$\forall f \in G(X)$, $f^{-1} \in G(X)$

→ S_X is the symmetric group.

S_X: Set of all bijections on X.

21|08|2019

Symmetric group or Permutation group:

Symmetric group is denoted by S_X is the set of all permutations (bijections) on a non-empty set X considered w.r.t. composition of mappings.

- If $|X| = n$ then $\boxed{S_X = S_n}$
- $\boxed{|S_n| = n!}$

* Let $|G| = n$

$n=1$, $\mathbb{Z}_1 = \{\bar{0}\}$

S_1

* $G = \{a, b\}$.

o	a	b
a	a	b
b	b	a

only 1 group with 2 elements.

$$S_2 = \left\{ id, \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix} \right\}$$

Cayley's Table

o	a	b	c
a			
b			
c			

$G = \{a, b, c\}$

* $G = \{a, b, c\}$

	a	b	c
a	a	b	c
b	b		
c	c		

Also check the associativity

c	a
a	b

Scanned by CamScanner

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

In a group $aa^{-1} = e$

$a^{-1}a = e$

Statement: Inverse of a in group is unique

Let b and c are inverses of a

$ba = e = ab$

$ca = e = ac$

$b = eb$

$= (ca)b = c(ab) = c(e) = c$

* Verify:

1) There is only one group of 3 elements.
2) How many groups are there till 6 elements?

* Some statements which we have proved or easy to prove.

(1) Inverse of an element in a group is unique.

(2) Identity element of a group is unique

(3) Cancellation laws hold in a group

$ab = ac \Rightarrow b = c$; $ba = ca \Rightarrow b = c$

This property is NOT neccessary in a monoid and semigroup.

Conventions

Abelian grp $\rightarrow (G, +)$

General grp $\rightarrow (G, \cdot)$

$a \cdot b = ab$

Proof: (Left) $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

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

$\Rightarrow eb = ec$

$\Rightarrow b = c$

(Right) $ba = ca \Rightarrow b = c$

Scanned by CamScanner

Notation:

For $n \in \mathbb{N}$

$a \in G$, $a^n = \underbrace{a.a.a \dots a}_{n \text{ times}}$

$(a^{-1})^n = \underbrace{a^{-1}.a^{-1} \dots a^{-1}}_{n \text{ times}}$

$a^0 = e$

Remark:

For $a \in G$, $\{a^n \mid n \in \mathbb{Z}\} \subseteq G$

Notation:

$\{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$

Defination:

Order of a group G is $|G|$

For $a \in G$, order of a denoted by $|a|$ or $O(a)$, is the least positive (non-negative & non-zero) integer k such that $a^k = e$

If k exist $\Rightarrow$ Order is k

If k does not exist $\Rightarrow$ Order of a is infinity $[k \in \mathbb{N}]$

Eg: $|\mathbb{Z}| \longrightarrow$ Infinite group.

$|\mathbb{Z}_n| = n$, $|S_n| = \angle n = n!$

Remark:

In any group, $O(e) = 1$

Scanned by CamScanner

Eg:

For $(\mathbb{Z},+)$, $O(1) = \infty$

For $a \in \mathbb{Z} \setminus \{0\}$, Order of $a = O(a) = \infty$

Remark:

If $|G|$ is finite, $\forall\, a \in G$ $O(a)$ is finite.

Proof:

Let $a \in G$ is of infinite order

$a^k \neq e \quad \forall\, k \in \mathbb{N}$

Note that $a, a^2, \ldots \in G$

Since G is finite, $a^i = a^j$ for $i \neq j$

$\Rightarrow a^{i-j} = e$

Since $i-j \in \mathbb{N}$, it is contradiction to our assumption that $O(a) = \infty$

Note:

Non-zero elements of finite order

$(\mathbb{Q},+)$ ✗	$(\mathbb{Q}^\times,\cdot) \longrightarrow (-1)$ is of order 2
$(\mathbb{R},+)$ ✗	
$(\mathbb{C},+)$ ✗	

Subgroup:

Let G be a group (with multiplication operation) (need not be)

Let H be a non-empty subset of G

H is said to be a SUB-GROUP of G if H is also a group w.r.t the same operation of G in which case we write $H \leq G$

Scanned by CamScanner

Eg:

① $\{e\} \leq G$ ② $G \leq G$

Improper subgroups.

∴ Trivial group

③ $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ w.r.t +

④ $(\mathbb{Q}^*, \cdot) \not\leq (\mathbb{Q}, +)$ even though $\mathbb{Q}^* \subseteq \mathbb{Q}$ [Operation must be same]

Remark:

i) For $a \in G$, $\langle a \rangle \leq G$

called the Sub-Group generated by a.

ii) $k \in \mathbb{Z}$, $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\} \leq \mathbb{Z}$

→ While checking sub-group H,

Result:

Let H be a non-empty subset of G

$H \subseteq G$

$H \leq G \iff \forall a, b \in H$, $ab \in H$ and $a^{-1} \in H$

(OR) $\iff \forall a, b \in H$, $ab^{-1} \in H$

Proof:

$\Rightarrow$ is obvious

$\Leftarrow$ For $a \in H$, $a^{-1} \in H$ (by 2nd condition)

$\Rightarrow aa^{-1} \in H$ (1st condition)

$\Rightarrow e \in H$

Scanned by CamScanner

* **Result:**

Let H be an finite non-empty subset of G such that $\forall a, b \in H$, $ab \in H$ then $H \leq G$

~~HOMOM~~

→ Let $H \leq G$

Define $\sim$ (a binary relation) on G

by $a \sim b \Leftrightarrow ab^{-1} \in H$

Note that $\sim$ is an equivalence relation.
(transitive, reflexive, symmetric)

Symmetric condition check.

Suppose $a \sim b \Rightarrow ab^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H$

$b \sim a \Leftrightarrow ba^{-1} \in H$

$\Rightarrow a \sim b \Leftrightarrow b \sim a \Rightarrow$ Symmetric.

$G/\sim$ is a partition with $\sim$

$[a] = \{ b \mid ab^{-1} \in H \}$

$= \{ ha \mid h \in H \}$

$= Ha$

→ $|H| = |Ha| = |He|$

$He = H$

Note: $|[a]| = |Ha| = |H|$

Scanned by CamScanner

→ Suppose G is finite

then $|H| \mid |G| \quad \forall H \leq G$

This is LAGRANGE's THEOREM

Right Coset:

Let $H \leq G$

For $a \in G$, $Ha = \{ha \mid h \in H\}$ is called the Right coset of a w.r.t H

Left Coset:

Let $H \leq G$

For $a \in G$, $aH = \{ah \mid h \in H\}$ is called the Left coset of a

Remark:

The no. of left cosets = No. of right cosets

Prove it by establishing a bijection.

INDEX of H in G:

Let $H \leq G$, the no. of left cosets (and hence no. of right cosets) is called INDEX of H in G denoted by $[G:H]$

→ Now if $|G| < \infty$

Then $|H| \cdot [G:H] = |G|$

$\Rightarrow |H| \mid |G|$

Exercise:

For $a \in G$, $\langle a \rangle \leq G$

If $o(a) = k$, $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$ & then $|\langle a \rangle| = o(a)$

Scanned by CamScanner

Corollary:

Let G be a finite group, $O(a) \mid O(G)$ $\forall a \in G$

i.e. $o(a) \mid |G|$

---

* Proving the remark by establishing a bijection.

$Ha \longmapsto aH$

$Ha = Hb \Rightarrow aH = bH$

$\Rightarrow a \sim b$

$\Rightarrow ab^{-1} \in H$

$\Rightarrow (b^{-1})^{-1} a^{-1} \in H \Rightarrow b^{-1}H = a^{-1}H$

Here we need to have $aH = a^{-1}H$

So take $Ha \longmapsto a^{-1}H$

Then we need to have $aH = aH$ which is true.

Hence the bijection we were looking for is $Ha \to a^{-1}H$

→ $a \in G$

If $a^n = e$ then $O(a) \mid n$

HOMOMORPHISM:

Let G_1 and G_2 be two groups.

$(G_1, *_1)$ $(G_2, *_2)$

A function $f: G_1 \longrightarrow G_2$ is homomorphism if

$f(a *_1 b) = f(a) *_2 f(b)$ $\forall$ $a, b \in G_1$

- Homomorphism is talked about same type of structures.
- Operation preserving mapping.

Scanned by CamScanner

Eg: (i) On any group G,

$$id : G \longrightarrow G$$

$$id(x) = x \quad \forall\ x \in G$$

$$id(xy) = xy = id(x).id(y)$$

(ii) $f : G \longrightarrow H$

$$f(x) = e_h \quad \forall\ x \in G$$

$$f(xy) = e_h = f(x)f(y) = e_h e_h$$

- $*_1, *_2$ should same k-ary operators.

(iii) $g : \mathbb{Z} \longrightarrow \mathbb{Z}$

$$g(x) = 2x \qquad x \in \mathbb{Z}$$

$$g(m+n) = 2(m+n) = 2m+2n = g(m) + g(n)$$

$\Rightarrow$ True for all $m, n \in \mathbb{Z}$

$\Rightarrow$ Homomorphism

ISOMORPHISM:

A bijective homomorphism is called as Isomorphism.

- G_1, G_2 are isomorphic is denoted by

$$G_1 \cong G_2$$

Remark:

$\cong$ is an equivalence relation in the class of all groups.

Scanned by CamScanner

Monomorphism:

The homomorphism which is one-one is called Monomorphism.

Epimorphism:

The homomorphism which is onto is called Epimorphism.

Endomorphism:

A homomorphism from one group to itself.

Cyclic Group:

A group G is said to be cyclic if $G = \langle a \rangle$ for some $a \in G$

Eg: Group of integers w.r.t $+$

Recall,

For $a \in G$, $O(a) \mid |G|$

Consequently, if $|G|$ is prime then G is cyclic.

Proof:

~~$(e \neq a) \in$~~ $(e \neq) a \in G$

$$O(a) = |G|$$

$$\Rightarrow \langle a \rangle = G$$

Eg: $(\mathbb{Z}_p, +)$ is cyclic.

$(\mathbb{Z}_n, +)$ is cyclic $\forall n \in \mathbb{N}$

Scanned by CamScanner

Theorem:

Every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some n

Proof:

Let G be a cyclic group, say $G = \langle a \rangle$

If G is infinite $f: \mathbb{Z} \longrightarrow G$

$$f(n) = a^n \quad \forall \ n \in \mathbb{Z}$$

Note that f is a bijective (i.e one-one & onto)

and $f(m+n) = a^{m+n} = a^m . a^n$

$= f(m) \cdot f(n)$

Hence f is an isomorphism hence $G \cong \mathbb{Z}$

If G is finite, say $|G| = n$

Define $f: \mathbb{Z}_n \longrightarrow G$ by $f(\bar{k}) = a^k$

Firstly let us see well definedness

$\bar{k_1} = \bar{k_2} \Rightarrow n | k_1 - k_2 \Rightarrow a^{k_1 - k_2} = e \Rightarrow a^{k_1} = a^{k_2}$

For one-one

If $a^{k_1} = a^{k_2} \Rightarrow a^{k_1 - k_2} = e \Rightarrow n | k_1 - k_2 \Rightarrow \bar{k_1} = \bar{k_2}$

Recall
$O(a) = n$
If $a^m = e \Rightarrow n | m$

For onto,

Take any element a^k, it has a pre image

$\therefore f$ is a bijection.

For homo
$f(\bar{k}_1 +$
$\Rightarrow$ Homor
$\therefore$ Bijective

Corollary:

Any t

$\rightarrow$ Recall,
Whi
1
2
3
(4)
5
7

Scanned by CamScanner

For homomorphic,

$$f(\bar{k}_1 + \bar{k}_2) = f(\overline{k_1+k_2}) = a^{k_1+k_2} = a^{k_1} \cdot a^{k_2} = f(\bar{k}_1) \cdot f(\bar{k}_2)$$

$\Rightarrow$ Homorphism

$\therefore$ Bijective homomorphism $\Rightarrow$ Isomorphism

Corollary:

Any two cyclic groups of same order are isomorphic

→ Recall,

While drawing the cayley's table

1
2
3
(4) $\mathbb{Z}_4$ $G = \{e, a, b, c\}$
5
7

for every prime, only one non-isom-orphic group is possible.

↳ If $O(x) = 4$ then $\mathbb{Z}_4$'s isomorphic group is formed.

↓ any element

$O(G) = 4$

$\Rightarrow O(x) \mid O(G)$

$\Rightarrow O(x) = 1$ (or) 2.

$\Downarrow$

e

$\Rightarrow$ For all other non-identity elements $O(x) = 2$

$\Rightarrow$ In cayley's table, a, b, c are self invertible

Now observe ab, bc, ca

W.l.o.g take ab

- $e \Rightarrow a = b$
- $a \Rightarrow b = e$
- $b \Rightarrow a = e$
- c

} Not possible as a, b, c, e are distinct

$\Rightarrow ab = c,\ bc = a,\ ca = b$

Scanned by CamScanner

Hence cayley's table looks like

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

⇒ There are only 2 non-isomorphic groups of order 4

↳ This group is called Klein Four-group K_4

* Exercise:

Find ~~non~~ number of non-isomorphic groups of order 6, 8.

CAYLEY's THEOREM:

Every group is isomorphic to a sub-group of S_X for some X (~~set~~ permutation group).

→ To prove this let us see some results,

$f: G \longrightarrow H$ homo

$Imf = \{ a \mid \exists x \in G \text{ with } f(x) = a \} \leq H$.

Let $a, b \in Imf$

⇒ $x, y \in G$ such that $f(x) = a$, $f(y) = b$

Remark: $f(e) = e$

$f(xy^{-1}) = f(x) \cdot f(y^{-1})$

$= f(x) \cdot (f(y))^{-1} = ab^{-1}$

$\forall a, b \in Imf$ ab^{-1} has a preimage i.e $ab^{-1} \in Imf$.

⇒ Imf is ~~homomorphism~~ subgroup of H

Scanned by CamScanner

Proof:

Let G_1 be a group

Consider S_G. (S_G is a symmetric group)

Given $a \in G_1$, define $f_a : G_1 \longrightarrow G_1$

by $f_a(x) = ax$

↓

This is a bijection

well defined & one-one: $x = y \Leftrightarrow ax = ay \Leftrightarrow f_a(x) = f_a(y)$

Onto: Take any b in G_1

Then $a^{-1}b \in G_1$ such that $f_a(a^{-1}b) = a(a^{-1}b) = b$.

$\Rightarrow \forall a, f_a \in S_{G_1}$

Claim: $\psi : G_1 \longrightarrow S_{G_1}$

$\psi(a) = f(a)$

↓

Observe that this is one-one, homomorphism & well defined ness also.

(Embedded)

---

* Let $f : G_1 \longrightarrow G_2$ a homomorphism

$\ker f = \{ a \in G_1 \mid f(a) = e_2 \}$

$\ker f \leq G_1$

$\ker f \neq \phi$, as $e_1 \in \ker f$

Let $a, b \in \ker f \Rightarrow f(a) = e_2 \quad f(b) = e_2$

Scanned by CamScanner

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

$= e_2 e_2^{-1} = e_2$

$\Rightarrow ab^{-1} \in \ker f$

* Let G be a group

$Z(G) = \{ a \in G \mid ab = ba \quad \forall\, b \in G \}$

is called a CENTRE OF G.

Remark:

1) If G is abelian, $Z(G) = G$

2) $Z(G) \leq G$

$e \in Z(G) \Rightarrow$ Non empty.

$a, b \in Z(G)$ then $ab^{-1} \in Z(G)$

$ax = xa$ ↓ $bx = xb$ $\quad ab^{-1}x$

$x = b^{-1}xb$ $\quad axb^{-1}$

$xb^{-1} = b^{-1}x$ $\quad xab^{-1}$

- Remark:

Let $H \leq G$

$\{ Ha \mid a \in G \}$

$G/H = \{ Ha \mid a \in G \}$.

For $Ha, Hb \in G/H$

Define $(Ha)(Hb) = Hab$

Scanned by CamScanner

1) Well-defined

In general this is NOT well-defined

↳ For this examples will NOT be in general possible for abelian groups.

Remark:

Converse of lagrange's theorem is NOT TRUE in general.

Result:

Converse of lagrange's theorem is TRUE in case of cyclic group.

Let $G = \langle a \rangle$ of size n and $d|n$ then $\exists H \leq G$ such that $|H| = d$

Proof: $k = n/d$

$b = a^k$

Let $H = \langle b \rangle$

Claim: $|H| = d$

* Infact, such H is unique

Suppose $|H_1| = |H_2| = d$

$\langle a^k \rangle \quad \langle a^t \rangle$

$\Rightarrow k = t$

Result: Every subgroup of a cyclic group is cyclic

$H \leq G = \langle a \rangle$

If $H = \{e\}$ then we are done

Else $H \neq \{e\}$

$b = a^k \in H \rightarrow a^k \in H$

$a^{-k} \in H$

Scanned by CamScanner

Consider the set of all +ve exponents of a in H

By well ordering, let m be the least element in this set.

<u>Claim:</u> $H = \langle a^m \rangle$

$\quad\quad\quad\quad \| $

$\quad\quad\quad\quad c$

Let $x \in H$

$x = a^n$ for some n

$n = mq + r \quad 0 \leq r < m$

$\Rightarrow x = a^{mq+r} \quad \Rightarrow a^{n-mq} = a^r$

$\Rightarrow a^r = (a^n)(a^m)^{-q} \in H.$

$\Rightarrow r = 0$

$\therefore a^{mq} = a^n \quad \Rightarrow x = a^n = a^{mq} = (a^m)^q = c^q$

$H = \langle c \rangle$

$\Rightarrow H$ is cyclic

Scanned by CamScanner

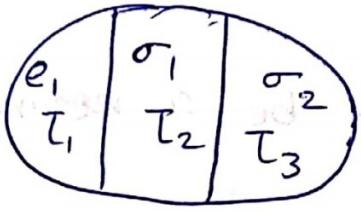
* $S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$

Consider $H = \{e, \tau_1\} \leq S_3$

$He = \{e, \tau_1\}$

$H\sigma_1 = \{\sigma_1, \tau_2\} = H\tau_2$

$H\sigma_2 = \{\sigma_2, \tau_3\} = H\tau_3$



* Eg:

Consider $n\mathbb{Z} \leq \mathbb{Z}$

Cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are

$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$

$a \sim b \iff a - b \in n\mathbb{Z}$

$\Rightarrow a \equiv b \pmod n$

So $(\mathbb{Z}/\sim, +_n)$

↳ equivalence relation

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{ab}$

$a_1 \sim a_2$

$b_1 \sim b_2$

$\Rightarrow a_1 + b_1 \sim a_2 + b_2$

* Now we want to compute $H\sigma_1, \ldots$ similar to above example.

$H_{\sigma_1\sigma_2} = He = H$

Scanned by CamScanner

$H_{\tau_2\tau_3} = H_{\sigma_1} \neq H$

Remark:

Let $H \leq G$

and G/H be the set of all right cosets of H

The operation $\cdot$ G/H defined by $H_a \cdot H_b = H_{ab}$ is not well defined in general.

NORMAL SUBGROUP:

Non-empty set H of G is said to be a normal subgroup if $xHx^{-1} \subset H \ \forall x \in G$.

In this case we write $H \trianglelefteq G$

Results:

Let $H < G$, the following are equivalent

(1) $H \trianglelefteq G$

(2) $xHx^{-1} = H \quad \forall x \in G$

(3) $Hx = xH \quad \forall x \in G$

i.e left and right cosets must be equal for every element.

(4) $H_x H_y = H_{xy} \quad \forall x, y \in G$

(1) $\Rightarrow$ (2) : For $x \in G$, $x^{-1} \in G$ so $x^{-1}Hx \subseteq H$

$H = eHe = x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$

Scanned by CamScanner

(2) $\Rightarrow$ 3 : $xHx^{-1} = H \Rightarrow xHx^{-1}x = Hx \Rightarrow xH = xH$

(3) $\Rightarrow$ (4) : $H(xH)y = H(Hx)y = (HH)(xy) = Hxy$

(4) $\Rightarrow$ (1) $\longrightarrow$ ab this

* Let G be an abelian group.
Every subgroup of G is NORMAL.

Proof:
Let $H < G$ write $[G:H] = 2$
$\Rightarrow$ There are two equivalence classes

$H, G-H = H_a \ (a \notin H)$

Scanned by CamScanner

→ For any algebraic structure, understanding the below three are important

1) Subgroups
2) Homomorphism
3) Products

→ Let G be a group

$H_1, H_2 \leq G$

(1) $H_1 \cap H_2 \leq G$

(2) $H_1 \cup H_2 \leq G$ iff $(H_1 \subseteq H_2 \;||\; H_2 \subseteq H_1)$

(3) $H_1 \cdot H_2 = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\}$

Scanned by CamScanner

$H_1 \cdot H_2 \leq G \iff H_1H_2 = H_2H_1$

For counter example of (3), take non-abelian groups.

⟶ Let G_1 ' $\circ$ and G_2 ' $*$

$$G_1 \times G_2 = \{ (a_1, a_2) \mid \begin{matrix} a_1 \in G_1 \\ a_2 \in G_2 \end{matrix} \}$$

$$(G_1 \times G_2, \dagger) = (a_1, a_2) \dagger (b_1, b_2) = (a_1 \circ b_1, a_2 * b_2)$$

↓

This is the product we are talking about.

Eg: $\mathbb{Z} \times \mathbb{Z} = \{ (a,b) \mid a, b \in \mathbb{Z} \}$

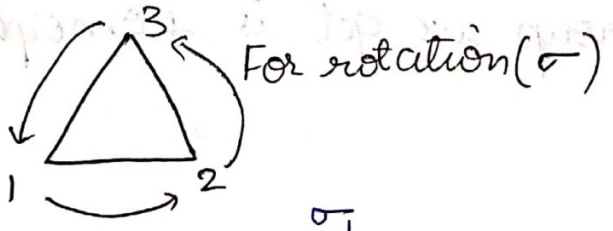
↳ Not isomorphic to $\mathbb{Z}$ because $\mathbb{Z}$ is cyclic but not $\mathbb{Z} \times \mathbb{Z}$

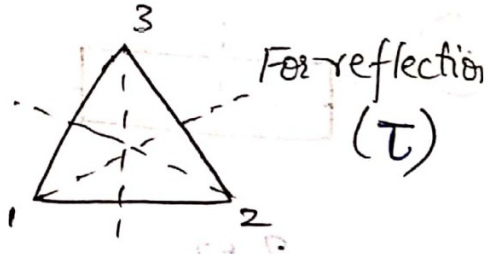
~~Symmetry~~: Symmetry:

↳ It is a bijection which preserves the distance.

$$d(x,y) = d(f(x), f(y))$$

Eg: (i) For equilateral triangle





$\sigma_0 = id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ [Rotations]

Essentially every point on each side is mapped with ~~other~~ other but we will represent just with the vertices.

$\tau_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Scanned by CamScanner

→ Analysis that above set of elements is a gro is easy geometrically and the above set is a subgroup of S_X.

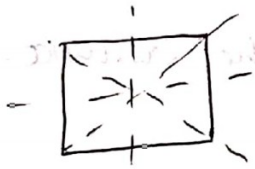
→ Eg: (i)

5+5

For a regular polygon of n sides
Size of group of symmetry
$= 2n$

If σ is a rotation
then σ^k gives all rotation
If τ is a reflection about a vertex
then $\sigma^k \tau$ gives all reflection

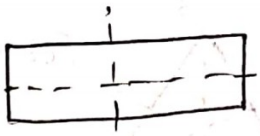
(ii)



square Similar argument shall be used

4+4

(iii)



2+2

The group we get is isomorphic to K_4

Note:

i) The group of symmetry of a regular polygon of n sides is called DIHEDRAL GROUP of degree n (D_n)

ii) Isometry is a mapping which preserves distances but there is no requirement to obtain exactly the same map.

Scanned by CamScanner

→ S_n

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 4 & 7 \end{pmatrix} = (1\ 3)(2)(4\ 5\ 6)(7)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 4 & 5 & 6 & 7 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 6 & 4 & 7 \end{pmatrix}$$

$(k) \rightarrow$ Identity

- The above representation of a transformation is called Cyclic representation i.e product of cycles.
- Every bijection can be written as product of cycles

Proof: By induction.

↳ Properly written statement would be

Every $\sigma \in S_n$ can be written as a product of cycles

- $(x, \sigma(x), \ldots, \sigma^{k-1}(x))$ where $\sigma^k(x) = x$ and k is the length of the cycle.

→ Let $\sigma = (a_1\ a_2 \ldots a_s)$

$\tau = (b_1\ b_2 \ldots b_t)$

σ and τ are DISJOINT if

$$\{a_1, \ldots, a_s\} \cap \{b_1, \ldots, b_t\} = \phi$$

Remark:

$\sigma\tau = \tau\sigma$ if τ, σ are disjoint cycles.

- Every $\sigma \in S_n$ can be written as product of Disjoint cycles and such representation is UNIQUE except that the order of the cycles and inclusion/omission of cycles of length 1.

Scanned by CamScanner

Result:

Every $\sigma \in S_n$ can be written as a product of cycles in a unique way, except that ....

Def:

A cycle of length 2 is called a Transposition.

Def:

For $\sigma \in S_n$

The cycle structure of σ is a list of numbers $n_1, n_2, \ldots$ where $n_1 \leq n_2 \leq \ldots \leq n_k$ are the lengths of the disjoint cycles $C_1, C_2, \ldots, C_k$ such that

$$\sigma = C_1 C_2 \ldots C_k \quad \left[\text{and here } \sum_{i=1}^{k} n_i = n\right]$$

Remark:

i) Given $\sigma \in S_n \longrightarrow \sigma$ gives a partition of n

Given a partition of $n \longrightarrow$ There is a $\sigma \in S_n$ whose cycle such that is the given partition.

ii) $\sigma = (a_1 \ldots a_k)$ then $\sigma^{-1} = (a_k \ldots a_1)$

Result:

If $\sigma \in S_n$ $(n \geq 2)$ is a product of r and s transpositions then both r and s are even or both of them are odd

↳ **Result:**

Every $\sigma \in S_n$ $(n \geq 2)$ can be written as a product transpositions.

$$(a_1 \ldots a_k) = (a_1\, a_k)(a_1\, a_{k-1}) \ldots (a_1 a_2)$$

Scanned by CamScanner

Def:
$\sigma \in S_n$ is said to be an EVEN PERMUTATION if σ is written as a product of even no. of transposition. Otherwise, σ is called ODD PERMUTATION.

→ For $n \geq 2$

$A_n = \{\sigma \in S_n \mid \sigma \text{ is an Even permutation}\}$

$id \in A_n \neq \phi$

Note that A_n is closed w.r.t composition and has an inverse.

Hence $A_n \leq S_n$

where A_n is the ALTERNATING GROUP.

→ **Result:**

$[S_n : A_n] = 2$ for $n \geq 2$

Hence $A_n \trianglelefteq S_n$

Proof:

Consider the group $G = \{-1, 1\}$ w.r.t multiplication

Define $f: S_n \longrightarrow G$ by $f(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{Otherwise} \end{cases}$

Note that f is an epimorphism

$\ker f = \{\sigma \in S_n \mid f(\sigma) = 1\}$

$= A_n$

$S_n / A_n \cong G$

Hence $[S_n : A_n] = 2$.

Scanned by CamScanner

Result: [FUNDAMENTAL THEOREM OF HOMOMORPHISM]

Let $f: G \longrightarrow G'$ be a homomorphism

Then $\boxed{G/\ker f \cong \operatorname{Im} f}$

If f is onto, then $G/\ker f \cong G'$

Proof: Note $\ker f \trianglelefteq G$ (K)

So consider the quotient group $G/\ker f$

$\bar{f}: G/\ker f \longrightarrow \operatorname{Im} f$

$\bar{f}(aK) = f(a)$

Well definedness & one-one of $\bar{f}$: $aK = bK \iff b^{-1}a \in K$

$\Downarrow$

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

$\Downarrow$

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

$\bar{f}(aK \cdot bK) = \bar{f}(abK) = f(ab) = f(a) \cdot f(b)$

$= \bar{f}(aK) \times \bar{f}(bK)$

$\Rightarrow \bar{f}$ is homomorphism.

Result:

Let $H, K \trianglelefteq G$ $K \subseteq H$

$(G/K)/(H/K) \cong G/H$

Proof: Define $f: G/K \longrightarrow G/H$

by $f(aK) = aH$

Scanned by CamScanner

For $a, b \in G$

$aK = bK \Rightarrow b^{-1}a \in K \Rightarrow b^{-1}a \in H \Rightarrow aH = bH$

$\Rightarrow$ Well-defined

$$f(aK * bK) = f(abK) = abH = (aH)(bH)$$
$$= f(aK) f(bK)$$

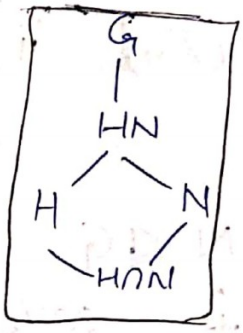
Note f is onto

$$\ker f = \{aK \mid f(aK) = H \text{ i.e } aH = H\}$$
$$= \{aK \mid a \in H\} = H/K$$

Result:

$H \leq G, \quad N \trianglelefteq G$

Then $H/H \cap N \cong HN/N$



* Let $f: G \longrightarrow G'$ is a homomorphism and onto

(i) $H \leq G \Rightarrow f(H) \leq G'$

(ii) $H' \leq G' \Rightarrow f^{-1}(H') \leq G$

↳ pre-image of H'

(iii) $H \trianglelefteq G \Rightarrow f(H) \trianglelefteq G'$

(iv) $H' \trianglelefteq G' \Rightarrow f^{-1}(H') \trianglelefteq G$

(v) $H \leq G$ containing $\ker f$ ($\ker f \subseteq H$)

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

$\mathcal{F} \quad \mathcal{G} = \{H' \mid H' \leq G'\}$.

$H \longmapsto f(H)$

↳ All subgroups of G contains $\ker f$

$\mathcal{F} = \{H < G \mid \ker f \subset H\}$

Scanned by CamScanner

* An Automorphism on G is an isomorphism from G to G $\quad Aut(G) = \{ f \mid f \text{ is auto on } G \}$

Eg: $f : G \longrightarrow G$

$f(x) = x \quad . \quad x \longmapsto a^{-1} x a$

* If $|G| = n$, $|Aut(G)| \leq n!$

→ For any group G, $Aut(G)$ is a group.

and infact $Aut(G) \leq S_G$

Exercises

i) $Aut(\mathbb{Z}_n)$ ii) $Aut(\mathbb{Z})$ (iii) $Aut(S_3)$

Def:

Let $N \trianglelefteq G$

N is called a Maximal normal subgroup of G if (i) $N \neq G$

(ii) $H \trianglelefteq G$ and $N \subseteq H$

$\Rightarrow N = H$ or $H = G$ ...

Def:

A group G is said to be SIMPLE if G has no proper normal subgroup.

Eg: For $\mathbb{Z}$ [Fo Maximal Normal subgroup]

$4\mathbb{Z} \leq \mathbb{Z}$

$2\mathbb{Z} \leq \mathbb{Z}$

↳ maximal

For prime p, $p\mathbb{Z} \leq \mathbb{Z}$ → maximal

Scanned by CamScanner

* S_3 is simple? (No, due to $\{e, \sigma_1, \sigma_2\}$)

Result:

For $n>4$, A_n is SIMPLE.

A_4 is not a SIMPLE (A_4 has a normal subgroup of order 4)
↳ also helps to contradict converse of Lagrange's Theorem.

Result:

For $n>4$, A_n is the only non-trivial normal subgroup of S_n

Eg: $A_4 = \{ e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)$
$(1\,2\,3), (1\,3\,4), (1\,2\,4), (2\,3\,4)$
$(1\,3\,2), (1\,4\,3), (1\,4\,2), (2\,4\,3)\}$

Exercise:

1) Every finite group is isomorphic to A_n for some n.

Generating Set:

Let G be a group and $X \subseteq G$

$$\langle X \rangle = \{ x_{i_1} x_{i_2} \cdots x_{i_k} \mid x_{i_j} \text{ or } x_{i_j}^{-1} \in X, \; k \geq 0 \}$$

Remark:

(i) If $X = \phi$, $\langle X \rangle = \{e\}$

(ii) For $X \subseteq G$, $\langle X \rangle \leq G$

$\langle X \rangle$ is called the "SUBGROUP generated by X".

Scanned by CamScanner

Result:

For $(\phi \neq) X \subseteq G$

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

Hence, $\langle X \rangle$ is the smallest subgroup containing X.

Def:

A group G is said to generated by $X \subseteq G$ if $\langle X \rangle = G$

Further if,

$$|X| < \infty$$

then we say G is finitely generated.

Remark:

Every finite groups is finitely generated.

Exercise:

(i) A_n can be generated by the set of 3-cycles on S_n

$$X = \{ 3\text{-cycles} \}$$

Eg: $(a\,b)(c\,d) = (a\,b\,c)(b\,c\,d)$

(ii) S_n is generated by $(1\ 2 \ldots n-1)$ and $(n-1\ \ n)$

$\longrightarrow$ D_n is generated by σ, τ

Extra

* Presentation of group

$$\langle a_1, \ldots, a_k \mid \text{Relators (Relations that relate the elements)} \rangle$$

$$\langle X \mid \text{Relators} \rangle$$

Scanned by CamScanner

Result:

Let $H_1, \ldots, H_n \leq G$ and $H = H_1 H_2 \cdots H_n$

Then the following statements are equivalent

1) If $H_1 \times \cdots \times H_n \cong H$ under the canonical map.

$(x_1, x_2, \ldots, x_n) \longmapsto x_1 x_2 \cdots x_n$

2) $H_i \trianglelefteq H$ and any element in H can be uniquely written as $x_1 x_2 \cdots x_n$ for $x_i \in H_i$;

Scanned by CamScanner

RING

$(R, +, \cdot)$

Eg: $(\mathbb{Z}, +, \cdot)$

$n \in \mathbb{N}$ $(\mathbb{Z}_n, +_n, \cdot_n)$

→ Let R be an arbitrary ring

$R[x]$ ⟶ Set of all polynomials with coefficients from R in variable x

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$q(x) = b_0 + b_1 x + \cdots + b_n x^n$$

$$p(x) + q(x) = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i$$

$p(x) \cdot q(x)$

Now observe that

$(R[x], +, \cdot)$ is a RING.

Notation: $a + (-b) = a - b$

→ If R is ring with unity

$(-1)a = -a$

→ $n \in \mathbb{N}$ $(M_n(R), +, \cdot)$ is also a RING

Subring:

Let R be a ring

A non-empty subset S of R is a subring if S is a ring w.r.t the operation of R

In a ring R

i) $a0 = 0a = 0$

$0 + a0 = a0 = a(0+0)$
$= a0 + a0$

$\Rightarrow a0 = 0$

ii) $a(-b) = (-a)b$
$= -ab$

$a(-b) + ab$
$= a(-b+b)$
$= a0 = 0$

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

Scanned by CamScanner

→ $(\phi \neq S) \subseteq R$ is a subring of R

$\Leftrightarrow a-b \in S$ $\quad \forall a,b \in S$

$ab \in S$

Eg: (i) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

(ii) $n\mathbb{Z} \leq \mathbb{Z}$

→ Let $S \subseteq R$ $\quad (S,+) \leq (R,+)$

$R/S = \{r+S \mid r \in R\}$

$(r_1+S)+(r_2+S) = (r_1+r_2)+S$ because $(S,+) \trianglelefteq (R,+)$

$(r_1+S)\cdot(r_2+S) = r_1r_2+S$ → Not ~~in general~~, well defined in general

Ideal:

A subring I of R is said to be an Ideal of R if $\forall a \in I$ and $r \in R$, $ar \in I$ and $ra \in I$

Eg: (i) $\mathbb{Z} \leq \mathbb{R}$ but not an ideal

(ii) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$

Exercise:

$S \trianglelefteq R \Leftrightarrow (r_1+S)\cdot(r_2+S) = r_1r_2+S \quad \forall r_1, r_2 \in R$ is well-defined.

$\Rightarrow$: Consider $(r_1+S)(r_2+S) = r_1r_2 + r_1S + Sr_2 + S$

$= r_1r_2 + S+S+S$

$= r_1r_2+S$

$\Leftarrow$: $(r_1+S)\cdot(r_2+S) = r_1r_2+S$

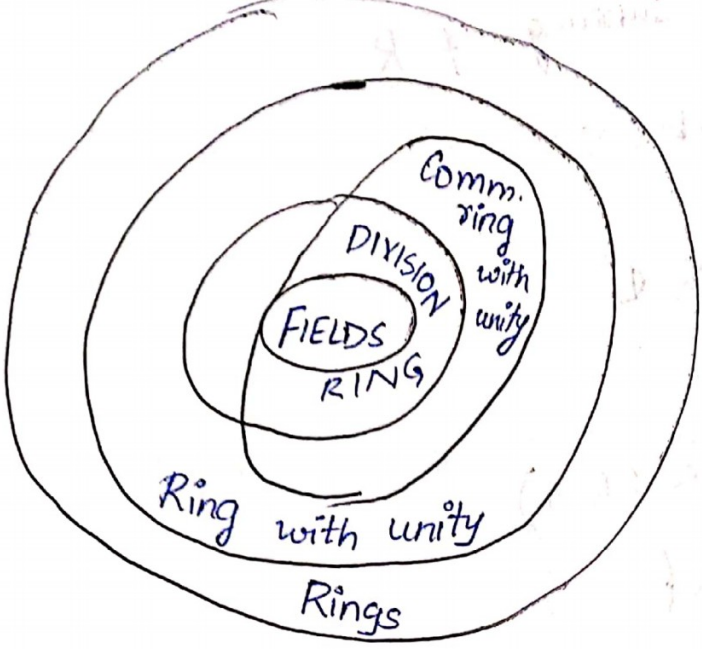
$\Rightarrow r_1r_2 + r_1S + Sr_2 + S = r_1r_2 + S$

$\Rightarrow r_1S + Sr_2 + S = S \Rightarrow r_1S \in S, Sr_2 \in S$

$\Rightarrow S \trianglelefteq R$

Scanned by CamScanner

*



* If I is an ideal of R i.e $I \trianglelefteq R \Leftrightarrow (r+I)(s+I) = rs+I$

then $(R/I, +, \cdot)$ is the Quotient Ring.

Eg: $n\mathbb{Z} \trianglelefteq \mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ is essentially the ring $\mathbb{Z}_n$

→ If $1 \in R$ then R/I also have a unity

If R is commutative then R/I is also commutative

→ $\{0\}$ and R are the only ideals in a field R

Proof:

Let $I \trianglelefteq R$ and $I \neq \{0\}$

Let $a \in I$ $(\neq 0)$

$a^{-1} \in R \Rightarrow a^{-1}a = 1 \in R$

⇒ By defination of ideal, $I = R$

Scanned by CamScanner

* Let $a \in R$

$\langle a \rangle$: Ideal generated by a

$\langle a \rangle$: Smallest ideal ~~gene~~ containing singleton a

Conventionally,

If $n > 0$ $\quad na = \underbrace{a + a + \dots + a}_{n \text{ times}}$

If $n = 0$, $na = 0$

If $n < 0$, $\quad na = \underbrace{(-a) + (-a) + \dots + (-a)}_{n \text{ times}}$

* $\langle a \rangle = \{ na \mid n \in \mathbb{Z}$

~~an $n \in \mathbb{N}$~~ → Redundant as it is a part of ra, ar.

$ra \quad r \in R$ }

$ar \quad r \in R$ }

* If R is ring with unity

denote unity with 1

$1 \in R$

$2 = 1 + 1 \in R$

$\vdots$

$n = 1 + 1 + \dots + 1 \in R$

So we are viewing (it may not be true) $\mathbb{Z} \subset R$

For more correct statement see ~~a~~ after 2 pages.

then $\langle a \rangle = \left\{ \begin{matrix} ra \\ ar \end{matrix} \mid r \in R \right\}$

If R is commutative ring with unity

$\langle a \rangle = \{ ra \mid r \in R \}$

PRINCIPAL IDEAL generated by a.

Scanned by CamScanner

* If R is a comm. ring with unity

$$\langle a, b \rangle = \{ r_1 a + r_2 b \mid r_1, r_2 \in R \}$$

* Let R be a comm. ring with unity

Prime Ideal:

A proper ideal I of R is said to be a prime ideal if $a, b \in R$ with $ab \in I$ then $a \in I$ or $b \in I$

Maximal Ideal:

A proper ideal I of R is said to be maximal if for any ideal J of R with $I \subseteq J \Rightarrow J = I$ (or) $J = R$

Eg:

(i) $\mathbb{Z}$; $\langle n \rangle$ is a prime ideal $\Leftrightarrow$ n is a prime number.

If n is prime then $\langle n \rangle$ is a maximal ideal.

Exercise:

Observe in $\mathbb{Z}[x]$, $\langle x \rangle$ is prime ideal but not maximal ideal.

Integral Domains (ID):

A commutative ring with unity is called an Integral Domain (ID) if it has no non-zero zero-divisors

→ $(\neq) a \in R$ is called a zero divisor if there is a $b \neq 0$ such that $ab = 0$

Alternatively,

$\forall a, b \in R$ if $ab = 0$ then $a = 0$ or $b = 0$

Eg: i) $(\mathbb{Z}, +, \cdot) \rightarrow$ ID ii) $\mathbb{Z}_n$ is ID $\Leftrightarrow$ n is prime

Scanned by CamScanner

→ Every field is an ID
For integral domains

Eg: $\mathbb{Z}$, $\mathbb{Z}_n$

The ring of gaussian integers $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$

Matrix ring; for $n=1$ & for real numbers

→ Characteristic of a ring R is a least positive integer n such that $na = 0 \quad \forall a \in R$ and denoted by $\text{Char}R$

↳ If such 'n' does not exist then $\text{Char}R = 0$

Eg: $\text{Char}\,\mathbb{Z}_n = n$

- In a ring with unity R

$$\text{Char } R = \begin{cases} O(1) \text{ under addition if it is finite} \\ \quad \hookrightarrow \text{Order of } 1 \\ 0 \end{cases}$$

Proof:

If order of 1 i.e $O(1)$ under addition is NOT finite then clearly $\text{char}R = 0$ bcoz $n1 \neq 0 \ \forall n$

Else suppose $O(1) = n \Rightarrow n \cdot 1 = 0$

Then $na = \underbrace{a+a+\dots+a}_{n \text{ times}}$

$= 1\cdot a + 1\cdot a + \dots + 1\cdot a$

$= (1+1+1+\dots+1)a = (n\cdot 1)a = 0a = 0$

and this 'n' is least.

* Char of Integral Domain R is 0 or prime

Proof: Suppose $\text{char}R \neq 0$

Then let $O(1) = n$

Suppose $n = rs \quad 1 \leq r, s \leq n$

Scanned by CamScanner

We know $n1 = 0$ → 'n' is NOT an element of ID

$\Rightarrow (rs)1 = 0$

$\Rightarrow (r1)(s1) = 0$

$\Rightarrow r1 = 0$ (or) $s1 = 0$

i.e $r = n$ (or) $s = n$ are 'n' is least

$\Rightarrow$ 'n' is prime.

** If R is a ring with unity,

if $charR = 0$ then $\mathbb{Z} \longrightarrow R$ } one-one.

if $charR = n$ then $\mathbb{Z}_n \longrightarrow R$ }

Core: Char (field) is either prime or '0'.

→ Let R be a commutative ring with unity and $I \trianglelefteq R$

R/I is an integral domain $\iff$ I is prime ideal

Proof:

$\Rightarrow$: $ab \in I$

'0' in R/I is I

~~If $(a+I)(b+I) = I$~~

$ab + I = I$ because $ab \in I$

$\Rightarrow (a+I)(b+I) = I$

$\Rightarrow a+I = I$ (or) $b+I = I$

$\Rightarrow a \in I$ (or) $b \in I$

$\therefore$ I is prime ideal

$\Leftarrow$: $(a+I)(b+I) = I$

~~$\Rightarrow (a+I) \in I$ (or) $b+I \in I$~~ $\Rightarrow ab + I = I$

Scanned by CamScanner

$\Rightarrow ab \in I$

$\Rightarrow a \in I$ or $b \in I$ since I is prime ideal

$\Rightarrow$ R/I is integral domain.

Result: R/I is a field $\Leftrightarrow$ I is maximal

Coro: For any commutative ring with unity, every maximal idial is prime

Proof:

$\Rightarrow$: Let J be an ideal of R s.t $I \subsetneq J$

Let $a \in J \setminus I$

then $a+I \neq I$

i.e $a+I$ is a non-zero element of R/I

Since, R/I is a field, $\exists$ $b+I$ s.t $(a+I)(b+I) = 1+I$

$\Rightarrow ab+I = 1+I$

$\Rightarrow (1-ab)+I = I \Rightarrow (1-ab) \in I$

$\Rightarrow (1-ab) \in J$

As $a \in J \Rightarrow ab \in J$

$\therefore (1-ab)+ab \in J \Rightarrow 1 \in I$

For any $x \in R$, x can be seen as $1 \cdot x$

As $1 \in J \Rightarrow 1 \cdot x \in J \Rightarrow J = R$

$\therefore J = R$

Hence, I is maximal.

$\Leftarrow$: Try this as an exercise.

Scanned by CamScanner

Homomorphisms:

A mapping from Ring R to Ring S is said to be homomorphism

$$f: R \longrightarrow S$$

$$f(a+b) = f(a) + f(b)$$

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

$\rightarrow f(0) = 0$

$\rightarrow f(-a) = -f(a)$

$\rightarrow f(R) \leq S$

If f is ONTO,

① $A \leq R \Rightarrow f(A) \leq S$; ③ $R/\ker f \cong S$

② $A \trianglelefteq R \Rightarrow f(A) \trianglelefteq S$; ④ $R/I \cong (R/J)/(I/J)$, $I, J \trianglelefteq R$ and $J \subseteq I$

$\rightarrow \ker f = \{ x \in R \mid f(x) = 0 \}$

Center of $R = Z(R) = \{ x \in R \mid ax = xa \ \forall a \in R \}$

$\rightarrow$ Some examples of rings

Let $X \neq \phi$

$$R = \{ f \mid f: X \longrightarrow \mathbb{R} \text{ a function} \}$$

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

$(fg)(x) = f(x) \cdot g(x)$

If second operation is composition rather than multiplication then $f(g+h)(x) = f(g(x) + h(x))$

↳ This distributivity must be satisfied

Scanned by CamScanner

But it is ~~[illegible]~~ in general NOT satisfied

If f is homomorphism, then it is satisfied
↳ under $+$

→ $(g+h)f(x) = (g+h)(f(x)) = g(f(x)) + h(f(x))$

→ Let $(G,+)$ be an abelian group

$R = Hom(G,G) = End(G)$ ring

Then $(R,+,\circ)$ is
↳ composition

→ Any ring can be embedded in a endomorphisms ring of a abelian group.

$R \longrightarrow End(A)$ ~~[illegible]~~

Natural choice for A is $R(+)$

$r \to f_r$ $\quad f_r(a) = a+r \longrightarrow$ Not satisfied

so take $f_r(a) = ra$

→ $(\mathcal{P}(X),+,\cdot)$ → It is a ring

if $A+B = (A \cup B) - (A \cap B)$

$AB = A \cap B$

Boolean ring → A ring $(R,+,\cdot)$ is said to be a Boolean ring if $a^2 = a \quad \forall\, a \in R$

Ex: In a boolean ring $2a = 0 \quad \forall\, a \in A$

i.e $char R = 2$

Scanned by CamScanner

* $(\mathbb{Z}, +, \cdot)$ ring

$f: \mathbb{Z} \longrightarrow \mathbb{Z}$

$f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$

i.e $f(1) = 0$ or $f(1) = 1$

$\Downarrow$ $\Downarrow$

$f(n) = 0$ $f(n) = n$

* $f: R \longrightarrow S$

$\ker f = \{0\} \iff f$ is 1-1.

→ Let R be an integral domain. There exists a field F (called a field of Quotients) over R such that R can be seen as a subring of F

Proof:

$$S = \{(a,b) \mid a,b \in R,\ b \neq 0\}$$

Define $\equiv$ on S by $(a,b) \equiv (c,d)$ iff $ad - bc = 0$

Note that $\equiv$ is equivalence relation on S.

$F = S/\equiv = \left\{ \frac{a}{b} \mid b \neq 0 \right\}$ $\frac{a}{b}$ → representation of (a,b)

Define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

↓

As $b \neq 0, d \neq 0$ and also R is ID

so $bd \neq 0$

$(F, +, \cdot)$ is a field.

$f: R \longrightarrow F$ by $f(a) = \frac{a}{1}$

Scanned by CamScanner

i.e every integral domain can be embedded into a field

Scanned by CamScanner

Def:

An integral domain is called a Principal Ideal domain (PID) if every ideal in it is a principal ideals.

Eg: ① $\mathbb{Z}$ is a PID

② $F[x]$ is a PID, where F is a field.

→ $\mathbb{Z}[x]$ is not a PID, for instance $\langle x, 2 \rangle$ is not a principal ideal.

- Division algorithm in $F[x]$, for a field F

Let $f(x), g(x) (\neq 0) \in F[x]$. Then there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

Scanned by CamScanner

Cor 1 (Remainder Theorem):

Let $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x-a$

$$f(x) = (x-a)q(x) + r(x)$$

Cor 2 (Factor Theorem):

$a \in F$ and $f(x) \in F[x]$

Then a is zero of $f(x) \iff x-a$ is the factor of $f(x)$

Cor 3:

A polynomial of degree n over a field has atmost n zeroes counting multiplicity

Exercise:

For $x^2+3x+2 \in \mathbb{Z}_6[x]$

Note $x = 1, 2, 4, 5$ are zeroes.

→ $F[x]/I$ gives us a field if I is maximal and this is a way to generate fields.

$\mathbb{Z}_p$: is a field & $F[x]$ is a field.

→ $F[x]/I$ if I is maximal, it is a field

Eg: $\mathbb{R}[x]$, $I = \langle x^2+1 \rangle$

$\phi(x) : \mathbb{R}[x] \longrightarrow \mathbb{C}$

$\phi(f(x)) = f(i)$

$a+bx \longmapsto a+ib$ onto

It is homomorphism

$\mathbb{R}[x]/\ker\phi \cong \mathbb{C}$

Scanned by CamScanner

$\ker \phi$ = polynomials with root 'i'

deg 1 ⟶ no polynomial

deg 2 ⟶ x^2+1 ⟵ generator for this degree

I is generated by $f(x)$ ⟵ min degree in I

$\ker \phi = \langle x^2+1 \rangle$

- Criterion on $f(x)$ such that $\langle f(x) \rangle$ is maximal in $F[x]$ is $f(x)$ is IRREDUCIBLE polynomial.

→ Let R be an integral domain

A non-zero non unit polynomial $f(x) \in R[x]$ is said to be irreducible over R whenever $f(x) = g(x).h(x)$ for $g(x), h(x) \in R[x]$ then $g(x)$ or $h(x)$ is a unit in $R[x]$

- On the other hand, $f(x)$ is called Reducible if it is NOT irreducible.

Eg: i) $f(x) = 2x^2+4 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$

ii) $f(x) = 2x^2+4 \in \mathbb{Z}[x]$

$= 2(x^2+2)$

is reducible over $\mathbb{Z}$ because '2' is NOT unit in $\mathbb{Z}$

iii) $x^2+1 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}, \mathbb{R}$

$\in \mathbb{R}[x]$

Scanned by CamScanner

Let F be a field and $p(x) \in F[x]$

$\langle p(x) \rangle$ is maximal in $F[x] \Leftrightarrow p(x)$ is irreducible over F

Proof:

$\Rightarrow$: Suppose $p(x) = g(x) \cdot h(x)$ for some $g(x), h(x) \in F[x]$.

$\Rightarrow \langle p(x) \rangle \subseteq \langle g(x) \rangle$

Since $\langle p(x) \rangle$ is maximal $\Rightarrow \langle p(x) \rangle = \langle g(x) \rangle$ or $\langle g(x) \rangle = F[x]$

$\langle p(x) \rangle = \langle g(x) \rangle \Rightarrow h(x)$ is unit $\Rightarrow p(x)$ is irreducible

(or)

$\langle g(x) \rangle = F[x] \Rightarrow g(x)$ is unit $\Rightarrow p(x)$ is irreducible

$\Leftarrow$: Let $\langle p(x) \rangle \subseteq J \subseteq F[x]$, $J = \langle q(x) \rangle$, say ($\because$ principal ideal)

$p(x) = q(x) \cdot t(x)$

~~if q(x)~~ $p(x)$ is irr

So if $q(x)$ is unit $\Rightarrow J = F[x] \Rightarrow \langle p(x) \rangle$ is maximal

if $t(x)$ is unit $\Rightarrow p(x) = q(x) \Rightarrow \langle p(x) \rangle$ is maximal

→ Exercise: $f(x) \in F[x]$ of degree 2 or 3 is irreducible over $F \Leftrightarrow f(x)$ has a root in F.

Scanned by CamScanner

One class in between

Def:

Let $f(x) \in F[x]$ be a non-constant polynomial and E an extension of F. We say $f(x)$ splits in E if there exist $a_1, a_2, \ldots, a_n \in E$ and $a \in F$ such that

$$f(x) = a(x-a_1)\cdots(x-a_n)$$

- The ~~Spl~~ Splitting field of $f(x)$ over F is $F(a_1, \ldots, a_n)$

Result:

$f(x) \in F[x]$
↳ non-constant
there exists a splitting field of $f(x)$ over F

Proof: By induction on degree on $f(x)$

If $f(x)$ is of degree 1 $\longrightarrow$ It is true

Assume the result is true for all fields and polynomials of degree < degree $f(x)$

By fundamental theorem of field theory, there is an extension E of F which has a zero, say a_1, of $f(x)$

$$f(x) = (x-a_1)g(x) \text{ where } g(x) \in E[x]$$
$$\deg g(x) < \deg f(x)$$

By induction hypothesis, there is a splitting field K of E contains all zero, say $a_2, a_3, \ldots a_n$ of $g(x)$

Scanned by CamScanner

Eg: (i) $x^2+1 \in \mathbb{Q}[x]$

$\mathbb{Q}(i) = \{ a+bi \mid a,b \in \mathbb{Q} \}$

(ii) $(x^2+1)(x^2-2) \in \mathbb{Q}[x]$

$\mathbb{Q}(i,\sqrt{2}) = \mathbb{Q}(i)(\sqrt{2}) = \{ \alpha+\beta\sqrt{2} \mid \alpha,\beta \in \mathbb{Q}(i) \}$

$= \{ (a+bi)+(c+di)\sqrt{2} \mid a,b,c,d \in \mathbb{Q} \}$

Remark:
$\mathbb{Q}[x]$ → Ring theory notation
$\mathbb{Q}(x)$ → field theory notation

Def:
Let E be an extension of F. Then the degree of E over F denoted by $[E:F]$ is the dimension of E (as vector space) over F.

→ If $[E:F]$ is finite, then we call E is a finite extension of F, otherwise E is an infinite extension of F

- $[\mathbb{C}:\mathbb{R}] = 2$
- $[\mathbb{C}:\mathbb{Q}]$ infinite → John's lemma.

Eg: $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}] = 4$

Result:
Let $p(x)$ be an irreducible polynomial over F. If a is a zero of $p(x)$ in some extension E of F then this $F(a)$ is isomorphic to $F[x]/\langle p(x) \rangle$

$F[x]/\langle p(x) \rangle = \{ f(x) + \langle p(x) \rangle \mid f(x) \in F[x] \}$

$= \{ r(x) + \langle p(x) \rangle \mid \deg r(x) < \deg p(x) \}$

Let $r(x), s(x) \in F[x]$
with $\deg r(x) < \deg p(x)$
$\deg s(x) < \deg p(x)$

and $r(x) + \langle p(x) \rangle = s(x) + \langle p(x) \rangle$
$\Rightarrow r(x) = s(x)$

Scanned by CamScanner

Furthermore, if $\deg p(x) = n$, then every element of $F(a)$ can be uniquely written as $c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}$ where $c_0, c_1, c_2, \ldots, c_{n-1} \in F$

Proof:

Define $\varphi : F[x] \longrightarrow F(a)$ by

$$\varphi(f(x)) = f(a)$$

Observe that this(φ) is a homomorphism

$$\ker\varphi = \{ f(x) \mid f(a) = 0 \}$$

Note that $p(x) \in \ker\varphi \Rightarrow \langle p(x) \rangle \subseteq \ker\varphi$

$p(x)$ is irreducible $\Rightarrow \langle p(x) \rangle$ is maximal

Since $\ker\varphi \neq F[x]$ ~~so~~ $\langle p(x) \rangle = \ker\varphi$,

Note, φ is ONTO

By fundamental theorem of field theorem,

$$F[x]/\ker\varphi \cong F(a)$$

Remark:

~~If~~ $[F(a) : F] = \deg p(x)$

Eg: (1) $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$

$\{ 2^{1/6}, \alpha, \alpha^2, \ldots, \alpha^5 \}$

Corollary:

If 'a' is a zero of $p(x)$ in some extension E

If 'b' is a zero of $p(x)$ in some extension E'

Then $F(a) \cong F(b)$

Scanned by CamScanner

Result (uniqueness):

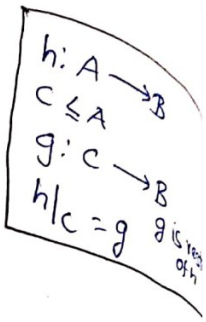
Let $f(x) \in F[x]$. Any two splitting fields of $f(x)$ over F are isomorphic.

In fact, let $\phi : F \cong F'$ and $f(x) \in F[x]$

If E is a splitting field of $f(x)$ over F

E' is a splitting field of $f(x)$ over F'

then there is isomorphism $\psi : E \longrightarrow E'$ which is an extension of ϕ



Def:

Let E be an extension of F and $a \in E$.

We call "a" is algebraic over F if a is a zero of some non-zero polynomial over F.

→ If every element of E is algebraic over F then E is algebraic over F.

- If a is NOT algebraic, then it is called TRANSCENDENTAL one

→ Let us denote the field of quotients over $F[x]$

$$F[x] = \left\{ f(x)/g(x) \;\middle|\; f(x), g(x) \in F[x],\ g(x) \neq 0 \right\}$$

Remark:

If a is transcendental over F, $F(a) \cong F[x]$

Proof: Define $\varphi : F[x] \longrightarrow F[a]$

$$\varphi(f(x)) = f(a)$$

$$\overline{\varphi} : F(x)$$

$$\overline{\varphi}\left(f(x)/g(x)\right) = f(a)/g(a)$$

- If a is algebraic then $F(a) \cong F[x]/\langle p(x) \rangle$

where $p(x)$ is a polynomial in $F[x]$ of min. degree s.t $p(a)=0$, Moreover $p(x)$ is irreducible.

→ Infact, there is unique monic irreducible polynomial $p(x) \in$ such that $p(a)=0$

Def: Minimal polynomial of a over F.

Scanned by CamScanner

- **Result:**

If $[E:F]=n$ then E is algebraic over F.

Proof:

$a \in E$, $[F(a):F] \to m$ is finite

$1, a, a^2, \ldots, a^{m-1}$

Is a algebraic extension finite ? ⟶ No

$\mathbb{Q}(A) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots)$ $\quad A = \{\sqrt[n]{2}, n \in \mathbb{N}\}$

Result:

For each prime p and $n \in \mathbb{N}$ then there is a unique field (upto isomorphism) of order p^n.

$GF(p^n)$ called Galois field of order p^n

Result:

As a group under addition, $GF(p^n) = \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p}_{\text{'n' times}}$

As a group under multiplication, $GF(p^n)^* \cong \mathbb{Z}_{p^n-1}$

and hence $GF(p^n)$ is cyclic

Scanned by CamScanner