
→ $H \trianglelefteq G_1 \Leftrightarrow H \cdot a \cdot Hb = Hab \ \forall a, b \in G_1$.
→ $H \leq G_1 : [G_1 : H] = 2 \Rightarrow H \trianglelefteq G_1$.
→ G_1 be abelian: $H \leq G_1 \Rightarrow H \trianglelefteq G_1$.
→ Let $N \trianglelefteq G_1 : H \leq G_1 \Rightarrow NH = HN$ & $HN \leq G_1$
→ $H \leq G_1 : N \trianglelefteq G_1 \Rightarrow H \cap N \trianglelefteq H$ & $N \trianglelefteq HN$
→ $N \trianglelefteq G_1 : M \trianglelefteq G_1 \Rightarrow NM \trianglelefteq G_1$
→ N is commutative with every complex of G_1
→ $M \trianglelefteq G_1 : N \trianglelefteq G_1$ s.t. $M \cap N = \{e\} \Rightarrow mn = nm$
→ $H \trianglelefteq G_1$. The set $\frac{G_1}{H}$ of all cosets of H in G_1 wrt coset multiplication is a group
→ Quotient group order $O(\frac{G_1}{H}) = \frac{O(G_1)}{O(H)}$
→ G_1 is abelian $\Rightarrow \frac{G_1}{H}$ is abelian.
→ G_1 is cyclic $\Rightarrow$ its every subgroup is normal
→ G_1 is cyclic $\Rightarrow \frac{G_1}{H}$ is cyclic. ($\frac{G_1}{Z}$ is cyclic $\Rightarrow G_1$ is abelian)
→ Conjugate elements: $a, b \in G_1$. $a \sim b$ if $\exists$ some $x \in G_1$ s.t. $a = x^{-1}bx$.
→ Relation of conjugacy is equivalence relation
→ $C(a) = \{x \in G_1 / x \sim a\} = \{y^{-1}ay / y \in G_1\}$
→ $f \in S_n$ s.t. $f: i \to j \Rightarrow \theta f \theta^{-1} : \theta(i) \to \theta(j)$ $\forall \theta \in S_n$. Ex: $\theta(1\,2\,3)\theta^{-1} = (\theta(1)\ \theta(2)\ \theta(3))$
→ G_1 is abelian $\Rightarrow C(a) = \{a\}$: $O(C(a)) = 1$.
→ $O(C(a)) = \frac{O(G_1)}{O(N(a))}$: $O(G_1) = \sum_{a \in G} O(C(a))$ (a.k.a class eqn of G_1)
→ $O(G_1) = O(Z) + \sum_{a \notin Z} \frac{O(G_1)}{O(N(a))}$ ← second form
→ If $O(G_1) = p^n$: p is prime, then $Z \neq \{e\}$: $o(Z) > 1$
→ If H is the ONLY subgroup of order n in G_1 then $H \trianglelefteq G_1$.

RINGS

M A Rawoof Shaik (IFoS 30 + CSE 309) 2021

→ $f: G \to G'$. $f(a \cdot b) = f(a) * f(b)$ $\forall a, b \in G \Rightarrow$ f is a homo. $(G, \cdot)$ & $(G, *)$ are 2 groups.

→ f is homo and onto $\Rightarrow G'$ is homomorphic image of G. i.e. $f(G) = G'$. $[G \simeq G']$

→ f is homo and 1-1 (injective) $\Rightarrow f$ is isomorphism

→ f is homo, 1-1, & onto (bijective) $\Rightarrow G'$ is isomorphic image of G. $[G \cong G']$

→ A homo $f: G \to G$ is called endomorphism

→ An iso $f: G \to G$ is called automorphism

→ $f(e) = e'$; $f(a^{-1}) = [f(a)]^{-1}$

→ The homomorphic image $f(G) \leq G'$

→ f is homo : G is abelian $\Rightarrow f(G)$ is abelian

→ f is iso : G is abelian $\Leftrightarrow f(G)$ is abelian

→ f is homo: $\text{Ker} f = \{x \in G / f(x) = e'\} = K \trianglelefteq G$

→ f is homo : $\text{Ker} f = \{e\} \Leftrightarrow f$ is 1-1.

→ **I FUND THEOREM OF HOMO:** Let $f: G \to \frac{G}{N}$ s.t. $f(x) = Nx$ $\forall x \in G \Rightarrow f$ is homo & $\text{Ker} f = N$

→ **II FUND TH OF HOMO:** $G \simeq G' \Rightarrow \frac{G}{K} \cong G'$.

→ f is homo $\Rightarrow O(a) / O(f(a))$; $O(a) = O(f(a))$ for iso

→ f is homo: G is cyclic $\Rightarrow G'$ is cyclic; $\Leftrightarrow$ for iso

→ Epimorphism = homo + onto; monomorphism = 1-1

→ When we find an isomorphic mapping $G \to G'$, then we must preserve identities, inverses, & orders.

→ Cayley: Every group is isomorphic to some subgroup of the group $A(S)$ of all permutations of some set S, i.e., $G \cong \psi(G) \leq A(G)$.

→ $f: G \to G'$ be a homo. if $H \leq G$, then $f(H) \leq G'$

→ A group of order pq : p & q are primes w/ $p > q$ has atmost 1 subgroup of order p.

→ $H \leq G$: $x^n \in H$ $\forall x \in G \Rightarrow H \trianglelefteq G$.

→ $\frac{G}{N}$ is abelian $\Leftrightarrow xyx^{-1}y^{-1} \in N$ $\forall x, y \in G$.

→ $(R, +, \times)$ is called a ring if it satisfies (i) $(R, +)$ is an abelian group, (ii) $(R, \times)$ is a semi-group, (iii) distributive laws {LDL, RDL}

→ If R contains x^n identity, then R is a ring w/unity

→ If $\forall a, b \in R \Rightarrow a \times b = b \times a$, then R is called a commutative ring.

→ If non-zero elts of R form a group w.r.t $\times^n$, then R is called a division ring.

→ If $a, b \in R$: $a \neq 0, b \neq 0$ and $ab = 0$, then R is a ring with zero divisors.

→ R is a ring w/o zero divisors if $a, b \in R$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$.

→ A commutative ring w/ unity and w/o zero divisors is called an integral domain (ID)

→ A commutative division ring is called field.

→ If $0, a, b \in R$, then (i) $0a = a0 = 0$, (ii) $a(-b) = (-a)b = -(ab)$, (iii) $(-a)(-b) = ab$, and (iv) $a(b - c) = ab - ac$.

→ R is without zero divisors iff cancellation laws hold.

→ A division ring (and a field) has no zero divisors.

→ Every field is an ID; finite ID $\Rightarrow$ field.

→ A finite comm. ring w/o zero divisors is a field.

→ To satisfy inverse property in order to show that ring is field, use R with some elt and multiply so one of the products is equal to 1 $\Rightarrow$ inv exists

→ $I_p = \{0, 1, 2, \ldots, p-1\}$. $(I_p, +_p, \times_p)$ forms a field when p is prime. If p is not prime, then I_p has zero divisors, & no x^{ve} inv may exist.

→ if $a^2 = a$ $\forall a \in R$, then R is called Boolean Ring

→ R is boolean $\Rightarrow$ (i) $a + a = 0$, (ii) $a + b = 0 \Rightarrow b = a$, (iii) R is abelian

→ The only idempotent elts in a field (or ID) are 0 and 1.

→ If $\exists n \in N$ s.t. $a^n = 0$, then a is called nilpotent element of R (for ex, 0).

→ An ID has no nilpotent other than 0.

→ Matrices can be a good example for questions on non commutative rings.

→ Let $S \neq \phi$, $S \subseteq R$. If S is a ring (field) wrt b-o defd. in R then S is called a subring (subfield) of R.

→ If $(S,+,\cdot)$ is a subfield of $(F,+,\cdot)$, then (a) $(S,+) \leq (F,+)$; (b) $(S-\{0\},\cdot) \leq (F-\{0\},\cdot)$.

→ If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$, then (a) $(S,+) \leq (R,+)$; (b) $(S,\cdot)$ is a subsemigroup of $(R,\cdot)$; (c) distributive laws hold.

→ S is a subring of R iff $a,b \in S \Rightarrow a-b \in S$ & $ab \in S$

→ K is a subfield of F iff $a,b \in K \Rightarrow a-b \in K$, $ab^{-1} \in K$.

→ The center of a ring R is a subring of R.

→ Char $R = n \Rightarrow n$ is the smallest +ve integer such that $na = 0 \ \forall a \in R$.

→ If $\exists$ no +ve integer n s.t. $na = 0 \ \forall a \in R$, then Char $R = 0$ or infinite.

→ In general, Char $Z_n = n$.

→ If R is a ring w/unity, then Char $R = p$ iff p is least +ve integer s.t. $p.1 = 0$.

→ The char of an ID (or field) is zero or prime. (for infinite ID (field))

→ R is Boolean $\Rightarrow$ Char $R = 2$.

→ $S \overset{*\phi}{\subseteq} R$ is called left ideal of R iff

(i) $(S,+) \leq (R,+)$, i.e. $\forall a,b \in S \Rightarrow a-b \in S$.

(ii) $s \in S$, $r \in R \Rightarrow rs \in S$ [$sr \in S$ for right ideal].

→ S is an ideal of R, if it is both left & right sided ideal.

→ $S = \{0\}$ is the null ideal; $S = R$ is unit ideal.

→ If S is [ideal of ring w/unity R] and $1 \in S$, then $S = R$.

→ A field has no proper ideals. [ideal of field contains 1]

→ S_1, S_2 are ideals of $R \Rightarrow S_1 \cap S_2$ is ideal of R.

→ A, B are ideals of $R \Rightarrow AB, A \cap B, A+B$ are ideals [$AB \subseteq A \cap B$]

→ Two ideals A & B of R satisfying $A+B=R$ are called co-maximal ideals.

→ $S \subseteq R$. An ideal U of R is said to be generated by S if (i) $S \subseteq U$, (ii) for any ideal V of R, $S \subseteq V \Rightarrow U \subseteq V$. [(S) or $\langle S \rangle = U$].

→ If ideal U of R is generated by a single element $S = \{a\}$, then U is called principal ideal.

→ If U is principal ideal of R generated by $a \in R \Rightarrow$ (i) $a \in U$ (ii) U is ideal of R (iii) V is any ideal of R & $a \in V \Rightarrow U \subseteq V$.

→ If R is comm, $1 \in R$, $a \in R$, then $U = \{ra / r \in R\}$ is the principal ideal of R generated by 'a'.

→ R is called a P.I. ring if every ideal in R is a P.I.

→ An integral domain R is a P.I. domain if every ideal in R is a P.I.

→ Every field is a Principal Ideal Domain.

→ S is an ideal of R. $S+a = \{s+a / s \in S\}$ is called the right coset of S in R. (i) If $a,b \in R$, then $S+a = S+b \Leftrightarrow a-b \in S$, (ii) $a \in S \Leftrightarrow S+a = S$. [cosets aka residue classes]

→ $[a] \Rightarrow \frac{R}{S} = \{S+a / a \in R, S \text{ is an ideal of } R\}$. is called the quotient ring or residue class ring.

→ An ideal P of R is called a prime ideal if for any $a,b \in R$; $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

→ Let R be comm ring. An ideal P of R is a prime ideal iff R/P is an integral domain.

→ An ideal $M \neq R$ is a maximal ideal if for any other ideal U s.t. $M \subset U \subset R$, then either $M = U$ or $U = R$.

→ For the ring of integers Z, any ideal generated by a prime integer is a maximal ideal.

→ If R is a comm ring with unity then an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

→ For a comm. ring w/unity, every maximal ideal is a prime ideal. [Converse NOT true]

→ Let $(R, +, \cdot)$ and $(R', \oplus, \otimes)$ be two rings $f: R \to R'$ is a homomorphism if (i) $f(a+b) = f(a) \oplus f(b)$, (ii) $f(a \cdot b) = f(a) \otimes f(b)$

→ If U is an ideal of R, then $\frac{R}{U} = \{x + U / x \in R\}$ is also a ring. $f: R \to R/U$ defd. by $f(x) = x + U$ $\forall x \in R$ is called natural homomorphism from R onto R/U $\left(\frac{R}{U} \cong R/U\right)$

→ Let $f: R \to R'$ be homo, then (i) $f(0) = 0'$, (ii) $f(-a) = -f(a)$ $\forall a \in R$, (iii) $f(a-b) = f(a) - f(b)$.

→ $f: R \to R'$ is homo, then $f(R)$ is subring of R'.

→ Every homomorphic image of a comm ring is a comm ring. Converse NOT True.

→ The homomorphic image of a ring w/unity is also a ring w/unity. Converse NOT true.

→ $\text{Ker} f = \{x \in R / f(x) = 0', 0' \text{ is identity in } R'\}$

→ $\text{Ker} f$ is an ideal of R.

→ f is homo. f is iso $\Leftrightarrow \text{Ker} f = \{0\}$

→ $R \cong R' \Rightarrow \frac{R}{\text{Ker} f} \cong R'$

→ If $(G, +)$ is abelian group then the set of all endomorphisms of G, $\text{Hom}(G, G)$, is a ring w/addition & composition of mappings. (homo + onto)

→ R is said to be imbedded in R' if $\exists$ an isomorphism $f: R \to R'$. R' is called extension ring or over ring of R.

→ R be any ring, then the extension ring w/unity is $R \times Z = \{(r, m) / r \in R, m \in Z\}$ and unity is $(0, 1)$.

$(r, m) + (s, n) = (r + s, m + n)$

$(r, m) \cdot (s, n) = (rs + ms + rn, mn)$

→ $f: R \to R \times Z : f(r) = (r, 0)$ $\forall r \in R$ is isp.

→ Every I.D. can be embedded in a field, i.e. from elts of D it is possible to construct $F : D' \subseteq F$ and $D \cong D'$.

→ An ideal I of comm ring R is called semi prime if $a^2 \in I \Rightarrow a \in I$ $\forall a \in R$. Clearly every prime ideal is semiprime.

→ An I.D. is said to be an Euclidian ring/domain if for every $a (\neq 0) \in R$, there is a defd. non-negative integer $d(a)$ s.t.

(i) $\forall a, b \in R$, $a \neq 0, b \neq 0$; $d(a) \leq d(ab)$, &

(ii) for any $a, b \in R$, $b \neq 0$, $\exists q, r \in R$ s.t. $a = bq + r$, where either $r = 0$ or $d(r) < d(b)$

Euclidian Valuation

→ From above note that $d: R - \{0\} \to Z$ is a mapping such that (i) $d(a) \geq 0$ $\forall a \in R - \{0\}$,

(ii) $d(a) \leq d(ab)$ for all $a, b \in R - \{0\}$,

(iii) $\exists q, r \in R$ so that $a = bq + r$: $r = 0$ or $d(r) < d(b)$ for any $a \in R$, $b \in R - \{0\}$.

Euclidian algorithm

→ Every field is an Euclidean ring.

→ Every Euclidean ring possesses unity elt.

→ Let R be a comm ring, and $a,b \in R$. If $\exists q \in R$ s.t. $b = aq$, then 'a' divides 'b'. a is a divisor / factor of b.

→ Every elt $a \in R$ is divisor / factor of '0'.

→ $a \in R$ is a unit in R if $\exists b \in R$ s.t. $ab = 1$. Here b is also a unit of R. (b is the multiplicative inverse of a)

→ If a, b are 2 units in R, then 'ab' is also a unit.

→ $a \neq 0$ is a unit of a E.D. $\Leftrightarrow d(a) = d(1)$.

→ a is an associate of b if $a = bu$, where u is a unit in R. $\therefore d(a) = d(bu) = d(b)$.

→ Let R be a comm ring and a, b be 2 non-zero elts. $d \in R$ is called h.c.f or g.c.d of a & b if (i) d/a and d/b, (ii) whenever $c \neq 0 \in R$ is s.t. c/a and c/b, then c/d. hcf is denoted by (a,b). $\ell \neq 0 \in R$ is called lcm of a & b if (i) a/ℓ & b/ℓ, (ii) whenever $x \neq 0 \in R$ is s.t. a/x & b/x, then ℓ/x. lcm is denoted by $[a,b]$.

→ If d_1, d_2 are 2 gcds of a & b, then d_1, d_2 are associates of the ring.

→ In a Euclidean ring R; a, b are relatively prime $\Leftrightarrow (a,b)$ = unit elt of R.

→ b is a proper divisor of a $\Rightarrow a = bd$ where d is not a unit. O.W its improper.

→ R is a comm ring w/ unity. A non-zero non-unit $p \in R$ is said to be an irreducible elt if $p = ab \Rightarrow a$ or b is a unit. i.e. p has no proper factors (p should have a unit associate).

→ A non-zero non-unit elt $p \in R$ is called a prime elt, if p/ab $(a,b \in R)$ $\Rightarrow$ either p/a or p/b.

→ A field has neither any irreducible element nor any prime element. (bcz every elt is unit)

→ Let R be an I.D. w/ unity, then every prime elt of R is irreducible.

→ In a PID, an elt is prime $\Leftrightarrow$ it is irreducible

(*) → R is a PID. $A = \langle a \rangle$ is a maximal ideal $\Leftrightarrow$ a is an irreducible elt of R. $\Leftrightarrow$ a is a prime elt of R.

→ R is a PID. A non-zero ideal $P \neq R$ is prime $\Leftrightarrow$ P is maximal.

→ Field $\Rightarrow$ ED $\Rightarrow$ PID $\Rightarrow$ UFD. (we can use algo in any ideal; define any mapping d)

→ $R[x] = \left\{ f(x) = a_0x^0 + a_1x^1 + \dots + a_nx^n / a_i \in R \text{ & } n \geq 0, n \in \mathbb{Z} \right\}$

→ R is comm $\Rightarrow R[x]$ is commutative
R has unity $\Rightarrow R[x]$ has unity
R is a field $\Rightarrow R[x]$ is an I.D.

→ Degree of zero polynomial is not defined.

→ $\deg(f(x) \pm g(x)) \leq \max\{\deg f(x), \deg g(x)\}$

→ $\deg(fg) \leq \deg f + \deg g$.

→ If R is an I.D. $\deg(fg) = \deg f + \deg g$

→ If R is an ID w/ unity, then units of R and R[x] are same.

→ Every ring R can be imbedded in R[x]. (i.e. $R \cong$ subring of $R[x]$)

→ R is an ID w/ unity then any irreducible elt of R is an irreducible elt of R[x].

→ If F is a field $\Rightarrow F[x]$ is an E.D.

→ F is a field $\Rightarrow F[x]$ is a P.I.D.

→ The ideal $A = \langle p(x) \rangle$ in $F[x]$ is a maximal ideal $\Leftrightarrow p(x)$ is an irreducible elt of $F[x] \Leftrightarrow \frac{F[x]}{\langle p(x) \rangle}$ is a field.

→ Let R be an ID w/unity. Then R is a UFD if every non-zero, non-unit elt $a \in R$ can be expressed (uniquely) as a product of finite no. of irreducible elements.

If $a = p_1 p_2 \dots p_m$ & $a = q_1 q_2 \dots q_n$, then $m = n$ and each p_i is an associate of some q_j.

→ In a UFD, a is prime $\Leftrightarrow a$ is irreducible

→ ∴ If R is an ID w/unity, then every non-zero, non-unit elt is a finite product of prime elts $\Leftrightarrow R$ is a UFD.

→ Let R be a UFD and $f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$. Then content of polynomial $c(f) = \gcd(a_0, a_1, \dots, a_n)$ and a poly $f_1(x)$ is said to be primitive if $c(f_1)$ is a unit. Also $f(x) = c(f) f_1(x)$.

→ R be an ID w/unity. $f(x) \in R[x]$ is said to be irreducible over R whenever $f(x) = g(x) h(x)$ then either $\deg(g(x)) = 0$ or $\deg(h(x)) = 0$.

→ Eisenstein Criterion of Irreducibility over $\mathbb{Q}$:
Let $f(x) = a_0 + a_1 x^1 + \dots + a_n x^n$ be a poly w/integer coeff. Let p be a prime s.t $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}$ $p \nmid a_n$ & $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$, the field of rational nos.

EXAMPLES:

→ An infinite group with finite no. of right cosets: $G_1 = I$, $H = 3I$.

→ An infinite group with infinite no. of right cosets: $G_1 = \mathbb{R}$ or $\mathbb{Q}$.

→ $[G_1 : H] = 2 \Rightarrow H \trianglelefteq G_1$, but converse NOT true. example is quaternion group. taking $H = \{1, -1\}$, $[G_1 : H] = 4$.

→ If G_1 is abelian $\Rightarrow N(a) = Z$.

→ Group is not cyclic but every proper subgroup is cyclic. Ex: is Quaternion group.

→ ~~If a composite~~ An infinite group in which infinitely many elements have finite order and infinitely many elements have infinite order is $C^* = C - \{0\} = \{a + ib / a, b \in \mathbb{R} : a, b \text{ both } \neq 0\}$

→ Every abelian grp is not cyclic. For ex, $G_1 = \{A, B, C, D\}$: $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

→ A non-abelian group whose every subgroup is normal is called Hamilton group.

→ Two groups of the same order may not be isomorphic. Ex: Z_6 & S_3 {∵ Z_6 is comm but S_3 is NOT}

→ Two groups may be commutative and finite, yet NOT isomorphic. Ex: Z_4 & K_4 {∵ Z_4 is cyclic & K_4 is non-cyclic}.

→ Two groups may be infinite & commutative, yet NOT isomorphic. Ex: $(\mathbb{Z}, +)$ & $(\mathbb{Q}, +)$.

→ Two groups may be infinite, noncyclic but commutative, yet NOT isomorphic. Ex: $(\mathbb{R}^*, \cdot)$ & $(\mathbb{C}^*, \cdot)$. {∵ $\mathbb{C}^*$ has i of order = 4, but $\mathbb{R}^*$ has no elt of order = 4}.

→ Union of 2 subrings need not be a subring. for ex, $R = I$, $S_1 = 2I$, $S_2 = 3I$. Same example also holds in case of ideals.

→ For a comm. ring w/o unity, a maximal ideal need not be a prime ideal. Ex: (4) is maximal ideal of $E = (2)$ but it is NOT prime ideal (∵ $2, 2 \in E$ $2 \cdot 2 = 4 \in (4)$ but $2 \notin (4)$)

→ The field $\mathbb{Q}$ with $d(a) = 1$ $\forall a \neq 0 \in \mathbb{Q}$ is a E.D. However, $\mathbb{Q}$ with $d(a) = |[a]|$ $\forall a \neq 0 \in \mathbb{Q}$ is not a E.D. (Euclidean Domain)

→ Let $S = \{0\}$ be an ideal of $(I, +, \times)$ then S is a prime ideal but S is NOT maximal.

→ Also any ideal generated by a prime no is a prime ideal. NOT true w/ composite no.

→ Every non-zero elt in a field is a unit. Thus a field has neither irreducible nor prime elts.

→ 2 grps are isomorphic ⇒ same order, both are commutative, cyclic together or both are NOT.

→ $H \leq G_1 \Rightarrow H^{-1} = H$. Converse NOT true. For ex $H = \{-1\} = H^{-1}$ ⊄ $G_1 = \{1, -1\}$.

→ P_3 is a non abelian group but its subgroup A_3 is abelian. Also Quaternion grp.

→ Sum of 2 subrings not a subring ⇒ $S_1 = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ $S_2 = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$ $S_1 + S_2 = \begin{pmatrix} a & c \\ b & 0 \end{pmatrix}$ is NOT a subring

finite / infinite
↓ commutative (Z_6 S_3)
↓ cyclic (Z_4 K_4) ($\mathbb{Z}^+$ R^+)
↓ order (R^* C^*)

→ A non-commutative ring without unity such that $(xy)^2 = x^2 y^2$ is $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} / a, b \in I \right\}$.

→ Ring is non-commutative, but subring is comm. ⇒ $R = M_{2\times 2}$ and $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} / a \in I \right\}$

Various Tricks Involved in Solving problems.

1) Use examples of matrices and permutations (commutative etc.)
2) Use division algorithm for ques on cyclic group.
3) Use orders and Lagrange theorem for subgroups and Δ.
4) Use Fund theorems of Homomorphism, lagrange theorem, orders of elts etc for homomorphisms and $\cong$.
5) Use Pigeon hole principle in IDs, fields, etc.
6) Use examples as $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ in Rings

EXAMPLES:

→ Center Z of R is a subring, but need not be an ideal:
Let $R = M_{2\times 2}$, then $Z = \left\{ \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \right\}$ is not an ideal.