Revision is the most crucial part of mathematics preparation in Civil Services Examination. For that purpose, I had prepared short notes on each topic of the syllabus which I am sharing here. I would suggest aspirants to use this as just a reference for quick revision and not as your primary source. This optional requires good understanding of the topic which cannot be derived from short notes.

It is the process of preparing such notes that gives a candidate confidence about his or her preparation and brings conceptual clarity. Hence I would encourage aspirants to do this exercise themselves even if it is time consuming.

All the best!

Regards,
Yogesh Kumbhejkar
AIR 8 - CSE 2015

MODERN ALGEBRA

Set I - A

(1) Cartesian Product $A \times B = \{(a,b) / a \in A, b \in B\}$
where (a,b) is an ordered pair.
Any subset of $A \times B$ is relation from A to B given both sets are non-empty.
Any subset of $A \times A$ is a binary relation given A is non-empty. Note it is different from binary operation.

A function $f: A \times A \to A$ is called a binary operation.

(2) A non-empty set equipped with one or more binary operation is an algebraic structure.

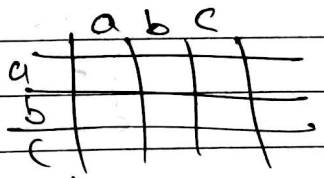
Property	Called
(1) Closure	Groupoid or Quasigroup
(2) Closure + Associativity	Semigroup or Demigroup
(3) Closure + Asso. + Identity	Monoid
(4) Closure + Asso. + Identity + Inverse	Group
(5) Group + Commutative	Abelian

(3) Number of elts. in a group is called order of the group & denoted by $O(G)$ or $|G|$.

(4) Properties of Groups
(a) In a group G, left & right cancellation laws hold.
(b) The linear eq. $ax = b$ & $ya = b$ have unique solutions in G for x & y.
(c) A finite semigroup that satisfies cancellation property is a group.
(Proof uses piegeonhole principle)

(5) Sufficient conditions for proving a structure is group
1. Closure Property
2. Associativity
3. Existance of left identity
i.e. $\exists\, e \in G$ s.t. $\forall a \in G \quad ea = a$
4. Existance of left inverse
i.e. $\forall a \in G \quad \exists\, a^{-1} \in G$ s.t. $a^{-1}a = e$

(6) Composition table for finite sets



(a) If all elts. of table are from G, closure is satisfied.
(b) If any row in table is identical to top row, identity exists & is equal to extreme left elt. of that row
(c) If every row & column contains identity, then inverse exists.
(d) If interchanging rows & columns doesn't change table, it mean abelian property.
(e) Note associativity has to be shown separately.

(7) Quaternion Group
$T = \{ \pm 1, \pm i, \pm j, \pm k \}$
multiplication given by $i^2 = j^2 = k^2 = -1$
& $ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$
This is a non-abelian group of order 8 known as quaternion group.

Set I-B

(1) Addition modulo m shown by $a +_m b$
Multiplication modulo m shown by $a._m b$

Congruence modulo m $\Rightarrow a \equiv b \pmod m$ means $a-b \mid m$.

(2) Congruence modulo m is an equivalence operation on integers. So it partitions Z into equivalence classes called residue classes modulo m.
$\{0, 1, \ldots m-1\}$ is called set of residues mod m.
$\{\bar{0}, \bar{1}, \ldots \overline{m-1}\}$ is residue classes mod m set.

(3) Addition of residue classes
$\bar{a} + \bar{b} = \overline{a+b}$
The set of residue classes mod m form an abelian group w.r.t. above addition operation.

(4) The group $\{1, 2, 3 \ldots, p-1\}$ forms abelian group if p is prime w.r.t. multiplication mod p.

Note for addition mod m, its $\{0, 1, \ldots m-1\}$ group & for multi. mod p; it is $\{1, 2 \ldots, p-1\}$ group (so no 0 in 2nd case)

(5) Defining integral exponents
$a^0 = e$, $a^1 = a$, $a^{n+1} = a^n . a$, $a^{-n} = (a^{-1})^n$
Above is obv. with multiplication operation.
With addition operation, it becomes na instead of a^n.

Then $(a^m)^n = a^{mn}$, $a^m . a^n = a^{m+n}$
& If G is abelian then $(ab)^n = a^n b^n$

(6) Order of an element a in group G.
$o(a) = n$ if $a^n = e$ & n is least +ve integer
If $\exists$ no such finite n, we call it is of zero/infinite order.

In a group $o(a) = o(a^{-1})$
$o(a^r) \leq o(a)$ $a \in G$ & $r \in N$
$o(ab) = o(ba)$
if p is prime, then $o(a^p) = o(a)$
Order of a is also denoted by $|a|$. Remember this. $|a|$ in M.Alg. questions is order & not modulus.

(7) All elements of order 5 or below are abelian.
If $o(G) = 4$ & every elt is its own inverse, that group is known as Klein-4 group.

(8) Good question

Find inverse in $\mathbb{Z}_5$ of following

$$\begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 3 \end{bmatrix}$$

$\Rightarrow$ In $\mathbb{R}$ inverse is $\begin{bmatrix} 1 & -1 & 4/3 \\ 0 & 1/2 & -2/3 \\ 0 & 0 & 1/3 \end{bmatrix}$

In $\mathbb{Z}_5$; we use; $\frac{1}{2} \cdot 2 = 1 \iff 3 \cdot 2 = 1$ (replace $\frac{1}{2}$ by 3)

$\frac{1}{3} \cdot 3 = 1 \iff 2 \cdot 3 = 1$ (replace $\frac{1}{3}$ by 2)

$\frac{4}{3} \cdot 3 = 4 \iff 3 \cdot 3 = 4$

($\mathbb{R}$) ($\mathbb{Z}_5$)

$\therefore$ inverse $\begin{bmatrix} 1 & -1 & 3 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{bmatrix}$ Brilliant.

PERMUTATION GROUPS

(1) Degree of permutation :- Number of elements in set A whose permutations we are taking.
i.e. Degree of group S_n is n while order is n!
S_n is called symmetric set of permutation of degree n.

(2) 2-line notation → $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ $a_i, b_i \in A$

for $n \leq 2$, S_n is abelian for $n \geq 3$, it is non-abelian

(3) * Orbit of 'a' under permutation f* $a \in A$
Let f be permutation of set A.
& let $f^n(a) = a$
then $\{a, f(a), f^2(a) \cdots, f^{n-1}(a)\}$ is called orbit of 'a' under f.
The ordered orbit above is called 'cycle of a'

(4) Cyclic Permutation
Cyclic permutation $(1, 2, 4, 5)$ on set $\{1 \text{ to } 8\}$ is cycle of length 4 & degree 8.

Cycle of length 1 → identity permutation
Cycle of length 2 → transposition

Disjoint cycles :- 2 cycles which have no element in common.
Product of disjoint cycles is commutative.

Inverse of $(1\ 2\ 3\ 4) = (4\ 3\ 2\ 1)$

(5) Order of Cyclic Permutation
Let f be cyclic permutation. Then smallest n s.t. $f^n = I$ is order of f.

(6) Every permutation can be expressed as product of disjoint groups.

Every cycle can be expressed as product of transpositions.

$f = (1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$

i.e. $f = (a_1\ a_2 \ldots a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \ldots (a_1\ a_2)$

(7) Even Permutation = Can be expressed as product of even number of transpositions.

Odd Permutation = Product of odd no. of transpositions.

Every transposition is odd permutation.

Identity is even permutation.

The cycle of length n = product of $(n-1)$ transpositions

$\therefore$ Even length cycle = odd permutation

Odd length cycle = Even permutation

Product of 2 odd permutation = even perm. (obv.!)

Out of $n!$ perm. of S_n, half are even & half are odd.

(8) A_n :- Alternating Set of permutations = Set of even permutations of S_n.

The alternating set A_n forms a group of order $\frac{n!}{2}$ w.r.t. multiplication of permutations.

(9) * Order of n-cycle *

Let $f = (a_1\ a_2 \dots a_n)$ be cycle of length n.

f^2 moves the elts. by 2 places.

i.e. $f^2 = (a_1\ a_3 \dots a_n)\ (a_2 a_4 \dots a_{n-1})$ (n be odd)

$f^3 = (a_1\ a_4\ a_7 \dots)\ (a_2\ a_5 \dots)(a_3\ a_6 \dots)$

$\vdots$

$f^n = (a_1)(a_2) \dots (a_n) = I$

So order of a cycle of length n is n.

(10) Let $f = f_1 f_2 f_3$ ∎

where f_1, f_2, f_3 are disjoint cycles of length m_1, m_2, m_3.

Then order $(f) = LCM(m_1, m_2, m_3)$

(11) Cayley's thm

Every group is isomorphic to a subgroup of P_n for an appropriate n.

→ Proof is simple, for a given group G, consider A(G) i.e. set of permutation of G. (obv. A(G) is a group)

Define mapping from $\phi: G \to A(G)$ as

$\forall g \in G$, $\phi(g) = \gamma_g$ where γ_g is permutation given by $x \to xg$.

This turns out to be an isomorphism.

(12) eg. Find Group G s.t. every proper subgroup of G is cyclic but G is not

→ Permutation groups help. Consider P_3. It is of order 6 & hence proper subgroups are of prime order 2 or 3 ∴ cyclic.

But P_3 is not abelian & hence not cyclic.

consider $(1,2)(2,3) = (2,3,1)$ & $(2,3)(1,2) = (1,3,2)$

(13) good example:- Find β & γ ($\in S_4$) when $\beta\gamma = (1432)$, $\gamma\beta = (1243)$ & $\beta(1) = 1$

→ $\gamma\beta(1) = \gamma(\beta(1)) = 2$ ∴ $\gamma(4) = 2$ & $\beta\gamma(4) = \beta(\gamma(4)) = 3$ ∴ $\beta(2) = 3$

& $\gamma\beta(2) = \gamma(\beta(2)) = 4$ ∴ $\gamma(3) = 4$ & so on, you get $\beta = (1423)$, $\gamma = (234)$

SUBGROUPS

(1) Complex

A non empty subset of group G is called complex of G.

Subgroup

G group & $H \subseteq G$, $H \neq \phi$ is called subgroup if it forms a group w.r.t. binary operation of G.

(2) Properties of Subgroup H

(a) $H^{-1} = H$

(b) $HH = H$

Let $H \subseteq G$; then H is a subgroup iff

(1) $a, b \in H \Rightarrow ab \in H$ & $a \in H \Rightarrow a^{-1} \in H$

Another sufficient condition

(2) $a, b \in H \Rightarrow ab^{-1} \in H$

Another sufficient condition

(3) $HH^{-1} \subseteq H$

Now if G is group & H is finite subset then H is subgroup iff $a, b \in H \Rightarrow ab \in H$

(3) Let $H \leq G$ & $K \leq G$, then $HK \leq G \iff HK = KH$

Intersection of arbitrary family of subgroups is subgroup
Union of subgroups need not be subgroup.

Union of 2 subgroups is subgroup iff. one subgroup is contained in another subgroup.

(4) *Normalizer of an element of a group*

Let $a \in G$ then

$N(a) = \{x \in G / xa = ax\}$

$N(a)$ is a subgroup of G.

Self conjugate or invariant elt. of G

$a \in G$ s.t. $a = x^{-1}ax \ \forall x \in G$ is called self conjugate element.

Set of all self conjugate elements is centre of G.

i.e. centre $Z = \{z \in G / zx = xz \ \forall x \in G\}$

Z is a normal subgroup of G.

(5) A group G can never be expressed as union of 2 of its proper subgroups.

(6) *Cosets*

Let $H \leq G$, then $aH = \{ah / h \in H\}$ is left coset of H generated by a.

$Ha = \{ha / h \in H\}$ is right coset of H generated by a.

Left & right coset need not be subgroup of G.

(7) If $a \in H$, $aH = Ha = H$

If $aH = bH \Rightarrow a^{-1}b \in H$

$Ha = Hb \Rightarrow ab^{-1} \in H$

(8) Any 2 left (right) cosets of a subgroup are either disjoint or identical.

Right coset decomposition of G = Set of all right cosets of H which give a partition of G.

If $H \leq G$, no. of left cosets = no. of right cosets

(9) Congruence Modulo H

Let $H \leq G$; then for $a, b \in G$ if $b^{-1}a \in H$, we say $a \equiv b \pmod{H}$

The relation $a \equiv b \pmod{H}$ is an equivalence relation.

(10) Index of subgroup H in G = No. of distinct right cosets of H = $[G : H] = i_G(H)$

(11) LAGRANGE'S THEOREM

Order of subgroup H divides order of group G.

This is for finite groups only.

$$i_G(H) = \frac{O(G)}{O(H)}$$

(12) Converse of Lagrange need not be true.

i.e. $m \mid O(G) \not\Rightarrow \exists$ subgroup of order m.

Cauchy's Thm for abelian groups $\Rightarrow$ Inverse is true for abelian group i.e. if $m \mid O(G) \Rightarrow \exists a \in G$ s.t. $a^m = e$, $\therefore \langle a \rangle$ is subgroup of size m.

(13) If G is finite group & $a \in G$ then order of a divides $O(G)$.
$a^{O(G)} = e \quad \forall a \in G$

also a group of order P (prime) doesn't have proper subgroups.

(14) ~~*~~ Poincare's Thm ~~*~~
If G is a group & H and K are 2 subgroups of finite index in G $\Rightarrow$ then $H \cap K$ will also be of finite index.

(15) ~~Thm~~ If H & K are finite subgroups then [useful item]

$$O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$$

This ~~group~~ gives corollary as
If $H, K \leq G$ & $O(H) > \sqrt{O(G)}$
$O(K) > \sqrt{O(G)}$
$\Rightarrow O(H \cap K) > 1.$

(16) A group of size 35 can have at max 1 subgroup of size 7.
$\rightarrow$ If possible let H & K be subgroups of order 7
Then $H \cap K$ is subgroup of H.
$\therefore O(H \cap K) \mid O(H) \quad \therefore O(H \cap K) = 1$ or 7
$O(H \cap K) = 7 \Rightarrow H = K$
$O(H \cap K) = 1 \Rightarrow O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)} = 49$ #

This also helps in proving why $G3$ is not a simple group i.e. doesn't contain proper normal subgroup
Think how!

CYCLIC GROUP

classmate
Date
Page 85

(1) Cyclic Group
If $\exists\, a \in G$ s.t. $G = \{a^n / n \in Z\}$
then a is generator of cyclic group G.
$\langle a \rangle = G$
Note we take $a^n / n \in Z$ & not $n \in N$. So $a^0 = e$ $(a^{-1})^n$ taken

(2) Let G be any group & $a \in G$ then
$H = \{a^n / n \in Z\}$ is cyclic subgroup of G generated by a.

(3) Set of residue classes mod m forms cyclic group with respect to addition.

(4) Every cyclic group is obviously abelian. Reverse is not true.

(5) If a is a generator, a^{-1} is also a generator.
An infinite set can have atmost 2 generators.

(6) Every subgroup of cyclic group is cyclic.
Every group of prime order is cyclic & $\therefore$ abelian
(later we see if $O(G) = p^2$ then also it is abelian)

(7) If finite group of order n contains an element of order n, then obv. it is cyclic.

(8) If a is generator & $O(a) = n$ then if $(m, n) = 1$ then a^m is also a generator.

So when m/n, we get subgroups of G with $\langle a^m \rangle$

(9) Euler - ϕ function
$\phi(n)$ is numbers less than n & coprime to n.

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$$

where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$

So, no. of generators of cyclic group G of order n is $\phi(n)$.

(10) Notation:- U_n denotes group of integers relatively prime to n.

(11) e.g. $|a|=12$ & $|b|=22$ & $\langle a\rangle \cap \langle b\rangle \neq \{e\}$ p.t. $a^6 = b^{11}$.
→ $\langle a\rangle \cap \langle b\rangle$ is a subgroup of $\langle a\rangle$.
$\therefore o(\langle a\rangle \cap \langle b\rangle) = 2, 3, 4, 6, 12$ — (1)
it is also a subgroup of $\langle b\rangle$
$\therefore o(\langle a\rangle \cap \langle b\rangle) = 2, 11, 22$ — (2)
$\therefore o(\langle a\rangle \cap \langle b\rangle) = 2$ $\therefore a^6 = b^{11}$.

(12) Determine no. of elements of order 2 in S_4.
→ We know for a cycle, order is equal to cycle length.
Now, S_4 has 6 elements (a,b) type. They are order 2.
(choosing any 2 elts. → $4\times3 = 12$ & $(a,b) = (b,a)$ $\therefore 12/2 = 6$)
then (a,b,c) type are 8 & (a,b,c,d) type are 6. (e) type is 1.
These are not order 2.
Now, product of disjoint cycles is abelian. Elements of type $(a,b)(c,d)$ are 3. Obv. they are order 2 since

$$(a,b)(c,d)(a,b)(c,d) = (e,b)(a,b)(c,d)(c,d)$$

$\therefore 6+3 = 9$ elts.

NORMAL SUBGROUP

(1) A subgroup H is normal subgroup if $\forall x \in G$ & $h \in H$, $x^{-1}hx \in H$.
$H = \{e\}$ & $H = G$ are improper / trivial subgroups.

(2) Hamilton Group
A non-abelian group whose every subgroup is normal.

(3) Simple Group
A group having no ~~simple~~ proper normal subgroup is known as simple group.
Every group of prime order is simple.

(4) A subgroup H is normal iff. every left coset of H is also a right coset of H.

Let $H \trianglelefteq G$, then multiplication of cosets is defined as $(Ha).(Hb) = Hab$

A subgroup H is normal iff product of every 2 right cosets is again a right coset.

(5) If $H \trianglelefteq G$, then following statements are equivalent
(i) $x^{-1}hx \in H$ $\forall x \in G$ & $h \in H$
(ii) $xHx^{-1} = H$ $\forall x \in G$
(iii) $xH = Hx$ $\forall x \in G$
(iv) The set of right (left) cosets is closed w.r.t. multiplication.

(6) Every subgroup of abelian group is normal.

(7) If H is a subgroup of index 2 then H is normal in G.

(8) A normal subgroup G is commutative with every complex of G.

(9) If H is the only subgroup of order m in G then H is normal subgroup.
This comes from the fact that conjugates of a subgroup also form subgroups.

e.g. S.t. product of elements of finite order in non-abelian group need not have finite order.

→ $A = \begin{bmatrix} 2 & -1 \\ 3 & -2 \end{bmatrix}$ $O(A) = 2$

$B = \begin{bmatrix} 3 & 2 \\ -4 & -3 \end{bmatrix}$ $O(B) = 2$ & $AB = \begin{bmatrix} 10 & 7 \\ 17 & 12 \end{bmatrix}$

order not finite.

QUOTIENT GROUP

① **Thm**: Let $H \trianglelefteq G$ then set of all ~~right~~ cosets of H in G i.e. $\frac{G}{H}$ forms a group w.r.t. multiplication

This is called quotient / factor group.

The identity element of $\frac{G}{H}$ is H.

$$O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$$

② Conjugate elements:
Let $a, b \in G$
We say a & b are conjugates & say $a \sim b$ if
$\exists\, x \in G$ s.t. $a = x^{-1} b x$

③ This forms equivalence classes of conjugate elements in G.
$C(a) = \{ y^{-1} a y \mid y \in G \}$ (also shown as $[a]$)
This partitions G into classes of conjugate elements.

$$G = \bigcup_{a \in G} C(a)$$

④ Naturally every normal subgroup becomes a union of some conjugacy classes. But every union of conjugacy classes need not be a subgroup

③ Conjugate classes in permutation groups

If $f \in S_n$ s.t. $f: i \to j$ then
$\theta f \theta^{-1} : \theta(i) \to \theta(j)$ $\forall\, \theta \in S_n$. note θ is fix & θ^{-1} later

Length of cycle remains same after conjugation.
∴ even remains even, odd remains odd.

Corollary: Conjugacy classes of P_n are given by sets that have same cyclic structure i.e. P_4 conjugacy classes are of type
$((a), (a,b), (a,b)(c,d), (a,b,c), (a,b,c,d))$

Useful results → Normal subgroup is union of conjugacy classes.
→ e.g. Prove Alternating group of P_4 has no subgroup of order 6.
→ Subgroup of order 6 in group of order 12 would have to be normal.
now, in this group conjugacy classes are given by (a) → 1, (ab)(cd) → 3, (abc) → 8. Thus no union can give normal subgroup of size 6. ∴ proved

(4) If G is finite group, then number of elements conjugate to a is the index of normalizer of 'a' in G.
i.e. $O[cl(a)] = \frac{O(G)}{O(N(a))}$

(5) 1st class equation of a group

If G is a finite group, then

$O(G) = \sum_{a \in G} i_G(N(a))$ where summation runs over a single a from each conjugate class

2nd form of class equation

$O(G) = O(Z) + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}$

(6) 2nd class equation gives some interesting results

(a) If $O(G) = p^n$, p is prime then $O(Z) > 1$.

(b) If $O(G) = p^2$ then G is abelian.
→ $O(Z) = p$ or p^2
let $O(Z) = p \Rightarrow O(G/Z) = p \Rightarrow$ cyclic
But if quotient of centre in a group is cyclic, it implies the group is abelian #. ($\because$ abelian $\Rightarrow O(Z) = p^2$)
$\therefore O(Z) = p^2$

If G/Z is cyclic ⇒ abelian. Simple proof.
→ let generator be tZ $(t \in G)$, $\Rightarrow xZ = t^p Z$ $\forall x \in G$
let $x, y \in G$, $\therefore xZ = tZ$ & $yZ = t^q Z \Rightarrow xZyZ = xyZ = t^{p+q} Z = yxZ$
$\Rightarrow xy = yx \quad \forall x, y \in G$

Homomorphism / Isomorphism

(1) Homomorphism

Let $(G,\cdot)$ & $(G',*)$ be 2 groups. Then $f: G \to G'$ is called homomorphism if $f(a\cdot b) = f(a) * f(b)$ $\forall a,b \in G$

If f is onto then G' is said to be homomorphic image of G. It is also called epimorphism. $G \simeq G'$

(2) Isomorphism

If $f: G \to G'$ is homomorphism & one-one it is called isomorphism.

If it is onto then G' is isomorphic image of G.

We write $G \cong G'$

Monomorphism = isomorphism + into

(3) Automorphism

An isomorphism of a group into itself is called automorphism.

A homomorphism of G into G is endomorphism.

(4) PROPERTIES OF HOMOMORPHISM

(a) If f is homomorphism from G to G' then

$f(e) = e'$, & $f(a^{-1}) = [f(a)]^{-1}$

(b) $f(G)$ (i.e. range of homomorphism) is a subgroup of G'.

(c) Every homomorphic image of abelian group is abelian.

Reverse need not be true.

Also isomorphic image of abelian group is abelian.

(d) Let G be group & G' a non empty set. If $\exists$ onto mapping f from G to G' s.t. $f(ab) = f(a) f(b)$ then G' is a group.

Note f needs to be onto, one-one not needed.

(5) Kernel of homomorphism
Let f be homomorphism. Then
Kernel $f = \{ x \in G \mid f(x) = e' \}$

Ker f is a normal subgroup of G.

(6) If a homomorphism has ker $f = \{e\}$ $\Leftrightarrow$ it is isomorphism

Thm:- Let Ker $f = K$ & let $a \in G$ s.t. $f(a) = a'$
now set of all elts. of G whose image is a' is given by coset aK
i.e. $aK = \{ x \in G \mid f(x) = a' \}$

(7) Let $N \trianglelefteq G$. Let $f : G \to \frac{G}{N}$ given by $f(x) = Nx$.

Then f is a homomorphism onto $\frac{G}{N}$ & ker $f = N$

∴ Every quotient group of a group is a homomorphic image of that group.

The mapping $f(x) = Nx$ is called natural or canonical homomorphism.

(8) FUNDAMENTAL THM. ON HOMOMORPHISM OF GROUPS
If G' is homomorphic image of G. Then quotient group $G/\text{ker}f$ is isomorphic to G'.
i.e. $\frac{G}{\text{Ker}f} \cong G'$

(9) Total no. of homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_n$ are gcd(m,n)
∵ Comes from fact that range of homo. is subgroup & kernel is subgroup hence size of kernel should be such that $\frac{m}{|\text{ker}f|}$ divides n. & then $\mathbb{Z}_m$ is cyclic so every subgroup has conjugates & so on. { not perfect but gives idea }

(9) If G' is an isomorphic image of G, then
$O(a) = o(f(a))$ (orders are same)

So while proving a group G is isomorphic to G', try to find a mapping which preserves identities, inverse & order.

(10) If H & N are subgroup of $N \trianglelefteq G$ then
$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$
Remember as left side has N 2 times & right side has H 2 times. Also obv. N & $H \cap N$ can be in denominator since only they are normal.

Homomorphism - Isomorphism in Rings

(1) $f: (R, +, \cdot) \to (R', \oplus, \odot)$ is homomorphism if
$\forall a, b \in R$ $f(a+b) = f(a) \oplus f(b)$
$f(a \cdot b) = f(a) \odot f(b)$
All other iso/homo. image etc. definitions are similar to group.

(2) Natural homomorphism onto from R to R/U
if U is ideal then $f(x) = U + x$ is onto homo from R to R/U.

(3) If f is homomorphism of R then $f(R)$ is subring of R'.

(4) Every homomorphic image of comm. ring is commutative ring.
Inverse is not true.
Homomorphic image of ring with unity is also a ring with unity. Inverse not true again (e.g. $I, 2I$) $f(x) = x/2$.

(5) Kernel of homomorphism $= \{ x \in R / f(x) = 0' \}$ ($0'$ add. identity of R')

(6) If $f: R \to R'$ is a homomorphism ; then Ker f is an ideal of R.

(7) A homomorphism $f: R \to R'$ is an isomorphism iff. $\text{Ker } f = \{0\}$

(8) Every quotient ring of R is a homomorphic image of R.

(9) FUNDAMENTAL THEOREM OF HOMOMORPHISM

Let $f: R \to R'$ be an onto homomorphism. Then R' is isomorphic to $\frac{R}{\text{Ker } f}$.

i.e. $R \simeq R' \Rightarrow \frac{R}{\text{Ker } f} \cong R'$

RINGS

① Definition
An algebraic structure $(G, +, \cdot)$ is a ring if
(a) $(G, +)$ is an abelian group
(b) $(G, \cdot)$ is a semigroup i.e. closure & associative
(c) Multiplication is distributive over addition
i.e. $a \cdot (b+c) = a \cdot b + a \cdot c$ (LDL)
& $(a+b) \cdot c = a \cdot c + b \cdot c$ (RDL)

② Ring with Unity :- Ring which contains a multiplicative identity

Commutative Ring :- Multiplication is commutative
(note commutative just means multi. is comm. & nothing about unity or inverse)

Division Ring or Skew field :-
If non-zero elements of G form a group w.r.t. multiplication; it is called division ring.

③ Zero divisor of a ring.
If $\exists\ a, b \in R$ $a \neq 0$ & $b \neq 0$ s.t. $ab = 0$
then a & b are called zero divisors of R.

④ Integral Domain
A commutative ring without zero divisors is known as integral domain.

⑤ Field
A commutative division ring is field.
i.e. Field $\Rightarrow$ $(G, +)$ & $(G^*, \cdot)$ both abelian groups.

(6) If R is a ring & $0, a, b \in R$ then
(i) $a \cdot 0 = 0 \cdot a = 0$
(ii) $a \cdot (-b) = (-a) \cdot b = -(ab)$
(iii) $(-a)(-b) = ab$
(iv) $a(b-c) = ab - ac$

(7) Null ring or Zero Ring → $(\{0\}, +, \cdot)$

$(I, +, \cdot)$ is an integral domain but not field.
Q, R, C are fields.

Set of matrices of $n \times n$ size (real no. elts.) is a ring with unity. Non-commutative ring.

(8) Cancellation laws in a ring
If $a, b, c \in R$, $a \neq 0$
& $ab = ac \Rightarrow b = c$ (LCL)
$ba = ca \Rightarrow b = c$ (RCL)
then we say cancellation laws hold in R.

(9) Thm:- Ring R is without zero divisors iff cancellation laws hold in R.

Thm:- Every field is an integral domain.

(10) Thm:- Every finite integral domain is a field.
→ Proof uses piegon-hole principle. Taka $a \in R$ & consider set aR, apply P-H & so on.

(11) Efficient way of proving a finite algebraic structure is a ring.

① Write 2 composition tables of addition & multiplication and with their help show all properties are satisfied

+	a	b	c	d
a				
b				
c				
d				

×	a	b	c	d
a				
b				
c				
d				

(12) If p is prime then $I_p = \{0, 1, 2 \ldots, p-1\}$ set forms a field w.r.t. addition & multiplication mod p.

If p is not prime, above is not a field.

(13) Boolean Ring

In a ring R, if $a^2 = a$ then a is an idempotent elt.

If every element of R is idempotent, then R is called a boolean ring.

Nilpotent element

Let $a \in R$ & if $\exists\ n \in N$ s.t. $a^n = 0$, then a is called nilpotent element.

If $a, b \in R$ are nilpotent elements in a commutative ring R then $(a+b)$ & $a \cdot b$ are nilpotent.

(14) If R is ring with unity satisfying $(xy)^2 = x^2y^2$ then R is commutative.

→ for proof first replace y by $y+1$; obtain an eq. then replace x by $x+1$; obtain another eq.

(15) Opposite ring of R : R^{op}

Let $(R, +, \cdot)$ be ring then $(R, +, \circ)$ will also be a ring where $x \cdot y = y \circ x$. This is opposite ring.

SUBRING

(1) Let R be a ring & $S \subseteq R$.
If S is a ring w.r.t. same binary operations, then S is called a subring of R.

Obv. $(S,+)$ is a subgroup of $(R,+)$.

(2) Let F be a field & $S \subseteq F$.
If S is a field w.r.t. b-Os, we say S is subfield of F.

If S is subfield of F then
$(S,+)$ is subgroup of $(F,+)$
& $(S-\{0\},\cdot)$ is subgroup of $(F-\{0\},\cdot)$

(3) $\{0\}$ & R are known as improper subrings.

(4) Thm: Let $S \subseteq R$. S is a subring of R iff.
$\forall a,b \in S$; $a-b \in S$
& $ab \in S$.

quite natural since for subgroup we have condition $ab^{-1} \in F$.

Thm. Let F be field & $S \subseteq F$.
S is a subfield of F iff
$\forall a,b \in S \Rightarrow a-b \in S$ & $ab^{-1} \in S$

Naturally, multiplication in ring is not group, i.e. we want only $ab \in S$ for subring

(5) Ring with unity may have subring without unity.
e.g. $(I,+,\cdot)$ has unity but subring $(2I,+,\cdot)$ doesn't have unity.

Centre of a ring is its subring.

Centre of a division ring is a field.

(6) (a) Arb. intersection of subrings = subrings
(b) Union need not be subring.
(c) If Union of 2 subrings is subring then one is contained in another.

(7) Again to prove finite subset is subring, draws 2 tables for operations a-b & ab. Show closure.

(8) CHARACTERISTIC OF A RING

A ring R is of finite characteristic if $\exists\, n \in N$ s.t. $na = 0 \quad \forall\, a \in R$.
Smallest positive integer P s.t. $Pa = 0 \; \forall\, a \in R$ is called the characteristics of ring R.

If no such ~~ring~~ integer n exists then it is called ring of characteristic zero or infinity.

(9) Thm If R is a ring with unity then R has characteristic $P > 0$ iff P is least +ve integer s.t. $P \cdot 1 = 0$

i.e. Characteristic of ring with unity is order of the unit element regarded as member of additive group.

Thm (2) Characteristic of an integral domain is either zero or prime. (so obvious) ($mn.1 = 0 \Rightarrow (m.1).(n.1) = 0$ # assumption unity ke (8)

(3) Obv. Same applies to char. of a field.
(1) Also applies to characteristic of a division ring
Read in (1)-(2)-(3) sequence.

(10) For a division ring with char p; order (additive) of each element is also p.

(11) If R is a finite integral domain then $O(R) = p^n$ where p is prime & $n \in \mathbb{N}$.

Proof :- If Char $R = 0$ → contradiction to finite elts. in R.

$\therefore$ Char $R = p$ (prime)

$\therefore$ Order of every elt. of R is p.

$\therefore p \mid O(R)$.

Now if $O(R) = p^n \cdot p_2$

Then by cauchy's thm for abelian groups, $\exists\, a \in R$ s.t. $O(a) = p_2$ #. $\therefore O(R) = p^n$

Obv. for ~~division~~ field, order is p^n

IDEAL

classmate Date Page 103

Definition

① Let $(R, +, \cdot)$ be a ring & $S \subseteq R$. S is called an ideal of R if
   (a) $(S, +)$ is a subgroup of R
   (b) $\forall s \in S, r \in R \quad sr \in S$ & $rs \in S$

If only $rs \in S$; we call it as left ideal.
If only $sr \in S$; we call it right ideal.

② R itself is an ideal of R. It is called unit ideal.
$S = \{0\}$ is called null / zero ideal of R.
Obv. these are improper ideals.

③ In a commutative ring, every left ideal is also a right ideal. ∴ In comm. ring, every left ideal is a 2-sided ideal.

Set of integers I is only a subring but not an ideal of set of rational numbers.

④ Every ideal is a subring of R. Converse not true.

⑤ Thm :- If S is an ideal of Ring R with unit element & if $i \in S$; then $S = R$.

IMP →

⑥ A field has no proper ideals.

⑦ Intersection of arbitrary family of ideals is an ideal

Union of 2 ideals is ideal iff one is contained in anoth

(8) If R is commutative ring & $a \in R$ then $aR = \{ar / r \in R\}$ is an ideal of R.

Corollary:- A commutative ring R with no proper ideals & having unit element is a field.

If R is a ring with unit element & R has no proper ideals then R is a division ring.

(9) The sum of 2 ideals is also an ideal:
i.e. $S_1 + S_2 = \{a+b / a \in S_1, b \in S_2\}$ is an ideal.

(10) Product of 2 ideals
$S_1 S_2 = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n / a_i \in S_1, b_i \in S_2 \text{ & } n \in \mathbb{N}\}$

$S_1 S_2$ is also an ideal.

(11) If A & B are ideals then $AB \subseteq A \cap B$ (naturally)

$Z(R)$ i.e. centre of a ring is subring of R & need not be an ideal.

(12) Co-maximal ideal
2 ideals A & B satisfying $A+B=R$ are co-maximal ideals.

Ideals satisfy distributive property
i.e. $A(B+C) = AB+AC$

(13)

(14)

(13) Radicle of A

$\sqrt{A} = \{ x \in R \mid x^n \in A \text{ for some } n \in \mathbb{N} \}$

(14) Ideal generated by subset of Ring

Let S be subset of R. An ideal U is said to be generated by S if it is the smallest ideal containing S.

i.e., if V ideal contains S $\Rightarrow$ $U \subseteq V$.

A+B is an ideal generated by AUB subset.

QUOTIENT RING

(1) Ring of residue classes / quotient ring.

Let R be ring & S be ideal of R then the set $\frac{R}{S} = \{S+a / a \in R\}$ of all residue classes in R is a ring for 2 compositions given below

$(S+a) + (S+b) = S + (a+b)$

$(S+a) \cdot (S+b) = S + (ab)$

It is also denoted as $[a]$ or $\bar{a}$ $= (S+a)$

then $[a] + [b] = [a+b]$ & $[a] \cdot [b] = [ab]$

(2) R is commutative $\Rightarrow \frac{R}{S}$ is commutative

R has unity elt. $\Rightarrow \frac{R}{S}$ has unity elt.

R is boolean ring $\Rightarrow \frac{R}{S}$ is boolean ring.

(3) PRIME IDEAL

Ideal P of R is prime ideal if $\forall a, b \in R$ if $ab \in P \Rightarrow a \in P$ or $b \in P$.

e.g. for prime P; PI is prime ideal of I.

Thm Let R be commutative ring.

An ideal P is prime ideal $\iff R/P$ is an integral domain

(4) MAXIMAL IDEAL

An ideal M is maximal if $\nexists$ no ideal bet" M & R.

e.g. 2I, 3I, 5I are maximal ideals in I.

nI is maximal iff. n is prime.

$\{0,2,4,6\}$ is maximal ideal in Z_8.

Obv. a ring may have more than 1 maximal ideal.

Every prime ideal is not a maximal ideal.
$\{0\}$ is prime ideal but not maximal.

(5) In questions of proving a given ideal is maximal; start with assuming $\exists U$ s.t. $M \subset U \subseteq R$. Then try to show U must contain unity element & this would imply $U = R$.

Good ex:- Consider ring of cont. functions of $[0,1]$.
P.T. $M = \{f(x) / f(\frac{1}{2}) = 0\}$ is a maximal ideal.

(6) If R is a commutative ring with unity then M is a maximal ideal $\iff \frac{R}{M}$ is a field.

note here we need unity also, for prime ideal $\iff$ int. domain; we dont need unity

(This can be used in questions of proving a given ideal is maximal. look at R/M & see if you can make it a field.)

Proof:- Let $a \notin M$ then $M + \langle a \rangle$ is ideal. $\because M$ maximal $\therefore M + \langle a \rangle = R$
$\therefore \exists\ m + ar = 1$ & so on.

(7) For a comm. ring with unity, maximal ideal is prime ideal.
→ Obv. since R/M is field $\therefore$ integral domain.
But a prime ideal need not be maximal ideal.
Also if no unity then maximal ideal $\not\Rightarrow$ prime ideal.
e.g. $R = 2I$ & $\text{Ideal} = 4I$.

(so unity unites prime & maximal ideal)

PRINCIPLE IDEAL

(1) An ideal U generated by single element a of R known as principle ideal & shown by (a) or ⟨a⟩.

When R has unit elt. then $(a) = \{ar / r \in R\}$
if R doesn't have unit elt. $(a) = \{ar + na / r \in R, n \in \mathbb{Z}\}$

Note that 2nd formula has na to ensure $a \in (a)$.
⟨a⟩ is the smallest ideal containing a.

(2) If R is not commutative then
Left ideal gen. by $a = \langle a \rangle_L = \{ra / r \in R\}$.
Right ideal gen. by $a = \langle a \rangle_R = \{ar / r \in R\}$
Ideal generated by $a = \{sar + na / s, r \in R, n \in \mathbb{N}\}$

(3) Null ideal is generated by zero elt.
Unit ideal i.e. R itself is generated by unit elt.

∴ Every ideal of a field is a ~~proper~~ principal ideal.

(4) PRINCIPLE IDEAL RING
A ring R is called PIR if every ideal in R is a principle ideal.

PRINCIPLE IDEAL DOMAIN
A commutative ring with unity & without zero divisors whose every ideal is principle ideal is PID.

(So, PID = I.D. + unity + every ideal principal
note that unity is needed as R itself is ideal & has to be generated by unity)

Obr. every field is P.I.D.

$(I, +, \cdot)$ is a P.I.D.

QUOTIENT FIELDS

Ring of endomorphisms of an abelian group.

(1) Endomorphism is homomorphism of G into itself.
Let Hom(G,G) represent set of all endomorphisms.
We define 2 operations on this set

$(f+g)(x) = f(x)+g(x)$
$(fg)(x) = f(g(x))$

Then Hom(G,G) forms a ring w.r.t. above 2 operations.

(2) Embedding of Rings
Ring R is said to be embedded in ring R' if ∃ an isomorphism of R into R'.
R' is said to be extension ring of R.
If that function is f then $R \cong f(R)$

(3) Every ring R can be embedded into a ring with unity.
→ That ring will be $R \times Z = \{(r,m) / r \in R, m \in Z\}$
b.o. are given by $(a_1,b_1)+(a_2,b_2) = (a_1+a_2, b_1+b_2)$
$(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2 + b_2a_1 + b_1a_2, b_1b_2)$
(quite intuitive product since 1st element ∈ R & hence b_1b_2 can't be added to it, it becomes 2nd element)

(4) FIELD OF QUOTIENTS
Every integral domain D can be integrated into a field F s.t. every element of F can be regarded as a quotient of 2 elements of D.

This field is called 'field of quotients' or quotient field.

(5) Motivation for quotient field comes from field of rational numbers which are essentially quotients of 2 integers. Also we have $\frac{a}{b} = \frac{c}{d}$ if $ad = bc$, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
& $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. We use these facts now.

(6) Finding Quotient Field

For given integral domain D, define equivalence relation $(a,b) \sim (c,d)$ if $ad = bc$

This partitions $D \times D$ set into equivalent classes

$$\frac{a}{b} = \{(x,y) \in D \times D \mid xb = ya\}$$

For these set of equivalence classes, we define binary operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

(7) Semi-Prime Ideal

Ideal I is called semi-prime if $a^2 \in I \Rightarrow a \in I$ $\forall a$

SOME TRICKS FOR FIELD/IDEAL PROBLEMS

(1) If we know that U is prime ideal & $a^2 \in U$ then $a \cdot a \in U \Rightarrow a \in U$.

Try to use this trick in manipulations of prime ideal problems.

e.g. R comm. with unity & M maximal s.t. $M^2 = \{0\}$. If N is other maximal ideal prove $N = M$

→ (comm. + unity + maximal ⇒ prime.

now $0 \in N$ (∵ ideal) ∴ $m^2 = 0 \Rightarrow m^2 \in N$

∵ prime ∴ $m \in N$ ∴ $M \subseteq N$ ∴ $M = N$.

EUCLIDEAN DOMAIN

(1) Definition
An Integral domain R is said to be an euclidean domain if ∃ a mapping $d: R-\{0\} \to Z$ s.t.
(a) $d(a) \geq 0 \quad \forall a \in R-\{0\}$
(b) $d(a) \leq d(ab) \quad \forall a, b \in R-\{0\}$
(c) $\forall a, b \in R-\{0\}$, ∃ $q, r \in R$ s.t. $a = bq + r$ where $d(r) < d(b)$ or $d(r) = 0$

$d(0)$ is not defined. Though sometimes it is taken as.

(2) S.T. Gaussian Integers form a euclidean ring.
→ We know that $Z[i] = \{a+bi \mid a, b \in Z\}$ is an integral dom.
Let $d(x+iy) = x^2+y^2$ Then it 2 conditions are V
Now, for division algorithm condition, consider

$$\frac{z_1}{z_2} = \frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{c^2+d^2} = p+iq = \lambda$$

where $p = \frac{ac+bd}{c^2+d^2}$ & $q = \frac{bc-ad}{c^2+d^2}$ are rationals

We can find integers p' & q' s.t.
$|p'-p| \leq 1/2$ & $|q'-q| \leq 1/2$
let $t = p'+iq'$ ∴ $z_1 = tz_2 + r$ where $r = (\lambda - t)z_2$

(3) d is called euclidean evaluation & 3rd condition is called euclidean algorithm.

Every field is a euclidean ring.
→ Define mapping $d(a) = 1 \quad \forall a \in F-\{0\}$

(4) S.T. $Z[\sqrt{2}] = \{m+n\sqrt{2}; m, n \in Z\}$ is a euclidean domain
→ To define d here, go for $z\bar{z}$ i.e. $|m^2-2n^2|$.
This way $d(z_1z_2) = d(z_1).d(z_2)$ & things get easier to prove.

Here also let $\frac{a}{b} = \frac{m+n\sqrt{2}}{m_1+n_1\sqrt{2}} = p+q\sqrt{2}$ (p & q rational)

Find integers p' & q' s.t. $|p-p'| \le \frac{1}{2}$ & $|q-q'| \le \frac{1}{2}$

& same as gaussian integer example

(5) Every Euclidean Ring is a principle ideal ring.

This is also intuitive P.I.D is about having generators for every ideal. Now euclidean domain $\Rightarrow$ euclidean algo & hence every ideal can be broken into smallest pieces $\therefore$ naturally it will be P.I.D.

Converse not true. $2\mathbb{I}$ is P.I.R. but not euclidean ring. (division algorithm fails)

easy to remember → till now we have only seen 2 types of rings - principal ideal ring & euclidean. Obv. euclidean is next step of P.I.D.

(6) Every euclidean ring possesses unity element.

Don't get confused with Principle ideal or maximal ideal as they don't characterize ring

→ let $R = \langle a \rangle$ $\because a \in R$, $\exists e$ s.t. $ae = a$

We can prove this e is unity of ring.

Corollary :- $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ are principle ideal domains.

(7) Divisibility :- Let R be a commutative ring & $a, b \in R$.

If $\exists\ q \in R$ s.t. $a = bq$ then we say $b \mid a$.

If a does not divide b then we write $a \nmid b$.

If $a \mid b$; we say a is a 'divisor of b' or a 'factor of b'.

Every element a is a factor of 0.

In ring of rationals, 3 divides 7 because $\frac{7}{3} \in \mathbb{Q}$ $\therefore 7 = 3 \cdot \frac{7}{3}$

(8) If R is a commutative ring with unity & $a, b, c \in R$

then (1) $a \mid a$ (2) $a \mid b, b \mid c \Rightarrow a \mid c$ (3) $a \mid b \Rightarrow a \mid bx$ $\forall x \in R$

(4) $a \mid b, a \mid c \Rightarrow a \mid (bx+cy)$ $\forall x, y \in R$

(5) simple representation →

Euclidean Domain $\Rightarrow$ P.I.D. $\Rightarrow$ Euclidean domain has unity

$\because \langle 1 \rangle = R$.

(9) UNITS

Let R be a commutative ring with unity. $a \in R$ is said to be a unit in R if $\exists\ b \in R$ s.t. $ab = 1$.
i.e units are those elements in R that have a multiplicative inverse.

There may be more than 1 unit element in R but unity element will always be unique
eg. ± 1 are units in I.
Every non-zero element of a field is a unit.

(10) Let $a, b \in R - \{0\}$ & R be euclidean domain.
(a) If b is a unit in R, $d(ab) = d(a)$ &
(b) If b is not a unit then $d(ab) > d(a)$
→ 1st is easy. 2nd part is proven using division algorithm.
Let b not be unit. $\exists\ q$ & r s.t. $a = q(ab) + r$
case (i) $r = 0 \Rightarrow a(1-qb) = 0$ # to b not being unit.
case (ii) $r \neq 0 \Rightarrow d(r) < d(ab)$ & $d(a(1-qb)) < d(ab)$
but $d(a(1-qb)) \geq d(a) \therefore d(a) < d(ab)$. ##

(11) A non-zero a of euclidean ring is unit iff $d(a) = d(1)$

(2) ASSOCIATES

Let R be comm. ring with unity. a & b are said to be associates if $a = bu$ where u is a unit of R

If a is a unit then $a = 1 \cdot a$. $\therefore 1$ is an associate of every unit element.

In ring of integers, a & $-a$ are only two associates for any $a \in \mathbb{Z}$

(13) Let a, b be non-zero in Integral domain R with unity. Then a, b are associates iff $a|b$ & $b|a$.

(14) Greatest Common Divisor / Highest common factor
d is gcd or hcf of a & b if
(a) $d|a$ & $d|b$
(b) if $c|a$ & $c|b \Rightarrow c|d$.
gcd of a, b is denoted by (a, b)

Least Common Multiple
C is lcm of a & b if
(a) $a|c$ & $b|c$
(b) if $\exists x \in R$ s.t. $a|x$ & $b|x \Rightarrow c|x$.
LCM of a, b shown by $[a, b]$

Any 2 elements of ring may or may not have gcd & lcm or they can have more than 1 gcd or lcm.

In 2I ring, 4 & 6 don't have gcd.
In $\mathbb{Z}$, 6 & -6 both are gcd of 18, 48.

(15) eg. P.T. $\bar{6}$ & $\bar{8}$ have no lcm in $\mathbb{Z}_{12}$
→ Let $\bar{x}$ be lcm. $\therefore \bar{6}|\bar{x} \Rightarrow \bar{x} = \bar{6}.\bar{a}$ $\therefore \bar{x} = \bar{0}$ or $\bar{6}$
LCM is never 0. $\therefore \bar{x} = \bar{6}$ $\therefore \bar{8}|\bar{x} \Rightarrow \bar{8}|\bar{6}$ #.

If d_1, d_2 are gcd of a & b; then $d_1|d_2$ & $d_2|d_1$
$\therefore d_1, d_2$ are associates of each other.
Hence, if gcd of a, b exists, it is unique apart from multiplication by units.

(16) a, b are said to be relatively prime if their gcd is a unit of R.

$\therefore a, b$ are relatively prime $\Leftrightarrow (a,b) =$ a unit of R
$\Leftrightarrow (a,b) = 1$
$\Leftrightarrow ax + by = 1$ for some $x, y \in R$

(17) b is a proper divisor of a if
$a = bd$ where d is not a unit.
Improper divisors :- For any element a, units of R & associates of a are divisors. They are improper divisors.

(18) IRREDUCIBLE ELEMENT
A non-zero $P \in R$ is irreducible if
(a) P is not a unit element.
(b) $P = ab \Rightarrow$ either a or b is a unit.

If P is reducible $\Rightarrow \exists\ a, b$ s.t. $P = ab$ & a, b not units.

PRIME ELEMENT
A non-zero $P \in R$ is a prime elt. if (a) P is non-unit
(b) $P \mid ab \Rightarrow P \mid a$ or $P \mid b$

Note, non-zero & non-unit are important for both prime & irreducible. [no need to be confused Let's prime & irreducible, irreducible naturally means something that can't be reduced further ; $P = ab \Rightarrow a$ or b unit, whereas 'prime' deals with factors of bigger no. : $P \mid ab \Rightarrow P \mid a$ or $P \mid b$]

(19) $1 + i$ is a prime element in $\mathbb{Z}[i]$.
P is not prime if $\exists\ a, b$ s.t. $P \nmid a$, $P \nmid b$ but $P \mid ab$.

Any field has no prime or irreducible elt since every non-zero member is a unit.

POLYNOMIAL RINGS

(20) Let R be a ring. Then following expression is called polynomial in x over R.

$f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \quad \forall a_i \in R$

& n is a non-negative integer.

If $a_n \neq 0$ & n is largest such no., a_n is called leading coefficient.

(21) $f(x) = a_0x^0 + a_1x^1 + \cdots + a_mx^m$

$g(x) = b_0x^0 + b_1x^1 + \cdots + b_nx^n$

$f(x) = g(x)$ iff all coefficients are same for them.

Monic Polynomial :- leading coefficient is unity element.

(22) Ring of Polynomials

Let R be a ring. The ring of polynomials over R is

$$R[x] = \{ f(x) = a_0x^0 + a_1x^1 + \cdots + a_nx^n \mid a_i \in R \ \forall n \geq 0 \}$$

R[x] forms a ring with addition & multiplication of polynomials

Additive identity = 0, Unity = 1 (if R has) & additive inverse = $-f(x)$

(23) If R is commutative $\Rightarrow$ R[x] is commutative

If R has unity $\Rightarrow$ R[x] has unity.

If F is a field, F[x] is commutative ring with unity. F[x] is not a field though. (natually)

If R is a integral domain $\Rightarrow$ R[x] is an I.D.

Degree of zero polynomial undefined & of constant polynomial is 0

(25) If $f(x)$ & $g(x)$ have degrees m & n then
$\deg(f(x)+g(x)) = \max(m,n)$ when $m \neq n$
$\leq m$ when $m = n$.
&
$\deg(f(x)\cdot g(x)) \leq \deg f(x) + \deg g(x)$

eg. In $Z_4[x]$ $f(x) = x^2+2x+3$ $g(x) = 3x^2+2x$
& $f(x)+g(x) = 3$
& let $P(x) = 2x^2+2x+3$ & $q(x) = 2x^2+2x$
$\Rightarrow P(x)\cdot q(x) = 2x^2+2x$ in $Z_4[x]$

(26) If R is an integral domain, $\deg(fg) = \deg(f)+\deg(g)$

(27) If R is I.D. with unity then units of R & $R[x]$ are same
(note we are talking of units & not just unity)
proof: Let $f[x]$ be unit in $R[x]$ $\therefore f(x)\,g(x) = 1$
By comparing degrees we get $f(x)$ & $g(x)$ are constant poly.

(28) Division Algorithm in $F[x]$ when F is field.
$\forall\ f(x), g(x) \in F[x]$; $\exists\ r(x)$ & $t(x)$ unique s.t.
$f(x) = t(x)\,g(x) + r(x)$
& $r(x) = 0$ or $\deg(r(x)) < \deg g(x)$
→ Proof :- Consider the set
$S = \{ f(x) - h(x)\,g(x) \mid h(x) \in F(x) \}$
Let $r(x)$ be polynomial of least degree in S.
$\therefore \exists\ q(x)$ s.t. $r(x) = f(x) - q(x)\,g(x)$ & so on.

(29) If F is a field, $F[x]$ is a euclidean domain.
→ In proof define euclidean evaluation function d as degree of $f(x)$. $\therefore \deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$
$\geq \deg f(x)$ & so on.

(30) If F is a field then F[x] is a principle ideal ring.
e.g. Z[x] is not a principle ideal ring. for counterexample, consider ideal generated by set $(x, 2)$ & show it is not principal ideal.

(31) Some Example of irreducible but not prime etc. elts.
Consider $Z[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in Z\}$
→ 1 & -1 are only units of $Z[i\sqrt{5}]$. This comes from fact that a unit will have $a^2 + 5b^2 = 1$

We can show 3, 2, $1 + i\sqrt{5}$ are irreducible elements of $Z[i\sqrt{5}]$
→ Let $3 = (a + ib\sqrt{5})(c + id\sqrt{5})$ $\therefore 9 = (a^2 + 5b^2)(c^2 + 5d^2)$
Only possible case $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$
$\therefore$ One of them will be unit $\Rightarrow$ irreducible.

But 3 is not prime. $3 \mid (1 + i\sqrt{5})(1 - i\sqrt{5})$ i.e. but 3 doesn't divide them individually.

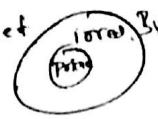
(32) e.g. P.T. $i\sqrt{5}$ is a prime element of $Z[i\sqrt{5}]$.
→ Remember to first prove it is non-unit & then go for $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

(32) In an integral domain with unity, every prime element is irreducible but converse is not true.
→ Let P be prime. Let $P = ab$ $\therefore P \mid a$ or $P \mid b$
Let $P \mid a \Rightarrow a = Pr$ $\therefore P = Prb$ $\therefore 1 = rb$ $\therefore b$ is unit. ✓

(33) In principal Ideal Domain irreducible $\Leftrightarrow$ prime.
→ Let P be irreducible. Let $P \mid ab$ & $P \nmid a$. We will show $P \mid b$.
$\langle P \rangle + \langle b \rangle$ is an ideal. Let $\langle P \rangle + \langle b \rangle = \langle d \rangle$ $\therefore P = dx$
& so on manipulations.

So in $a + ib\sqrt{5}$ we had irred. but not prime $\Rightarrow$ $a + ib\sqrt{5}$ is not P.I.D. & hence not euclidean domain

→ So remember that being prime generally implies irreducible (the word is bigger so venn diagram set is bigger) but for irreducible ⇔ prime; we need P.I.D.



(34) Show that $\mathbb{Z}[\sqrt{-5}]$ is not a PID.
→ 3 is irreducible but not prime ∴ no PID.

(35) Let R be PID but not a field. Then $\langle a \rangle$ is maximal ideal ⇔ irreducible.
→ Manipulations used here are pretty std. for these problems.
(I) Let $\langle a \rangle$ be maximal. Let $a = bc$
$\therefore \langle a \rangle \subseteq \langle b \rangle \subseteq R$ case (i) $\langle b \rangle = \langle a \rangle \Rightarrow b = ad \Rightarrow a = adc$
$\therefore c$ is a unit ∴
case (ii) $\langle b \rangle = R \Rightarrow \exists\, d$ s.t. $bd = 1$ ∴ b is unit.
(II) Let a be irreducible. Let $\langle a \rangle \subseteq \langle d \rangle \subseteq R$
$\therefore a = dc$ case (i) d is unit $\Rightarrow de = 1$ ∴ $\langle d \rangle = R$
case (ii) c is unit $\exists\, f$ s.t. $cf = 1$ ∴ $af = dcf = d$ ∴ $\langle d \rangle \subseteq \langle a \rangle$
∴ $\langle d \rangle = \langle a \rangle$

(36) $\frac{F[x]}{\langle f(x) \rangle}$ is a field iff $f(x)$ is irreducible element of $F[x]$.
→ Follows from 2 theorems
(a) Ideal M of R maximal ⇔ R/M is field.
& (b) $\langle f(x) \rangle$ is maximal iff $f(x)$ is irreducible.

Unique Factorization Domain

classmate Date Page 121

(1) An integral domain R with unity is UFD if its elts. are
(a) either unit elt. or reducible to product of finite irreducible elts. of R
(b) Above factorization is unique upto associates & order of the irreducible elements involved.

Existance of gcd is assured in UFD.

(2) If R is a UFD then so is R[x].
[∵ Z is euclidean domain; it is UFD & hence Z[x] is U.F.D.]
Euclidean domain is always a unique factorization domain. So euclidean is best → it is both PID & UFD.
Also, every PID is UFD.
But we can have U.F.D. which are not even P.I.D let alone euclidean dom
e.g. Z[x] is U.F.D. but not P.I.D. (ideal generated by (x,2) & so on)

(3) Obviously If F is a field then F[x] is UFD. (as F[x] is already eu-dom; F[x] is also E.D ⇒ PID ⇒ UF

(4) Good example clarifying all these concepts.
→ S.T. Z[x] is UFD but not PID. Can you give example of PID that is not UFD.
→ We can easily show that Z is UFD & hence Z[x] is also UFD
Consider ideal generated by (2,x) to show it is not PID.
Every PID is UFD. ∴ No example.

(5) Every PID is UFD:

→ We make use of property that in a PID, irred. are also primes.

Let a number S be shown as 2 different products of irreducibles

$\therefore S = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$ (say $m < n$)

Since all p_i & q_i are also primes; $\therefore p_1$ divides $q_1 q_2 \ldots q_n$

& hence p_1 divides some q_i.

By rearranging we can get $p_1 \mid q_1$.

let $p_1 = u_1 q_1$ (both irred. $\therefore$ associates)

$q_1 = u_1 p_1$

$\therefore p_1 p_2 \ldots p_m = u_1 q p_1 q_2 \ldots q_n$

$\therefore p_2 \ldots p_m = u_1 q_2 \ldots q_n$

again with same logic we introduce u_2 & so on & so forth

$\therefore 1 = u_1 u_2 \ldots u_m q_{m+1} \ldots q_n$

but q_i are not units $\therefore m = n$ & hence p_i, q_i are associates of each other.

$\therefore$ PID $\Rightarrow$ UFD.

(6) Some questions ask 'Show given domain (ring) is PID'

→ It's hard to show every ideal will be principle.

In such questions first see if it is E.D bcoz E.D ⇒ PID

Then if it is $F[x]$; then remember if F is field, then $F[x]$ is E.D. ⇒ PID

$\therefore$ we get $Q[x]$, $R[x]$ as PID but not $\mathbb{Z}[x]$.

Showing something is not PID → show it is not UFD or show irreducible ≠ prime

Showing something is not E.D. → show it is not PID or it is not UFD.