~~Semi sub group~~

Sub monoid

~~In~~ a sub monoid, identity element ~~lies outside the set~~.

$(\{0, 1\}, OR)$

a	b	a OR b.
0	0	0
0	1	1
1	0	1
1	1	1

OR	0	1
0	0	1
1	1	1

Associative, Commutative, Closed

Identity element is 0.

$a + b \% m + 1$

$\Rightarrow$ Monoid.

Not a group (No inverse)

$\Rightarrow$ Not an Abelian group.

We don't have an element a^{-1} such that $1 * a^{-1} = e = 0$

~~Modulo addition~~ b Addition Modulo.

$$\boxed{a +_m b = (a+b) \bmod m}$$

$(a+b) \% m$

$= (a \% m + b \% m) \% m$

$a +_m (b +_m c)$

$= a +_m ((b+c) \% m)$

$= (a + (b+c) \% m) \% m.$

$(a +_m b) +_m c$

$= (a+b) \% m +_m c$

$= ((a+b) \% m + c) \% m$

$(Z_m, +_m)$

$(Z_3, +_m) \cdot (\{0, 1, 2\}, +_m)$

$(3+5) \% 5 = 3$

$(3+10) \% 5 = 3$.

$(Z_5, +_5) = (\{0,1,2,3,4\}, +_5)$ $\quad (a+a^{-1}) \% m = e$.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

String operations

$S = \{0, 1\}$

$S^* = \{0, 1, 00, 01, 10, 11, 000, 001, 010, 011 \ldots\}$

S^* is called Kleene closure

$S^* \rightarrow$ Set of all possible strings that can be formed using symbols from the set.

$S^0 = \{\epsilon\}$ $\quad \epsilon \rightarrow$ empty string

$S^2 \Rightarrow$ Set of strings that can be by taking symbols twice.

S^* is an infinite set

Positive closure $\rightarrow$ If we remove null string from S^*, it is called a positive closure.

$S = \{a, b\}$

$S^* = \{\epsilon, a, b, aa, ab, ba, bb, \ldots\}$

$S^+ = \{a, b, aa, ab, ba \ldots\}$

$S^+ = S^* \setminus \{\epsilon\}$

abc
abc

Q) Consider $(S^*, .)$ concantination.

Ans) * It is closed

* Identity?

$x.e = x = e.x$

$\Rightarrow e = \epsilon$

* No binverse.

$(S^+, .)$ is called a free semigroup, (∵ identity doesn't belong to S^+).

Cancellation property

For any group S and * opeation $(S, *)$

if for $x, a, b \in S$.

if $x*a = x*b$.

$\Rightarrow a = b$

Subsemigroup

$(S, *)$

Let S be a semigroup and T a subset of S. If the set T is closed under * , then $(T, *)$ is said to be a subsemigroup of $(S, *)$.

Submonoid

Let $(M, *, e)$ be a monoid, and T is a subset of M, If T is closed under * and e belongs to T, then $(T, *, e)$ is said to be a submonoid of $(M, *, e)$

Properties

* For any semi group $(S, *)$, $(S, *)$ itself is a trivial sub semigroup.
* For any $a \in S$, the set consisting of all powers of a, under the operation $*$ is a sub semi group, i.e., $T = \{a, a^2, a^3, \ldots\}$. Here T is called a cyclic semigroup, which is a sub semigroup of $(S, *)$ generated by the element a.

Homomorphism

Homomorphism -

$(X, \cdot)$ and $(Y, *)$

Let $(X, \cdot)$ and $(Y, *)$ be two algebraic systems of same type, a mapping

$g : X \to Y$ is called a homomorphism for $(X, \cdot)$ to $(Y, *)$ if for any $a, b \in X$

$$g(a \cdot b) = g(a) * g(b)$$

Epimorphism

If g is onto, it is called epimorphism.

Monomorphism - if g is one to one

If g is one to one and on to, it is Isomorphism.

Let $(X, \cdot)$ and $(Y, *)$ be two algebraic systems such that ~~$Y \subset X$~~ $Y \subset X$. A homomorphism ~~f~~ g from $(X, \cdot)$ to $(Y, *)$, in such a case is called an endomorphism.

If $Y = X$, then an isomorphism from $(X, \cdot)$ to $(Y, *)$ is called automorphism.

eg) Let $(N, +)$ be a semi group and $(S, *)$ be the semigroup on $S = \{e, 0, 1\}$ with $*$ operation defined by the table given below.

$*$	e	0	1
e	e	e	e
0	0	0	0
1	1	0	1

and define a mapping g from N to S given by $g(0) = 1$ and $g(x) = 0$ for $x \neq 0$.

$a, b \in N$

$$g(a+b) = g(a) * g(b)$$

Q) Let $A = \{0, 1\}$ and consider the semigroup $(A^*, \cdot)$ $\cdot$ is concantination operation and $(A, +)$

+	0	1
0	0	1
1	1	0

and define function $g : A^* \to A$ and $g(\alpha) = \begin{cases} 0, & \alpha \text{ has even no. of ones} \\ 1, & \alpha \text{ has an odd no. of 1s.} \end{cases}$

Is g a homomorphism?

Ans) $\alpha, \beta \in A^*$,

To, be a homomorphism, it should satisfy the following condition. $g(\alpha.\beta) = g(\alpha) + g(\beta)$.

if $\alpha.\beta$ has even no. of ones the $g(\alpha.\beta)$ is 1

$g(\alpha.\beta)$	$g(\alpha) + g(\beta)$	
0 ← even	odd	odd → 0
0 ← even	even	even → 0
1 ← odd	odd	even → 1
1 ← odd	even	odd → 1

⇒ g is a homomorphism

g is also an onto fn.

hence, epimorphism.

Q) Let G be the set of all non-zero real numbers, and let $a * b = \frac{ab}{2}$ where, * is the operation on G. Show that $(G, *)$ is an Abelian group.

$(\mathbb{R}, \cdot)$ $(\mathbb{R}, *)$

[	[0]
	[1]
	[1]

(i) closed

Ans) ~~a*b * is~~ $a, b \in G$, $a * b = \frac{ab}{2} \in G$.

$\Rightarrow$ G is closed with respect to the operation *.

(ii) $(a*b)*c = \left(\frac{ab}{2}\right)*c$

$= \frac{abc}{4}$ — ①

$a*(b*c) = a*\left(\frac{bc}{2}\right)$

$= \frac{abc}{4}$ — ②

From ① and ② * is associative.

(iii) Identity element.

$a*e = e*a = a$

$a*e = a$

$\frac{ae}{2} = a$

$e = 2$

Identity element is 2.

(iv) Inverse ~~element~~.

$a*a^{-1} = e = a^{-1}*a$

$\frac{aa^{-1}}{2} = 2$

$\Rightarrow a a^{-1} = 4$

$a^{-1} = \frac{4}{a}$

Inverse ~~of~~ of a is $\frac{4}{a}$

(v) Commutative

$a*b = \frac{ab}{2}$

$b*a = \frac{ba}{2} = \frac{ab}{2} = a*b$

$\Rightarrow$ Commutative.

That means ~~a*b if~~ $(G, *)$ is an Abelian group.

Theorem:

If f is a homomorphism from a commutative semigroup $(S, *)$ onto a ~~a onto~~ semigroup $(T, *')$, then $(T, *')$ is also commutative

$f : (S, *) \to (T, *')$

$a, b \in S$

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

$f(a), f(b) \in T$

$t_1 = f(a) \quad t_2 = f(b)$

$f(a*b) = t_1 *' t_2$

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

$= t_2 *' t_1$

$f(a*b) = t_1 *' t_2$

$f(b*a) = t_2 *' t_1$

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

$\Rightarrow t_1 *' t_2 = t_2 *' t_1$

$*'$ is commutative

$\Rightarrow (T, *')$ is "

Theorem:

~~A)~~ Let G be a group, each element a in G has only one inverse in G,

Let $a \in G$, and ~~a' & a'' are both inve~~ Let us assume, a' and a'' are ~~inverses of a~~ distinct inverses of a.

If a' is an inverse of a,

$\Rightarrow a * a' = e = a' * a$.

a'' is an inverse of a

$\Rightarrow a * a'' = e = a'' * a$.

$\Rightarrow a * a' = a * a''$

$\Rightarrow a' = a''$ (left cancellation property)

Q) Prove that $a * b = a * c \Rightarrow b = c$

Ans) $a * b = a * c$

$\Rightarrow a^{-1} * a * b = a^{-1} * a * c$

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$

Theorem:

Let G be a group, and $a, b \in G$, then $(a^{-1})^{-1} = a$.

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

(ii) $(ab)^{-1} = b^{-1}a^{-1}$

~~Ans~~) (i) $a^{-1} * a = e$

If we consider a^{-1} as as the element, then its inverse is a.

(ii) $(ab)^{-1} = b^{-1}a^{-1}$

$ab \cdot (ab)^{-1} = e$

Theorem:

Let ~~S and T~~ $(S, *)$ and $(T, *')$ be monoids with identities e and e' respectively. Let f from $S \to T$ be an isomorphism, then $f(e) = e'$.

$a \longrightarrow b \; a'$

Let, $a, b \in S$.

$\Rightarrow f(a*b) = f(a) *' f(b)$

$\Rightarrow f(a * a^{-1}) = f(a) *' f(a^{-1})$

$\therefore f(e) = f(a) *' f(a^{-1})$

Since f is an isomorphism,

for any $b \in T$, $\exists$ a, such that $f(a) = b$.

$f : S \to T$

For any $b \in T$, $\exists$ a, s.t. $f(a) = b$.

$\Rightarrow f(a*e) = b$

$f(a*e) = f(a) *' f(e) = f(a)$

$f(e*a) = f(e) *' f(a) = f(a)$

$\Rightarrow f(e)$ is the identity element of $*'$

Any one to one mapping of a set S is called permutation of S.

Every row or column in the composition table of a group $(G, *)$ is a the permutation of elements of G.

Order of the group $(G, *)$ denoted $|G|$ is the no. of elements of G, when G is finite.

ie, if the group is of order 1, then it implies e is the only element in it.

Q) If $(G,*)$ is an Abelian group, then $\forall a, b \in G$, show that $(a*b)^n = a^n * b^n$.

Ans) $(a*b)^n = a*b*a*b*b*a*b \ldots$ n times.

$= a*a*b*b*a*b \ldots$

$= a^*$

Theorem:

Q) For any commutative monoid $(M,*)$, the set of idempotent elements of a form submonoid.

Note: Idempotent elements are elements with $a*a = a$.

$(M,*) \rightarrow$ commutative monoid.

$S \subseteq M$

$\forall\ a \in S \Rightarrow a*a = a$.

We need to prove that S is a submonoid.

ie (i) closed within S

(ii) $e \in S$.

(ii) $e*e = e$

$\Rightarrow e \in S$

(i) Take $a, b \in S$.

$\Rightarrow a*a = a$, $b*b = b$.

We need to prove,

$a*b*a*b = a*b$

$\Rightarrow a*a*b*b = a*b$ ($\because a, b, \in S$).

Subgroups.

Let $(G, *)$ be a group and S is subset of G, such that it satisfies the following conditions.

(i) $e \in S$, e is identity of $(G, *)$ $\{e\}$.

(ii) For any $a \in S$, $a^{-1} \in S$.

(iii) For $a, b \in S$, $a*b \in S$.

Then $(S, *)$ is called a subgroup of $(G, *)$.

A subgroup with only identity element is called trivial subgroup, all other subgroups are called proper subgroups.

Let $(G, *)$ and (H, Δ) be two groups, a mapping from G to H is called a group homomorphism from $(G, *)$ to (H, Δ), if for any $a, b \in G$,

$$g(a*b) = g(a) \Delta g(b)$$

Let $(G, *)$ be a group, Then for any $a \in G$.

$a^0 = e$

$a^1 = a$

$a^2 = a*a$

$a^3 = a*a*a$.

$a^i = a * a * a \ldots$ i times.

$a^{n+1} = a^n * a.$

$a^i * a^j = a^{i+j}$

$(a^{-1})^n = a^{-n}.$

$(G, *)$ is said to be cyclic if there exists an element $a \in G$, such that every element can be represented as a power of a. Such an element a of the group is called generator of the group.

Here we say, the cyclic group is generated by a, or a is the generator of the group.

Theorem:

Let $(G, *)$ be a finite cyclic group, generated by $a \in G$, if G is of order n, then $a^n = e$, so that $G = \{a, a^2, a^3, \ldots a^n\}$.

Furthermore, n is the least +ve integer, for which $a^n = e$.

Proof:

Let us assume that $m \in G$ and $m < n$ such that $a^m = e$

(ii) Take $a, b \in S$. $a*a = a$, $b*b = a$

i.e., we need to prove

$a*b*a*b = a*b$

$a*a*b*b = a*b$ $(\because a, b \in S)$.

Q) Consider integer modulo 4 denoted by Z_4 with addition modulo 4 denoted as $+_4$. forms the semigroup $(Z_4, +_4)$. Now consider the set $\{1, 3, 7, 9\}$ and the operation multiplication modulo 10 $(S, \times_{10})$ and the operation tables are given by

$= \{0, 1, 2, 3\}$

Ans.

$(Z_4, +_4)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(S, \times_{10})$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$a, b \in Z_4$

Find an isomorphism from Z_4 to S.

$a, b \in Z$

$g(a +_4 b) = g(a) \times_{10} g(b)$

$f(a +_4 b) = f(a) \times_{10} f(b)$

$f: Z_4 \to S$

$f(0) = 1$

$f(1) = 3$

$f(2) = 9$

$f(3) = 7$.

$f(1) = 3$. | $3 \times_{10} 3$

$f((2+3)_4) = 1$ | 9×7

$f(1+2) = 7$ |

$g(3) = f(1 +_4 3)$

$= f(1) \times_{10} f(3)$

$1 = 3 \times 9$

$= 27$

Q) Consider the group of real nos with addition as operation $G_1 : (R, +)$ and group $G' = (R^+, *)$. Find a homomorphism from G to G'

$$g(a) = e^a$$

$$g(a) = 2^a$$

$$g(a+b) = g(a) * g(b).$$

Theorem: Let $(G, *)$ and $(H, \oplus)$ are groups and $g: G \to H$ is a homomorphism. Let e_G and e_H represent the identities of G and H respectively, then

(i) $g(e_G) = e_H$.

(ii) $g(a^{-1}) = [g(a)]^{-1}$

$$g(a * b) = g(a) \oplus g(b)$$

$$g(a * e_H) = g(a) \oplus g(e_G)$$

$$g(a) = g(a) \oplus g(e_G)$$

$$g(e_G) = e_H.$$

$$g(a * a^{-1}) = g(a) \oplus g(a^{-1})$$

$$g(e_G) = g(a) \oplus g(a^{-1})$$

$$e_H = g(a) \oplus g(a^{-1})$$

$$g(a^{-1}) = [g(a)]^{-1}$$

Algebraic system with two binary operators

Rings

Let there be an algebraic system $(A, *, +)$. This is called a ring if

(i) $(A, *)$ is an Abelian group

(ii) $(A, +)$ is a semi group

(iii) $+$ should be distributive over $*$

$(\because a + (b * c) = (a + b) * (a + c)$

$a * b^{-1} e$

$b = a^{-1}$

$a(b + c)$

$= ab + ac$

eg) $(R, +, *)$

For rings, first operators identity is called "zero element"
" second " " called " unit element".

Commutative ring,
If second operator is also commutative, a ring becomes commutative ring.

Ring with identity
Second operator should have an identity within the set.

Subring
A set S which is a subset of R, ~~is called when~~ ~~of~~ $(R, +, \cdot)$ is a ring is called a subring ~~of~~ of $(R, +, \cdot)$ if $(S, +, \cdot)$ itself is a ring. $\{-1, 0, 1\}$

Subgroups and homomorphism

$(G, *)$ (H, Δ)
$g: G \to H$
$a, b \in G$
$g(a*b) = g(a) \Delta g(b)$
$g(e_G) = e_H$
Let S be ~~group~~ subgroup
$g(S)$ represents collection of images of S.
Show that $g(S)$ is a subgroup of (H, Δ).
(i) $e_G \in S$
$g(e_G) = e_H$
$e_H \in g(S)$

(ii) $h_1, h_2 \in g(S)$

$h_1 * h_2 \in g(S)$

(iii) For any $h \in g(S)$

$h^{-1} \in g(S)$

s.t $h * h^{-1} = e_H$.

(i) $a, b \in S \quad g(a*b) = g(a) * g(b)$

$S_1 = S_1 * S_2$.

$g(a*b) \in g(S)$

$g(a) \in g(S)$

$g(b) \in g(S)$

(ii) $s \in g(S)$

$s' \in g(S)$

show that $s * s^{-1} = e_H$.

$a \in S$.

$\Rightarrow a^{-1} \in S$.

$g(a * a^{-1}) = g(a) * g(a^{-1})$

$g(e_H) = g(a) * g(a^{-1})$

$e_H = g(a) * g(a^{-1})$

$\Rightarrow [g(a)]^{-1} = g(a^{-1})$

$g(a^{-1}) \in g(S)$

$\Rightarrow$

Kernal of a homomorphism

$(G, *)$, (H, Δ)

$g : G \to H$.

Then all the elements which are mapped to e_H are called kernal of homomorphism, $ker(g)$.

Theorem: Kernal of a homomorphism g from a group $(G, *)$ to (H, Δ) is a subgroup of $(G, *)$.

$a, b \in$ kernal

$$g(a * b) = g(a) \Delta g(b)$$
$$= e_H \Delta e_H$$
$$= e_H.$$

$\Rightarrow (a * b) \in ker(g)$

Consider $a \in ker(g)$ $a^{-1} \in G$.

$$g(a * a^{-1}) = g(a) \Delta g(a^{-1})$$
$$g(e_G) = e_H \Delta g(a^{-1})$$
~~$\Rightarrow g(e_H) = g(a^{-1})$~~
$$e_H = e_H \Delta g(a^{-1})$$
$$\Rightarrow g(a^{-1}) = e_H.$$

$\Rightarrow a^{-1}$ is some element mapped to e_H.

Cosets

$(G, *)$ $(H, *)$

equivalence relation.

$a, b \in G$

$\boxed{a \equiv b \bmod H}$

$b^{-1} * a \in H$

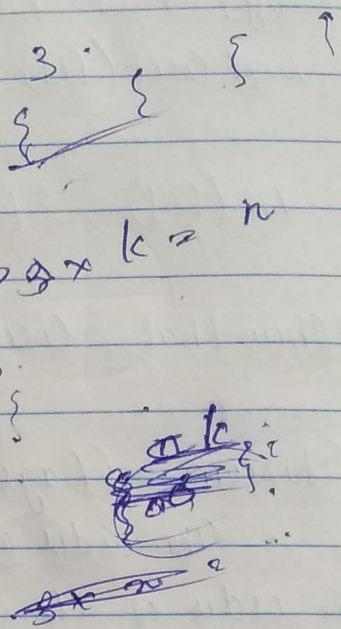
$b^{-1} * a = h \in H$

$b * b^{-1} * a = b * h$

$a = b * h$

$b \in G$

$[b] = \{x \mid x = b * h,\ h \in H\}$.



e.g.,

$(Z, +)$, $(M, +)$

$M = \{-10, -5, 0, 5, 10 \ldots\}$

$[0] = \{x \mid x = 0 + h,\ h \in M\} = \{-10, -5, 0, 5, 10 \ldots\}$

$[1] = \{x \mid x = 1 + h,\ h \in M\} = \{\ldots -9, -4, -1, 6, 11 \ldots\}$

$[2] = \{x \mid x = 2 + h,\ h \in M\} = \{\ldots -8, -3, 2, 7, 12 \ldots\}$

$[3] = \{x \mid x = 3 + h,\ h \in M\} = \{\ldots -7, -2, 3, 8, 13 \ldots\}$

$[4] = \{x \mid x = 4 + h,\ h \in M\} = \{\ldots -6, -1, 4, 9, 14 \ldots\}$

$[5] = \{x \mid x = 5 + h = h \in M\} = \{\ldots -5, 0, 5, 10, 15 \ldots\}$

$[0] \Rightarrow$ is a coset.

Union of all the cosets give the group itself

$Z_4 = \{[0], [1], [2], [3]\}$

$(Z_4, +_4)$

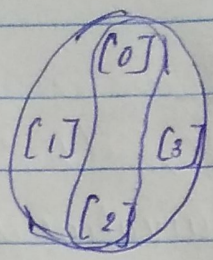
$[x] = S$

$[y] = T$

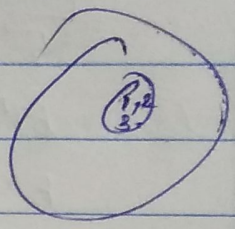
Left Coset $([1]) = \{[1] +_4 [0], [1] +_4 [2]\}$

$= \{[1], [3]\}$

$LC([3]) = \{[1], [3]\}$.



Q) Show that Coset relation is an equivalence relation.



Theorem: (Lagrange's Theorem)

The order of a subgroup of a finite group divides the order of the group.

Proof:

$a * H = \{a*1, a*2, a*3\}$

$|G| = n$

$|H| = m$.

Size of a left coset w.r.t $H = m$

Let k be the no. of left cosets.

$k * m = n$

$\Rightarrow m | n$.

Q) Prove that relation left coset on a group is an equivalence relation.

Ans) $(G, *)$, $(H, *)$

$a \equiv b \bmod H$

$\boxed{b^{-1} * a = h \in H}$

$a = b * h$, $h \in H$.

Reflexive $a \equiv a \bmod H$

$a^{-1} * a = e_H = e \in H$.

∴ It is reflexive.

Symmetric.

is $a \equiv b \bmod H$ = $b \equiv a \bmod H$.

ie, we have to show

$b^{-1} * a \in H \Rightarrow a^{-1} * b \in H$.

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

$\Rightarrow$ $a^{-1} * b$ is the inverse of $b^{-1} * a$.

Since its a subgroup,

if an element exists in the subgroup, then its inverse also exists in the subgroup.

~~Transitivity~~

Note: If $aH = Ha$; then the sub group is called Normal subgroup.

Q) Determine whether $(\mathbb{Z}, \oplus, \odot)$ is a ring with binary operations defined as follows.

$x \oplus y = x + y - 7$

$x \odot y = x + y - 3xy$.

Q) $M(\mathbb{Z})$ is the set of all 2×2 matrices with integer entries. Check if it's a ring. Operations are matrix addition and multiplication.

Ans) Closure property

Let $A, B \in M(\mathbb{Z})$.

Let $A + B = C$

Associativity of $\times$

$$(A \times B) \times C = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} aei + bgi + afk + bfk & aej + bgj + afl + bhl \\ cei + dgi + cfk + dhk & cej + dgj + cfl + dhl \end{bmatrix}$$

Special types of rings

Let $(R, +, \cdot)$ be a ring. If

(i) $ab = ba$ $\forall a, b \in R$, then R is called commutative ring. $a \cdot b = ab$.

(ii) A ring is said to have no proper divisors of zero if $\forall a, b \in R$,

$ab = z \Rightarrow a = z$ or $b = z$. (z is zero element)

zero element means, identity of first operation.

~~(iii)~~ (Proper divisors of zero means that, they have non-zero elements whose product is the zero element of the ring)

(iii) If $u \in R$ and $u \neq z$ (where u is unity), and $au = ua = a$, for all $a \in R$, then R is called a ring with unity.

Note: Identity of first operation is generally called additive identity. and identity of second operator is called multiplicative identity.

(iv) Let R be a commutative ring with unity, then R is called an integral domain. If R has no proper divisors of zero.

(a) R is called a field if every non zero element of R is a unit.

~~Q) Let~~

Let R be a ring with unity u, if $a \in R$, $b \in R$ $ab = ba = u$, ~~then~~ we say that b is the multiplicative inverse of a and a is the unit of R.

Q) $u = \{1, 2\}$, $R = P(u)$, $+$ and $\cdot$ $\quad (\mathbb{Z}, +, \cdot)$

$A + B = A \Delta B$ $\qquad A - B \cup B - A$

$A \cdot B = A \cap B$.

Check if it's a ring.

Ans)

+	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
ϕ	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	ϕ	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	ϕ	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	ϕ

$P(u) = \{\phi, \{1\}, \{2\}, \{1,2\}\}$

·	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$
ϕ	ϕ	ϕ	ϕ	ϕ
$\{1\}$	ϕ	$\{1\}$	ϕ	$\{1\}$
$\{2\}$	ϕ	ϕ	$\{2\}$	$\{2\}$
$\{1,2\}$	ϕ	$\{1\}$	$\{2\}$	$\{1,2\}$

Commutative ring with identity ?

proper zero divisors? $\{1\}$ $\{2\}$

It is not an integral domain

Ring homomorphism

$(R, +, \cdot)$ & $(S, \oplus, \odot)$

is called a ring homomorphism

if $f : R \to S$.

for any $a, b \in R$

$f(a+b) = f(a) \oplus f(b)$ and

$f(a.b) = f(a) \odot f(b)$

8) Check whether Z_5 is a field & ? Check also Z_6.

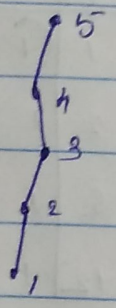
Lattice

Lattice is a kind of algebraic structures with two operations. GLB LUB. meet

$(A, \vee, \wedge)$, $(A, +, \cdot)$ → join.

$((A, \leq), \vee, \wedge)$

$A = \{1, 2, 3, 4, 5\}, \leq)$



For any pair of elements $i, j \in A$

i, j posses a LUB & and GLB, ~~we have~~ it, this a lattice.

Consider the ~~poset~~ poset $(P(S), \subseteq)$

Here the meet is $\cap$ $A \cap B$ and join is $A \cup B$.

$(D_{35}, |)$ D_{35} All +ve divisors of 35.

$D_{35} = \{1, 5, 7, 35\}$

Let $a, b \in D_{35}$

$LUB(a, b) = LCM(a, b)$

$GLB(a, b) = HCF(a, b)$.

Dual or inverse lattice

$(A, \leq) = (A, \vee, \wedge)$

$(A, \geq) = (A, \wedge, \vee)$

$(P(S), \subseteq) = (P(S), \cup, \cap)$

$(P(S), \supseteq) = (P(S), \cap, \cup)$

$A = (\{1, 2, 3, 12\}, |)$

Matrix table
mult, join.

(+)

lub	1	2	3	12
1	1	2	3	12
2	2	2	12	12
3	3	12	3	12
12	12	12	12	12

glb (.)	1	2	3	12
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
12	1	2	3	12

glb and lub are commutative.
ie, the matrices are symmetric. So instead of storing redundant data, we will store both these in a single matrix.

ie

. \ +	1	2	3	12
1	1	2	3	12
2	1	2	12	12
3	1	1	3	12
12	1	2		12

Sublattice

If $(A, \leq)$ is a lattice, then, a non empty subset B of A is called a sublattice of A if for any $a, b \in B$, a join b and a meet $b \in B$.

$(\mathbb{Z}^+, |)$

$(D_n, |)$

$a, b \in D_n$

$a \vee b$
$a \wedge b$ $\in D_n$?

$1 \in D_n$

$n \in D_n$

Draw D_{24}. Find all sublattices of D_{24}, that contains atleast 5 elements. Also gives examples of ~~sub~~lattice which are not sub lattices.

$D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$