MA 222

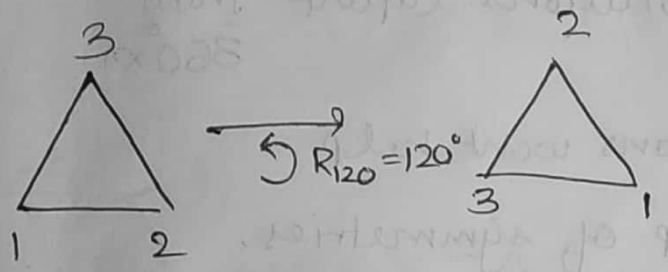
Let $X \subseteq \mathbb{R}^2$ (plane)

Symmetries on X (basically a bijection that gives the same group).

Isometry $\leftrightarrow$ distance preserving map

$f: \mathbb{R}^2 \to \mathbb{R}^2$

$d(x,y) = d(f(x), f(y)) \quad \forall \ (x,y) \in \mathbb{R}^2$



$R_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ order 1

$R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ order 3

$R_{240} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ order 3

take any convention (clockwise or anti to be +ve)

R ⇒ rotation

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ Order 2

$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ Order 2

$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ order 2

(f ⇒ reflection)

If $f: X \to X$ is a symmetry for X, the triangle

then, $f \in S_X$.

$S_3 \leq S_X$.

Above group is essentially isomorphic to S_3.

It is called Group of Symmetries (f's).

(not to be confused with symmetric group)

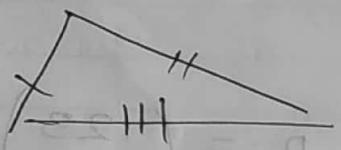
Note:

All the functions can be written of the form $\sigma^k z$.

Group of symmetries are generally not isomorphic to Symmetric groups.

(for S_3, it is true, $S_4, \ldots$ not true)

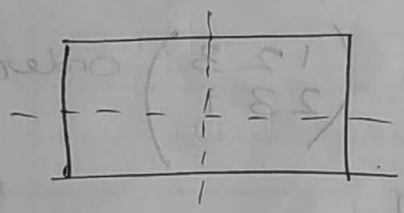
For Scalene Δ,



Rotations (apart from $360° \times n$)

Reflections wont help.

So, $\{e\} \rightarrow$ Group of symmetries.

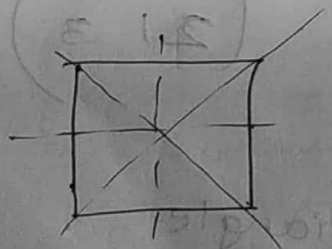


180° rotations

2 + 2 reflections = 4

$\cong K_4$ group.

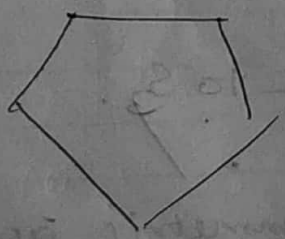
(every one has order 2)



4 reflections + 4 rotations

(8) ✓

For an n-sided polygon,



The group of symmetries of a regular polygon with n sides forms a dihedral group (D_n) of degree n and order 2n.

Proof is simple $|D_n| = 2n$

(visualize for even, and odd)

Ex-1

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 4 & 6 & 7 & 8 & 2 \end{pmatrix} = \sigma$$

$1 \to 3 \to 5 \to 6 \to 7 \to 8 \to 2 \to 1$

$\sigma = (1\,3\,5\,6\,7\,8\,2)\,(4)$

Ex-2

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 3 & 1 & 6 & 7 \end{pmatrix} = \sigma_1$$

identity mapping

$$(125)(34)(6)(7) = \sigma_1$$

Basically, $(a\ \sigma a\ \sigma^2 a\ \sigma^3 a \cdots \sigma^{k-1} a)$

$\sigma^k a = a$

$(a_1, a_2, a_3, \ldots a_k)$

then, $\sigma(b) = b \quad \forall b \in X - \{a_1, a_2, \ldots a_k\}$

ex: $(125) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 1 & 6 & 7 \\ & & id & & & id & \end{pmatrix}$

Basically for $(125)(34)$, we can treat it as a composition/product of cycles.

$\left\{\right.$ 1 - goes to 1 in $(3,4)$
goes to 2 in (125)

- Thus, composition: $1 \to 2$

$3 \to 4$ in $(3,4)$ & $4 \to 4$ in $(125) \Rightarrow 3 \to 4$ overall

and so on for the rest -

$\sigma = (a_1\ a_2 \dots\ a_r)$
$\tau = (b_1\ b_2 \dots\ b_k)$ are said to be disjoint
if $\{a_1, a_2, \dots a_r\} \cap \{b_1, b_2, \dots b_k\} = \emptyset$

Remark

If σ and τ are disjoint cycles,

* $\sigma\tau = \tau\sigma$

length 1 cycle → identity map

Result

Every σ in S_n (finiten) can be written as a product of disjoint cycles.

* Proof using Induction

(Assume for S_k)

$\sigma = (x\ \sigma x\ \sigma x^2 \dots\ \sigma^k x)$

$\sigma_1 = \{a_1, a_2, \dots, a_{k+1}\}$

~~$\sigma = \sigma_1 (\sigma) \sigma$ the~~

However, the rep is unique except that inclusion of all cycles of length 1 and order in which we write the cycles.

$\sigma \in S_n$

$\sigma = \sigma_1 \sigma_2 \sigma_3 \sigma_4 \ldots \sigma_k$

where $\sigma_1, \sigma_2, \sigma_3 \ldots \sigma_k$ are cycles including those of length 1.

Let $n_1, n_2, n_3 \ldots n_k$ be the lengths of $\sigma_1, \sigma_2, \sigma_k$ and $n_1 \leq n_2 \leq n_3 \ldots \leq n_k$,

$$\sum_{i=1}^{k} n_i = n$$

We call $(n_1, n_2, n_3 \ldots n_k)$ cycle structure of σ. Conversely given a partition of n, say $m_1, m_2, \ldots m_r$, there exists $\tau \in S_n$ such that $(m_1, m_2, \ldots m_r)$ is a cycle structure of τ.

Ex: → given $n=6$,

$6 = 1+1+2+2$.

$\tau = (1)(2)(34)(56)$

Excercise

Determine the equivalence classes w.r.t. cycle structure.

$\rho \to \tau \sigma \tau^{-1}$ Conjugate Bijections form equivalence

α - a permutation of S_n that has c cycles in its cycle
τ - a transposition of S_n

No. of cycles in $\tau\alpha$ or $\alpha\tau$ is either $c+1$ or $c-1$.

elements of τ in same cycle. | elements of τ in diff. cycle

Remark:

Every $\sigma \in S_n$ can be written as a product of transpositions - cycles of length 2.

Eg: $(12)(21) = \text{identity}$ | $(a_1, a_2, \ldots a_k)$

they are not disjoint

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

Result:

If $\sigma \in S_n$ is written as product of r and s no. of transpositions, then both r and s are either even or odd.

(Try proving it) ★ Refer to pdf

$\sigma \in S_n$ is said to be even permutation if it is a product of even no. of transpositions. Otherwise we call it odd permutation.

For $n \geq 2$, $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$

$\text{id} \in A_n \neq \emptyset$

$\sigma, \tau \in A_n$

$\Rightarrow \sigma\tau \in A_n$

Also, $\sigma^{-1} \in A_n$

$\sigma^{-1} = (\sigma_1 \sigma_2)^{-1}$

$= \sigma_2^{-1} \sigma_1^{-1}$

Excercise

$(a_1 a_2 \ldots a_k)^{-1}$

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

$A_n \leq S_n$

A_n is called an alternating group of degree n.

Result:

For $n \geq 2$, $[S_n : A_n] = 2$

Hence, $A_n \trianglelefteq S_n$ and $|A_n| = \frac{n!}{2}$

Proof, Consider $G_1 = \{1, -1\}$ w.r.t. multiplication.

Define $f : S_n \to G_1$

by $f(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{else} \end{cases}$

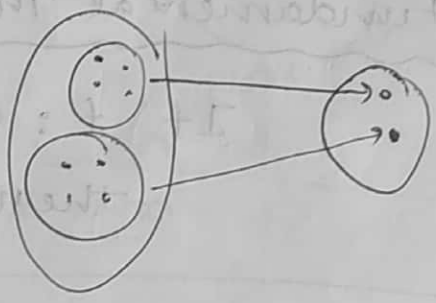
Note that f is an epimorphism.

$\ker f = A_n$. (A_n is a normal subgroup of S_n).

And, $S_n/A_n \cong G_1$.

$\bar{f} : S_n/A_n \to G_1$.

it is a monomorphism.



Result: Let $f : G_1 \to G_1'$ be a homo.

$G_1/\ker f \cong \text{Im } f$

If f is onto, $G_1/\ker f \cong G_1'$.

Proof:

Consider $\ker f = K$.

Define $\bar{f} : G/K \to \text{Im } f$

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

For $a, b \in G$,

$$aK = bK \iff b^{-1}a \in K \iff f(b^{-1}a) = e'$$
$$\iff f(a) = f(b)$$

well defined and one-one.

Note that $\bar{f}$ is onto.

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

Fundamental Theorem of homomorphism.

If $f : G \to G'$ a homo,

then $G/\ker f \cong \text{Im } f$

---

let $H, K \trianglelefteq G$ and $K \subseteq H$

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

Proof :

$f : G/K \to G/H$

$f(aK) = aH$

For $a, b \in G_1$

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

(well definedness)

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

(Homomorphism)

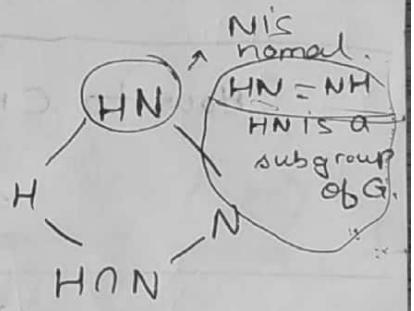
$\text{Ker } f = \{ aK \mid f(aK) = H \}$

$= \{ aK \mid a \in H \} = H/K$

$H \leq G_1$

and $N \trianglelefteq G_1$.

$\frac{HN}{N} \cong \frac{H}{H \cap N}$



If $f : G_1 \to G_1'$ a homo, which is onto.

(1) $H \leq G_1 \Rightarrow f(H) \leq G_1'$

(2) $H' \leq G_1' \Rightarrow f^{-1}(H') \leq G_1$

(3) $H \trianglelefteq G_1 \Rightarrow f(H) \trianglelefteq G_1'$

(4) $H' \trianglelefteq G_1' \Rightarrow f^{-1}(H') \trianglelefteq G_1$

* (5) $H \leq G_1$ and $\text{Ker } f \subseteq H \Rightarrow H = f^{-1}(f(H))$

$\mathcal{F} = \{ H \mid H \leq G_1 \text{ and } \text{Ker } f \subseteq H \}$

$\mathcal{G} = \{ H' \mid H' \leq G_1' \}$

$\mathcal{F} \longleftrightarrow \mathcal{G}$

$H \longmapsto f(H)$

Def: An automorphism on G is an isomorphism from G to G.

identity ✓

Example

For any $a \in G$,

$x \mapsto axa^{-1}$.

$\mathrm{Aut}(G) = \{f \mid f \text{ is an automorphism on } G\}$

This is a group.

$\leq S_G$.

How to create automorphism?

send generator to generator.

$\mathrm{Aut}(\mathbb{Z}) = \{id, \text{inverse}\}$ ↳ abelian should be satisfied

$\mathrm{Aut}(\mathbb{Z}_n) =$

↳ $x \to x^m$

(m and n are relatively prime)

Def^n: Let $N \trianglelefteq G$, N is said to be a maximal normal subgroup of G if

(i) $N \neq G$

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

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

$p\mathbb{Z}$ is maximal subgroups

Def: A group G is said to be a simple group if G has no proper normal subgroup.

$|G| = p \Rightarrow$ no proper normal subgroup possible.

Automata?

Result: For $n > 4$, A_n (= Alternating Group) is simple. (Proof can be done as a excercise)

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

$n = 4$

$A_4 = \{ e, (12)(34), (13)(24), (14)(23), (123), (132) \ldots \}$

6 divides 12 but there is no subgroup of order 6 in A_4. A_4 has a normal subgroup of order 4.

Every finite group is isomorphic to a subgroup of A_m. Excercise?

Def: $X \subseteq G$.

$$\langle X \rangle = \{ x_{i1} x_{i2} \cdots x_{ik} \mid x_{ij} \in X \text{ or } x_{ij}^{-1} \in X \}$$

$k \geq 0$

(1) $e \in \langle X \rangle$

(2) $a, b \in \langle X \rangle$

$\Rightarrow ab \in \langle X \rangle$ and $a^{-1} \in \langle X \rangle$

Hence $\langle X \rangle \leq G$.

Def:

Let $X \subseteq G$.

We say that X is a generating set of G if G is said to be generated by X.

if $\langle X \rangle = G$.

Def: If X is finite, then we say that G is finitely generated.

Any finite group.

$D_n = \langle \{\sigma, \tau\} \rangle$

$\hookrightarrow X \quad (1\ 2\ 3 \ldots n)$

$(K \ K+1) = \sigma^{K-1} \tau \sigma^{1-K}$

* S_n is generated by $(1\ 2\ 3 \ldots n)$ and $(n-1\ n)$
* A_n is generated by $\frac{n!}{2}$ 3-cycles in S_n $\rightarrow (ab)(cd) = (abc)(bcd)$

$(ab)(ac) = (acb)$

G a presentation tells which elements are equivalent.

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

X: generating set.

a b a
b a c
a b c
c b a

a b c
a b
(a c b)

Result:

Let $H_1, H_2, \ldots, H_n \leq G$

and $H = H_1 H_2 H_3 \ldots H_n$

(1) $H_1 \times H_2 \times \ldots \times H_n \cong H$ under the canonical map $(x_1, x_2, \ldots x_n) \mapsto x_1 x_2 \ldots x_n$ for $x_i \in H_i$

$|H_1 H_2| = \frac{|H_1|\,|H_2|}{|H_1 \cap H_2|}$

$|H_1 \times H_2| = |H_1|\,|H_2|$

(2) $H_i \trianglelefteq H$ and every elt. x of H can be uniquely written as $x = x_1 x_2 \cdots x_m$ for $x_i \in H_i$

(3) $H_i \trianglelefteq H$ and if $x_1 \cdots x_n = e \Rightarrow x_i = e \ \forall i$.

(4) $H_i \trianglelefteq H$ and $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\} \quad \forall i$

Rings

$(\mathbb{Z}, +, \cdot)$ ~~$n \in \mathbb{N}$~~

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

Let R be a ring.

$R[x]$ the set of all polynomials with variable x and the coefficient from R.

$$p(x) = \sum_0^n a_i x^i \qquad q(x) = \sum_0^m b_i x^i$$

$$p(x) + q(x) = \sum_{j=0}^{K} (a_j + b_j) x^j \qquad K \text{ is } \max\{m, n\}$$

In a ring,

$a0 = 0a = 0$

$a0 = a(0+0) \quad \forall a \in R$

$\downarrow$

$a0 + a0$

Apply cancellation law

$a0 = 0.$

Here identity element is zero polynomial.

$M_n(R)$ the set of all $n \times n$ matrices with entries from R.

$$(M_n(R), +, \cdot)$$

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

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

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

Notation:

$a + (-b) = a - b$ Not

★ If R has unity 1, $(-1)a = -a$.

Subring A subset (non-empty) S of R is a subring if S is a ring ~~with~~ w.r.t. operation on R.

let $S (\neq \emptyset) \subseteq R$

S is a subring of $R \Leftrightarrow$ $a-b \in S$, $ab \in S$ $\forall a, b \in S$

$\mathbb{Z} \leq Q \leq \mathbb{R}, \mathbb{C}$

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

$\{0\} \leq R$

$R \leq R$

Let $S \leq R$. (Eq. Relation, $a-b \in S$)

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

$(r_1 + S) + (r_2 + S) = (r_1 + r_2 + S)$ is well defined as $(S, +)$ is ~~an abelian~~ a normal subgroup.

"Every subgroup of a abelian group is a normal subgroup"

$(r_1 + S)\cdot(r_2 + S) = r_1 r_2 + S$

is not well defined in general. (Counterexample)

Ideal

A subring I of R is said to be an ideal if $a \in I$ and $r \in R$, then (ar and ra) $\in I$.

$nZ \leq Z$ is an ideal.

$I \trianglelefteq R$ (Normal subgroup counterpart)

If $I \trianglelefteq R \iff (r+I)(s+I) = rs + I \quad \forall r, s \in R$ is well defined.

$(R/I, +, \cdot)$ is ring (Quotient Ring)

* If R is commutative, R/I is commutative.

Notation

$n \in \mathbb{N}$ $na = a + a + a \ldots + a$

$n = 0$ $\cdot na = 0$

$n \in \mathbb{Z}^-$ $na = (-a) + (-a) + \ldots (-a)$

(n times)

For $a \in R$

$\langle a \rangle =$

$$\left\{ \begin{matrix} na \\ ra \\ ar \end{matrix} \;\middle|\; \begin{matrix} n \in \mathbb{Z} \\ r \in R \end{matrix} \right.$$

$R \rightarrow$ ~~Normed~~ Ring

a^k is included in ra.

If R is a comm. ring with unity

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

geometrically

If R is a ring with unity.

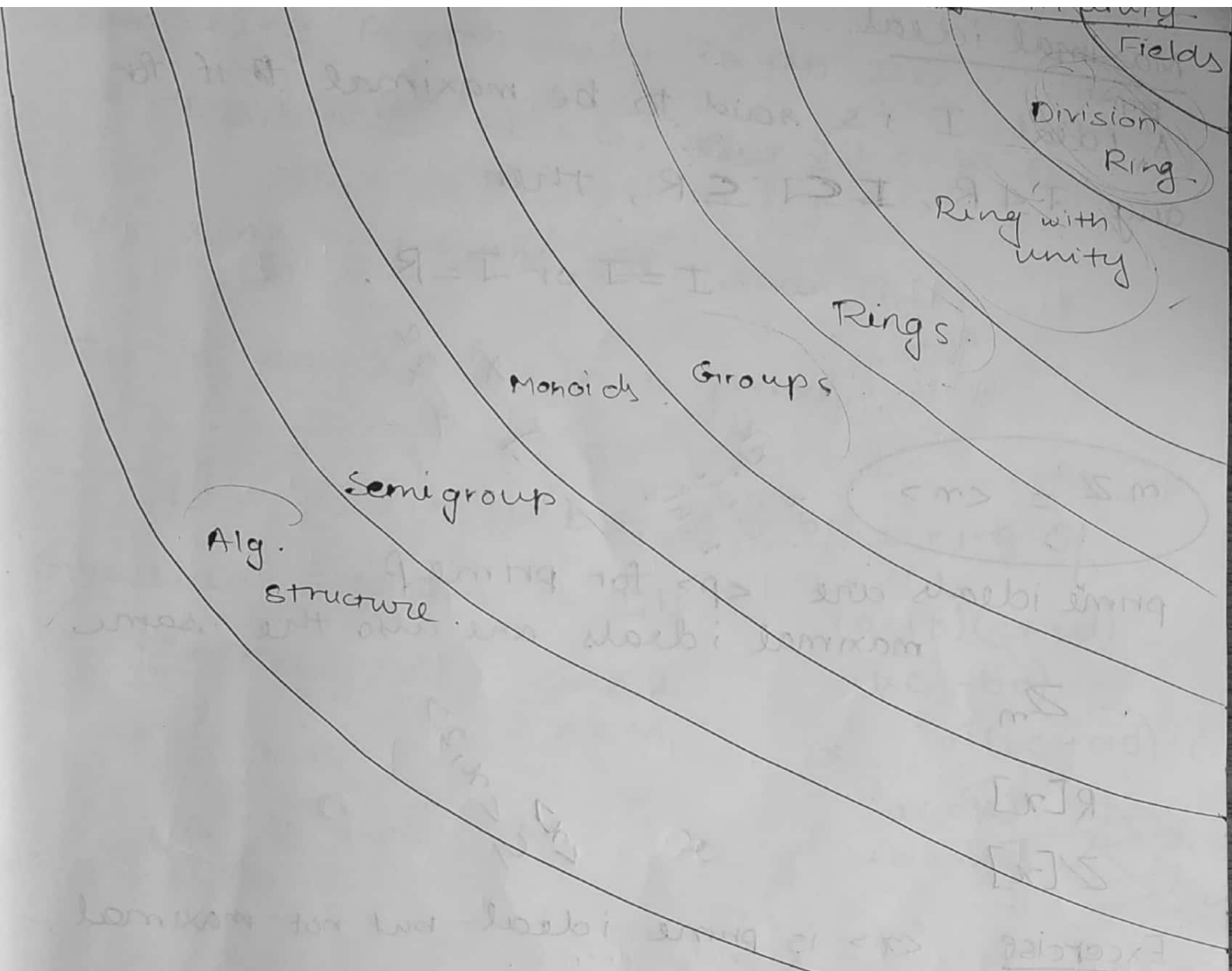
$$\langle a \rangle = \left\{ \begin{matrix} ra \\ ar \end{matrix} \;\middle|\; r \in R \right\}$$

R is a commutative ring with unity

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

$R[x]$

$\langle x \rangle$ $\{ xp(x) \}$



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

all ideals are principle ideals

★ In any ring.

$$(na)(mb) = (mn)(ab)$$

$a, b \in R \qquad m, n \in \mathbb{Z}$

Prime ideal

Let R be a comm. ring with unity

A proper ideal I is said to be prime ideal if $\forall\ a, b \in R$ with $ab \in I$, Then

$a \in I$ or $b \in I$.

Maximal ideal

proper

A ideal I is said to be maximal if for any $J \trianglelefteq R$, $I \subseteq J \subseteq R$, then

$$I = J \text{ or } J = R.$$

$n\mathbb{Z} = \langle n \rangle$

prime ideals are $\langle p \rangle$ for prime p

maximal ideals are also the same

$\mathbb{Z}_n$

$R[x]$

$\mathbb{Z}[x]$

Excercise $\langle x \rangle$ is prime ideal but not maximal

Integral domains

A comm. ring with unity is said to be an integral domain if it has no non-zero zero divisors.

(For all $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$)

$(\mathbb{Z}, +, \cdot)$ ✓ integral domain

$(\mathbb{Z}_6, +, \cdot)$ × integral domain

$(\mathbb{Z}_p, +, \cdot)$ ✓ integral domain.

Comm. ring R with unity is an ID.

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

The ring of integers $\mathbb{Z}$ is an ID.

$\mathbb{Z}_n$ is an ID $\iff$ n is prime.

$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ the ring of Gaussian integers is ID.

$(a+ib)(c+id)$

$(ac - bd)$

$+i(bc + ad) = 0$

$ac = bd$

$-bc = ad$

$-\frac{a}{b} = \frac{b}{a}$

Matrix ring. $n \geq 2$, $n \times n$.

a $[a]$

Every field is an ID

$ab = 0$

if $a \neq 0$, $a^{-1}(ab) = a^{-1}0$,

$\Rightarrow b = 0$.

Characteristic of a ring R is the least positive integer n such that $na = 0$ $\forall\ a \in R$

If no such positive int. exists, then we say

$\text{char } R = 0$

$\text{char } R$ → characteristic of ring

Result

Let R be a ring with unity. If order of 1 under addition is infinite, then char R = 0

Else if order of 1 ~~is n~~ under addition is n. then char R = n.

$$n1 = 0 \Rightarrow na = 0 \quad \forall a \in R$$

Proof: $na = a + a + 0 \ldots + a$

$= (1 + 1 + 1 \ldots 1)\, a$

$= (n1)a$

$= 0a$

$= 0$

$\therefore$

* char of ID is 0 or a prime.

Proof:

$n = \text{char } R$

$n = rs$

$1 \le r, s < n$

$n1 = 0$

i.e. $(rs)1 = 0$

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

Let R be a comm. ring with unity and $I \trianglelefteq R$.

Result

R/I is ID $\Leftrightarrow$ I is prime ideal.

(1) $ab \in I$

(2) $\Rightarrow ab + I = I$

(3) $(a+I)(b+I) = I$

(4) $a+I = I$ or $b+I = I$

(5) $a \in I$ or $b \in I$.

Suppose $(a+I)(b+I) = I$

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

$ab + I = I$

$ab \in I$

$a \in I$, $b \in I$

$a+I = I$, $b+I = I$

* Result

R/I is a field $\Leftrightarrow$ I is maximal.

Coro: in a comm. ring with unity, every maximal ideal is prime.

Assume R/I is a field.

Suppose $J \trianglelefteq R$ such that $I \subsetneq J$

let $a \in J \setminus I$, $a + I \neq I$

$(a \notin I)$

$\Rightarrow \exists\ b+I \in R/I$ s.t. $(a+I)(b+I) = 1+I$

$ab + I = 1 + I$

$1 - ab \in I$, $\Rightarrow 1 - ab$

Since $a \in J$, we ha

$ab \in J$,

$\Rightarrow 1 - ab + ab \in J$

$\Rightarrow 1 \in J$

For any $a \in R$,

$a = a.1 \in J$

$\Rightarrow R = J$

Hence, I is maximal ideal.

Homomorphism

$f: R \to S$

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

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

$R = \{f \mid f: X \to R$ a function$\}$

$(R, +, \cdot)$

$X = R$

$M(R)$

$X = [0, 1]$

Let $(G,+)$ be an abl. group

$R = \text{Hom}(G,G) = \text{End}(G) = \{f / f: G \to G$ a homo $\}$

↓ set of all functions

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

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

$(R, +, \cdot)$ is a ring.

$P(X)$ ↓ power set we can make a ring

(by $(A-B) \cup (B-A)$)

↑ $A+B$

$AB = A \cap B$.

Let R be a ring.

$x \in R$ is said to be idempotent if $x^2 = x$.

Boolean ring A ring is said to be a boolean ring if every elt is idempotent.

Let $f: R \to S$ a homo.

$\text{Ker} f = \{x \in R / f(x) = 0\}$

$\text{Ker} f \trianglelefteq R$

f is $1-1$ $\Leftrightarrow$ $\text{Ker} f = \{0\}$.

Let f be onto

① $A \leq R \Rightarrow f(A) \leq S$

② $B \leq S \Rightarrow f^{-1}(B) \leq R$

③ $A \trianglelefteq R \Rightarrow f(A) \trianglelefteq S$

④ $B \trianglelefteq S \Rightarrow f^{-1}(B) \trianglelefteq R$

⑤ There is a 1-1 correspondence b/w ideals of S and the ideals of R containing $\ker f$.

★

① $f: R \to S$ onto

$R/\ker f \cong S$.

② $R/I \cong (R/J)/(I/J)$

$I, J \trianglelefteq R \Rightarrow J \subseteq I$

$\mathbb{Z} \to \mathbb{Z}$

possible homomorphisms (w.r.t. ring)

$f(n) = 0$

or

$f(n) = n$

★ what are the homomorphisms b/w $F \to R$?

Field of fraction / quotients

Let R be an integral domain. Then, there exists a field F (Field of fraction / quotient of F) that contains F as a subring isomorphic to R.

Proof

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

Define $\equiv$ on S by

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

$\equiv$ is an equivalence relation on S

Set $F = S/\equiv$

write $\frac{a}{b}$ to denote the class

$$F = \left\{\frac{a}{b} \mid b \neq 0\right\}$$

Define:

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

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

Note that the operations are well defined

$R \to F$

$r \mapsto (r, 1)$

homomorphism.

For

$$f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$$

with $a_n \neq 0$, this degree of $f(x)$

$$\deg f(x) = n$$

a_n is the leading case

If $a_n = 1$, then $f(x)$ is called monic polynomial.

$$U(\mathbb{Z}_n) = \{ \bar{a} \in \mathbb{Z}_n \mid \overset{\gcd}{(a, n)} = 1 \}$$

Remark $U(R)$ is a multiplicative gro

Division Algo

Result: Let F be a field and $f(x)$, $(0 \neq g(x))$ $\in F[x]$, there $\exists$ a unique $q(x), r(x) \in F[x]$ such that $f(x) = g(x)\, q(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof:

If $f(x) = 0$ or $\deg f(x) < \deg g(x)$, then choose $q(x) = 0$ and $r(x) = f(x)$

Supp. $n = \deg f(x) \geq \deg g(x) = m$

Let

$$f(x) = a_0 + a_1 x + a_2 x^2 \ldots + a_n x^n$$

$$g(x) = b_0 + b_1 x + b_2 x^2 \ldots + b_n x^n$$

Let $f_1(x) = f(x) - (a_n b_m^{-1} x^{n-m}) g(x)$

Then, $f_1(x) = 0$ or $\deg(f_1(x)) < \deg f(x)$.

By induction, there exist $q_1(x)$ and $r_1(x) \in F[x]$ such that $f_1(x) = g(x) q_1(x) + r_1(x)$

when $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$

Then, $f(x) = f_1(x) + a_n b_m^{-1} x^{n-m} g(x)$

$= g(x) q_1(x) + r_1(x) + a_n b_m^{-1} x^{n-m} g(x)$

$= g(x)\left(q_1(x) + a_n b_m^{-1} x^{n-m}\right) + r_1(x)$

$g q_1 + r_1 = g q_2 + r_2$

$g(q_1 - q_2) = r_2 - r_1$

has to be zero.

Let R be an ID and $k = \max(n-m+1, 0)$ and a be the leading coefficient of $g(x)$.

$$a^k f(x) = q(x) g(x) + r(x)$$

Cor 1: (Remainder Thm.)

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

then $f(a)$ is the remainder in the division of $f(x)$ by $(x-a)$.

Cor 2 (Factor Th.)

Let $a \in F$ and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $(x-a)$ is a factor of $f(x)$.

Cor 3

A polynomial of degree n over a field has at most n zeroes counting the multiplicity.

* Every ideal is a principal ideal in $\mathbb{Z}$.

Result: Let F be a field. Every ideal in $F[x]$ is a principal ideal.

Def: An integral domain is said to be a principal ideal domain (PID) if every ideal is principal ideal in it.

Example ① $\mathbb{Z}$ ② F ③ $F[x]$, for a field F

$I \trianglelefteq \mathbb{Z}$

Result: For a field F, $F[x]$ is a PID.

Proof: we know $F[x]$ is an ID.

Let $I \trianglelefteq F[x]$ If $I = \{0\}$ clearly it is $\langle 0 \rangle$

Suppose $I \neq \{0\}$ let $f(x)$ be a polynomial of least degree in I. Claim $\langle f(x) \rangle = I$

To prove: If $g(x) \in I$, then $g(x) \in \langle f(x) \rangle$

$\langle f(x) \rangle \subseteq I$ Let $g(x) \in I$,

By div. algo,

$g(x) = q(x) f(x) + r(x)$

where $r(x) = 0$ or degree $(r(x)) <$ deg $f(x)$

$\Rightarrow r(x) = g(x) - q(x) f(x) \in I$

$\Rightarrow r(x) = 0$

$$\langle x \rangle = \{ x f(x) \mid f(x) \in \mathbb{Z}[x] \}$$

$$= \{ h(x) \mid h(0) = 0 \}$$

$F[x]/(I = \langle g(x) \rangle)$

$(I \neq \langle 0 \rangle)$

Result

$I \trianglelefteq F[x]$ F = field.

$I = \langle g(x) \rangle \iff g(x)$ is a non-zero polynomial of least degree in I.

$$= \{ f(x) + I \mid f(x) \in F[x] \}$$

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

$f(x) = q(x)\, g(x) + r(x) \Rightarrow \{ r(x) + \langle g(x) \rangle \mid \deg r < \deg g \}$

$$\mathbb{Z}_5[x]/\langle x^3 \rangle = \{ f(x) + \langle x^3 \rangle \mid f(x) \in \mathbb{Z}_5[x] \text{ and } \deg f < 3 \}$$

$0, 1, 2$

Irreducible polynomial

Let R be an ID.

A poly $f(x) \in R[x]$, which is neither zero nor unit, is called an irreducible polynomial whenever it can be expressed as $f(x) = g(x)\, h(x)$ for $g(x)$, $h(x) \in R[x]$, then $g(x)$ or $h(x)$ must be a unit in $R[x]$.

On the other hand, a non-zero unit in $R[x]$ called reducible it is not irreducible.

$$U[F[x]) = \{ a / a(\neq 0) \in F \}$$

i.e. unit elements.

$\langle 1 \rangle = F[x]$

$\langle a \rangle = F[x]$ as $(aa^{-1} = 1$ comes in $H)$

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

" " R

reducible over C.

$f(x) = 2(x^2+2)$ $\quad 2(x+i\sqrt{2})(x-i$

irreducible in $\mathbb{Q}$

reducible over $\mathbb{Z}$

(2 is not invertible)

$h : R[x] \longrightarrow \mathbb{C}$

by $h(f(x)) = f(i)$ Onto ✓ Homo ✓

$$\frac{F[x]}{R[x]/\langle x^2+1 \rangle} \cong C.$$

Result: Let F be a field and $p(x) \in F[x]$. Then, $\langle p(x) \rangle$ is maximal in $F[x] \Leftrightarrow p(x)$ is irreducible over F.

Proof: $\langle p(x) \rangle$ is maximal

$p(x) \neq 0$ and irreducible

Suppose, $p(x) = g(x)\,h(x)$

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

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

can only happen when degree of $p(x)$ and $g(x)$ is same.

So, $h(x)$ has to be a unit.

So, $p(x)$ is irr.

Suppose $\langle p(x) \rangle \subseteq I \subseteq F[x]$

$I \hookrightarrow$ PID, $g(x)$, $F[x] \hookrightarrow$ is PID

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

$p(x) = g(x)\,h(x)$

So, $I \hookrightarrow$ PID.

Corr. $F[x]/\langle p(x) \rangle$ is a field.

if $p(x)$ is irr over F.

Coro: (Euclid's Lemma)

$\Rightarrow p(x) \mid a(x)\,b(x)$

$\Rightarrow p(x) \mid a(x)$ or $p(x) \mid b(x)$

Proof: Note $\langle p(x) \rangle$ is maximal ($p(x)$ is irr.)

$\langle p(x) \rangle$ is prime ideal.

As $a(x)b(x) \in \langle p(x) \rangle$

$\Rightarrow a(x) \in \langle p(x) \rangle$ or $b(x) \in \langle p(x) \rangle$

$\mathbb{Z}_2[x] / \langle p(x) \rangle$

↳ deg 3

$= \{ f(x) + \langle p(x) \rangle \mid f(x) \in \mathbb{Z}_2[x], \deg f(x) \leq 2 \}$

Result: Let F be a field $f(x) \in F[x]$ of degree 2 or 3, then $f(x)$ is irr over F

$\Leftrightarrow$ $f(x)$ has no zeroes over F.

$\{ a + bx + cx^2 + \langle p(x) \rangle \mid a, b, c \in \mathbb{Z}_2 \}$

Conclusion

Construction of a field of size p^k, prime

$\mathbb{Z}_p[x] / \langle p(x) \rangle$

degree $= k$.

$\left| \mathbb{Z}_p[x] / \langle p(x) \rangle \right| = p^k$

$a + bx + cx^2$

$x^4 + 2x^2 + 1 = (x^2 + 1)^2$

$x^4 + 2x^2 + 1 = (x^2+1)^2$

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

No roots, but still reducible.

Extension Field

A Field E is said to be an extension field of F if

$F \leq E$,

$F \hookrightarrow E$

Fundamental Thm. of field Theory

Let F be a field and $f(x)$ be a non-const polynomial over F. Then, there is an extension field E of F such that $f(x)$ has a zero in E.

Proof: Note that

$f(x) \in F[x]$ has an irreducible factor say $p(x)$.

Set $F[x]/\langle p(x)\rangle$ Note E is a field.

$\phi : F \to E$

$\phi(a) = a + \langle p(x)\rangle$

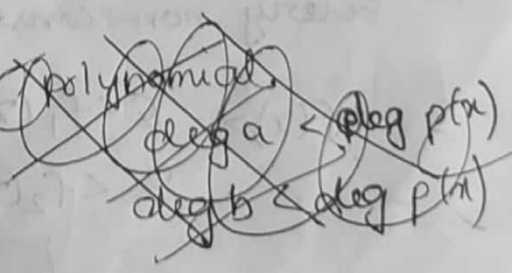
$a + \langle p(x)\rangle = b + \langle p(x)\rangle$

$a - b \in \langle p(x)\rangle$

$a = b$.

$\therefore$ Hence, E is an extension of F.

Claim: $p(x)$ has a zero in E.



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

$$p(x + \langle p(x) \rangle) =$$

$$a_0 + a_1 (x + \langle p(x) \rangle) + a_2 (x + \langle p(x) \rangle)^2$$

$$\ldots\ldots a_n (x + \langle p(x) \rangle)^n$$

$$= a_0 + a_1 (x + \langle p(x) \rangle) + a_2 (x^2 + \langle p(x) \rangle)$$

$$\ldots\ldots + a_n (x^n + \langle p(x) \rangle)$$

$$= p(x) + \langle p(x) \rangle = \boxed{0 + \langle p(x) \rangle}$$

identity el^n.

a → In a PID, any strictly ↑sing chain of ideals is stationary.

$$I_1 \subsetneq I_2 \subsetneq I_3 \ldots \subsetneq I_K = I_{K+1}.$$

ideal ← $I = \bigcup_i I_i \trianglelefteq R$

only if they are contained with in each other.

$I = \langle a \rangle$

$a \in I \Rightarrow a \in I_K$

$\Rightarrow \langle a \rangle \subseteq I_K$

$I \subseteq I_K$

★ Every non-constant poly. over F has an irred. fa

$\langle f(x) \rangle \subsetneq \langle f_1(x) \rangle$

$\subsetneq \langle f_2(x) \rangle$

$f(x) = f_1(x)\, g_1(x)$

$f_1(x) = f_2(x)\, g_2(x)$

has to terminate somewhere

over an ID

Cor: Every non-const poly$_{/\Lambda}$ has a zero in some ext. field of given ID.

$P \hookrightarrow F \hookrightarrow E$. $\quad D \times D^* / \equiv$

→ $2x+1 \in \mathbb{Z}_4[x]$ $\quad \mathbb{Z}_4 \leq$ Ring. | $\mathbb{Z}_p$ is an ID if p = prime.

$\mathbb{Z}_4[x]$ is not an ID.

Let Ring be an ext. with α a zero of $2x+1$.

$2\alpha+1=0 \quad \nearrow (2\cdot 2)\alpha + 2$

$2(2\alpha+1)=0 \Rightarrow 2\cdot 0 = 0$

but 2 is not 0 in $\mathbb{Z}_4$.

Notation: Let F be a field.

and $a_1, a_2, \ldots a_n \in E \geq F$.

$F(a_1, a_2, \ldots a_n)$ denotes the smallest field containing F and $\{a_1, a_2, \ldots a_n\}$

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

$f(x) = a(x-a_1)\ldots(x-a_n)$. The splitting field of $f(x)$ over F is $F(a_1, a_2, \ldots a_n)$.

Result: Let $f(x) \in F[x]$. then there is a splitting field E of $f(x)$ over F. (non. const.)

Note: let $f(x) \in F[x]$.

$F(a_1, a_2, \ldots a_n)$, $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$

Result: let $f(x)$ be a non-const. polynomial over F. then, there exists a splitting field over F.

Proof: by induction on $\deg f(x)$.

If $\deg f(x) = 1$,

Suppose the result is true for all fields in polynomials of $\deg < \deg f(x)$.

By Fund. Th. of FT, $\exists$ an extension E of F which has a zero say a_1 of $f(x)$.

$f(x) = (x - a_1) g(x)$ where $g(x) \in E[x]$.

and $\deg g(x) < \deg f(x)$

By induction, $g(x)$ has splitting field K (over E) which has all the zeros of $g(x)$. - $a_1, a_2, \ldots a_n$. Thus,

$K = F(a_1, a_2, \ldots a_n)$.

~~**Result:** let $p(x)$ be an irr. polynomial over F. If a is a zero of $p(x)$ in some ...~~

Def^n: Suppose E is an extension of F. The deg of E over F denoted by $[E : F]$ is the dimension of E (as a vector space) over F. if $[E : F]$ is finite, then we call E as a finite extension otherwise call it infinite extension.

$[C : R] = 2$

$[C : \mathbb{Q}] = \infty$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, basis: $(1, \sqrt{2})$

$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] \to 4$, basis $(i, i\sqrt{2}, 1, \sqrt{2})$

$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$, basis $\{1, 2^{1/6}, 2^{2/6}, 2^{3/6} \ldots 2^{5/6}\}$

Extra: every vector space has a basis, John's lemma, infinite basis.

Result: let $p(x)$ be a irr. polynomial of F, if a is a zero of $p(x)$ in some ext. E of F. Thus, $F(a)$ is isomorphic to $F[x] / \langle p(x) \rangle$. Furthermore, if $\deg p(x) = n$, then every elt. can be written as $c_0 + c_1 a \ldots$

* $F \le E \le K$.

$[K : F] = [K : E][E : F]$

$F(a) \cong F[x]/\langle p(x) \rangle$

Every elt. of $F(a)$ can be uniquely written as $c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1} a^{n-1}$.

where $c_0, c_1, c_2, \ldots, c_{n-1} \in F$ & $\deg p(x) = n$.

Coro Let a be a zero of $p(x)$ in some ext^n E and b be a zero of $p(x)$ in some other extension E', then $F(a) \cong F(b)$.

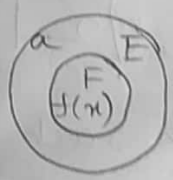
Result: Let $f(x) \in F[x]$. Any 2 splitting fields of $f(x)$ over F are isomorphic.

$\phi : F \cong F'$ and let $f(x) \in F[x]$. Let E be a splitting field of $f(x)$ over F and E' be a splitting field of $\phi(f(x))$ over F'.

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

We call a is algebraic over F if there is a non-zero polynomial in $F[x]$ for which a is a zero.

If a is not algebraic over F, then we call it as transcedental elements.



Field of fractions

Consider the field of quotients of $F[x]$

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

Remark : If a is transcedental over F, then

$$F(a) \cong F(x)$$

$$\phi : F[x] \longrightarrow F(a)$$

$$f(x) \to f(a)$$

$$\text{Ker } f = \{0 \text{ zero polynomial only}\}$$

If a is algebraic over F, there is unique monic irreducible polynomial $p(x)$ in $F[x]$, $p(a) = 0$

↓

def: minimal polynomial.

Remark: $[F(a) : F] = n$

Result: If E is a finite extension of F, then E is an algebraic extension of F.

$$[E : F] = n.$$

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2} \ldots)$$

$$\sqrt[n]{2} \mid n \in \mathbb{N}$$

infinte algebraic extension

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

(denoted by $GF(p^n)$ - Galois field of order p^n)

Results As a group under addition,

$$GF(p^n) \cong Z_p \oplus Z_p \oplus \cdots \oplus Z_p$$

(n times)

As a group under multiplication,

$GF(p^n)^* \cong Z_{p^n-1}$

Hence it is cyclic.

Coro: $[GF(p^n) : GF(p)] = n$.

Pro: Let $\langle a \rangle = GF(p^n)^*$. Then a is algebraic over $GF(p)$ of degree n.

external direct product

If $H_1, H_2 \trianglelefteq G$, $H_1 \times H_2 \cong H_1 H_2$ (↳ internal direct product)

(H_1, H_2 ↳ normal subgroups)

& $H_1 \cap H_2 = \{e\}$

For additive groups,

$H_1 H_2$ may be written as $H_1 + H_2$.

$H_1 H_2$ is direct $\Rightarrow$ $H_1, H_2 \rightarrow$ normal subgroups and $H_1 \cap H_2 = \{e\}$

$H_1 \oplus H_2 \rightarrow$ for additive groups $(H_1 \times H_2)$

↳ direct sum

Fundamental theorem of finitely generated abelian groups:

$$G = \langle a_1, a_2, \ldots\ldots a_n \rangle \quad \text{abelian.}$$

Any f.g. abl group G can be decomposed as a direct sum of a finite number of cyclic groups. Precisely,

$$G = C_1 \oplus C_2 \oplus C_3 \oplus \ldots\ldots \oplus C_K$$

Either all C_i are infinite or some $j \leq K$ $C_1, C_2, \ldots\ldots C_j$ are of orders $m_1, m_2, \ldots m_j$ (and rest are infinite).

$$G = \underbrace{C_1 \oplus C_2 \oplus \ldots\ldots \oplus C_j}_{\text{Torsion}} \oplus \overbrace{C_{j+1} \ldots C_K}^{\text{Torsion free.}}$$

Result: $m_1 | m_2 | m_3 | m_4 \ldots\ldots | m_K$.

If G is finite abelian group,

$$|G| = m_1 m_2 \ldots\ldots m_K$$

$$G \cong Z_{m_1} \oplus Z_{m_2} \oplus \ldots\ldots \oplus Z_{m_K}$$

For finite groups, the list of integers which satisfy $m_1 | m_2 | \ldots | m_K$ are called invariants of G.

OR

G is of type $(m_1, m_2, \ldots, m_K)$

Example:

$8 = 2^3$

$\mathbb{Z}_8$

$\mathbb{Z}_2 \oplus \mathbb{Z}_4$ } check isomorphism

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$G \hookrightarrow p^{\alpha}$

$(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_K})$

$\alpha_1 \leq \alpha_2 \cdots \leq \alpha_K$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_K^{\alpha_K}$

$4725 = 3^3 \times 5^2 \times 7$

(3)	(2)	(1)
$2+1$	2	1
$1+1+1$	$1+1$	

So, there are 6 possibilities of non-isomorphic groups of order 4725.

Ex: $\mathbb{Z}_3 \oplus \mathbb{Z}_5^2 \oplus \mathbb{Z}_7$

$\not\cong \mathbb{Z}_3^2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5^2 \oplus \mathbb{Z}_7$

$\not\cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5^2 \oplus \mathbb{Z}_7$

and so on - - -

So, here what we do is:

take a particular group.

$\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m,n) = 1$

$\mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$

3 ; 1+1 ; 1

$\cong$ $3^3 \cdot 5 \cdot 7$; 5

$\mathbb{Z}_{945} \oplus \mathbb{Z}_5$

invariant

$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$

1+1+1 ; 1+1 ; 1

3.5.7 ; 3.5 ; 3

$\mathbb{Z}_{105} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_3$

invariant

Ex: what is the no. of cyclic groups of order 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$.?

$G \times H$ $o(a,b) = \text{lcm}(o(a), o(b))$

$10 \mid 100$ $\therefore$ $\exists$ exactly 1 subgroup of order 10 in $\mathbb{Z}_{100}$. $\mathbb{Z}_{25}$ has order 25

$25 \nmid 100$.

$\mathbb{Z}_{100}$	$\mathbb{Z}_{25}$	
10	1	$\phi(10) \times \phi(1) = 4$
2	5	$+\phi(2) \times \phi(5)$ 4
10	5	$+\phi(10) \times \phi(5)$ 16
		$= 24$