Algebra

Defn: manipulates symbols with operators and symbols assume some numbers.

Symbols can be variables or constants.

Why Symbols

↳ They represent a wide variety of numbers

$x+y$, x, y can be any numbers

This algebra is called classical algebra.

In modern algebra, the vars can be anything

for eg, x = man

Modern algebra is also called Abstract algebra.

In this algebra, we need: ① a set (S)

② Operators $(o_1, o_2, \ldots, o_n)$

Algebraic Structure

A set and collection of operators over the set is called algebraic structure.

if op are $+, /, -, *$, it is called classic algebraic structure.

Boolean Algebra $(K, \wedge, \vee, ')$

A boolean algebra is a set K together with two binary operations $\wedge$ & $\vee$ and one unary operation $'$ on K satisfying

① $A \wedge (B \wedge C) = (A \wedge B) \wedge C$

② $A \vee (B \vee C) = (A \vee B) \vee C$

③ $A \wedge B = B \wedge A$

④ $A \vee B = B \vee A$

⑤ $A \vee (B \wedge C)$

$= (A \vee B) \wedge (A \vee C)$

⑥ $A \wedge (B \vee C)$

$= (A \wedge B) \vee (A \wedge C)$

⑦ $\exists$ zero in K s.t $A \vee 0 = A$

⑧ $\exists$ one in K s.t $A \wedge 1 = A$

⑨ $A \vee A' = 1$

⑩ $A \wedge A' = 0$

Q $A=\{a,b\}$, is $(P(A), \cup, \cap, ')$ a boolean algebra?

Ans i) $\{a\} \cup (\{a,b\} \cap \{b\}) = \{a,b\} = (\{a\} \cup \{a,b\}) \cap \{b\}$

ii) $\{a\} \cap (\{a,b\} \cap \{b\}) = \phi = (\{a\} \cap \{a,b\}) \cap \{b\}$

iii) $\{a\} \cap \{b\} = \phi = \{b\} \cap \{a\}$

iv) $\{a\} \cup \{b\} = \{a,b\} = \{b\} \cup \{a\}$

v) Show distributive

vi)

vii) $x \cup \phi = x$

viii) $x \cap P(A) = x$

ix) $\{a\} \cup \{a\}' = \{a\} \cup \{b\} = P(A)$ = one.

x) $\{a\} \cap \{a\}' = \{a\} \cap \{b\} =$ zero.

Q Show, $S=\{1,2,6,9,18\} \Rightarrow (S, GCD, LCM, ')$ is a boolean algebra?

Ans → 6 has no complement in S

→ also $gcd(6,9) = 3 \notin S$

not a boolean algebra.

Q Is a complemented ~~boolean algebra~~ lattice a boolean algebra?

Ans ① Commutative:

$x \wedge y = y \wedge x$ & $x \vee y = y \vee x$

by defn, $x \wedge y = glb(x,y)$ & $x \vee y = lub(x,y)$

$x \wedge y = glb(x,y) = glb(y,x) = y \wedge x$

Similarly, $x \vee y = lub(x,y) = lub(y,x) = y \vee x$

② Associative

$x \wedge (y \wedge z) = glb(x, y \wedge z) = glb(x, glb(y,z)) = glb(x,y,z)$

$= glb(x \wedge y, z) = (x \wedge y) \wedge z$.

Similarly for $x \vee (y \vee z) = (x \vee y) \vee z$

③ Identity

$x \wedge 1 = glb(1,x)$

Since 1 is a upper bound, $x \geq 1$

Hence $glb(x,1) = x$.

$x \vee 0 = lub(x, 0)$

as 0 is a lower bound,

$0 \leq x$

$lub(0, x) = x \vee 0$

④ Complent and Distributive

↳ since the lattice is distributive and complemented both of the laws are true

Permutation

↳ it is essentially a bijective function, from a set of n elements to itself.

Th $|S_n| = n!$

Proof) $S_n \Rightarrow$ n elements & bijective function

for $a_1 \rightarrow$ there are n choices

" $a_2 \rightarrow$ " " n-1 "

"

" $a_n \rightarrow$ " " 1 choice

So, total choices $= n \times (n-1) \times \cdots \times 1$

$= n!$

If S_n is a set of permutation & $\circ$ is an operator, $(S_n, \circ)$ is called a symmetric group under $\circ$.

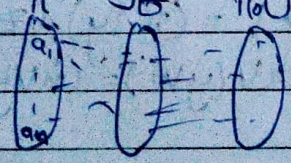
Conditions

① if $\pi, \sigma \in G$ then $\pi \circ \sigma \in G$

② if $\pi \in G$, then $\pi^{-1} \in G$

③ $Id \in G$

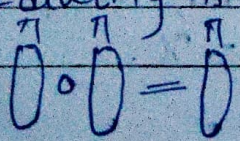
Proof ① Let's say the set is $A = \{a_1, \ldots, a_n\}$



← this also permutation

② Since, bijective, inverse exist

③ Identity is $f(n) = n$



Proposition: Let π and σ be two permutation of S_n then
$(\pi \circ \sigma)^{-1} = \sigma^{-1} \circ \pi^{-1}$

Proof) $(\pi \circ \sigma) \circ (\sigma^{-1} \circ \pi^{-1})$
$= \pi \circ (\sigma \circ \sigma^{-1}) \circ \pi^{-1}$
$= \pi \circ (Id) \circ \pi^{-1}$ Hence proved.
$= \pi \circ \pi^{-1} \circ Id$
$= Id \circ Id = Id$.

Q does π_1, π_2, π_3 form a permutation group

Ans $\pi_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ $\pi_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$ $\pi_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$

$\pi_2 \circ \pi_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \notin G$ hence not permutation group.

Abstract Group

Defn) A group $(G, \cdot)$ is ~~a set~~ G ~~together with a binary operation~~ $\cdot$ ~~satisfying~~:

i) G is closed under $\cdot$; $a.b \in G \ \forall a, b \in G$

ii) $\cdot$ is associative ; $(a.b).c = a.(b.c) \ \forall a, b, c \in G$

iii) there is an identity element $e \in G$ such that $e.a = a.e = a$ $\forall a \in G$

iv) Each element $a \in G$ has an inverse element $a^{-1} \in G$ such that $a.a^{-1} = a^{-1}.a = e$.

If a group is commutative, $(a.b = b.a \ \forall a, b \in G)$ it is called a abelian group.

eg $G = \{i, -1, -i, 1\}$ $\cdot \rightarrow$ multiplication
Is it a group?

Ans We've to make a table.

·	i	-1	-i	1
i	-1	-i	1	i
-1	-i	1	i	-1
-i	1	i	-1	-i
1	i	-1	-i	1

i) for $\forall a, b \in G$, $ab \in G$ → this is evident

ii) Multiplication is associative

iii) 1 is identity element

anything · 1 = 1 · anything = anything

iv) Inverse here is $1/a$

$i \to 1/i \Rightarrow -i$

$1 \to 1/1 \Rightarrow 1$

$-1 \to 1/-1 \Rightarrow -1$

$-i \Rightarrow 1/-i \Rightarrow i$

Each group must have at least one element, its identity, this element is called trivial.

Some imp stuff

(i) Composition will be a group.

Th Let $*$ be a binary op on set S, that has identity e. then a has an inverse, that is unique

Proof) Let b & c are both inverses of a

$\therefore a*b = b*a = e$ & $a*c = c*a = e$ (identity)

$b = b*e = b*(a*c) = (b*a)*c = e*c = c$

hence, $b = c$ ↳ (associative)

Th if a, b, c are elements of group G.

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

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

iii) $ab = ac$ or $ba = ca \to b = c$ (cancellation law)

Proof) i) $a \cdot a^{-1} = e$ (by inverse)
$\rightarrow a^{-1} \cdot (a^{-1})^{-1} = e$ (by inverse)
a^{-1} has unique inverse.
so $a = (a^{-1})^{-1}$ proved.

ii) $(ab)(b^{-1} a^{-1})$
$= a(bb^{-1})a^{-1}$
$= a(e)a^{-1} = e \cdot e = e$

iii) Let $ab = ac$
$\rightarrow a^{-1}(ab) = a^{-1}(ac)$
$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$
$\rightarrow b = c$

similarly, the other is true as well.
proved

Eg $(Z, +)$ is group?
Ans i) addition is closed
ii) " , associative
iii) Identity $= 0$
iv) inverse is zero.
Yes

Eg $(Z, \times)$ is group?
Ans iv) inverse is $\frac{1}{a} \notin Z$
No

Eg $(R, \times)$ is group?
Ans iv) inverse of 0 is $\frac{1}{0} = \infty \notin R$
No

Subgroup

Defn If G is a group on $\cdot$, H is a non-empty subset of G, then $(H, \cdot)$ is a subgroup of $(G, \cdot)$ if
i) $a.b \in H, \forall a, b \in H$ (closure)
ii) $a^{-1} \in H, \forall a \in H$ (Inverse)

Th if H is a subgroup of $(G,\cdot)$ $(H,\cdot)$ is a group.

Proof From def^n,
H is closed & has inverse

① Associative
↳ $a,b,c \in H$, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ as all in G.
So it's associative.

② Identity
$a\cdot a^{-1} = one \in G \Rightarrow \in H$
So it has identity.

Th If H is a non empty finite subset of group G and $ab \in H$. $\forall a,b \in H$, then H is a subgroup of G.

Proof We have to show for $a \in H$, it's inverse is in H.
so if $a \in H$, $a\cdot a = a^2 \in H$
$\Rightarrow a\cdot a\cdot a = a^3 \in H$ ....
Since H is finite they will repeat after some time.
$\Rightarrow a^i = a^j$ for some $i,j \in \mathbb{Z}$
$\Rightarrow a^{i-j} = e$ (by cancellation law)
$\Rightarrow a\cdot a^{i-j-1} = e$
$\Rightarrow$ a's inverse is a^{i-j-1}
hence inverse exists.

Cyclic Groups

Order of group $\Rightarrow$ It is the number of elements in G.
if $|G|$ is finite, finite group
if $|G|$ " infinite, infinite group.

Def^n A group $(G,\cdot)$ is called cyclic if there exists an element $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$
g is called the generator of cyclic group.

Eg $G = \{1,-1,i,-i\} \Rightarrow (G,\cdot)$
Ans $i = i$ $i^3 = -i$ $i \rightarrow$ generator element
$i^2 = -1$ $i^4 = 1$ it is a cyclic group.

Order of an element

↳ The order of an element $g \in G$ is the least positive integer r such that $g^r = e$.
if r doesn't exist, it's an infinite group.

Th Let a be an element of order r in a group G. Then for $k \in \mathbb{Z}$, $g^k = e$ iff $r \mid k$.

Ans if $k = rm$, $m \in \mathbb{Z}$
then $a^k = a^{rm} = (a^r)^m = e^m = e$
Converse, if $a^k = e$, $k = qr + s$

$$a^s = a^{k-qr} = a^k (a^r)^{-q} = a^k (e)^{-q} = e$$

↳ So $k = qr$

Th Every subgroup of a cyclic group is cyclic

Ans Let G is cyclic with g and $H \subset G$ is a subgroup.
if $H = \{e\}$, it is cyclic with e.
Otherwise, Let $g^k \in H$, $k \neq 0$

$$\Rightarrow (g^k)^{-1} \in H$$

So, we have some $g^m \in H$, $m \neq 0$.
Let m be as small as possible.
Let $h = g^m$ ⇒ we need to show h generates H
obviously, $h^k \in H$ $\forall k$ as closure property.
To show $\forall a \in H$, $a^{\text{power}} \in H$.
↳ since $a \in G \Rightarrow a = g^s$ for some $s = qm + r$ $(0 \leq r < m)$

$$\Rightarrow a^r = g^{s-qm} = (g^s)(g^m)^{-q} = a\,h^{-q} \in H$$

$r = 0$, by choosing suitable m

$$\Rightarrow a = g^s = g^{qm} = (g^m)^q = h^q$$

proved

Th If g is any element of order k in a group $(G, \cdot)$ then $H = \{g^r \mid r \in \mathbb{Z}\}$ is a subgroup ~~generated by~~ of order k in $(G, \cdot)$ [also called cyclic subgroup]

Proof) First let's check if H is a subgroup of G

i) $g^r, g^s \in H \quad g^r \cdot g^s \Rightarrow g^{r+s} \in H$ (closure)

ii) $g^r \in H \Rightarrow g^{-r} \in H$ (inverse)

if order is infinite,

↳ need to show g^0 are all distinct

Let $g^r = g^s$, $r > s$

$\Rightarrow g^{r-s} = e$ (cancellation Law)

$\Rightarrow$ contradicts that it has int order

if order of g is k,

↳ need to show $H = \{g^0 = e, g^1, g^2, \dots, g^{k-1}\}$

Let $g^r = g^s$, $0 < s < r < k-1$

$\Rightarrow g^{r-s} = e$ (cancellation Law)

$\Rightarrow$ contradicts that k is order

hence $g^0, g^1, \dots, g^k$ are all distinct.

but if $g^t \in H$, where $t = qk + r$ $0 < r < k$.

$$g^t = g^{qk+r} = (g^k)^q (g^r) = (e^q) g^r = g^r$$

Hence, $H = \{g^0, g^1, \dots, g^{k-1}\}$, $|H| = k$.

Th If finite group G is order n, and has elements of order n, G is a cyclic group generated by g.

Proof) from earlier, we know H, a subgroup of G generated by g, has order n, Therefore H is a subset of G, Hence $G = H$ proved.

Q Is $H = \{1, -1\}$ subgroup of $G = \{1, -1, i, -i\}$

Ans i) Closure $\Rightarrow$ $1 \cdot -1 = -1$ $-1 \cdot -1 = 1$ $1 \cdot 1 = 1$ ✓

(ii) Inverse $\Rightarrow$ $\frac{1}{-1} = -1$ $\frac{1}{1} = 1$ ✓

Morphism

Def If $(G,\cdot)$ & $(H,*)$ are two groups, the function $f: G \to H$ is called a group morphism.

If the groups had different operations $(G,\cdot)$ & $(H,*)$ then,

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

this is $f: (G,\cdot) \to (H,*)$ and called homomorphism.

A group morphism, which is bijective is called isomorphism. denoted as

$$(G,\cdot) \cong (H,*)$$

Common group morphisms

① trivial function that maps G to H.

② $f: \mathbb{Z} \to \{1,-1\}$ $f(n) = 1$ even
$= -1$ odd

③ $G \to 2\times 2$ invertible matrix. $L \to$ Linear transforms
G & L form isomorphism.

Th Let $f: G \to H$ be group morphism and e_G & e_H be indentities

i) $f(e_G) = e_H$

ii) $f(a^{-1}) = f(a)^{-1}$ $\forall a \in G$

Proof i) $f(e_G) f(e_G) = f(e_G \cdot e_G) = f(e_G) = f(e_G) e^H$

by cancellation,

$f(e_G) = e^H$

ii) $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H$

Th Cyclic groups of same order are isomorphic

Proof Let $G = \{g^r \mid r \in \mathbb{Z}\}$ & $H = \{h^r \mid r \in \mathbb{Z}\}$

if G & H are infinite.

$g^r = g^s$ iff $r = s$. hence $f(g^r) = h^r$ is a bijection

$f(g^r g^s) = f(g^{r+s}) = h^{r+s} = h^r \cdot h^s = f(g^r) f(g^s)$

...ite integral domain that is not a field.

...nly if n is prime.

...$a] = [0]$ in $\mathbb{Z}_n$. Then $n|ab$. So ...). Hence $[a] = [0]$ or ... it follows from ...

if $|G| = |H| = n$,

$G = \{g^0, g^1, \ldots, g^{n-1}\}$ $H = \{h^0, h^1, \ldots, h^{n-1}\}$

Let $f(g^r) = h^r$ for $f: G \to H$.

it is bijective as all are unique & distinct.

let $r+s = kn+L$ $0 \le L < n$

$f(g^r \cdot g^s) = f(g^{r+s}) = f(g^{kn+L}) = f((g^n)^k \cdot g^L) = f(e^k \cdot g^L)$

$= f(g^L) = h^L$

$f(g^r) f(g^s) = h^r \cdot h^s = h^{r+s} = h^{kn+L} = (h^n)^k \cdot h^L$

$= e^k \cdot h^L = h^L$.

so, f is an isomorphism.

Th Elements under a group isomorphism have same order.

Proof) Let $f: G \to H$ & $f(g) = h$.

let g have order m & h have order n.

$h^m = f(g)^m = f(g^m) = f(e) = e$

hence $m = n$

Cayley's Theorem

Defn Every group $(G, \cdot)$ is isomorphic to a subgroup of its symmetric group $(S(G), \circ)$

Corollary If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof) For each element $g \in G$, define $\pi_g: G \to G$ as $\pi_g(x) = g.x$

It's surjective as $\forall y \in G$, $\pi_g(g^{-1}y) = \pi_g(yg^{-1}) = y$.

It's injective as $\pi_g(x) = \pi_g(y)$ means

$g.x = g.y$

$x = y$

Hence it is a bijection. & $\pi_g \in S(G)$

Let $H = \{\Pi_g \in S(G) \mid g \in G\}$

To show, $(H, \circ)$ is a subgroup of $(S(G), \circ)$ isomorphic to $(G, \cdot)$.

Let $\varphi(g) = \Pi_g$

it is surjective ; Obvious

" " injective, as $\varphi(g) = \varphi(h)$

$\Rightarrow \Pi_g = \Pi_h$

$\Rightarrow g = h$.

for group morphism,

if $g, h \in G$, $\Pi_{g.h}(x) = (g.h)x$

$= g.(h.x)$

$= \Pi_g(h.x) = (\Pi_g \circ \Pi_h)(x)$

$\rightarrow \Pi_{g.h} = \Pi_g \circ \Pi_h$.

Also $\Pi_{g.g^{-1}} = \Pi_{g^{-1}.g} = \Pi_e$ thus $(\Pi_h)^{-1} = \Pi_{h^{-1}}$

Hence H is a subgroup of $S(G)$ & $\varphi(g.h) = \varphi(g).\varphi(h)$

Monoid

↳ A monoid $(M, *)$ consists of a set M together with a binary operation $*$ on M such that

i) $a*(b*c) = (a*b)*c$ (associative)

ii) Identity exists $e \in M$, s.t $a*e = e*a = a$ $\forall a \in M$

→ All groups are monoids but the reverse isn't true.

→ if $a*b = b*a$, it is called commutative monoid.

Semigroup.

↳ Semigroup $(S, *)$ is a set S together with an associative binary operation $*$.

eg → $(\mathbb{Z}^+, +)$ is a semigroup, but not monoid.

11. Let X be any set and let $X^X = \{f : X \to X\}$ be the set of all maps from $X \to X$ then $(X^X, \circ)$ is a monoid. This is called transformation monoid.

Proof: If $f, g \in X^X$, then $fog \in X^X$

composition is always associative

Identity function $I : I_X(x) = x$

Hence it is a monoid.

8. Prove $(\mathbb{Z}, *)$ is a commutative monoid where $x * y = 6 - 2x - 2y + xy \quad \forall x, y \in \mathbb{Z}$.

Ans $\forall x, y \in \mathbb{Z}$, $x * y \in \mathbb{Z}$ and $x * y = y * x$ (Obvious)

$$x * (y * z) = x * (6 - 2y - 2z + yz)$$
$$= 6 + 4x + 4y + 4z - 2xy - 2xz - 2yz + xyz$$

$$(x * y) * z = (6 - 2y - 2x + xy) * z$$
$$= 6 + 4x + 4y + 4z - 2xy - 2xz - 2yz + xyz$$

$\therefore$ Associative ✓

Let $e * x = x$

$\therefore 6 + 2e - 2x + ex = x$

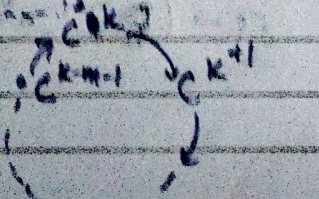
$(x - 2)(e - 3) = 0$

$\therefore e = 3 \leftarrow$ Identity.

Def: The monoid $(M, *)$ is said to be generated by the subset A if every element of M can be written as finite combination of power of element of A. If $m \in M$

$$m = a_1^{r_1} * a_2^{r_2} * \dots * a_n^{r_n}$$

↳ This is cyclic monoid



Let $A = \{a, b\}$

$A_n \rightarrow$ be set of length n strings

$A^3 = \{aaa, aab, aba, \ldots, bbb\}$

Let $FM(A)$ denote the set of all words from A,

$$FM(A) = A^0 \cup A^1 \cup A^2 \cup A^3 \cup \ldots = \bigcup_{n=0}^{\infty} A^n$$

$(FM(A), *)$ is called free monoid generated by A.

if we don't include A^0, it's called free semigroup.

Ring

A ring $(R, +, \cdot)$ is a set R, with two binary operations $+$ and $\cdot$ on R satisfying the following $(a, b, c \in R)$

i) $(a+b)+c = a+(b+c)$
ii) $a+b = b+a$
iii) $\exists\ 0 \in R$, called zero s.t $a+0=a$
iv) $\exists\ -a \in R$, s.t. $a+(-a)=0$

} Abelian group on $+$

v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
vi) $\exists\ 1 \in R$ s.t $1 \cdot a = a \cdot 1 = a$

} Monoid on $\cdot$

vii) $a \cdot (b+c) = ab + a \cdot c$
$(b+c) \cdot a = b \cdot a + c \cdot a$

} distributive on $+$ under $\cdot$

Commutative ring :- if $a \cdot b = b \cdot a$

Q $R = \{ev, odd\}$ is $(R, +, \cdot)$ a ring?

Ans

+	ev	odd
ev	ev	odd
odd	odd	ev

×	ev	odd
ev	ev	ev
odd	ev	odd

(1) $+$ is commutative
(2) $+$ " "
(3) Id = even
(4) $(odd)^{-1} = odd$
$(even)^{-1} = even$
(5) $\cdot$ is associative
(6) Id = odd
(7) $+, \cdot$ always distibutive

hence it is a ring.

Q $(\mathbb{Z}_n, +, \cdot) \Rightarrow [x]+[y]=[x+y]$
$[x].[y]=[x \cdot y]$

Ans $(\mathbb{Z}, +)$ is abelian [earlier done]
zero $\equiv [0]$ unit $\equiv [1]$
distributive is true
$[x]=[x']$ $[y]=[y']$
$\Rightarrow x \equiv x' \pmod n$ $y \equiv y' \pmod n$
$\Rightarrow x = x' + kn$ $y = y' + ln$
$\Rightarrow x.y \equiv x'.y' \pmod n$
$\Rightarrow [x.y]=[x'.y']$
Mult is well defined so must be associative

Q $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ a ring? $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

Ans $\mathbb{Q}\sqrt{2} \in \mathbb{R}$
i) Addition is commutative
ii) " associative
iii) $0 \in \mathbb{Q}\sqrt{2}$ $0+a=a$
iv) $a+b\sqrt{2} \Leftrightarrow (-a)+(-b)\sqrt{2}$, add to get 0
v) Multiplication is associative
vi) Identity $\Rightarrow 1$ $1 \cdot (a+b\sqrt{2})=(a+b\sqrt{2}).1=a+b\sqrt{2}$
vii) Multiplication & Addition are distributive
To show, $+, \cdot$ are binary o/p.
(+) $a+b\sqrt{2}+c+d\sqrt{2}=(a+c)+(d+b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$
(·) $(a+b\sqrt{2})(c+d\sqrt{2})=ac+2bd+\sqrt{2}(ad+bc) \in \mathbb{Q}\sqrt{2}$

Th If $(R, +, \cdot)$ is a ring, then $\forall a,b \in R$
i) $a.0=0.a=0$
ii) $a.(-b)=(-b).a=-(a.b)$
iii) $(-a).(-b)=a.b$
iv) $(-1).a=-a$
v) $(-1).(-1)=1$

Proof) i) $a.0 = a(0+0)$

$= a.0 + a.0$

$-a.0 + a.0 = a.0 + a.0 - a.0$

$a.0 = 0$

similarly $0.a = 0$

ii) $a.(-b) + a.b = a(-b+b)$

$= a.0 = 0$

$\therefore a.(-b) = -(a.b)$

Similarly, $(-a).b = -(a.b)$

iii) $(-a).(-b) = -(a.(-b))$

$= -(-(a.b))$

$= a.b$

iv) $(-1).a = -(1.a) = -a$

v) $(-1).(-1) = (-(-1.1)) = -(-1)$

$= 1$

Th ring has only one element 0, if 0=1, it is called trivial ring. Rest are called non-trivial.

Proof) $0 = 1$

$a = a.1 = a.0 = 0 \Rightarrow$ ring has only 0.

Integral Domain

If $(R, +, \cdot)$ is a commutative ring, a non-zero $a \in R$ is called zero divisor if there exists a non-zero element $b \in R$ s.t $a.b = 0$. A non trivial commutative ring is called integral domain if it has no zero divisors.

In integral domain, $a.b = 0 \Rightarrow a = 0$ or $b = 0$.

Th If a is a non-zero element of ID R and $a \cdot b = a \cdot c$ then $b = c$.

Proof if $a \cdot b = a \cdot c$ then

$$a(b-c) = a \cdot b - a \cdot c = 0$$

Since $a \neq 0 \Rightarrow b - c = 0 \Rightarrow b = c$

Field

↳ commutative ring with extra axiom

ix) for each non zero element $a \in R$

$\exists\ a^{-1} \in R$ s.t $a \cdot a^{-1} = 1$.

Q $(\mathbb{Z}, +, \cdot)$ Field?

Ans $(\mathbb{Z}, \cdot)$ not abelian

Q $(\mathbb{Z}_5, +, \cdot)$ field?

Ans $[2] \cdot [1] = [1] \cdot [2] = [2]$

inv exists.

Th $\mathbb{Z}_n$ is a field if and only if n is prime.

Proof Let $n \Rightarrow$ prime and $[a] \cdot [b] = [0]$ in $\mathbb{Z}_n$

$\Rightarrow n \mid ab$ so $n \mid a$ or $n \mid b$ by euclid's lemma.

hence $[a] = [0]$ or $[b] = [0]$ and $\mathbb{Z}_n$ is an ID

Since $\mathbb{Z}_n$ is finite, $\mathbb{Z}_n$ is a field (we will prove this later).

Let $n \Rightarrow$ not prime.

$n = rs$ $1 \leq r \leq n$ & $1 < s < n$

Now $[r] \neq 0$, $[s] \neq 0$ but $[r][s] = [rs] = [0]$

hence $\mathbb{Z}_n$ has zero divisors hence not ID nor a field.

Th Every field is ID.

Proof Let $a \cdot b = 0$ in F

if $a \neq 0$, $\exists\ a^{-1} \in F$

and $b = (a^{-1}a) \cdot b$

$= (a^{-1})(a \cdot b) = a^{-1} \cdot 0 = 0$

Hence either $a = 0$ or $b = 0$

& F is a ID

Th A finite ID is a field

Pf Let $D = \{x_0, x_1, \ldots, x_n\}$ be a finite ID with x_0 as 0 & x_1 as 1.

if x_i is non zero,

To show $x_i D = \{x_i x_0, \ldots, x_i x_n\}$ is same as D.

if $x_i x_j = x_i x_k \Rightarrow x_j = x_k$. and,

① all of $x_i x_0, \ldots, x_i x_n$ are distinct

② $x_i D \subseteq D$

③ $x_i D$ & D have same no of elements

(as $x_i D = D$)

But $\exists$ some x_j s.t

$$x_i x_j = x_1 = 1$$

$$\Rightarrow x_j = x_i^{-1} \Rightarrow D \text{ is a field.}$$

Q $(\mathbb{Q}\sqrt{2}, +, \cdot)$ a field?

Ans ↳ it is commutative ring done earlier.

To show inverse.

Let $a + b\sqrt{2}$ be non-zero so $a \neq 0$ or $b \neq 0$ or $a \neq b \neq 0$

hence $a - b\sqrt{2} \neq 0$ so,

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

It is a field.