3 Chapter : I : Number theory

II : Ring theorey

III : Group theorey

1.1 - Division algorithm

ex. $46/7 = 7 \cdot (6) + (4)$ → remainder, (6) → Quotient

Theorem(1.1): let $a, b \in \mathbb{Z}$ $(b>0)$, $\exists!\ q, r \in \mathbb{Z}$ such that $a = b \cdot q + r$, $0 \le r < b$.

Ex1. Q: $a = 1231$, $b = 53$?

A: $1231 = 53 \cdot q + r$

$\Downarrow$

$q = 23$; $r = 12$

Ex2. Q = -2022, $b = 90$?

$-2022 = 90q + r$.

$\Downarrow$

$q = -23$; $r = 48$

Prove: a > Exist : Suppose $S = \{a - bx \ge 0 \mid x \in \mathbb{Z}\}$.

- $S \neq \emptyset$: By take $x < 0$ [negative enough]
- $r :=$ minimal of S ($\min S$)

  $r \in S$, so $r = a - bq$ for some $q \in \mathbb{Z}$.

  and $r \ge 0$
- $r < b$: otherwise $r \ge b$

  $a = bq + r$

  $a = b(q+1) + (r-b)$

  So $r - b \in S$

  but $r - b < r$ ("x")

  ↖ Min S.

b > uniqueness: $bq_1 + r_1 = bq_2 + r_2$ (Assu)

where $0 \le r_1, r_2 < b$

$bq_1 - bq_2 = r_2 - r_1$

$\Downarrow$

$-b < r_2 - r_1 < b$

$\Downarrow$

$-b < b(q_1 - q_2) < b$

$\Downarrow$

$-1 < q_1 - q_2 < 1$

Since $q_1, q_2 \in \mathbb{Z}$, then $q_1 = q_2$

then, $r_2 = r_1$

1.2 - divisibility

Defn: $a, b \in \mathbb{Z}$. we say b divides a and we write b/a if $\exists c \in \mathbb{Z}$ such that $a = bc$ "b = divisor"

Remarks:

- write $a = bq + r$ as before
  then b divide a iff $r = 0$

$a \neq 0$!!!

- Sign is irrelavent $\rightarrow$ division!
  $b/a \rightarrow -b/a\ ;\ b/-a\ ;\ -b/-a.$
- any number is a divisor of zero "0", $\forall b \in \mathbb{Z}$, $b/0$
- $b/a \rightarrow |b| \le |a| \Rightarrow$ any number has finite many divisors

---

Def: $a, b \in \mathbb{Z}$ (Not both 0)

The greastest common divisor (GCD) is a positive number $d \in \mathbb{Z}$, such that • $d \mid a, b$

• if $c \mid a, b$, then $c \le d$.

we denote gcd "$d = (a, b)$"

ex1. $(20, 15) = 5$

ex2. $(2^3 \cdot 3^2 \cdot 5,\ 2^2 3^4, 7) = 2^2 \cdot 3^2 = 36$

ex3. $(4, 0) = 4 \Rightarrow (a, 0) \Rightarrow a$ if $a > 0$

Theorem 1.2. if $a, b \in \mathbb{Z}$ (Not both 0), $\exists u, v \in \mathbb{Z}$.

$$(a, b) = ua - vb$$

proof: Set $S = \{ax - by > 0 \mid x, y \in \mathbb{Z}\}$.

— $S \neq \emptyset$; take $x = a$, $y = b$.

— Defn $d = \min S$

we show $d = (a, b)$

a) why d/a?: $a = dq + r$ where $0 \le r < d$ and $r = 0$

if $r \neq 0$, $r = a + (-q)d$

$= a + (-q)(ax + by)$

$= (1 - qx)a + (-qy)b$

$\Rightarrow r \in S$ but $r < d = \min S$

contridiction !!!

b) In the same way, d/b

c) show d is the greastest, says $c \mid a, b$.

$\rightarrow c \mid d = ax + by$

$\rightarrow c \le d$

Remarks: proof

① • gcd is the smallest combination of a and b

ex1. if $ax + by = 1 \Rightarrow (a, b) = 1$

collary ② • gcd is unique

③ • if c is a common divisor, then $c \mid \gcd$.

Theorem 1.4 ; let $(a,b)=1$, then we says that a, b are "co-prime"

Then if $a \mid b \cdot c$, then $a \mid c$

ex1 [$4 \mid 2 \cdot 2$ and $4 \nmid 2$]

pf : let $(a,b)=1$. if $a \mid bc$: then By theorem 1.2 $\exists u, v \in \mathbb{Z}$

$$1 = ua + vb$$
$$\Rightarrow c = uac + vbc$$
$$\Rightarrow c = (uc)a + (vq)a$$
$$\Rightarrow c = ka \quad !!!$$

☆ = Euclid Algorithm

!!! $(a,b) = (a = bq + r, b) = (r, b)$

smaller number !

Example : $(210, 45)$

EA : $(210, 45) = (45, 30)$

$= (30, 15)$

$= (15, 0)$

$= 15$

9.12 notes.

$$\left(\begin{array}{l} (a,b)=1 \\ a \mid bc \longrightarrow a \mid c \end{array} \right)$$

1.3 prime and unique factorization

Def: $p \in \mathbb{Z}$, $p \neq 0, \pm 1$ is a prime number, if its only divisors are $\pm 1, \pm p$; otherwise it is composite.

i.e $p = ab$ such that $|a| \cdot |b| < |p|$

Remark: 1. p prime $\Longleftrightarrow$ $-p$ prime

2. There are infinite prime number.

Theorem 1.7: Every integer $(\neq 0, \pm 1)$ is finite product of prime number.

proof: Select a, b $(\neq, \pm 1)$

if a prime $\rightarrow$ done ✓

if $a \neq$ prime $\Longrightarrow$ $a = a_1 \cdot a_2$ where $|a_1|\,|a_2| < |a|$

$\Longrightarrow$ Then we look at a_1 and do the same.

$\Longrightarrow$ we keep decomposing until we get prime.

why stop?

because use of the reduction of the absolute number.

uniqueness? Theorem 1.5 let $p \neq 0, \pm 1$, $p \rightarrow$ prime $\Longleftrightarrow$ if $p \mid ab$, then $p \mid a$ or $p \mid b$

proof: a) Assume p is prime and $p \mid ab$ [WTS $p \mid a$ or $p \mid b$]

$$\begin{cases} (a,p) \mid p \text{ which is prime} \\ (a,p) = p \rightarrow p \mid a \ \checkmark \\ (a,p) = 1 \rightarrow p \mid ab \rightarrow p \mid b \ \checkmark \end{cases}$$

b> Assume $a \mid p$, (WTS $a = \pm 1, \pm p$), so $p = a \cdot b$ for some $b \in \mathbb{Z}$.

so $p \mid ab \rightarrow p \mid a$ or $p \mid b$

$\Downarrow a \mid p$ its $\pm p = a$

$\Downarrow b \mid p$ $b = \pm p$ $\Downarrow$ $a = \pm 1$.

Corollary: p is prime, if $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i

---

Them 1.8 = [uniqueness of prime factorization].

factor → into prime is unique (up to order and sign)

eg1: $6 = 2 \cdot 3 = (-2) \cdot (-3) = 3 \cdot 2$

---

ie: $P_1 \cdots P_n = q_1 \cdots q_m$. P_i, q_j's prime.

then n must be equal to m.

and we get $P_i = \pm q_m$.

proof: Assume. $P_1 \cdots P_n = q_1 \cdots q_m$. P_i, q_j's prime.

If $P_1 \mid P_1 \cdots P_n$, then $P_1 \mid q_1 \cdots q_m$.

So by theorem 1.6. P_1 must divide. $P_1 \mid q_j$ for some

but q_i is prime. so $P_1 = \pm 1$ or $P_1 = \pm 1$

$p_i = q_j$ or $p_i = 1$.

relabel the q's such that $q_1 = P_1 \Rightarrow P_1 P_2 \cdots P_n = P_1 q_2 \cdots q_n$

$1 = \underbrace{q_{m-n} \cdots q_n}_{\text{but they are prime.}}$

$P_2 \cdots P_n = q_2 \cdots q_m$

$\Downarrow$ (def prime)

2.1 congruent modulo n

Fix $1 < n \in \mathbb{N}$.

Def: we say two number are congruence modulo n.

if $n \mid a-b$.

$\Downarrow$

$\iff a-b = nk$ (for k in $\mathbb{Z}$)

$\iff a = nk+b$ (for k in $\mathbb{Z}$)

So we can reach a from b by multiples of n.

we write $a \equiv b \pmod n$

01·190·206.

Theorem 2.1: Congruence modulo n is an equivalence relation

(i) reflexive: $\forall a$: $a = a \pmod n$

(ii) symmetric : if $a \equiv b \pmod n$, then $b \equiv a \pmod n$

(iii) transtive : if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

Def: let $a \in \mathbb{Z}$, the congruence class of a modulo n is the set

$$[a] = [a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod n\} = \{a + nk \mid k \in \mathbb{Z}\}.$$

Remark: $a \in [a]$

ex 1: ① $n = 2$: $[0]$ = all the even number = $\{2k \mid k \in \mathbb{Z}\}$

$= 2\mathbb{Z}$ no identify.

② $n = 2$: $[1]$ = all the odd number = $\{2k+1 \mid k \in \mathbb{Z}\}$

$= 2\mathbb{Z} + 1$

③ $n = 2$: $[2]$ = all the even number = $\{2(k+1) \mid k \in \mathbb{Z}\}$

$= 2\mathbb{Z}$. no identity.

B) ① $n = 3$ $[0] = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$.

$[1] = \{1 + 3k, k \in \mathbb{Z}\} = 3\mathbb{Z} + 1$.

$[2] = \{2 + 3k, k \in \mathbb{Z}\} = 3\mathbb{Z} + 2$

$[3] = [0]$

$\Rightarrow$ The same class have infinite different representatives.

Theorem $[a] = [b]$ iff $a \equiv b \pmod n$

$[a] \cap [b] = \emptyset$ iff $a \not\equiv b \pmod n$

---

let $c \in [a] \cap [b]$. $a \not\equiv b \pmod n$.

$c \in [a]$ so $n = c \pmod n$

$c \in [b]$ so $b \equiv c \pmod n$.

$\Downarrow$

$a \equiv b \pmod n$

contra

Corrollary: $a \in \mathbb{Z}$

(1) write $a = qn + r$, then $[a] = [r]$.

(2) There are exactly n cong classes $[0], [1], \cdots [n-1]$

proof: (1) $n \mid a - r$, so it indicate $a \equiv r \pmod n$

(2) by long division, we have unique r, $0 \le r < n$ such that $a = qn + r$.
and then by (1): $[a] = [r]$.

$$a \equiv b \pmod n \iff n \mid a-b \;/\; b = a + nk \ (k \in \mathbb{Z})$$

9.14. classnote

Section 2.2 - modular arithmetic

Def: $\mathbb{Z}_n = \{[a] \mid a \in \mathbb{Z}\} = \{[0], [1], \cdots [n-1]\}$. "+" "·"

1> addition $[a] + [b] = [a+b]$

2> multiplication $[a] \cdot [b] = [ab]$

prob: it might depend on representative.

Theo 2.6 ($+$, $\cdot$ are well defined on $\mathbb{Z}_n$)

proof: let $[a_1] = [a_2]$, $[b_1] = [b_2]$, $c \in F$ $\Rightarrow$ $n \mid a_2 - a_1$, $n \mid b_2 - b_1$

WTS : $[a_1 + b_1] = [a_2+b_2]$

$C[a_1b_1] = C[a_2b_2]$.

① For addition $n \mid (a_2-a_1) + (b_2-b_1) = (a_2+b_2) - (a_1+b_1)$

so, $(a_1+b_1) \equiv (b_2+a_2) \pmod n$

so, $(a_1+b_2) = (b_2+a_2)$

— To describe Z_n with its operation, we can use operation table.

Example: $Z_3 = \{[0], [1], [2]\}$.

①

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

②

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Theorem 2.7 (properties)

① $([a]+[b])+[c] = [a]+([b]+[c])$ associative

② $[a]+[b] = [b]+[a]$ commutative

③ $[a]+[0] = [a]$, $\forall a$

④ $[a]+[-a] = [0]$. "negative"

⑤ $([a]\cdot[b])[c] = ([a]\cdot[b])\cdot[c]$

⑥ $[a]\cdot[b] = [b]\cdot[a]$

⑦ $[a][1] = [a]$

⑧ $([a]+[b])[c] = [a][c] + [b]\cdot[c]$.

— denote:

$\forall\, n \in N \quad [a]^n = \overbrace{[a]\cdot[a]\cdots[a]}^{n \text{ times}}$

2) $[a]^0 = [1]$

Exam: calculations are become easier!!!

Ex1: Zs find $[12^7] = [12]^7$

$= [2]^7$

$= [2]^2 \cdot [2]^2 \cdot [2]^2 \cdot [2]$

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

$= [-2]$

$= [3]$ (mod 10)

Ex2: what is the last digit of 209^{2022}?

$a_n \cdot a_{n-1} \cdots a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots a_0$

So mod 10 $[a_n \cdots a_0] = [a_n 10^n] \cdots [a_0] = [a_0]$

We need $[209^{2022}] = [9]^{2022} = [-1]^{2022} = [1]$

Section 2.3 Structure → Z_n

☆ We stop using parentcess [ ] !

units: $a \in Z_n$ is called a unit
倒数 if $\exists b \in Z_n$ such that $ab = 1$
and b is called inverse of a, denoted $a^{-1} = b$

- ex1: in Z_{15}, $2 \cdot 8 = 1$. then 2 and 8 are units, $2^{-1} = 8 / 8^{-1} = 2$
- ex2: in Z_4, $3 \cdot 3 = 1$. then 3 is unit $3^{-1} = 3$.

Remarks: ① the inverse is unique!

② the inverse is also a unit. $(a^{-1})^{-1} = a$

Theorem 2.10: In $\mathbb{Z}_n$, the $[a]$ is unit $\iff$ $(a,n)=1$

$\Updownarrow$

$\exists u, v$, such that $au+nv=1$

Mzm [s]

proof: ① let $ua+vn=1$, for some $u, v \in \mathbb{Z}$.

so $[ua]+[vn]=[1]$

$\Rightarrow [u]\cdot[a]+[v]\cdot[n]=[1]$

$\Rightarrow [u]\cdot[a]=[1]$.

$\Rightarrow [a]^{-1}=[u]$

② let $[a]$ is a unit, then $\exists b \in \mathbb{Z}_n$, such that $[a \cdot b]=1$

so $ab \equiv 1 \pmod n$

then $ab=1+nk$ for some $k \in \mathbb{Z}$

$ab+n(-k)=1$

then $\gcd(a,n)=1$

Ex. in $\mathbb{Z}_{10}$, units: $[1]$ (always unit), $[3]$, $[7]$, $[9]$,

in $\mathbb{Z}_5$, units: $[1]$, $[2]$, $[3]$, $[4]$

Theorem 2.8: (part I) all non-zero element are units iff n is prime.

(part II) Zero divisors. an element $[a] \in \mathbb{Z}_n$ is a zero divisor

(i) $[a] \neq [0]$

(ii) $\exists b \neq 0 \in \mathbb{Z}_n$: $ab=0$

Example: $\mathbb{Z}_6$, $[2]\cdot[3]=[0]$, so $[2]$, $[3]$ zero divisor

$\mathbb{Z}_4$, $[2]\cdot[2]=0$, so $[2]$ zero divisor.

Theorem 2.8(11) In $\mathbb{Z}_n$, There are no zero divisor $\Leftrightarrow$ n is a prime.

proof ($\Rightarrow$) Suppose n is not a prime. "WTS there are zero divisor."

$1<|a|,|b|<n$: $n=ab \longrightarrow [n]=[a]\cdot[b]=[0]$

then, $[a][b]$ are zero divisor.

Def: A ring is a set R with two operation "Addition" / "Multiplication" such that

"+" { ① $a+b\in R$ [Closure]
② $a+(b+c)=(a+b)+c$ [Asso]
③ $a+b=b+a$
④ $0+a=a\cdot \exists 0\in R$
⑤ $\forall a.\ \exists b.\ a+b=0$ [neg] }

"·" { ⑥ $a\cdot b\in R$
⑦ $(ab)c=a(bc)$ }

⑧: $(a+b)c=ac+bc$

Ex: ① $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ (mod) } comm, with Identity.

② $2\mathbb{Z}$ = even number ↘ No.8 } comm, with Identity.

③ $M_n(R)$ = $n\times n$ matrix over R } not comm, $1=I_n$.

④ $\mathbb{N}$ not a ring

Def: - R is communitive if $\forall a,b$ $ab=ba$

- R is said to be identity / with 1 if

$\exists 1\in R$, $a\cdot 1_R=1_R\cdot a=a$

Example : The polynomial rings.

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R,\ n \in N\}.$$

Theorem (properties of +)

① 0 is unique

② The negative is also unique

③ $-(-a) = a$

proof : 1) let $0_1, 0_2$ are 0

then $0_1 \overset{0_2}{=} 0_1 + 0_2 \overset{0_1}{=} 0_2$

2) let b_1, b_2 are negative $\to a$.

$b_1 = b_1 + 0 = b_1 + a + b_2 = 0 + b_2 = b_2$

3) let $b = -a$ [wts $-b = a$, ie $a + b = 0$] $\Rightarrow$ $a + b = a + (-a) = 0$

$\Downarrow$

$-(-a) = a$

Def: Subtraction is defined $a - b = a + (-b)$

Theorem 3.4 (cancellation for +)

if $a + b = a + c$, then $b = c$

proof : $a + b + (-a) = a + c + (-a)$

$b = c$

QED

Def: $S \subseteq R$ is called sub-ring if it is a ring with same operation as R.

$2\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq R \subseteq \mathbb{C}$

Z_n is not a subring $\to R$.

ie. $M_n(\mathbb{Z}) \subseteq M_n(R)$: Subring

Thm 3.2 $S \subseteq R$ it is subring.

Show $\iff$ ① Closure for $+$
② 0 of $R \in S$
③ Closure for $\cdot$
④ $\forall a \in S$: $-a \in S$

!!! • $0_R \in S$
• Closure $a, b \Rightarrow$ Subtraction $\forall a, b \in S$, $a-b \in S$
• Closure to $\cdot$

Example: ① $S = \mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is subring

proof: ① let $a = b = 0$. then $a + b\sqrt{2} = 0 \in S$

② Assume $a_1 + \sqrt{2}b_1 \in S$; $a_2 + \sqrt{2}b_2 \in S$. ($a_1, a_2, b_1, b_2 \in \mathbb{Z}$)

then $(a_1+\sqrt{2}b_1) - (a_2+\sqrt{2}b_2) = (a_1 - a_2) + \sqrt{2}(b_1 - b_2) \in S$

③ $(a_1+\sqrt{2}b_1)(a_2+\sqrt{2}b_2) = a_1a_2 + \sqrt{2}a_1b_2 + \sqrt{2}a_2b_1 + 2b_1b_2$

$= (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \in S$

Ex2 let $S = \{0, 3\} \subseteq \mathbb{Z}_6$ subring

proof: i) in $\mathbb{Z}_6 = [0] \Rightarrow 0 \in S$

ii) $0-0 = 0 \in S$
$0-3 = 3 \in S$
$3-0 = 3 \in S$
$3-3 = 0 \in S$
$\Rightarrow$ Closure to Sub

iii) $0 \cdot 0 = 0 \in S$
$0 \cdot 3 = 0 \in S$
$3 \cdot 0 = 0 \in S$
$3 \cdot 3 = 3 \in S$
$\Rightarrow$ Closure to $\cdot$

[Remarks: $\mathbb{Z}_6$ and S have different 1's $1_{\mathbb{Z}_6} = 1$; $1_S = 3$]

Ex 3.

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in R \right\} \leq M_2 R$$

proof: i) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in D$ where $a = b = 0$

Notice $M_2(R)$ and D have same 1's. D is comm. but $M_2(R)$ is not.

ii) Sub: $\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in D$

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{pmatrix} \in D$$

iii) $$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{pmatrix} \in D$$

3.2 - properties of rings.

theorem 3.5 (properties of $\cdot$)

① $a \cdot 0 = 0$. "0" is unique (defined in addition)

② $a(-b) = (-a)b = -(ab)$

③ $(-a)(-b) = ab$

④ $-(a+b) = -a - b$; $-(a-b) = -a + b$

⑤ If $1 \in R$, $-a = (-1) \cdot a$

proof: ① $a \cdot 0 = a(0+0) \xrightarrow{\text{distrib}} a0 + a0$

By cancellation law. $a0 = 0$ Similarly $0 \cdot a = 0$

② → WTS $a(-b) + ab = 0$

$\bigcirc$ - WTS $ac(-b)+ab=0$

$\downarrow$

$ac(-b)+ab \overset{dis}{=} a((-b)+b) \overset{by(1)}{=} 0 \Rightarrow ac(-b) = -(ab)$

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

⑤ $(-1)\cdot a + a = 0$ "WTS"

$\Downarrow$

$(-1)a + 1(a) = (1+(-1))a = 0\cdot a = 0 \Rightarrow -a = (-1)a$

3.2 Properties → rings

Units : let R be a ring, then $x \in R$ is a unit if $\exists y \in R, xy = yx = 1$

$y \in R$ is an inverse of x, and unique $y = x^{-1}$.

Ex. — unit in $\mathbb{Z}$: ± 1

— unit in $\mathbb{Z}_n$: $[n]$ where $(n,k)=1$

— unit in $\mathbb{Q}$: all but $0 = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

— unit in R : R^*

Note: 0 is never a unit and 1 is always a unit.

Def: if R is communicative and all non-zero of R are units.

then R is a field.

Ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p \to$ prime.

Zero divisor : Def: an element $X \in R$ is zero divisor

if

if $x \neq 0$ and $\exists y \neq 0 \in K$

such that $xy = 0$ or $yx = 0$

Ex: • $\mathbb{Z}_4$: $2 \cdot 2 = 0 \Rightarrow x = y = 2 = 0 \pmod 4$

• $M_2(R)$: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0_{M_2(R)}$

• $\mathbb{R}^2$: $(1,0)(0,1) = (0,0) = 0_{\mathbb{R}^2}$

Def: if R is communicative and has no zero divisor, then R is called integral domain

Ex: $\mathbb{Z}$, $\mathbb{Z}_p \to$ prime,

Theorem 3.7. [multi. cancellation]

R be an "int. domain", then if $ab = ac$, and $a \neq 0$, then $b = c$.

proof: let $ab - ac = 0 \Rightarrow a(b-c) = 0$

let R is an int domain

so $a = 0$ or $b - c = 0$

$\Rightarrow b = c$

Claim: A unit is never zero divisor $\Leftrightarrow$ zero divisor is never unit

Suppose x is unit, and that $xy = 0$ (WTS $y = 0$)

$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1} \cdot 0 = 0$

Similarly if $yx = 0 \Rightarrow x = 0$ as well

Remark: an element can be neither a unit / zero divisor.

for example: $2 \in \mathbb{Z}$.

Colloray 3.8: if R is a field, then int-domain R.

Section 3.3 - homosphism / isomorsphism

"idem" compare the algebraic info $\to$ rings.

Def: R, S are rings, a function $f: R \to S$ is homosphism, if

(a) $f(a+b) = f(a) + f(b)$ (+ in R on the left, + in S on the right)

(b) $f(ab) = f(a) \cdot f(b)$ ($\cdot$ in R on the left, $\cdot$ in S on the right)

Example: ① $f: R \to S$, $f(x) = 0_S$ is a homomorphism

(a) $f(x+y) \overset{?}{=} f(a) + f(b)$, $0_S = 0_S + 0_S$ ② $f(xy) \overset{?}{=} f(a) \cdot f(b)$, $0_S = 0_S \cdot 0_S$

③ $\varphi_n : \mathbb{Z} \to \mathbb{Z}_n \Rightarrow$ homomorphism

$\varphi_n(a) = [a]$.

(a) $\varphi_n(x+y) = \varphi_n(x) + \varphi_n(y)$, $[x+y] = [x] + [y]$, By def of $\mathbb{Z}_n$, satisfied

(b) $\varphi_n(xy) \overset{?}{=} \varphi_n(x) \quad \varphi_n(y)$; $[xy] \overset{\checkmark}{=} [x] \cdot [y]$

④ $f: \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x$ } isomorphism

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

$f(ab) = 2ab \neq 2a \cdot 2b = f(a) \cdot f(b)$

$2 = f(1,1) \overset{?}{\neq} f(1) \cdot f(1) = 4$

Remark: composition of homom is a homom.

Theorem 3.10.(1) $f: R \to S$ is homom

① $f(0_R) = 0_S$

② $f(-a) = -f(a)$

③ $f(a-b) = f(a) - f(b)$

proof: (1) $f(0_R) = f(0_R + 0_R) \overset{\text{homo}}{=} f(0) + f(0) \Rightarrow f(0_R) = 0_S \in S$

(2) $f(-a) + f(a) \overset{\text{homom}}{=} f(a-a) = f(0_R) = 0_S \in S$

$\Downarrow$

$f(-a) = -f(a)$

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

Def: $f: R \to S$ homom, the $\mathrm{Im} f = \{f(r) \mid r \in R\} \subseteq S$ (subring)

$\ker f = \{r \in R \mid f(r) = 0_S\} \subseteq R$ (subring)

Claim (i): $\mathrm{Im} f = S$ iff f is surjective

(ii) $\ker f = \{0_R\}$ iff f is injective (one on one)

proof(ii): "$\Leftarrow$" ✓ obvious

"$\Rightarrow$" let $f(a) = f(b)$ - ("WTS $a = b$)

$f(a) - f(b) = 0_S$

$f(a-b) = 0_S \longrightarrow a-b$ is in $\ker f = \{0\}$.

then $a-b$ must be $0 \Rightarrow a = b$. ▨

Back to Example: ① $f: R \to S$ $f(x) = 0_S$.

$\mathrm{im} f = \{0_S\}$ not surj

$\ker f = \{r \in R \mid 0_S \in 0_S\} = R$ is not inj

② $\varphi_n : \mathbb{Z} \to \mathbb{Z}_n$

$\mathrm{Im} f = \mathbb{Z}_n$ is surj

$(\forall [a] \in \mathbb{Z}_n \quad f(a) = [a])$

$\ker = \{a \in \mathbb{Z} \mid \varphi_n(a) = [0]\} = \{a \mid [a] = [0]\}$.

$= \{a \mid a \equiv 0 \pmod n \Leftrightarrow n \mid a\} = n\mathbb{Z}$

$= \{nk \mid k \in \mathbb{Z}\}$

$\longrightarrow \varphi_n$ is not inj

③ $f: R \to M_2(R)$

$f(x) = \begin{pmatrix} x & 0 \\ \cdot & \cdot \end{pmatrix}$

$f(x) = (0, x)$

f is not surjective $\Rightarrow$ counter $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(R)$

$\ker f = \left\{ x \in R \mid \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \Rightarrow x = \{0_R\}. \Rightarrow f$ is injective.

Def: A homom function $R \to S$ is an isomorphism if it is homom + bijective (surj + injective)

if there is such a function, we say R and S are isomorphsic $R \cong S$

$\Downarrow$

R, S are in same ring.

判断 no 用 int-domain

Example: ① identity: $R - R$ } is isomorphism
$id_f(x) = x$

Example: $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in R \right\} \subseteq M_2(R)$ (subring)

Claim $f: K \to \mathbb{C}$ $\longrightarrow$ isophism

$f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + ib.$

Sec 4.1/4.2 $\quad \mathbb{Z}, \mathbb{Q}, R, \mathbb{C}, \mathbb{Z}_p, M_2(R)$

Polynomial Def: $R[x]$ the polynomial ring generate by R, with element of the form

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

$g(x) = b_0 + b_1 x + \cdots b_r x^r$

ex: $3x^2 + 2x = f_1(x)$ } add satisfied.
$2x - 1 = g(x)$ } mul

i) $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x_1 + \cdots + (a_r + b_r)x^r + \cdots (a_n)x^n$

ii) $f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_r x^{n+r}$

Def: degree denoted $\deg(f) = n$, where a_n is the largest non-zero coefficient

Theorem: if R is int domain, then in $R[x]$, $\deg(f \cdot g) = \deg f \cdot \deg g$

Counterif: in $\mathbb{Z}_4[x] \Rightarrow (2x^2+1)(2x^2-1) = \underset{\| \; 0}{4x^4} - 1 \quad \deg(f \cdot g) = 0 \neq \deg f \cdot \deg g$

⚠: $\deg[0]$ $0 \in R[x]$ $0 \cdot x^0 + 0 \cdot x^1 + \cdots$ no $a_n \neq 0$

Calculation: field polynomial

Division algorithm. in $Q[x]$.

$$\begin{array}{r|l} x^3 - x + 2 & x^2 - x \\ \hline x^3 + x^2 & \\ \hline -x^2 - x + 2 & \\ -x^2 - x & \\ \hline 2 & \end{array}$$

$x+1$

In $\mathbb{Z}$

$a, b \in \mathbb{Z}$, with $|b| \leq |a|$, $\exists!\ q, r$ st $bq + r = a$ and $0 \leq r \leq |a|$

In $F[x]$, F is field ($\mathbb{Q}, \mathbb{Z}_p, \mathbb{R}$)

$\forall f(x), g(x) \in F[x]$, $\deg g \geq \deg f$ $\exists!\ q(x), r(x)$, st $f(x) \cdot q(x) + r(x) = g(x)$

$\deg(r(x)) \leq \deg q(x)$ or $r(x) = 0$

$\Rightarrow (x+1)(x^2 - x) + 2 = x^3 - x + 2$

Ex. In $\mathbb{Z}_5[x]$, $2x^3 + 4$

$$\begin{array}{r|l} 3x^4 + 4x^3 + 2 & 4x + 2 \\ \hline 3x^4 + x & \\ \hline 4x^3 - x + 2 & \\ 4x^3 + 3 & \\ \hline -x - 1 & \end{array}$$

$\Rightarrow 3x^4 + 4x^2 + 2 = (2x^3 + 4)(4x + 2) + (4x + 4)$

Divisibility: "$2 \mid 6 \Rightarrow 3 \cdot 2 = 6$"

in $\mathbb{Z}$, if $a \mid b$, then $\exists c \in \mathbb{Z}$, $ac = b$

in $F[x]$, if $f(x) \mid g(x)$, then $\exists h(x)$, $h(x) f(x) = g(x)$

Theorem 4.7

(1) If $a(x) \mid b(x) \iff c \cdot a(x) \mid b(x)$ $c \in F^*$ (since $x+1 \mid x^2+2x+1$, then $2(x+1) \mid x^2+2x+1$)

(2) $a(x) \mid b(x) \Rightarrow \deg(a) \leq \deg(b)$

Proof: (1) WTS $c \cdot a(x) \mid b(x)$

- $a(x) \mid b(x) \Rightarrow \exists g(x)$, st $a(x) \cdot g(x) = b(x)$.
- consider $c \cdot a(x)$, as F is a field, then we have $c^{-1} \in F$
- so $(c \cdot a(x)) \cdot \underbrace{(c^{-1} g(x))}_{h(x)} = c \cdot c^{-1} \cdot a(x) \cdot g(x) = b(x)$.

then $c \cdot a(x) \mid b(x)$.

(2) WTS $\deg(a) \leq \deg(b)$

- $a(x) \mid b(x) \iff \exists g(x)$, st $a(x) \cdot g(x) = b(x)$
- F is an integer domain, so $\deg(a \cdot b) = \deg(a) + \deg(b)$.

$\deg(a \cdot g) = \deg(a) + \deg(g) = \deg(b)$.

since $\deg(a) = \deg(b) - \deg(g)$.

As $\deg \geq 0 \Rightarrow \deg(a) \leq \deg(b)$

If $a(x) \mid b(x) \cdot c(x) \wedge (a(x), c(x)) = 1$

$\Rightarrow$ ...

"GCD" $\exists f, g\ ((a(x), b(x)) = a(x) \cdot f(x) + b(x) \cdot g(x)$

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

WTS: $\exists \phi(x)$. st $\varphi(x)\, a(x) = b(x)$

- $a \mid bc \Rightarrow \exists d.\ ad = bc$
- $\gcd = 1 \Rightarrow 1 = af + cg \Rightarrow 1 - af = cg$
  $\Rightarrow adg = b(1-af)$

$adg = b - abf$

$a(dg + bf) = b$

$\varphi(x)$. so. $a \cdot \varphi = b$ ▨

GCD: $f(x), g(x) \in F[x]$

$h(x) = (f(x), g(x)) =$ GCD of f/g is the polynomial

① $h(x) \mid f(x)$ and $h(x) \mid g(x)$

② $\forall d(x),\ d(x) \mid f(x), g(x) \Rightarrow \deg(d(x)) \leq \deg(h(x))$

③ $h(x)$ is a monic ($a_n = 1$)

Def: Monic associate of $f(x)$, when f has leading coefficient in F ex. $x^3 + 2x + 2$. ✓ $2x+1$. ✗

$f(x), g(x)$ are associates if $f(x) = c \cdot g(x)$ for some $c \in F$.

$2x + 2 \overset{\text{monic}}{\Rightarrow} 2^{-1}(2x+2) = x+1$.

Aside: $2 \mid 6 \Rightarrow -2 \mid 6$ in integer. we count 0, ± 1 does all included. (c is unit, if $cd = 1$)

In $F(x)$ our unit are all of F^*

In $F(x)$, $0 \cdot (x+2) \cdot g(x) = 1$, $\frac{1}{x+2} \notin Q[x]$.

② $\deg(x+2) + \deg(x) = 0 \Rightarrow$ "$\deg(g(x))$ can not be zero"

GCD Caculation

In $\mathbb{Z}$: $(24, 142) = (24, 22) = (22, 2) = (2, 0)$

In $R[x]$: $(x-1, x^3-1) = (x^2+x+1, 0) = x^2+x+1$

$(1, x - \frac{1}{2})$ stop !!!

$\deg(1) = 0$

$(5x+4x+1,\ x^2+1)$ in $\mathbb{Z}_5$ $\Rightarrow$ $(x+1,\ 3x^2+4x+1) \Rightarrow x+1$

$$
\begin{array}{r}
2x^3+4x^2+4x \\
3x^2+4x+1 \overline{)\ x^5+1} \\
x^5+3x^4+2x^3 \\
\hline
-3x^4-2x^3+1 \\
-3x^4-4x^3-x^2 \\
\hline
2x^3+x^2+1 \\
2x^3+x^2+4x \\
\hline
x+1
\end{array}
$$

$$
\begin{array}{r}
3x+1 \\
x+1 \overline{)\ 3x^2+4x+1} \\
3x^2+3x \\
\hline
x+1 \\
x+1 \\
\hline
0,
\end{array}
$$

$(x+1,\ 0)$

4.3^4.4

Factoring

Roots

Def: $f(x) \in F[x]$. We say $f(x)$ is irreducible, if it only trivial (constant, associative).

ex. $x^2+1 = 2\left(\frac{1}{2}x^2+\frac{1}{2}\right)$

const; associative: $cf(x)$ $c \in F^*$

Irreducibility: depend on F

x^2+1 in $\mathbb{C}[x]$ $= (x+i)(x-i)$

x^2+1 in $\mathbb{Z}_2$ $= (x+1)\cdot(x+1)$

Def: $f(x) \in F[x]$ is reducible if $\exists g(x), h(x)$ nontrivial s.t. $f(x) = g(x)\cdot h(x)$.

Ie: irreducible in $F[x]$ is the prime in $\mathbb{Z}$.

Recall: $f(x) \mid g(x)\cdot h(x) \Rightarrow \mathrm{GCD}(f(x), g(x)) = 1 \Rightarrow f(x) \mid h(x)$.

proof: if $p(x)$ is irreducible $\iff$ ($p \mid ab \Rightarrow p \mid a$ or $p \mid b$)

"$\Rightarrow$" $p(x)$ irreducible. "WTS $p \mid a\cdot b \Rightarrow p \mid a$ or $p \mid b$."

Case I: $(p, a) = P \Rightarrow p \mid a$

Case II: $(p, a) = 1$ (constant) by recall, $p \mid b$.

In both cases $p \mid a$ or $p \mid b$.

"$\Leftarrow$" if $p \mid ab$ and $p \mid a$ or $p \mid b$.

$p = ab \Longrightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$ (wlog)

$b, a \mid p$ and $p \mid a$, then a is associtive of b. which means it is trivial

Collary

if $p(x)$ is irreducible, and $p(x) \mid a_1(x)\, a_2(x) \cdots a_n(x)$

then $\exists\, a_i(x)$, st $p(x) \mid a_i(x)$

Proof: ie $p \mid a_1 \cdots a_n$, then $p \mid a_1 \cdot (a_2 \cdots a_n)$

By theorem $p \mid a_1$ or $p \mid a_2 \cdots a_n$

Case I. proof done

Case II. $p \mid a_2 \cdots a_n$, we can repeat the process, and finilly $p \mid a_{n-1} \cdot a_n$ must have one $\exists$.

Theorem.

all $f(x) \in F[x]$ can be written as product of irreducible. unique / exist

"In $\mathbb{Z}$, all number can be $\rightarrow$ product of primes"

Proof: let $f(x) = a_1(x) \cdot a_2(x) \cdots a_n(x)$ where some a_i is reducible $a_i(x) = b_i(x) \cdot c_i(x)$.

then $f(x) = a_1 \cdot a_2 \cdots (b_i \cdot c_i) \cdots a_n$

$\Downarrow$

Eventually: we will have irreducible / poly. deg ≥ 1

Eventually we will have irreducible / poly deg > 1

if b_i or c_i are reducible, then repeat will this end?

$$k = \deg(f(x)) = \deg(a_1 \cdots a_n) = \deg a_1 + \deg a_2 + \cdots + \deg a_n$$

$$a_i = b_i \cdot c_i \quad (\deg \geq 1) \quad \text{then } \deg(a_i) \geq 1$$

Theorem: Factoring irreducible in $F[x]$ is unique upto units and order

$$(x^2-1) = (x+1)(x-1) = (x-1)(x+1) = (2x+2)(\tfrac{1}{2}x - \tfrac{1}{2})$$

proof: let $f(x) = a_1 x \cdots a_n x = b_1 x \cdots b_k x$

$a_1 \mid b_1 x \cdots b_k x$, $\exists\, b_j$ st $a_i \mid b_j$

WLOG. let $b_j = b_1$.

$a_1(a_2 \cdots a_n) = b_1(b_2 \cdots b_k)$

$a_2 \cdots a_n = b_2 \cdots b_k$

$a_2 \mid b_2 x \cdots b_k x$, $\exists\, b_3$ st $a_2 \mid b_3$

$a_2(a_3 \cdots a_n) = b_2(b_3 \cdots b_k)$

$(a_3 \cdots a_n) = (b_3 \cdots b_k)$

Case I. if $k = n$, then end with $1 = 1$

if $n > k$, then eventually we will have some $a_{k+1} \cdots a_n = 1$

as $a_{k+1} \cdots a_n$ each have $\deg(a_i) \geq 1$, and $\deg(1) = 0$ which contradicts a

Similarly for $k < n$

Roots: if $f(a) = 0 \Rightarrow a$ is a root $x-a$ is a factor of f. $f(x) = x^2 - 1$, $f(1) = 0 \Rightarrow (x-1) \mid (x^2-1)$

Polynomials: just an arrangement, to do evaluations)

$\varphi_a(f(x))$: The evaluation non-momorphism

.

$\varphi_a : F[x] \to F$

by homomor ① $\varphi_a(f(x)+g(x)) = \varphi_a(f(x)) + \varphi_a(g(x))$

$= f(a) + g(a)$

② $\varphi_a(f(x) \cdot g(x)) = f(a) \cdot g(a) = \varphi_a(f(a)) \cdot \varphi_a(g(a))$

$\varphi_a(f(x)) = f(a)$ ⇓ φ is homo

Def: $a \in F$ is a root of $f(x) \in F[x]$ iff $\varphi_a(f(x)) = 0_F$

Theorem: $\varphi_a(f(a)) = 0 \iff (x-a) \mid f(x)$

"$\Rightarrow$" let divide f by $(x-a)$. $(x-a)\cdot q(x) + r = f(x)$ $(r \in F)$

$\varphi_a((x-a)\cdot q(x) + r) = \varphi_a((f(a))$

$(a-a)q(x) + r = f(a) = 0 \Rightarrow r = 0 \Rightarrow (x-a) \mid f(x)$.

$\Leftarrow$ $(x-a) \mid f(x) \Rightarrow (x-a)\cdot g(x) = f(x)$

$\varphi_a(x-a)\cdot g(x) = \varphi_a f(x)$

$(a-a)\cdot g(a) = f(a)$

$0 = f(a)$

Corollary:

- If $f(x)$ is irred, and $\deg(f) \geq 2$, then $f(x)$ has no roots.

> f: the only factor are $c / f(x)$
> but a root is a factor of $\deg(1)$

- If $f(x)$ has no roots and $\deg(f) \leq 3$, then f is irred

  supp: $f = ab$, $\deg(f) = \deg(a) + \deg(b)$

if f has $\deg(2)$, $2 = 2+0$ ← trivial. $2 = 1+1$ ← contridict

if f has $\deg(3)$. $3 = 3+0$ ← trivial $3 = 2+1$ ← root.

if f has $\deg(4)$ $4 = 2+2$ (trib)

$f(x) = x^3 - x$ in $\mathbb{Z}_3$

① $x(x^2-1) = x(x+1)(x-1)$

② $\begin{cases} f(0) = 0, \text{ then } (x-0) \mid f \\ f(1) = 1-1 = 0, \text{ then } x-1 \mid f \\ f(2) = 2-2 = 0 \text{ then } x-2 \mid f \end{cases} \Rightarrow f(x) = x(x+1)(x+2)$

in $\mathbb{Q}(x)$ $x^2+1 \to$ irredu

① in $\mathbb{C}[x]$ x^2+1 is reducible $(x+i)(x-i)$
but $i \notin \mathbb{Q}$, then in $\mathbb{Q}$ is irred

x^3+x+1 in $\mathbb{Z}_5$.
$f(0) = 1 \quad x \qquad \times f(4) = -1$
$f(1) = 3 \quad x \qquad \Rightarrow$ · $\deg f \leq 3$
$f(2) = 1 \quad x$ · f has no root $\Rightarrow$ irredu
$f(3) = 1 \quad x$

② Assume $x^2+1 = (ax+b)(cx+d)$

$x^2+1 = acx^2 + (bc+ad)x + bd$

$0 = (ac-1)x^2 + (bc+ad)x + (bd-1)$

$\Downarrow$

$ac = 1$, $bd = 1$, where $ac+bd$ can not be 0

$M_2(R)$

$I_{M_2(R)} = e_{11} + e_{22}$

$\subseteq M_2(R)$ I.

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

- Given poly in $\mathbb{Q}[x]$, we can always find associate of $f(x)$ in $\mathbb{Z}[x]$
- what connection factorization in $\mathbb{Q}[x] \Leftrightarrow \mathbb{Z}[x]$?

proper factorization in $\mathbb{Z}[x]$ is also a factorization in $\mathbb{Q}[x]$

but ····· in $\mathbb{Q}[x]$ does not necessary $\longrightarrow \mathbb{Z}[x]$

Theorm ∀ fact in $\mathbb{Q}[x]$ can be fixed in fact in $\mathbb{Z}[x]$

$$x^2-1 = (\tfrac{1}{2}x-\tfrac{1}{2})(2x+2)$$

$$\overset{\text{fix}}{=} (x-1)\cdot(x+1)$$

claim $p \to$ prime. def: $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$

$$\phi_p(a_n x^n + \cdots + a_0) = [a_n]x^n + \cdots [a_1]x + [a_0]$$

is a homo surjective "reduction modulo p"

lemma 4.22 $g(x), h(x) \in \mathbb{Z}[x]$, p is prime. if $p \mid g\cdot h$ (p divide every coefficient of $f\cdot g$)

then $p \mid g(x)$ or $p \mid h(x)$

proof if $p \mid g\cdot h$ then $\phi_p(g\cdot h) = 0$

$\phi_p g(x) \cdot \phi_p h(x)$ $\quad p\mid g(x) \Uparrow \quad p\mid h(x) \Uparrow$

but $\mathbb{Z}_p[x]$ is int-domain $\Rightarrow \phi_p(g)=0$ or $\phi_p(h)=0$

"Gauss's lemma" Thm 4.23 $f(x) \in \mathbb{Z}[x]$, non-constant

$f(x) = g(x)\cdot h(x)$ for some $g_1, h_1 \in \mathbb{Q}[x]$ of deg $= n/m$

$\iff$ $f(x) = g_2(x)\cdot h_2(x)$ for some $g_2(x), h_2(x) \in \mathbb{Z}[x]$ of deg $= n/m$

proof: "$\Leftarrow$" is obvious

"$\Rightarrow$" Given $f(x) = g_1(x)\cdot h_1(x)$, multiply by commen denomenator

$af(x) = g_2(x)\cdot h_2(x)$, $g_2, h_2 \in \mathbb{Z}[x]$

if p is prime factor $\to a$, $p \mid a$

then $p \mid g_2(x)\cdot h_2(x) \xrightarrow{\text{lemma}} p \mid g_2$ or $p \mid h_2$. so we can divide by p

$a' = \frac{"a"}{p} f(x) = \frac{g_2(x)}{p}\cdot h_2(x)$ or $g_2(x)\cdot \frac{h_2(x)}{p}$

keep dividing by prime factor of a, until $a' = \pm 1$. and thus $\Rightarrow \pm f(x) = g_n(x)\cdot h_n(x)$ of deg m/n.

Tools from $\mathbb{Z} \Rightarrow$ Tools in $\mathbb{Q}[x]$

(1) divisnn root

Theorem 4.21 rational root test

$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$

if $(r,s)=1$ and $\frac{r}{s} \neq 0 \Rightarrow$ of $f(x)$ = root then $\begin{cases} r \mid a_0 \\ s \mid a_n \end{cases}$

proof: $f(\frac{r}{s}) = a_n \frac{r^n}{s^n} + \cdots + a_1 \frac{r}{s} + a_0 = 0$

s divides

$a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$

r divids $\cdots$

$r \mid -a_0 s^n = a_n r^n + \cdots a_1 r s^{n-1} \Rightarrow r \mid a_0$ as $(r,s)=1$

similary $s \mid -a_n r^n = a_{n-1} r^{n-1} + \cdots a_n s^n \Rightarrow s \mid a_n$ as $(r,s)=1$. ▨

Ex ① $f(x) = \frac{1}{2}x^3 + x + \frac{1}{2} \Rightarrow 2f(x) = x^3 + 2x + 1$

if $\frac{r}{s}$ is root $\rightarrow f(x)$, then $r \mid 1$ and $s \mid 1$ $\begin{cases} 1 = \pm 1 \\ s = \pm 1 \end{cases} \Rightarrow \frac{r}{s} = \pm 1$

$g(1) = 4 \neq 0 \quad g(-1) = -2 \neq 0$

then no root in $\mathbb{Q}[x]$. $\Rightarrow g(x)$ has no root and $\deg g = 3 \Rightarrow \mathbb{Q}[x]$ is irreducible.

② $f(x) = 2x^4 + x^3 - 121x^2 - 14x + 12$

if $\frac{r}{s}$ is root $r \mid 12$, $s \mid 2$

$\rightarrow \frac{r}{s} = \pm 12, \pm 6, \pm 4, \pm 3, \pm \frac{3}{2}, \pm 2, \pm 1, \pm \frac{1}{2}. \Rightarrow$ roots $(\frac{1}{2}), (-3)$

$\rightarrow (x - \frac{1}{2}) \cdot (x+3) \mid f(x)$

$f(x) = (x - \frac{1}{2})(x+3) \cdot (2x^2 - 4x + 8)$ ("+2")

$(x - \frac{1}{2})$: irre; $(x+3)$: irre; $(2x^2 - 4x + 8)$: irre

Tool 2. reduction "mod p" p be prime

Theorem 4.25 let $f(x) = a_n x^n + \cdots + a_1 x + x_0 \in \mathbb{Z}[x]$

st $p \nmid a_n$. then if $\phi_p(f)$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$

proof: if $f(x)$ is reducible so $f(x) = g(x) \cdot h(x)$; $g, h \in \mathbb{Z}[x]$ (by Gauss's lemma)

$\phi_p(f) = \phi_p(g) \cdot \phi_p(h)$ $\deg(m,n)$

as $p \nmid a_n$, the $\deg(\phi_p f) = \deg f \Rightarrow \deg \phi_p(g) = \deg(g)$

so $\phi_p(f)$ is also reducible.

by contrapositive $\rightarrow$ ▨

Ex $f(x) = x^3 + 2x + 2$

$\begin{cases} -c^2 + b + \frac{1}{b} = 0 \\ bc + (-c) \cdot \frac{1}{b} = 0 \end{cases}$.

$\varphi_2(f) = x$

$\varphi_3(f) = x^3 + 2x + 2$

check root $x=[0] \Rightarrow \varphi_3(f) = 2$ ×

$x=[1] \Rightarrow \varphi_3(f) = 1$ ×

$x=[2] \Rightarrow \varphi_4(f) = -1$ ×

} no root, so $\varphi_3(f)$ is irreducible.

$\frac{b^2-c^2+1}{b} = 0 \quad \frac{b^2c-c}{b} = 0.$

$b^2 = c^2 - 1 \qquad (c^2-1)c = 0$

$c = \pm 1$

Ex2 $f(x) = x^5 + 8x^4 + 3x^3 + 4x + 7$

$\varphi_2(f) = x^5 + x^3 + 1$

no roots $\Rightarrow$ x linear factors

if $\varphi_2(f)$ is reducible $= (x^2+bx+c)(x^3+\cdots+)$

easy that the only irredu polyno $\to 2$ in $\mathbb{Z}_2[x]$ is

x^2+x+1 ! if reducible $(x^2+x+1)(x^3+ax^2+bx+c)$

$\mathbb{Q}[x]$ ire $\Leftarrow$ $\varphi_2(f)$ ire $\Leftarrow$ no solution $\Leftarrow$

$1+a = 0 \Rightarrow a = -1$ contradiction

$1+a+b = 1$

$a+b+c = 0 \Rightarrow a = 0$

$b+c = 0 \Rightarrow b = -1$

$c = 1$

!!! **Tool 3**

Eisenstein's criterion

Theorem 4.24. let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_n$

$\exists$ p prime num $\begin{cases} p \nmid a_n \\ p \mid a_{n-1}, \cdots a_1, a_0 \\ p^2 \nmid a_0 \end{cases}$ then $f(x)$ is irreducible.

proof: Assume $\exists p \to$ prime ①.②.③ and f is reducible

$f(x) = g(x) \cdot h(x) = (b_m x^m + \cdots + b_0)(C_n x^n + \cdots + C_0)$

By Gauss's lemma. $h(x), g(x) \in \mathbb{Z}[x]$.

$\Rightarrow \varphi_p(f) = [a_n] x^n = \varphi_p(g \cdot h) = \varphi_p(g) \cdot \varphi_p(h) = [b_m] x^m \cdot [C_k] x^k$

$\Rightarrow [b_0] = [C_0] = [0]. \Rightarrow p \mid b_0, C_0 \Rightarrow p^2 \mid b_0 C_0 = a_0 \Rightarrow$ contradiction

① $22x^5 + 27x + 15 \Rightarrow p = 3$

② $2x^7 + 16x^3 + 20 \sim x^7 + 8x^3 + 10 \Rightarrow$ prime $= 2$ - irreducible

$x^n - p$ prime

4.6 — irreducible in $\mathbb{R}[x]$ and $\mathbb{C}[x]$

Theo 4.26 [the fundamental theo of algebra]

Every non-const poly has a root in $\mathbb{C}$ [$\mathbb{C}$ algebraically closed].

$\Leftrightarrow$ only irreducible in $\mathbb{C}[x]$ are linear

lemma: 4.29. if $z \in \mathbb{C}$ is a root of $f(x) \in \mathbb{R}[x]$, then so is $\bar{z}$.

Notice $(x-z)(x-\bar{z}) \in \mathbb{R}[x]$

Theorem 4.30. irreduci $\to$ polynom in $\mathbb{R}[x]$ are (cond) the linear one $+ ax^2+bx+c$ $b^2-4ac<0$

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

$\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \Leftrightarrow \gcd(2,3)=1$.

$f(x) \in \mathbb{Z}_6[x] \Rightarrow g(x) \cdot h(x) = f(x)$ where $g(x) \in \mathbb{Z}_3[x]$ and $h(x) \in \mathbb{Z}_2[x]$

if $(x-a)(x-b) \in \mathbb{Z}_6$

then root at a = root at $[a]$ in $\mathbb{Z}_6$

then $f(x) \in \mathbb{Z}_3[x]$ has two roots

and $f(x) \in \mathbb{Z}_2[x]$ "has three roots"

Sec 5.1

Def: Fix $p(x) \in F[x]$ non-constant

$f(x)$ congruent to $g(x)$ mod $p(x)$

if $p(x) \mid f(x)-g(x)$

$\equiv$ $f(x)-g(x) = p(x)\cdot k(x)$ for some $k(x) \in F[x]$

$\equiv$ $f(x) = g(x) + p(x)\cdot k(x)$ for some $k(x) \in F[x]$

$\equiv$ $f(x) \in g(x) + p(x)F[x]$ ($p(x)$)

$f \equiv g \pmod{p}$

Ex. ① $x^2+x+1 \equiv x+2 \pmod{x+1}$

check $x^2+x+1-x-2 = x^2-1 = (x+1)(x-1)$

divisible by $p(x)$ ✓

② $\mathbb{R}[x]$ $p(x)=x^2+1$ take $2x+1 \equiv 2x+1+1\cdot(x^2+1) = x^2+2x+2$

$2x+1 \equiv 2x+1+x\cdot(x^2+1) = x^3+3x+1$

Theorem 5.1 Congruence mod $p(x)$ is equivalence relation

- symmetric: if $f(x) \equiv g(x) \bmod p(x)$ then $g \equiv f \pmod{p}$
- reflective: $f(x) \equiv f(x) \pmod{p(x)}$
- transitive: if $f \equiv g \pmod{p}$, $g \equiv h \pmod{p} \Rightarrow f \equiv h \pmod{p(x)}$

Def: the congr-class (residue class) of $f(x)$ mod $p(x)$ is the set

$$[f(x)] = \{ g(x) \in F[x] \mid f(x) \equiv g(x) \pmod{p(x)} \} = \{ f(x)+p(x)k(x) \mid k(x) \in F[x] \} = f(x)+p(x)F[x]$$

ex. $p(x) = x^2+x+1 \in \mathbb{Q}[x]$

$[0] = \{0 + p(x)k(x)\} = \{(x^2+x+1)k(x)\} = (x^2+x+1)\cdot\mathbb{Q}[x]$

$[1] = \{1 + p(x)k(x)\} = \{1,\ x^2+x+2,\ x^3+x^2+x+1, \cdots\}.$

$[x^2+x+1] = \{(x^2+x+1)\cdot k(x)\} = (x^2+x+1)\cdot\mathbb{Q}[x]$

Theorem 5.3 $[f(x)] = [g(x)] \iff f \equiv g \pmod p$

$[f] \cap [g] = \emptyset \iff f \not\equiv g \pmod p$

Cor 5.5 ① if $f(x) = q(x)\cdot p(x) + r(x)$
then $[f(x)] = [r(x)]$

② Every congruence class has a unique representative = 0 / of deg << deg(p(x))

pf: use long divison $f = q\cdot p + r$ $r=0$ or $\deg(r) < \deg(p)$ then $[f] = [r]$ unique by remainder ∎

Ex. $p(x) = x^2+1 \in R[x]$ $[6x^3+13x^2+5] = [-6x-8]$.

$$\begin{array}{r} 6x+13 \\ x^2+1 \;\overline{)\; 6x^3+13x^2+5} \\ 6x^3+6x \\ \hline 13x^2-6x+5 \\ 13x^2+13 \\ \hline -6x-8 \end{array}$$

Def: the set of all congruence classes is $\frac{F[x]}{(p(x))} := (F[x] \bmod p(x)) = \{[f(x)] \mid f(x) \in F[x]\} = \{[f(x)] \mid \begin{smallmatrix} f=0 \text{ or} \\ \deg f < \deg p \end{smallmatrix}\}$.

Ex. ① $\frac{\mathbb{Z}_2[x]}{(x^2+1)} = \{[f] \mid \begin{smallmatrix} f=0 \\ \text{or } \deg(f)<2 \end{smallmatrix}\} = \{[ax+b] \mid a,b \in \mathbb{Z}_2\} = \{[0], [1], [x+0], [x+1]\}$. finite set.

② $\frac{\mathbb{R}[x]}{(x^2+1)} = \{[ax+b] \mid a,b \in \mathbb{R}\}$ infinite set $\approx \mathbb{C}$

③ $\frac{\mathbb{Q}[x]}{x-7} = \{[a] \mid a \in \mathbb{Q}\} \approx \mathbb{Q}$

ie. $x-7 \approx 0 \Rightarrow x \approx 7$.

5.2 congru-class arithmetic

i) $[f(x)] + [g(x)] = [f(x)+g(x)]$
ii) $[f(x)]\cdot[g(x)] = [f(x)\cdot g(x)]$
} well-defined

Thm 5.6 (+· well defined in $\frac{F[x]}{p(x)}$)
if $[f_1]+[f_2]$, $[g_1]=[g_2]$ then $[f_1+g_1] = [f_2+g_2]$.
$[f_1\cdot g_1] = [f_2\cdot g_2]$.

(multi) pf: $[f_1]=[f_2] \longrightarrow f_2 = f_1 + k_1 p$
$[g_1]=[g_2] \longrightarrow g_2 = g_1 + k_2 p$
for some $k_1, k_2 \in F[x]$

$$f_2 \cdot g_2 = (f_1 + k_1 p)(g_1 + k_2 p) = f_1 g_1 + k_1 p g_1 + k_2 p f_1 + k_1 k_2 p^2$$
$$= f_1 g_1 + p(k_1 g_1 + k_2 f_1) + k_1 k_2 p^2$$
$$= f_1 g_1 + p(k_1 g_1 + k_2 f_1 + p k_1 p_2)$$
$$\Rightarrow f_1 g_1 \equiv f_2 g_2 \pmod p$$

Ex $\dfrac{R[x]}{(x^2+1)} = \{[ax+b] \mid a, b \in R\}$.

$$[ax+b] + [cx+d] = [(a+c)x + (b+d)].$$
$$[ax+b] \cdot [cx+d] = [(ac)x^2 + (ad+bc)x + bd] \longrightarrow [(ad+bd)x + (bd-ac)]$$
$$= [ac][x^2] + [\quad]x + [bd]$$
$$\Downarrow$$
$$[-1]$$

Thm 5.7 $\dfrac{F[x]}{(p(x))}$ is a ring $\Rightarrow$ $0_{\frac{F[x]}{p(x)}} = [0]$,

commutative

$$1_{\frac{F[x]}{p(x)}} = [1] \text{ unit}$$

$$-[f(x)] = [-f(x)]$$

Ex: in $\dfrac{Q[x]}{(x^2-2x+1)}$ $\quad [x^3+4x^2-5] = [\,?\,]$

$$[x^2-2x+1] = [0] \qquad [x^3+4x^2-5] = [3x-2+8x-4-5] = [11x-11].$$
$$\Downarrow \qquad\qquad \Uparrow$$
$$[x^2] = [2x-1] \Rightarrow [x^3] = [2x^2-x] = [3x-2]$$

5.2

Calculation
↓
Z_n properties
↓
non Z_n - properties
↓
C is a field

$\dfrac{R[x]}{\langle x^2+1\rangle}$

① $[2x+1] + [3x+5] = [5x+6]$

② $[2x+1] \cdot [3x+5] = [6x^2+13x+5] = [6][x^2+1] + [13x-1] = [13x-1]$

Remark: i) $\forall f \in F[x]$, $\exists!\ g(x)$ st $[f] = [g]$, and $\deg(g) < \deg(p)$ (or $g=0$)

ii) Set of representative is all polynomial of $\deg < \deg(p)$

$\Downarrow$

Ex: $\dfrac{R[x]}{\langle x^2+1\rangle} = \{[ax+b],\ a, b \in R\}$: "$[x^2+1] = 0 \Rightarrow [x^2] = [-1]$"

b) $\dfrac{Z_2[x]}{\langle x^2+1\rangle} = \{[ax+b],\ a, b \in Z_2\} = \{[0], [1], [x+0], [x+1]\}$.

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	
	Similarly

c) Units

Thm 5.9 ㊗ f is a unit iff $(f, p)=1$ $\left(\frac{F[x]}{\langle p(x)\rangle}\right)$

pf: "$\Leftarrow$" $\exists\, g, j \in F[x]$

$f\cdot g + pj = 1$

$fg = 1 - pj$

$[fg] = 1$

"$\Rightarrow$" $\exists g \in F, g\neq 0$, st $f\cdot g = 1$

$\Rightarrow f\cdot g + kp = 1 + jp$

$fg + (k-j)p = 1$

then $(f, p) = 1$ ▨

Thm 5.10 $\frac{F[x]}{p(x)}$ is a field iff $p(x)$ is irreducible

"ex $\frac{R[x]}{\langle x^2+x\rangle} = [x]\cdot[x+1]$ zero divisor.

$\Rightarrow \forall f$, if $[f]=0$, otherwise $(f, p)=1$ or p, but pick $\deg(f) < \deg(p)$ ✓

$\therefore f$ is a unit, all non zero polynomial are units.

if $p(x)$ is reducible, then $\frac{F[x]}{\langle p(x)\rangle}$ has zero divisor $\Leftrightarrow$ $p(x)$ is irreducible. ▨

Ex. $\frac{\mathbb{Z}_2[x]}{x^2+x+1}$ fields

$S = \{[0], [1], [x], [x+1]\}$.

$x^2 = [x+1]$

·	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$\Rightarrow$

① Elements don't tell you the ring in $\mathbb{Z}_n$ $\{[0], [1], [2], [3]\}$.

② $F \longrightarrow \frac{F[x]}{\langle p(x)\rangle}$ injection

③ lemma:

pf: $\varphi: F \to \frac{F[x]}{p(x)}$

$\varphi(a) = [a]$

Show homo: i) $\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a) + \varphi(b)$

ii) $\varphi(ab) = [ab] = [a][b] = \varphi(a)\cdot\varphi(b)$

- Injective: $\ker(\varphi) = \{a \mid a\in F, [a] = [0]\}$.

$\Rightarrow a = p(x)\cdot g(x) = 0$ (as $x\cdot 0 = 0$)

therefore $\ker(\varphi) = 0 \Rightarrow$ Injective

Interpret $\ker(\varphi) = 0 \Rightarrow$ injective.

Ex's: Test field: $\frac{\mathbb{Q}[x]}{x^5-15x+3}$ as by eisenstein when $p=5$. $x^2-15x+3$ is irreducible

$\Downarrow$

This is a field.

$\frac{R[x]}{x^2+2x+1}$ as $(x+1)(x+1)=0$, zero divisor $\Rightarrow$ $\times$ field.

Define $\mathbb{C}[x]$!!!

$\frac{R[x]}{x^2+1}$ as $(a+bx)(c+dx) = ac + (ad+bc)x + bdx^2$

$[x^2] = [-1]$

$= ac + (ad+bc)x - [bd]$

$= (ac-bd) + (ad+bc)x$

ie: $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$ $\quad i^2=-1 \Rightarrow i=\sqrt{-1}$

then $\mathbb{C} \cong \frac{R[x]}{x^2+1} \Rightarrow x^2+1$ is irreducible.

$\downarrow$

"sending $i \to x$"

Ideals: $\frac{\mathbb{Z}}{\langle n\rangle} \cong \mathbb{Z}_n$ $\quad \langle n\rangle = \{[n]\}$.

$\frac{F[x]}{\langle p(x)\rangle}$ $\quad R[x]/p(x)$: $x^2 = \{3x^2, x^3, x^3+\cdots\}$.

$= \{\underbrace{f(x)\cdot x^2}_{\text{"}p(x)\text{"}} \mid f \in F[x]\}$.

Properties: Absorbtion.

$\forall r \in R$, $\forall i \in I$, $ri \in I$.

$4 \in \mathbb{Z}$, $-6 \in \langle 3\rangle$, then $4(-6) \in \langle 3\rangle$.

$\langle x^2, x+1\rangle = \{(x^2)f(x) + (x+1)g(x) \mid f, g \in R[x]\}$.

$k(x) \in F[x]$

$= x^2\cdot(f\cdot k) + (x+1)(g\cdot k) \in \langle x^2, x+1\rangle$

$\langle 3, 6\rangle = \{3m+6n\}$.

$= \{3n\} = \langle 3\rangle$ principle ideal

kernal always be ideal

homo: $\varphi: \mathbb{Z} \to \mathbb{Z}$

$\varphi(a) = 3a$

$\ker(\varphi) = \{\varphi(a) = 0 = 3a \Rightarrow a = 0\}$.

$= \{0\} = \langle 0\rangle$

5.3 properties

Thm 5.9 $[f(x)]$ is a unit in $\frac{F[x]}{p(x)} \iff (f(x), g(x)) = 1$

Ex. $[x^2-1]$ is a unit in $\frac{\mathbb{Q}[x]}{(x^3-2)}$

$(x^2-1,\ x^3-2) = 1$

↓ irreducible

prop. if $p(x) \in F[x]$ is reducible, then $\frac{F[x]}{p(x)}$ has zero divisor

$f, g \neq 0$

pf) if $p(x) = f(x) \cdot g(x)$ "$\deg f, g < \deg p$", then $[f], [g] \neq 0$, but $[f]\cdot[g] = [p(x)] = [0]$.

⇓

Them 5.10 $\frac{F[x]}{p(x)}$ is a field $\Leftrightarrow$ $p(x)$ is irreducible.

Example "Are the following ring fields ?" if not point out zero divisor

- $\frac{\mathbb{Q}[x]}{x^5-15x+3}$: rep by eisenstein $\Rightarrow$ $x^5-15x+3$ is irreducible
- $\frac{\mathbb{R}[x]}{x^2+2x+1}$: No, $x^2+2x+1 = (x+1)^2 \Rightarrow$ reducible : zero divisor $[x+1]$.

Sec 6.1 Congruency (Ideals)

Q_1, To define congruency, we need only def $[0]$.

ie. How to generate congruency ? ⇓

$\mathbb{Z}_n$: $a \equiv b \pmod n$ $\quad$ Q_2, How to choose $[0]$ st. cong will be eq relation and operation defined.

⇕

$a-b \in n\mathbb{Z} = [0]$

$\frac{F[x]}{p(x)}$: $f \equiv g \pmod p$

⇕

$f-g \in p(x)F[x] = [0]$

Def: Ideal is a subring $I \subseteq R$ if $\forall r \in R$ $i \in I$: $\begin{cases} ri \in I & \text{("absorbtion")} \\ ir \in I \end{cases}$

we denote $I \lhd R$

In order to show $I \subseteq R$ is ideal, requirement : i. $0 \in I$

ii. $\forall a, b \in I$ $a-b \in I$

iii. absorbtion from both side

important

ideal $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in M(R)$.

$= \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. ideal.

Ex. ① $\{0\}$ is ideal → any rings
② R is ideal → any rings
} trivial ideals

③ $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\} = I \lhd \mathbb{Z}$ General: $n\mathbb{Z} \lhd \mathbb{Z}$

④ $(x^3+1)\mathbb{Q}[x] = \{(x^3+1)k(x) \mid k(x) \in \mathbb{Q}[x]\} \lhd \mathbb{Q}[x]$. General: $p(x)F[x] \lhd F[x]$

⑤ $I = \{a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] \mid a_0 \text{ is even}\} \lhd \mathbb{Z}[x]$.

pf i) $0 \in I$ (free coeff $= 0$ is even)

ii) $(2a_0 + a_1x + \cdots a_nx^n) - (2b_0 + b_1x + \cdots + b_nx^n)$

$= 2(a_0 - b_0)$ even (✓)

iii) $(2a_0 + a_1x + \cdots + a_nx^n)(b_0 + \cdots + b_nx^n) = 2a_0b_0 + \cdots$

($2a_0 + \cdots \in I[x]$, $b_0 + \cdots \in \mathbb{Z}[x]$, $2a_0b_0 + \cdots$ even $\in I$)

$\mathbb{Z}[x]$ is commutative, so we got absorbtion on the other side

⑤ $\mathbb{Z} \subset \mathbb{Q}$ subring but Not ideal !

ie. $2 \cdot \frac{1}{3} = \frac{2}{3} \notin \mathbb{Z}$, no absorbtion.

sets of the form "all things divisible by x" is ideal

Def: Let R be commutative, $a \in R$
$\langle a \rangle = Ra = \{ra \mid r \in R\}$. is called the Principle ideal generated by a.

Remark $x \in \langle a \rangle \iff a \mid x$

Why it is ideal ? i. $0 \in R$, $0 \cdot a \in \langle a \rangle$

ii. $r_1, r_2 \in R$, $r_1a - r_2a = (r_1 - r_2)a \in \langle a \rangle$ ($r_1 - r_2 \in R$)

iii take $(ra) \cdot r' = rr'a$ as $rr' \in R$, then $rr'a \in \langle a \rangle$

$r'(ra) = (r'r)a \in \langle a \rangle$

The $\langle a \rangle$ is ideal ▨

Ex's
- $\langle 0 \rangle = R \cdot 0 = \{0\}$.
- $\langle 1 \rangle = R \cdot 1 = \{r \mid r \in R\}. = R$
- $\langle 3 \rangle = 3 \cdot \mathbb{Z}$ for $3 \in \mathbb{Z}$
- $p(x) \in F[x]$ $\langle p(x) \rangle = p(x) \cdot F[x]$

☆ $I = \{a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] \mid a_0 \text{ is even}\} \lhd \mathbb{Z}[x]$. is not a principle ideal !

pf. Assume $I = \langle f(x) \rangle$ in $\mathbb{Z}[x]$ for some $f(x) \in \mathbb{Z}[x]$.

take $2, x \in I$, if $I = \langle f(x) \rangle$ so $f \mid 2$ and $f \mid x$ in $\mathbb{Z}[x]$ and so in $\mathbb{Q}[x]$.

$\Longrightarrow f \mid (2, x)_{\text{gcd}} = 1 \Rightarrow f = \pm 1 \Rightarrow \langle \pm 1 \rangle = \mathbb{Z}[x] \neq I$

$\Downarrow$ contradiction !

Def: R is comm, $a_1, \cdots a_n \in R$

the ideal generate by $a_1, \cdots a_n$ is

$\langle a_1, \cdots a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\} \trianglelefteq R$

Prop: $I \trianglelefteq R$

$(a_1, \cdots a_R) \subseteq I \iff a_1, \cdots a_n \in I$

"$\langle a_1, \cdots a_R \rangle$ is the smallest ideal containing $a_1, \cdots a_n$".

Ex. $I \trianglelefteq \mathbb{Z}[x]$ from before: $I = \langle 2, x \rangle = \{2 \cdot f(x) + x \cdot g(x) \mid f, g \in \mathbb{Z}[x]\}$.

pf: "$\Leftarrow$" as $2, x \in I$, then $\langle 2, x \rangle \subseteq I$

"$\Rightarrow$" let $2a_0 + a_1 x + \cdots + a_n x^n \in I$

$2a_0 + x(a_1 + a_2 x + \cdots + a_n x^{n-1}) \in \langle 2, x \rangle$ ☐

General: • In $\mathbb{Z}$ $\langle n, m \rangle = \langle \gcd(n, m) \rangle$

similarly in $F[x]$ $\langle f(x), g(x) \rangle = \langle \gcd(f(x), g(x)) \rangle$

Notice only in Field.

Congruency:

Def: Fix $I \trianglelefteq R$ for $a, b \in R$, we say a is congruent to b modulo I if $a - b \in I$

we write $a \equiv b \pmod I$

$\iff a = b + i$ for some $i \in I$

$(a) r_1 = (b) r_2$.

$a = (b)\left(\frac{r_2}{r_1}\right)$ as R is integer domain.

Ex: $I = \langle n \rangle \trianglelefteq \mathbb{Z}$

$a \equiv b \pmod I$ iff $a - b \in \langle n \rangle \iff a \equiv b \pmod n$

$a = b(r_2 \cdot r_1^{-1})$.

then. $(r_2^{-1} \cdot r_1)(r_2 r_1^{-1}) = 1_R$.

$I = \langle p(x) \rangle \trianglelefteq F[x]$

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

$I = \langle 2, x \rangle \trianglelefteq \mathbb{Z}[x]$

$$x^3-3x+5 \equiv 1 \pmod{I}$$

$$\Rightarrow x^3-3x+4 \in I = \langle 2, x \rangle$$

as $x(x^2-3)+2\cdot 2 \in \langle 2, x \rangle$

Them 6.4 congruce mod I is equivalence relation

(i) reflexive: $\forall a \in R \quad a \equiv a \pmod{I}$
(ii) symmetric: $\forall a, b \in R \quad a \equiv b \pmod{I}$ then $b \equiv a \pmod{I}$
(iii) transitive: if $\begin{cases} a \equiv b \pmod{I} \\ b \equiv c \pmod{I} \end{cases}$ then $a \equiv c \pmod{I}$

pf: (i) $a-a=0 \in I$ ✓

(ii) if $a \equiv b \pmod{I} \Rightarrow a-b \in I \Rightarrow -(a-b) \in I \Rightarrow b-a \in I \in b \equiv a \pmod{I}$

(iii) same by close addition.

Def: The congruence class of $a \in R$ mod I is called coset of I in R

$$[a] = \{b \in R \mid b \equiv a \pmod{I}\}$$

$$[a] = \{b \in R \mid b = a+i \text{ for some } i \in I\}.$$

$$[a] = \{a+i \mid i \in I\} =: a+I$$

Them 6.6: $a+I = b+I$ iff $a \equiv b \pmod{I}$

in pericular $i \in I \Leftrightarrow i+I = 0+I = I$

$(a+I) \cap (b+I) = \emptyset \Leftrightarrow a \not\equiv b \pmod{I}$

Oct 24th 加油哦! 兔宝宝一定有推荐信! ✓ (谢谢家宝猪!!!).

Sec 6.2 Quotient rings and homo-morphism

Remind!: $I \lhd R$, subring + absorbption $ir \in I$ for $i \in I$ $r \in R$

$a \equiv b \pmod{I}$ iff $a-b \in I$ (consider I as zero)

equivalence relation: $[a] = a+I$ coset $[a] = [b] \Leftrightarrow a \equiv b \pmod{I}$

Operation: Example: ① take $I = 3\mathbb{Z} \lhd \mathbb{Z}$

$\begin{cases} [0] = 0+3\mathbb{Z} = 3\mathbb{Z} \\ [1] = 1+3\mathbb{Z} \end{cases}$

$1_{\mathbb{Z}[2]} = 2+3\mathbb{Z}$

② take $I = \langle 2, x\rangle \trianglelefteq \mathbb{Z}[x]$

$1 \equiv x^3 - 3x + 5 \pmod{I}$

implies $1+I = x^3-3x+5+I$

$$\{\underbrace{x^3-3x+5+i}_{=1} \mid i \in I\} = \{x^3-3x+5 + xf(x) + 2\cdot g(x) \mid f, g \in \mathbb{Z}[x]\}$$

$$= \{x\cdot(\underbrace{f - x^2 - 3}_{\tilde{f}}) + 2(\underbrace{g+2}_{\tilde{g}}) + 1 \mid f \cdot g\}$$

$$= \{1 + x\cdot\underbrace{\tilde{f}}_{\text{f}} + 2\cdot\tilde{g} \mid \tilde{f}, \tilde{g} \in \mathbb{Z}[x]\}.$$

then some $\in I \Rightarrow 1 = x^3 - 3x + 5$.

Denote: the set of all coset of I by $:= R/I = \{a+I \mid a \in R\}$.

Example: $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z},\ 1+3\mathbb{Z},\ 2+3\mathbb{Z}\}$.

$$\frac{F[x]}{\langle p(x)\rangle} = \frac{F[x]}{(p(x))} = \{f(x) + \langle p(x)\rangle \mid f=0 \text{ or } \deg f < \deg(p)\}.$$

$$\frac{\mathbb{Z}[x]}{\langle 2, x\rangle} = \{f(x) + \langle 2, x\rangle \mid f(x) \in \mathbb{Z}[x]\}. \quad \text{☆ i.e}$$

$$= \{a_0 + \underbrace{a_1 x + \cdots a_n x^n}_{\text{in } I} + I \;\Big|\; \begin{matrix} a_i \in R \\ n \in N \end{matrix}\}.$$

$$= \{a_0 + I \mid a_0 \in \mathbb{Z}\}. \quad = \text{if } a_0 \text{ is even then } a_0 + I = I$$

a_0 is odd, then $a_0 = 2\hat{a_0}+1 \Rightarrow a_0 + I = 1 + I$.

$$= \{I, 1+I\}.$$

midterm !!! ④

$$\frac{R\times R}{R\times\{0\}} = \{(a,b)+I \mid (a,b)\in R^2\} = \{(0,b)+I \mid b\in R\}. \text{ "unique"}$$

$R\times\{0\} \subseteq I$ ideal

$(a,0)+(0,b) \Leftrightarrow (0,b)+I$

$\Downarrow$ "$\in I$"

Operations !!!

General Def

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

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

Theorem 6.8 operation $(+,\cdot)$ are well defined

$I \lhd R$, then R/I is a ring with operation above.

① $(a+I)+(b+I) = (a+b)+I$

② $(a+I)(b+I) = ab+I$

R/I is called "coset ring"

Pf: say $a+I = a'+I$, $b+I = b'+I$ WTS $\begin{cases} a+b+I = a'+b'+I \\ ab+I = a'b'+I \end{cases}$

$\Rightarrow a-a' \in I$; $b-b' \in I$

① $\Rightarrow (a+b)-(a'+b') = \underbrace{(a-a')}_{\in I} + \underbrace{(b-b')}_{\in I} \in I$ so $a+b+I = a'+b'+I$ closed addition.

② $\Rightarrow ab-a'b' = ab-a'b+a'b-a'b' = \overbrace{(a-a')}^{I}b + a'\overbrace{(b-b')}^{I} \Rightarrow ab+I = a'b'+I$.
($(a-a') \in I$, absorb, $(b-b') \in I$)

① $0_{R/I} = 0+I = I$!!! zero element

② $-(a+I) = -a+I$

③ Remark: Identity • if R is with 1. with identity $1_{R/I} = 1+I$

Commutative • if R is comm, so is R/I

Example: ① $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$

② $\frac{R\times R}{R\times\{0\}} = \{(0,b)+I \mid b\in R\} \cong R$

ie: $(0,b_1)+I + (0,b_2)+I = (0,b_1+b_2)+I$

$((0,b_1)+I)((0,b_2)+I) = (0,b_1b_2)+I$

$\left(\frac{R\times R}{R\times\{0\}} \xrightarrow{\text{isom}} R\right)$, $(0,b)+I \longrightarrow b$

③ $\frac{\mathbb{Z}[x]}{\langle 2,x\rangle} = \{I, 1+I\}$.

① $1+I = I$ ② $1+I+1+I = I$ ③ $1+I+I = 1+I$.

① $I\cdot I = I$ ② $(1+I)(1+I) = 1+I$ ③ $I(1+I) = I$

homomorphism → quotient set.

Them 6.6 For a homo $\varphi: R\to S$, $\ker(\varphi) \lhd R$

Pf: ① subring ✓

② absorbption: $r\in R$, $a\in\ker\varphi$ (WTS $ra, ar \in \ker(\varphi)$)

i. $\varphi(ra) = \varphi(r)\cdot\varphi(a) = \varphi(r)\cdot 0 = 0 \in \ker(\varphi)$

ii. $\varphi(ar) = \varphi(a)\cdot\varphi(r) = 0\cdot\varphi(r) = 0 \in \ker(\varphi)$. ▨

Ex. ① $\varphi_n : \mathbb{Z} \to \mathbb{Z}_n$

$\varphi_n(a) = [a]$

$\ker\varphi_n = \{a\in\mathbb{Z} \mid \varphi_n(a) = [0]\} = \{a \mid [a]\equiv[0] \pmod n\}$. iff $n|a \iff a\in n\mathbb{Z}$

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

② $R\times R \to R$ homo !

$\pi_1(a,b) = a$

$\ker(\pi_1) = \{(a,b) \mid \pi_1(a,b)=0\} = \{(a,b) \mid a=0\} = \{0\}\times R \lhd R^2$.

Thm 6.12 if $I \lhd R$ the normal map $\pi : R \to R/I$ is a homo and $\ker\pi = I$

$\pi(r) = r+I$

pf: $\ker\pi = \{r\in R \mid \pi(r) = 0_{R/I} = I\} = \{r \mid r+I = I\} = I$

$\Downarrow$

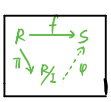
$r\in I$

Thm 6.13 if $f: R\to S$ surj - homo (of rings)

$$\frac{R}{\ker(f)} \cong S$$

pf: build $\varphi : \frac{R}{k} \to S$ isom

$\varphi(r+k) = f(r)$

ie 

ie: $R/I \cong S$ prove

we build $f: R\to S$ - homo + surj

$-\ker f = I$

then by Thm 6.12 $\to R/I \cong S$

▽ Check φ well defined? homo + sur + inj.

say that $r_1+k = r_2+k \Rightarrow r_1 - r_2 \in k = \ker f$

$\Rightarrow f(r_1 - r_2) = 0_S$

$\Rightarrow f(r_1) - f(r_2) = 0 \Rightarrow f(r_1) = f(r_2)$

$\Rightarrow \varphi(r_1+k) = \varphi(r_2+k)$

$\varphi(r_1+k+r_2+k) \overset{?}{=} \varphi(r_1+k) + \varphi(r_2+k)$

$\varphi(r_1+r_2+k) = f(r_1) + f(r_2)$

$f(r_1+r_2) \overset{\text{homo}}{=} f(r_1) + f(r_2)$

Check homo ✓

☺ injective : $\ker\varphi = \{r+k \mid \varphi(r+k) = 0_S\} = \{r+k \mid f(r) = 0_S\}$.

$\Downarrow$

$\{r+k \mid r\in\ker f = k\} = \{k = 0_{R/k}\} \Rightarrow \varphi$ is inj.

Example

① $\varphi_n : \mathbb{Z}\to\mathbb{Z}_n$ we know φ_n is homo + surj

$\varphi_n(a) = [a]$ (ie: $\ker(\varphi_n) = n\mathbb{Z}$

$\mathbb{Z}_{20}/\ker(f) \cong \mathbb{Z}_5$ $\quad \mathbb{Z}_{20} \cong \mathbb{Z}_5$

f: subject.

$\ker f = \{x\in\mathbb{Z}_{20} \text{ for all } f(x) = 0\}$.

$\ker f = \{[0],[5],[10],[15]\}$.

$= \{5\cdot(x\in\mathbb{Z}_{20})\ [0],[5],[10],[15]\}$.

$\langle 5\rangle < \ker f$.

↘ so by the 1st isom them

↳ $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

$f(x) = [x]_5$.

$x \in [\mathbb{Z}]_{20}$: $\mathbb{Z}_{20} \to \mathbb{Z}_5$, $f(x) = [x]_{20} = [x]_5$

② $\varphi_0 : \mathbb{Z}[x] \to \mathbb{Z}$ we know homo, surj $\varphi_0(c) = n$ "$c = n$"

$\varphi_0(p(x)) = p(0)$

↳ ie: $\ker(\varphi_0) = \{p(x) \mid p(0) = 0\}. = \{p(x) = a_n x^n + \cdots + a_1 x + a_0 = 0\}$

↳ By Isom Thm

↳ $\frac{\mathbb{Z}[x]}{\langle x \rangle} \cong \mathbb{Z}$

$\Rightarrow \{p(x) = a_n x^n + \cdots + a_1 x\}$

$= \{x(a_n x_n + \cdots a_1)\}. = \langle x \rangle$ ($p(x)$)

③ Prove $\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \cong \mathbb{C}$

given: $f : \mathbb{R}[x] \to \mathbb{C}$, $f(p(x)) = p(i)$

1) f is homo (substitution)

2) $a + ib \in \mathbb{C}$: WTS $f(a+bx) = a+ib$

3) $\ker(f) = \{p(x) \in \mathbb{R} \mid f(p(x)) = 0_{\mathbb{C}} = 0\}. = \{p(x) \mid p(i) = 0\}. \overset{?}{=} \langle x^2+1 \rangle$

4) By 1st isom them → $\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \cong \mathbb{C}$ ▨

"$\supseteq$" need to show $x^2+1 \in \ker(f)$

indeed $i^2+1 = 0$

"$\subseteq$" by long division, let $p(x) \in \ker f$

$p(x) \in \langle x^2+1 \rangle$ then $p(i) = 0$ (WTS $x^2+1 \mid p(x)$)

$p(x) = q(x) \cdot (x^2+1) + r(x)$

$x^2+1 \mid p(x)$ $r(x) = 0$ or $\deg r(x) < 2$

$r(x) = ax + b$: subst $p(i) = q(i)(i$ $+($

$\Rightarrow 0 = p(i) = ai + b$

$i = -\frac{b}{a} \in \mathbb{R}$. contradiction → $r(x)$

Sec 6.3 - R/I for special ideal (R communicative)

Q: when is R/I int-dom

when is R/I field

Def: An ideal $p \lhd R$ is called prime id $\begin{cases} \text{if } p \neq R \\ \text{if } ab \in p \text{ than } a \in p \text{ or } b \in p \end{cases}$

Ex: ① p is prime number, $\langle p \rangle = p\mathbb{Z} \lhd \mathbb{Z}$ is prime ideal

ie: (say $ab \in \langle p \rangle \leftrightarrow p \mid ab \xleftrightarrow{p \text{ prime}} p \mid b$ or $p \mid a \leftrightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$)

② $\langle p(x) \rangle \lhd F[x]$ is prime ideal iff $p[x]$ is irreducible

ie: say $f(x)g(x) \in \langle p(x) \rangle \leftrightarrow p(x) \mid f(x)g(x) \xleftrightarrow{p(x) \text{ irre}} p \mid f$ or $p \mid g \leftrightarrow f \in \langle p \rangle$ or $g \in \langle p \rangle$)

③ $\langle x \rangle \lhd \mathbb{Z}[x]$ is prime ideal

$f(x) \cdot g(x) \in \langle x \rangle \rightarrow x \mid f \cdot g \xrightarrow{\text{in } Q[x]} x \mid g$ or $x \mid f \rightarrow f(x) \in \langle x \rangle$ or $g(x) \in \langle x \rangle$) (in $Q[x] \rightarrow$ in $\mathbb{Z}[x]$.)

④ $4\mathbb{Z} \lhd \mathbb{Z}$ is not prime $2 \cdot 2 \in 4\mathbb{Z}$ but $2 \& 4\mathbb{Z}$

Them: $P \subsetneq R$. then p is prime ideal $\iff R/p$ is an int domain

pf: $\Rightarrow$ say $(a+P)(b+P) = 0_{R/p} = P$

$\downarrow$

$ab + P = P$ $\Leftarrow$ Assum int-dom and $ab \in p$ ⇑ ⇑ ✓ ✓

$\downarrow$

$ab \in P$

$\downarrow$ P prime

$a \in P$ $\quad$ $b \in P$

$\downarrow$ $\quad$ $\downarrow$

$a + P = P$ $\quad$ $b + P = P$

int-dom = ① comm ② one of $(a+P)/(b+P) = 0$

so R/p is an int-domain

Exam:

① $\langle x \rangle \lhd \mathbb{Z}[x]$ is prime ideal since (as) $\frac{\mathbb{Z}[x]}{\langle x \rangle} \cong \mathbb{Z}$ int. dom

② $\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p$ int domain $\longrightarrow$ $p\mathbb{Z} \lhd \mathbb{Z}$ ideal

③ $\{0\} \times R \lhd R \times R$ is ideal prime $\Leftrightarrow$ $\frac{R \times R}{0 \times R} \cong R$ int domain

---

Def: when is R/I is a field?

$M \lhd R$ is a **maximal ideal** if $M \neq R$

$\exists$ no ideal $J \lhd R$ st: $M \subsetneq J \subsetneq R$

i.e: if $M \subseteq J \lhd R$, then $M = J$ or $J = R$

Ex1. if p prime, $p\mathbb{Z} \lhd \mathbb{Z}$ is maximal!

i.e: $p\mathbb{Z} \subseteq n\mathbb{Z} \lhd \mathbb{Z}$

$n \mid p \xrightarrow{\text{prime}} n = \pm 1, \pm p$

$n\mathbb{Z} = \mathbb{Z}$ $\quad$ $n\mathbb{Z} = p\mathbb{Z}$

② $\langle x \rangle \lhd \mathbb{Z}[x]$ is **not** maximal: ie $\langle x \rangle \subsetneq \langle x, 2 \rangle \neq \mathbb{Z}[x]$

Them 6.15 $M \lhd R$, $M \neq R$

M is max-ideal $\Longleftrightarrow$ R/M is a field

Example: ① $\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p$ is a field

② $\frac{F[x]}{\langle p(x) \rangle}$ field $\Leftrightarrow$ $\langle p(x) \rangle$ max $\Leftrightarrow$ $p(x)$ irreducible

③ $(x] \lhd \mathbb{Z}[x]$ is not Max since $\frac{\mathbb{Z}[x]}{\langle x \rangle} \cong \mathbb{Z}$ is not a field.

Corollary: if the ideal $p \lhd R$ is Max-Id then it is prime.

pf if $p = \max \text{Id} \rightarrow R/p$ is field $\rightarrow$ int-domain p is prime

but $\langle x \rangle \lhd \mathbb{Z}[x]$ is prime but not max.

Sec 7.1 Group : def. examples

Def: A Group is a non-empty set G with an operation $*$ $(G, *)$

such that ① $\forall a, b \in G$, $a * b \in G$ (closure)

② $a * (b * c) = (a * b) * c$ (asso)

③ $\exists$ element $e \in G$ such that $e * a = a * e = a$ $\forall a \in G$. e is called unique identity of G.

④ $\forall a \in G$ has an unique inverse: $\exists b \in G$: $a * b = b * a = e$. : $b = a^{-1}$

Example :

① $(\mathbb{Z}, +)$:= "$\mathbb{Z}$ with addition" $(R, \overset{e=0}{+})$; $(Q, +)$; $(M_n(R), +)$

"In general if R is ring $(R, +)$ is a group" $\equiv$ Abiliam group

② $(\mathbb{Z}, \cdot)$ is not group as no inverse.

$(Q, \cdot)$ is not group as "0" has no inverse

"In general if R is ring $(R, \cdot)$ is never a group (maybe don't have 1; and even if, 0 has no inverse)

③ Let R is a ring with 1, then $\mathcal{U}(R) = \{$units of $R\}$ is a multiplicative group! $\equiv$ depend on Ring.
if R is commun → Abiliam

Ex → $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$. $e = 1$ (Abiliam - $|\mathcal{U}(\mathbb{Z})| = 2$)

$\mathcal{U}(Q) = Q^* = Q / \{0\}$. (Abiliam - $|\mathcal{U}(Q)| = \infty$)

$\mathcal{U}(F) = F^* = F / \{0\}$. (Abiliam $|\mathcal{U}(F)| = \infty$)

$\mathcal{U}(M_n(R)) = \{A \in M_n(R) \mid \det A \neq 0\} =: $ General linear Group $= GL(n, R)$ (not abiliam)

$\mathcal{U}(\mathbb{Z}_n) = \{[a] \mid (a, n) = 1\} =: U_n$ (abiliam $|U| = n$.)

④ X set $S_X = \{f : X \to X$ bij function$\}$. "symmetry group"

S_X is a group with $* = \circ$ (composition)

$(S_X, \circ)$ if X has at least 3 element : not abiliam.

pf: ③ $e = id_X$ (identity function by sending $\forall x \to x$)

④ invertible function as bij.

Def: a group is called Abelian if $a*b = b*a \quad \forall a,b \in G$.

The order of a group is $|G|$ = num of element in G.

if G is infinite, $|G| = \infty$

S_n : the symmetry group

if $X = \{1, 2, \cdots n\}$. then $S_X = S_n$. and called the elements in this group permutations.

We write permutations in S_n by $\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ 2xn matrix (1: order, $f(1)$: image)

Ex: ① $f \in S_3$

$$\begin{cases} f(1)=2 \\ f(2)=3 \\ f(3)=1 \end{cases} \Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

② $G \in S_3$

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \Rightarrow \begin{matrix} g(1)=2 \\ g(2)=1 \\ g(3)=3 \end{matrix}$$

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

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

$\neq \Rightarrow$ S_n is not Abelian for $n \geq 3$.

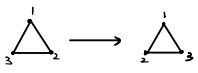
The order of S_n is $|S_n| = n! = n(n-1)\cdots 2\cdot 1$.

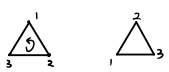
We can find the inverse by "fliping": ④ $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rightarrow f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

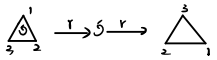
D_n - dihedral groups

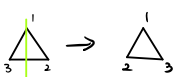
Ex. D_3 = symmetries of equilateral triangle

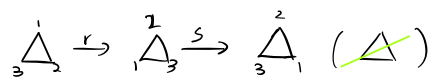
= bij function preserving distance.

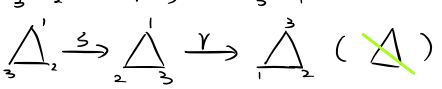
ie: id:  $r^3 = id$

r: rotation:  rotation $120° = \frac{360°}{3}$ and anti-clockwise

r^2:  (clock wise $120°$)

S: reflexion  reflexion along symm-axis 

$s^2 = id$ ie, sr = 

rs = 

$\Rightarrow$ D_3 is not abeliam ! as $sr = rs$

ie : we can check $sr = r^2s = r^{-1}s$

$\Rightarrow$ $D_3 = \{r^i s^j \mid i,j\} = \{id, r, r^2, s, rs, r^2s\}$.

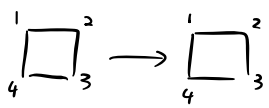
$|D_3| = 6$ we don't need geometry to work with D_3.

D_3 is generated by two elements : r, s with the relations : $\begin{cases} r^3 = s^2 = id \\ sr = r^2s \end{cases}$

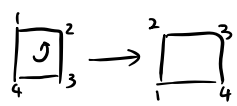
Example : $(rs)(r^2s) = r\cdot(sr)\cdot rs = r\cdot r^2(sr)s = rr^2\cdot r^2ss = r^2$.

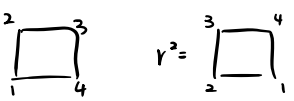
$(rs)\cdot(rs) = r(sr)s = r\cdot r^2s\cdot s = id$.

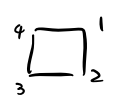
D_4 = symmetries of a squre

id : 

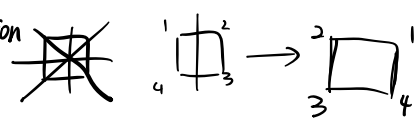
rotate : r $90° = \frac{360}{4}$ anticlockwise.

r: 

r^2= 

r^3= 

$r^4 = Id$.

s: reflexion 

$s^2 = Id$

and $sr = r^3s = r^{-1}s$

$\Rightarrow$ $D_4 = \{id, r, r^2, r^3, s, rs, r^2s, r^3s\}$. = non abeliam

$|D_4| = 8$ in General D_n = symmetries of a regular n-polygon

$D_n = \{id, r, r^2 \cdots r^{n-1}, s, rs, r^2s \cdots r^{n-1}s\}$. non abeliam.

$|D_n| = 2n$. D_n is generate by r,s $\begin{cases} r^n = s^2 = Id \\ sr = r^{n-1}s = r^{-1}s \end{cases}$

Sec 7.2 basic properties → Group

Recall: $D_n = \{id, r, r^2 \cdots r^{n-1}, s, rs, \cdots r^{n-1}s\}$.

$$s^2 = r^n = id$$
$$sr = r^{n-1}s$$

Thm 7.5: let $G \in$ group

Basic

(1) $\exists!$ e (identity)

(2) $\exists!$ g^{-1} (inverse)

"pf the same as ring"

(3) cancelation law: $\begin{cases} a*c = b*c \Rightarrow a = b \\ c*a = c*b \Rightarrow c = b \end{cases}$

pf: if $a*c = b*c$ / c^{-1} from right

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

$ae = be \Rightarrow a = b$ ▨

(4) $\begin{cases} (ab)^{-1} = b^{-1}\cdot a^{-1} \\ (a^{-1})^{-1} = a \end{cases}$

Notation: $\begin{cases} n \in N \\ a \in G \end{cases}$

① $a^n := \underbrace{a*a*\cdots*a}_{n \text{ times}}$

② $a^{-n} := \underbrace{a^{-1}*a^{-1}*\cdots*a^{-1}}_{n \text{ times}}$

③ $a^0 := e$

Thm 7.7: $n, m \in Z$, $a \in G$ $\begin{cases} a^n * a^m = a^{n+m} \\ (a^n)^m = a^{n\cdot m} \end{cases}$

Warning: ie

mult	add
ab	$a+b$
a^{-1}	$-a$
a^n	na
a^{-n}	$-na$
$(e=1)$	$(e=0)$

Warning:
- we usually use multiplic-notation.
- but groups can be additive as well "Translate"
- Then we use additive notation.

Def: $a \in G$ "the order of a" is the smallest $n \in \mathbb{N}^{+}$ st. $a^n = e$

Denoted it by $|a|$ ($ord(a)$)

if there $\exists$ no such n, then $|a| = \infty$

Examples ① $e \Rightarrow$ is the only element of order 1 ($a^1 = a = e$)

② $G = S_3$ if $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq id$ $f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$|G| = 3 \Leftarrow f^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

③ $G = U_8 = U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ (U: unit)

$\begin{cases} a = 3 \\ \downarrow \\ a^2 = 9 = 1 \end{cases} \Rightarrow |a| = 2$ $\qquad$ $\begin{cases} b = 5 \\ b^2 = 25 = 1 \\ \downarrow \\ |b| = 1 \end{cases}$

④ $G = D_n$ $|r| = n$; $|s| = 2$

⑤ $G = \mathbb{Z}$ (additive) $\quad a = 5 \longrightarrow a^2 = 10 \longrightarrow a^3 = 15 \Rightarrow |a| = \infty$

ie: $na = 5n > 0$

⑥ $G = \mathbb{Z}_{12}$ (additive) $\quad a = 3 \longrightarrow a^2 = 6 \longrightarrow a^3 = 9 \longrightarrow a^4 = 0 \Rightarrow |a| = 4.$

Them 7.9. $\{a^i\}$!!!

$|a| = n < \infty$, then ① $k \in \mathbb{Z}$, $a^k = e \Leftrightarrow n \mid k$

② $a^i = a^j \Leftrightarrow i \equiv j \pmod{n}$

proof: ① "$\Leftarrow$" if $n|k \Rightarrow k = nt$

ie: $a^k = a^{nt} = (a^n)^t = (e)^t = e$

"$\Rightarrow$" Assume $a^k = e$ (WTS $n|k$ by long-divison)

"$k = qn + r \quad (0 \le r < n)$"

$\Rightarrow a^{qn+r} = a^{qn} * a^r = (a^n)^q * a^r = e * a^r = a^r = e$

since $r < n$ and n is the smallest $N \Rightarrow 0 \le r \le 0$

then $r = 0$, which means $n|k$ ▨

② if $a^i = a^j \iff a^j a^{-i} = e$

"$j \ge i$"

$a^{j-i} = e \iff n|j-i \Rightarrow j \equiv i \pmod n$

Example $|a| = 6$, $a^{13} = a^1 \;/\; a^9 = a^3 \;/\; a^{-1} = a^5$

Them 7.8: $\{a^k\}_{k\in\mathbb{Z}}$ has the same size as the order of a

- if $|a| = n$, $\{a^k\}_{k\in\mathbb{Z}} = \{e, a, a^2, \cdots a^{n-1}\}$.
- if $|a| = \infty$, $\{a^k\}_{k\in\mathbb{Z}}$ are all distinct.

Pf: ① if $|a| = n$, then this follow 7.9 Them

② if $|a| = \infty$, we claim that for any $i \ne j$: $a^i \ne a^j$

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

which means $j - i = 0 \Rightarrow j = i$ ▨

Them 7.9 + : $|a| = n < \infty$

- Case I: if $k \mid n$, then $|a^{\frac{n}{k}}| = k$
- Case II: if $(n,k) = 1$, the $|a^k| = n$
- Case III: in General $|a^k| = \frac{n}{(n,k)}$

Pf : i) $b = a^{\frac{n}{k}}$ (order)

$$b^k = (a^{\frac{n}{k}})^k = a^{\frac{nk}{k}} = a^n = e$$

if $b^t = e$, then $(a^{\frac{n}{k}})^t = e$ (small) "$t>0$"

$\Rightarrow n \mid \frac{n}{k}t \Rightarrow 1 \mid \frac{t}{k} \Rightarrow k \mid t$. $k \le t$ ▨

Ex. $|a| = 6$ $|a^2| = 3 \Rightarrow |a^4| = \frac{6}{2} = 3 \Rightarrow |a^5| = \frac{6}{1} = 6$

Summary: if we know $|a|$, we know perfectly $\{a^k\}_{k \in \mathbb{Z}}$. "subgroup"

Nov. 7th.

Recall: $a \in G$ order of a $|a|$ = smallest n s.t $a^n = e$.

(additive $|a|$ = smallest pos n. st $na = e$)

- $\{a^i\}_{i \in \mathbb{Z}}$ is of size $|a|$
- ① if $|a| = n$, than $a^i = a^j \iff i \equiv j \pmod{n}$

Sec 7.3 – subgroup

Def: $H \subseteq G$ is a subgroup $\to G$ if it's a group under same operation.

prove subgroup:

1) $\equiv$
- ① Closed operation $a, b \in H \to a * b \in H$.
- ② $e_G \in H$
- ③ $\forall a \in H \to a^{-1} \in H$

2) $\equiv$
- (i) $e \in H$
- (ii) $a, b \in H$ $a * b^{-1} \in H$

Ex. 1) $\{e\}$, G are trivial sub-G. "smallest possi"

2) $2\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ "subrings" $\Rightarrow$ "Sub-G"

3) $H = \{1, 3\} \subseteq U_8$ is a sub-G.

1) identity $1 \in H$ ✓ 3) Close inverse as $3 \cdot 3 = 1 \Rightarrow 3^{-1} = 3$. $\Rightarrow$ Inverse ✓

2) Check mult: $1 \cdot 1 = 1 \in H$. ; $1 \cdot 3 = 3 \in H$. ; $3 \cdot 3 = 1 \in H$. ✓

4) $\{A \mid \det A = 1\} \subseteq GL(n, R)$

"$SL(n,R)$"

special linear group

$\Rightarrow$ ① Identity matrix $\det(I_n) = 1 \in SL(n,R)$

② take $A, B \in SL(n,R)$

$\det A = \det B = 1$.

$\det(A * B^{-1}) = \det A \cdot \det(B^{-1}) = \frac{1}{\det B}$

$= 1 \cdot 1 = 1$.

Thus $AB^{-1} \in SL(n,R)$.

5) $Z(G) = \{a \in G \mid \forall x \in G : a * x = x * a\}$. "the center of G"

Note: if G Abilian $\Leftrightarrow$ $Z(G) = G$.

$Z(S_3) = \{id\}$.

" The center is always a sub-G "

pf: (i) $e \in Z(G)$ $\forall g \in G$. $eg = ge = g$.

(ii) take $a, b \in Z(G)$. WTS "$ab \in Z(G)$."

let $g \in G$: $g(ab) = a(gb) = a(bg) = (ab)g$

as $a \in Z(G)$; $b \in Z(G)$

then $ab \in Z(G)$.

(iii) $a \in Z(G)$ "WTS $a^{-1} \in Z(G)$"

$\Downarrow$

$\forall g \in G$ $ag = ga$. / a^{-1} from left + right.

$\Downarrow$

$a^{-1}aga^{-1} = a^{-1}gaa^{-1}$

$ega^{-1} = a^{-1}ge$

$ga^{-1} = a^{-1}g \Rightarrow a^{-1}$ is also in $Z(G)$.

Cyclic group-sub

Def: $a \in G$, $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$. is the cyclic-sub-G generated by a.

for additative: $\langle a \rangle = \{ia \mid i \in \mathbb{Z}\}$.

Them 7.15: $\langle a \rangle$ is always a sub-$G \to G$.

pf:

i) $e = a^0 \in \langle a \rangle$.

ii) take $a^i, a^j \in \langle a \rangle \Rightarrow a^i a^j = a^{i+j} \in \langle a \rangle$

iii) let $a^i \in \langle a \rangle$. $(a^i)^{-1} = a^{-i} \Rightarrow a^{-i} \in \langle a \rangle$ ▨

Example

(1) $3 \in U_8$ $\langle 3 \rangle = \{3^i \mid i \in \mathbb{Z}\}. = \{1, 3, 1, 3 \cdots\} = \{1, 3\}$.

(2) $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in GL(2, \mathbb{R})$ $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}^i \middle| i \in \mathbb{Z} \right\} = \left\{ \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \middle| i \in \mathbb{Z} \right\}$.

(3) $2 \in \mathbb{Z}$, $\langle 2 \rangle = 2\mathbb{Z} = \{2^i \mid i \in \mathbb{Z}\}. = \{2i \mid i \in \mathbb{Z}\}$.

Extend ie: $\langle n \rangle = n\mathbb{Z}$.

(4) Claim: $\langle a \rangle$ is the smallest sub-G containing a ($a \in H \leftrightarrow \langle a \rangle \subseteq H$)

Def: G is all cyclic if $\exists\, a \in G$, $G = \langle a \rangle$

Ex: • $\mathbb{Z} = \langle 1 \rangle$ "additive" $= \langle -1 \rangle$. Cyclic

- $\mathbb{Z}_n = \langle 1 \rangle = \langle n-1 \rangle$ "additive" Cyclic
- $U_{10} = \{1, 3, 7, 9\} = \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3\}$. cyclic
- **$\mathbb{Q}$ is not cyclic** : if $\mathbb{Q} = \langle \frac{a}{b} \rangle = \{\frac{a}{b} i \mid i \in \mathbb{Z}\}$. "ie Clearly $\frac{a}{2b} \notin \langle \frac{a}{b} \rangle$"

$$\text{so, } \langle \tfrac{a}{b} \rangle \neq \mathbb{Q}$$

($\langle 1 \rangle = \{1i \mid i \in \mathbb{Z}\} = \mathbb{Z}$ in $\mathbb{Q}$)

Notice: a group is cyclic $\longrightarrow$ G must be abeliam

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

so S_n, D_n are not cyclic

However $\mathbb{Q}$ is abeliam but not cyclic.

Recall: if $\{a^i \mid i \in \mathbb{Z}\}$ has size $|a|$

Them: The order of $\langle a \rangle$ is the order of a " $|\langle a \rangle| = |a|$ "

↓

Application: Corlorary: if $|G| = n$, then G is cyclic $\iff$ G contains an element s.t $|\langle g \rangle| = n$.

pf: $\Rightarrow$ if $G = \langle a \rangle$ and $n = |G| = |\langle a \rangle| = |a|$

$\Leftarrow$ if $|a| = n$, then $\langle a \rangle \subseteq G$ is a subset of size n, same as G. so $\langle a \rangle = G$. and G is cyclic.

Ex: • $|U_{10}| = 4 = |\langle 3 \rangle| = 4$

$3 \neq 1$

$3^2 = 9 \neq 1$

$3^3 = 7 \neq 1$

$3^4 = 1 = 1$

• $\mathbb{Z}_2 \times \mathbb{Z}_2$. (additive) ① $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4. = |\mathbb{Z}_2| \cdot |\mathbb{Z}_2|$

② order of element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \leq 2$.

prove②: since $2(a,b) = (a,b)+(a,b) = (2a, 2b) = (0,0) = e_{\mathbb{Z}_2 \times \mathbb{Z}_2}$.

then we can't have an element of order 4.

$\Rightarrow$ $\mathbb{Z}_2 \times \mathbb{Z}_2$ is Not cyclic.

Them: if G is cyclic, every sub-group $\to G$ is cyclic.

Counterexample for $\Leftarrow$ by intro "Q".

pf: $G = \langle a \rangle$ Take $n = \min$ posi-num where $a^n \in H$.

$H \subseteq G$ ↓

We claim $H = \langle a^n \rangle$ "□"

Cor: The sub-group of $\mathbb{Z}$ are $\langle n \rangle = n\mathbb{Z}$ "The only ideal"

TA: we say $I \subseteq R$ of ring is ideal: I is subring + Absorbtion.

Quotient ring: $R/I = \{r + I \mid r \in R\}$. "Set of set"

$$r+I = \{r+i \mid i \in I\}.$$

Def: $(r+I)+(s+I) = (r+s)+I$

$(r+I)\cdot(s+I) = rs+I$

well-definedness: $r+I = r'+I \iff r-r' \in I$

ie: $(r+I)+(s+I) = (r+s)+I$

$(r'+I)+(s+I) = (r'+s)+I$

ie: General: $a+I = b+I \iff a-b \in I$.

then $(r+s)-(r'+s) = r-r' \in I$

$$\begin{cases} (r+I)(s+I) = rs+I \\ (r'+I)(s+I) = r's+I \end{cases} \Rightarrow rs-r's = (r-r')s \text{ by absorbtion}$$

then $(r-r')s \in I$.

Prove well-definedness if $[x] = [y] \Rightarrow h(x) = h(y)$

Prim+ Max: we say ideal P is prime iff $ab \in P \to a \in P$ or $b \in P$

$\Updownarrow$

R/p is integer domain.

$\Updownarrow$

if $x, y \in R/p$ and $xy = 0$, then $x = 0$ or $y = 0$.

$ab+P = P \Rightarrow ab \in P.$

$\|$

$(a+P)(b+P) = P$

$a \in P \Rightarrow at \in P$

Max-Ideal: We say m is max iff ($M \subseteq I \subseteq R$ for some ideal; then $I = M$ or $I = R$)

$\Updownarrow$

all M are prime $\iff$ R/M is a field.

Prob: 21. $R = \{a+bi \mid a, b \in \mathbb{Z}\}$.

$J = \{a+bi \mid 5|a \text{ and } 5|b\} = 5R$.

Show that J is not Max. ideal!

$5 = (2+i)(2-i)$

zero divisor

$R/5R$ is not an integer domain $\Leftarrow$ $((2+i)+5R)((2-i)+5R) = 5+5R = 5R$.

$\begin{cases} p \equiv 1 \pmod 4 \Rightarrow x \text{ prime} \\ p \equiv 3(4) \Rightarrow \text{prime}. \end{cases}$

Prob: A cyclic group $\begin{cases} ① \text{ infinite} & C \cong (\mathbb{Z}, +) \\ ② \text{ finite} & C \cong (\mathbb{Z}/n\mathbb{Z}, +) \end{cases}$

Every groups has cyclic sub-groups.

Recipe: $X \neq 1_G \in G$, then $\langle X \rangle = \{\cdots x^{-2}, x^{-1}, 1, x, x^2, \cdots\}$. is cyclic sub-g.

$|x| = |\langle x \rangle|$ ie $\langle x \rangle = \{x, x^2, \cdots x^n\}$.

$|x| =$ minimal $n \Rightarrow \{x^n = 1_G\}$. $|\langle x \rangle| = n$.

if $x^n \neq 1$, then $x^{n+1} = x \cdot x^n \neq x$.

then $|\langle x \rangle| > n$.

if $d < n$ and $x^d = 1$. then $\langle 1, x, x^2, \cdots x^d \rangle \subsetneq \langle x \rangle$

$x^{d+1} = x^d x = x$.

$F - L \qquad F' \qquad Aut(F/L)$

$= \{\phi \in F\text{-}F \mid \phi|_L = I_L\}$.

Nov. 9

Sec 7.4 "isomo + homo"

NM

Def: $(G, *), (H, \circ)$ "Both Group"

A function $f: G \to H$ is called "homo" (of Group) if $f(g_1 *_{\text{in } G} g_2) = f(g_1) \circ_{\text{in } H} f(g_2)$

Ex: 1) $id: G \to G$, $id(x) = x$ | $id(g_1 g_2) = g_1 g_2 = id(g_1) \cdot id(g_2)$

$\mathrm{Im}(f) = G$ + $\ker f = \{e_G\}$ = Isomorphism

2) $f: R^* \to R^*$ (Group without "0")

$f(x) \to x^2$ | $f(g_1 g_2) = (g_1 g_2)^2 = (g_1)^2 \cdot (g_2)^2 = f(g_1) \cdot f(g_2)$ (abelian) $= \{\pm 1\}. \neq e_G$ "Not inject"

$\mathrm{Im}(f) \neq R^*$ as only positive + $\ker f = \{x \in R^* \mid f(x) = 1\}$.

3) $\varphi_n: \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(a) = [a]$ | $\varphi(a_1 + b_1) = [a_1 + b_1]_{mod\, n} = [a_1] + [b_1] = \varphi(a_1) + \varphi(b_1)$

"additative"

$\mathrm{Im}(f) = \mathbb{Z}_n$ + $\ker(f) = n\mathbb{Z} \neq 0$

4) $f: \mathbb{Z} \to R^*$, $f(n) = e^n$ | $f(n+m) = e^{n+m} = e^n \cdot e^m = f(n) * f(m)$

$\mathrm{Im}(f) \neq R^*$ as $e^n > 0$

$\ker(f) = \{g \in G \mid e^g = 1\} \Rightarrow \{0\} = e_{\mathbb{Z}}$

Them 7.20: Let $f: G \to H$ homom!

1) $f(e_G) = e_H$
2) $f(a^{-1}) = f(a)^{-1}$

| Just like rings proof ▨

Proposition: $f: G \to H$ is homom!

1) $\mathrm{Im} f \subseteq H$ is a subgroup

f is surjective $\iff \mathrm{Im}(f) = H$

2) $\ker f = \{g \in G \mid f(g) = e_H\}. \subseteq G$ is a subgroup

f is injective $\iff \ker(f) = \{e_G\}$. "The only e_G in there"

Pf: just like rmg.

♛ Def: see example: if $f: G \to H$ is isomom (of Group)

① – f is homo

② – surjective + injective

We say G is isomophic to H := $G \cong H$ (means that G/H are essentially same)

Remark: If f is a bijective homom, f^{-1} is also an homom!

(2) homom-rings induce homom (additive) Group

+

isomo-rings induce isom (additive) Group

($f: 1R \to R$, $f(x) = 2x$ homo-group but not homo-ring)

Ex. ① $\mathbb{Z} \cong 2\mathbb{Z}$, $f(n) = 2n$

1) $f(n+m) = 2(n+m) = 2n+2m = f(n)+f(m)$

2) let $2n \in 2\mathbb{Z}$, then as $f(n) = 2n$, $\Rightarrow 2\mathbb{Z} \subseteq Im(f) \Rightarrow$ Surjective.

3) $\ker(f) = \{z \in \mathbb{Z} \mid 2z = 0\} = \{0\} = 0_{\mathbb{Z}}$

② $D_3 \cong S_3$ by comparing operation tables.

$r \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f$

$s \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = g$

$(2S)^{-1} = S^{-1}2^{-1}$,

③ $H = \langle r \rangle \subset D_4$. $= \{id, r, r^2, r^3\}$.

$f: H \xrightarrow{\cong} \mathbb{Z}_4$, $f(r^i) = [i]$. $i = 0,1,2,3$

(recall: $|a| = n$, $a^i = a^j \Leftrightarrow i \equiv j \pmod n$)

pf: 1) f is homom: $f(r^i r^j) = [ij] = [i] + [j] = f(r^i) + f(r^j)$

ie: $= f[r^{i+j}]$

$k = ij \bmod n$ $= f(r^k)$

$= [k]$

surjective ✓

injective: $\ker(f) = \{r^i \in H \mid [i] = [0]\}_{i=0,1,2,3} = \{r^0\} = e_H$

We can Generate ↑↑ by Thm 7.19 (Classification of cyclic group)

Let G be a cyclic group (1) if $|G|=n$, then $G \cong \mathbb{Z}_n$

(2) if $|G|=\infty$, then $G \cong \mathbb{Z}$

pf: write $G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$.

(1) base case Recall $|a| = |\langle a \rangle| = |G|$

$f: G \to \mathbb{Z}_n$, $f(a^i) = [i]$, $i = 0, 1, \cdots n-1$ [pf like above Example]

(2) $f: G \to \mathbb{Z}$, $f(a^i) = i$ | pf: homom ✓ $f(a^i \cdot a^j) = f(a^{i+j}) = i+j = f(a^i) + f(a^j)$

[subject take $i \in \mathbb{Z}$, then $f(a^i) = i$. ⇒

[injective: $\{a^i \in G \mid i = 0\} = \{a^0\} = \{id\} = e_G$

$\Rightarrow G \cong \mathbb{Z}$

Ex. somehow find function 转化到

① $2\mathbb{Z} = \langle 2 \rangle$ (additive) cyclic, $|2\mathbb{Z}| = \infty$

then: $2\mathbb{Z} \cong \mathbb{Z}$ by theorem 7. Classification)

f ↓

② $H = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle \leq S_3$

H is cyclic $|H| = |f| = 3$ $f^1 \neq id$

$f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq id$

$f^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id$

then $H \cong \mathbb{Z}_3$.

③ R is not cyclic (ie if R is cyclic $\to R \cong \mathbb{Z}$ contradiction)

(sets theory reasons)

WTS Prove Not Isomorphism !

$G \ncong H$ is enough to point out a property preserve by isom (= invariant)

that One has / The other don't have.

1) The order
2) Cyclic
3) The order of elements
4) "Abeliam"

Example:

① $\mathbb{Z}_5 \ncong \mathbb{Z}_{10}$ (The order of the Group)

$|\langle 1\rangle| = 5 \quad |\langle 1\rangle| = 10$

Different order

② $D_4 \cong \mathbb{Z}_8$ (X Abeliam / Abe.)

③ $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$ ($\mathbb{Z}_2 \times \mathbb{Z}_2$ not / $\mathbb{Z}_4$ (cyclic)) $\Rightarrow$ $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic as it does not has generator.

④ $|\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2| \ncong |\mathbb{Z}_4 \times \mathbb{Z}_2| = 4$ since $\mathbb{Z}_4 \times \mathbb{Z}_2$ has an element of order 4 $(1,0)/(1,1)$

$2(a,b,c) = (0,0,0)$ $\quad 4(a,b) = (4a, 4b) \Rightarrow (0,0)$

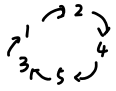
but $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ the order of elements are bounded by $2 \leq 2$

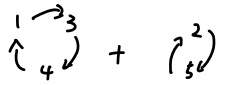
order of the element

Nov 14th.

Sec 7.5 Cycles / Alternative groups.

ex. elements in S_n $\begin{pmatrix} 1 & 2 & \cdots & n \\ f_{(1)} & f_{(2)} & \cdots & f_{(n)} \end{pmatrix}$

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$  "cycle"

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$ 

Def: A cycle of length k (k-cycle) is the permutation of the form $(a_1, a_2, \cdots a_k)$

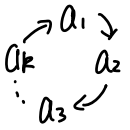
$a_1 \longmapsto a_2$

$a_2 \longmapsto a_3$

$a_3 \longmapsto a_4$

$\vdots$

$a_k \longmapsto a_1$



and $b \longrightarrow b$ for all other num

Example: • $(1, 3, 2, 5) \in S_5$

$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$

$\| $

$(3, 2, 5, 1)$

• $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \Longrightarrow (1\ 3\ 4\ 2) \in S_4 = (3, 4, 2, 1)$

• $id = (1) = (2) =$ empty cycle

• $(1, 3, 2)(4, 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

Def: cycles are disjoint if they have no common element.

$(1, 2, 3)(4, 5, 6, 7)$ disjoint

$(1, 5, 3)\ (2, 3, 4, 6)$ are not disjoint

Them 7.23 : if σ, τ are disjoint cycle, then $\sigma\tau = \tau\sigma$

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

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

Them 7.24.

Every permutation can be written as a product of disjoint cycles in a unique way (up to order)

Example

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

② $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 1 & 4 \end{pmatrix} = (1,3,5)\underbrace{(2)}_{\text{"id"}}(4\ 6) = (1,3,5)(4,6)$

③ $(1,2,3,6)(3,1,5) = (1,5,6)(2,3)\underbrace{(4)}_{\text{"id"}}$

prop: $(a_1, a_2, \cdots a_k)^{-1} = (a_k a_{k-1} \cdots a_2 a_1)$

(flip the array)

example: $\sigma = (1,2,6)(5,4,3)$ (disjoint!)

$\downarrow$

$\sigma' = ((1,2,6)(5,4,3))^{-1} = (1,2,6)^{-1}(5,4,3)^{-1} = (6,2,1)(3,4,5)$

Them 7.25: The order of a cycle is its length

The order of a permutation is the lcm (lcm = least common divisor) of the length of the disjoint cycle

[lcm $(k_n, \cdots, k_m)$:= smallest positive number l st. every $k_i \mid l$] "common denominator"

$= \frac{k_n \cdots k_m}{\gcd(k_n, k_m \cdots)}$

Ex: • $(1,2,3)$ is the order of "length = 3" $(1,2,3)^3 = id$

• $(1,2)(3,4,5)$ order of 6 $(\mathrm{lcm}(2,3) = 6)$
"2" "3"

• $(1,2)(3,4,5,6)$ is 4 $(\mathrm{lcm}(2,4) = 4)$
"2" "4"

• $(- - - - -)(- - -)$ is 30 $(\mathrm{lcm}(6,15) = 30)$
6 15

The Alternation Group :

Def: a 2-cycle is called a transportation

Note: if σ is a transportation, $|\sigma| = 2 \rightarrow \sigma^{-1} = \sigma$

Thm 7.26: Any permutation can be written as a product of transportation

"proof": $\boxed{(a_1, a_2 \cdots a_k) = (a_1, a_2)(a_2 a_3) \cdots (a_{k-1} a_k)}$ formula

identity: $(1,2)(1,2) =$

if k is odd → even permutation
if k is even → odd permutation
(k-1)組

Example:

• $(1,2,3) = (1,2)(2,3)$
$\Downarrow$
$(2,3,1) = (2,3)(3,1) \Rightarrow$ Not unique for transpor
$\Downarrow$
$(3,1,2) = (3,1)(1,2)$

• $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (1,4,5)(2,3) = (1,4)(4,5)(2,3)$
$= (2,3)(1,4)(4,5) = (1,4)(2,3)(4,5)$

• $id = (1,2)(1,2) = (1,2)(1,2)(2,3)(2,3) \cdots\cdots$

Def: A permutation is called [even permutation] if it can be written as a product of Even numbers of transportations

A permutation is called odd permutation $\cdots\cdot$ as a product of odd number of tran

Ex.1) $id = (1,2)(1,2) \longrightarrow$ even

2) $(1,2,3) = (1,2)(2,3) \longrightarrow$ even

3) $(1,2,3,4) = (1,2)(2,3)(3,4) \longrightarrow$ odd.

even odd even

4) $(1,2,3)(1,5,6,7)(3,1,6) =$ odd permutation

Them 7.28

No permutation in S_n is both even and odd

$\longrightarrow$ purity is unque ! / well defined

Def: $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$.

ex. $A_3 = \{id, (1,2,3), (1,3,2)\}$. $\Leftarrow (S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\})$

Them 7.29: $A_n \leq S_n$ is a subgroup of order $\frac{n!}{2}$

pf: i) the identity $\in A_n$ always as id is even

ii) if $\sigma_1, \sigma_2 \in A_n$, then $\sigma_1 \sigma_2$ is also even

iii) if $\sigma \in A_n \longrightarrow \sigma = \tau_1 \tau_2 \cdots \tau_{2m}$ (τ_i transportation)

$\sigma^{-1} = \tau_{2m}^{-1} \cdots \tau_2^{-1} \tau_1^{-1} = \tau_{2m} \cdots \tau_2 \tau_1 \longrightarrow$ even

["$(ab)^{-1} = b^{-1}a^{-1}$"] so $\sigma^{-1} \in A_n$.

ex. $\sigma = (1,2)(2,4)(2,5)(6,1)$

$\sigma^{-1} = (1,6)(5,2)(4,2)(2,1)$ = even

$= (6,1)^{-1}(2,5)^{-1}(2,4)^{-1}(1,2)^{-1}$

Def: A_n is called the <u>alternating group</u>

Claim: sgn function: $S_n \longrightarrow Z_2$ (homomorphism)

$$\operatorname{sgn}(\sigma) = \begin{cases} 0 & \text{even} \\ 1 & \text{odd} \end{cases}$$

"$\ker(\operatorname{sgn}) = A_n$"

pf: 1) $\operatorname{sgn}(\sigma_1\sigma_2) \stackrel{?}{=} \operatorname{sgn}(\sigma_1) + \operatorname{sgn}(\sigma_2)$

table

σ_2 \ σ_1	odd	even
odd	even(0)	odd(1)
even	odd(1)	even(0)

$\Leftrightarrow$

1) $\operatorname{sgn}(\sigma_1) + \operatorname{sgn}(\sigma_1) = 1+1 = 0$

2) $\operatorname{sgn}(\sigma_1) + \operatorname{sgn}(\sigma_2) = 1+0 = 0$

3) $\operatorname{sgn}(\sigma_1) + \operatorname{sgn}(\sigma_2) = 0+1 = 1$

4) $\operatorname{sgn}(\sigma_1) + \operatorname{sgn}(\sigma_2) = 0+0 = 0$

2)

1. $P(x) = x^2+x+6 \in \mathbb{Z}_5[x]$

(a) Is $\mathbb{Z}_5[x]/(P(x))$ a field?

(b) Find the unique representatives of $[x^4-2x^2-2x]$ in $\mathbb{Z}_5[x]$

(C) $\mathbb{Q}[x]/(5x^4-50x^2-25]$ as field?

($\mathbb{Z}_p$ for $p \neq 2$)

快速看 reducible / not

$\mathbb{Z}_p/f(x)$

↑

$|p^n|$ $n = \deg(f)$

(a) $\varphi_5(P(x))$: when $x=0 \Rightarrow P(x) = [1]$

$x=1 \Rightarrow P(x) = [3]$

$x=2 \Rightarrow P[x] = [2]$

$x=3 \Rightarrow P[x] = [3]$

$x=4 \Rightarrow P[x] = [1]$

$P(x)$ does not have roots

+

$\deg P(x) < 3$

$\Rightarrow P(x)$ is irreducible $\Leftrightarrow$ $\mathbb{Z}_5[x]/P(x)$ is a filed

(b)

$[ax+b] = r(x)$ with $a \in [5]$ $b \in [5]$ are all unique representative.

$x^2+x+6 = [0] \Rightarrow [x]^2 = [-x-6]$

$x^4 = [-x-6]^2 = [-x-1]^2 = x^2+2x+1$

+

$2x^2 = 2[4x+4] = 2x+2$ + $-2x$ is unique

$= x^2+2x+2x-2x+1+2$

$= [x^2+2x]$

$= 2x-x+3$

$= x+2$.

(c)

$p(x) = 5(x^4 - 10x^2 - 5)$

let $p=5 \Rightarrow$ by eisenstein theorem $5 \mid 10,\ 25 \nmid -5,\ 5 \mid -5,\ 5 \nmid 1$

then $5(x^4-10x^2-5)$ is irreducible in $R[x] \Rightarrow$ irreducible in $Q[x]$.

$\Rightarrow \frac{Q[x]}{(5(x^4-10x^2-5))}$ is a field.

x^4+x^2+1 is irreducible in $\mathbb{Z}_2$

- Check no roots

$[0] := 0+0+1 = [1] \neq 0$

$[1] := 1+1+1 = [1] \neq 0$ $\Rightarrow$ No roots

$x^4+x^2+1 = (x^2+ax+b)(x^2+cx+d)$

$= x^4 + (a+c)x^3 + (b+d+ac)x^2 + (bc+ad)x + bd$

$\Rightarrow \begin{cases} a+c=0 \\ b+d+ac=1 \\ bc+ad=0 \\ bd=1 \end{cases} \Rightarrow (x^2+x+1)(x^2+x+1)$

$\Rightarrow \begin{cases} b+d-a^2=1 \Rightarrow a=1, c=1 \\ a(d-b)=0. \\ bd=1. \Rightarrow b=d=1 \end{cases}$

(b) divison

$$
\begin{array}{r}
x^2-x+3 \\
x^2+x+1 \overline{)\ x^4+3x^2+2x} \\
\underline{x^4+x^3+x^2} \\
-x^3+2x^2+3x \\
\underline{-x^3-x^2-x} \\
3x^2+4x \\
\underline{3x^2+3x+3} \\
x-3 = [x+2]
\end{array}
$$

Prob 2. (a) Show that ideal $\langle x-1 \rangle$ in $\mathbb{Z}[x]$ is prime / is maxmal ?

Hint: $f(p(x)) = p(1)$

Answer:

eval: $f : \mathbb{Z}[x] \to \mathbb{Z}$

$f(kx) = k \leftarrow k \in \mathbb{Z}$. surjective

$\ker(f) \subseteq \langle (x-1) \rangle$: 1) let $p(x) \in \ker(f)$ $f(p(x)) = 0$

$\Updownarrow$

$p(1) = 0$

$\Updownarrow$

$(x-1) \mid p(x)$

$\langle (x-1) \rangle \subseteq \ker(f)$:

2) let $p(x) \in \langle (x-1) \rangle$

$\Updownarrow$

$p(x) = (x-1) \cdot l(x)$

$f(p(x)) = f((x-1)l(x)) = (1-1) \cdot l(1) = 0 \in \ker(f)$

$\frac{\mathbb{Z}[x]}{\langle (x-1) \rangle} \cong \mathbb{Z}$

← not a field $\Leftrightarrow$ not a maximal ideal

↑ integer domain $\Leftrightarrow$ prime ideal

ie : P is prime $\Leftrightarrow$ R/P is int-dom

P is max $\Leftrightarrow$ R/P is field

every field is an integer domain but $\forall$ int-dom is a field

$\Updownarrow$

$\forall$ max ideal $\rightarrow$ prime ideal

$\forall$ prime ideal $\neq$ max ideal

3. (a) if G is a group and $a, b \in G$ Show $|ba| = |ab|$

say $|ab| = n$ $|ba| = m < \infty$

Answer $(ab)\cdot(ab)\cdots(ab) = 1$ (n times) $\qquad (ba)\cdot(ba)\cdots(ba) = 1$ (m times)

for $(ab)^n = 1$

$(ab)^n \cdot a = a$

$a\underbrace{(ba)\cdots(ba)}_{\text{"ba" } n \text{ times}} = a \Rightarrow (ba)^n = 1$, then $m \le n$ and

similarly for $(ba)^m = 1$

$(ba)^m \cdot b = b$

$\Downarrow$

$m = n$

$\Uparrow$

$b\underbrace{(ab)\cdot(ab)\cdots(ab)}_{m \text{ time}} = b \Rightarrow (ab)^m = 1$, then $m \ge n$.

(b) Show that explicitly for rs and $sr \in D_4$.

$r^4 = 1$, $s^2 = 1$, $sr = r^3 s$

$rs = r^5 \cdot s = r^2 r^3 s = r^2 sr$

$rs = r \cdot r^3 \cdot ss = r^4 \cdot s^2 = 1 \cdot 1 = 1$

$(sr)^2 = (sr)\cdot(sr) = (r^3 s)(sr) = r^4 = 1$.

4. (a) Prove $H = \{(a, b) \mid a - b = 0\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

is a cyclic - sub group

$\boxed{H = \langle (1,1) \rangle}$

(b) Explain why $H \cong \mathbb{Z}$ and $H \ncong S_{\mathbb{Z}}$.

① $f: \mathbb{Z} \to H \quad a \to (a,a)$
prove isomorphism.

② $S_{\mathbb{Z}}$ is not cyclic ($S_{\mathbb{Z}} = \{\sigma : \mathbb{Z} \to \mathbb{Z} \mid \sigma \text{ is a bijection}\}$.

$\sigma : n \to -n$
$\sigma^2 = 1$

(c) Show $f: \underset{\| \text{lc}}{H} \to \underset{\| \text{ls}}{2\mathbb{Z}}$ defined by $f(a,b) = a+b$ is an iso.
$\langle (1,1) \rangle \quad \langle 2 \rangle$

$f(1,1) = 2$

the homomphism

Nov 16th. (Futurama theorem.)

transposition $(1,2)$

$id = (1,2)$? $(1,2)^{-1} = (1,2)$

can we write $(1,2)$ using transposition. without using $(1,2)$ and any transposition twice?

Answer: No for S_3, Yes for $S_n : n \geq 4$.

Chapter 8 !!! great success !!!

8.1 Congruence

[in rings: $a \equiv b \pmod I \iff a-b \in I$]

$\downarrow$ multiplicative notation

$ab^{-1} \in I$ [?]

Let $k \subseteq G$ subgroup, $a, b \in G$ we say a congruent to $b \pmod k$ "$a \equiv b \pmod k$"

($\uparrow$ additive: $a-b \in K$; $a = k-b$, $\uparrow$ additive)

if $ab^{-1} \in k \iff \exists k, ab^{-1} = k \in k \iff \exists k: a = kb$

Ex: ① $K = n\mathbb{Z} \subseteq \mathbb{Z}$ if $a \equiv b \pmod k \iff a-b \in K \iff a \equiv b \pmod n$

② $k = \langle r \rangle \subseteq D_4$ (= $\{id, r, r^2, r^3\}$)

• $s \equiv rs \pmod k$ since $s(rs)^{-1} = s(s^{-1} \cdot r^{-1}) = r^3 \in k$

[or $a = s$ $b = rs$

$s = r^2(rs)$ and $r^2 \in K$, so $s \equiv rs \pmod K$]

③ · $s \equiv r^2 s \pmod k \Rightarrow s(r^2 s)^{-1} = s \cdot s^{-1} \cdot (r^2)^{-1} = r^2 \in k$

④ $H = \{f \in S_4 \mid f(4) = 4\} \subseteq S_4$

$= \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ * & * & * & 4 \end{pmatrix} \right\} \cong S_3$

$= \{id, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

$(1\,2)(3\,4) \equiv (3\,4) \pmod H$ since $(1\,2)(3\,4)[(3\,4)^{-1}] = (1\,2)(3\,4)(4\,3)$

$= (1\,2)$

or $(1\,2)(3\,4) = (1\,2)(3\,4) \Rightarrow (1\,2)(3\,4) \equiv (3\,4) \pmod H$

($(1\,2) \in H$)

Them: 8.1 Congruent modulo K is an equivalent relation:

1) reflexive: $a \equiv a \pmod{K}$ $\forall a \in G$

2) symmetric: $a \equiv b \pmod{K} \iff b \equiv a \pmod{K}$

3) transitive: $\left.\begin{matrix} a \equiv b \pmod{K} \\ b \equiv c \pmod{K} \end{matrix}\right\} \to a \equiv c \pmod{K}$

pf: (i) $e = aa^{-1} \in K \longrightarrow a \equiv a \pmod{K}$

(ii) say $a \equiv b \pmod{K} \to ab^{-1} \in K \overset{K \text{ subgroup}}{\Rightarrow} (ab^{-1})^{-1} \in K \to ba^{-1} \in K \to b \equiv a \pmod{K}$

(iii) say $\begin{matrix} a \equiv b \pmod{K} \to ab^{-1} \in K \\ b \equiv c \pmod{K} \to bc^{-1} \in K \end{matrix}$ $\overset{K \text{ subgroup} = \text{close multiplication}}{\Rightarrow} (ab^{-1})(bc^{-1}) \in K \Rightarrow ac^{-1} \in K \to a \equiv c \pmod{K}$

Def: Let $a \in G$, $K \subseteq G$ subgroup, the congruent class of $a \pmod{K}$ is the set

$$[a] = \{b \in G \mid b \equiv a \pmod{K}\} = \{ka \mid k \in K\} = Ka$$

$\left(\begin{matrix} ba^{-1} \in K \\ b = ka \text{ for some } k \in K \end{matrix}\right.$ "Ka is called a (right) coset"

Warning: we can also define left cosets: aK, in general $Ka \neq aK$

If G is additative, then $[a] = K + a$

Example $H = \{f(4) = 4\} \subseteq S_4$.

find coset represented by $\sigma = (1\,2\,4) \in S_4$.

$$[\sigma] = H\sigma = \{id. (12). (13) (23) (123) (132)\}\sigma$$

$$= \{(124)\ (24)\ (1234)\ (1324), (13)(24), (343)\}.$$

practice: $(123)(124) = (13)(24)$

$[(24)] = H = \{(24),\ (12)(24)\ (13)(24)\ (23)(24)\ (123)(24)\ (132)(24)\}$

(24) (124) $(13)(24)$ (243) (1243) (1324)

$(123)(24) = (1243)$

$[(124)] = [(24)]$

Theorem 8.2:

$$a \equiv b \pmod{K} \iff Ka = Kb$$

$$a \not\equiv b \pmod{K} \iff Ka \neq Kb \text{ and } Ka \cap Kb = \emptyset \text{ (disjoint)}$$

In particular $Ka = Ke = K \iff ae^{-1} \in K \iff a \in K$

Example: $H \leq S_4$ find all the right cosets

$$H = H_{id} = \{id.\ (12),\ (13)\ (23)\ (123)\ (132)\}$$
$$= [(12)] = [(13)] = [(23)] = \cdots$$

pick element $[(14)]$ $H_{(14)} = \{(14)\ (142)\ (143).\ (23)(14),\ (1423)\ (1342)\}$

$$= H_{(142)} \text{ -----}$$

$H_{(124)} = H_6 =$ 6 elements

$H_{(34)} = \{(34),\ (12)(34),\ (134),\ (234),\ (1234)\ (1342)\}$

$S_4 = H \cup H_{(14)} \cup H_{(24)} \cup H_{(34)}$

we got 4 cosets.

Nov 28th (Classify)

Sec 8.1 - continued

Recall: if we have $K \subseteq G$ (subgroup) "$\frac{a}{b}$"

mult: $a \equiv b \pmod{K}$ if $ab^{-1} \in K \iff a = kb$ (for some $k \in K$)

add: $a \equiv b \pmod{K}$ if $a - b \in K \iff a \in Kb$

"We saw it is an equivalence relation"

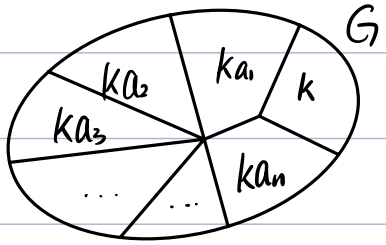
equivalence class $[a] = \{b \in G \mid a \equiv b \pmod{K}\} = Ka$ "right coset"

$= (K+a$ in additive$)$

- $Ka = Kb \iff a \equiv b \pmod{K} \iff b \in Ka$ or $a \in Kb$

$[Ka = K$ iff $a \in K]$

- $Ka \cap Kb = \emptyset \iff a \not\equiv b \pmod{K}$



- $G = \bigcup_{a \in G} Ka$

Example: ① $H = \{f \in S_4 \mid f(4) = 4\} \subseteq S_4$.

i) $H = H_{id}$

ii) $H_{(1,2,4)} = \{(1,2,4), (2,4), \cdots\} = H_{(2,4)}$

iii) $H_{(1,4)} \supset H_{(3,4)}$ "All the element"

$S_4 = H \cup H(24) \cup H(14) \cup H(34)$

② $K = \langle r \rangle \subseteq D_4$

$K = K_{id} = \{id, r, r^2, r^3\} = Kr = Kr^2 = Kr^3$ 8 element.

$Ks = \{s, rs, r^2s, r^3s\} = Ks = Krs = Kr^3s$

$D_4 = K \cup Ks$

Def: The index of K in G "$[G:K]$" = # of distinct right coset of K in G.

Example: ① $[S_4 : H] = 4$

② $[D_4 : K] = 2$

③ $[\mathbb{Z} : n\mathbb{Z}] = n$

infinite ④ $[\mathbb{Q} : \mathbb{Z}] = \infty \longrightarrow \mathbb{Z} + \frac{1}{n} \neq \mathbb{Z} + \frac{1}{n+1}$ for any $n \in \mathbb{N}$

since $\frac{1}{n} - \frac{1}{n+1} = \frac{1}{n+1} \notin \mathbb{Z}$

so $\frac{1}{n} \not\equiv \frac{1}{n+1} \pmod{\mathbb{Z}}$

In fact: we get infinite $\{\mathbb{Z}, \mathbb{Z}+\frac{1}{2}, \mathbb{Z}+\frac{1}{3}, \cdots\}$ infinite of distinct cosets

lemma 8.4: $\forall a \in G$. $K \subseteq G$ subgroup

The # of elements in $Ka = |K|$ "order"

proof: There is a bijection function $\varphi : K \to Ka$

$\varphi(k) = ka$

- surjective: let $ka \in Ka$. then $\exists\ \varphi(k) = ka$ $Ka = \mathrm{Im}\varphi$
- injective: if $\varphi(k_1) = \varphi(k_2)$

$k_1 a = k_2 a \Rightarrow$ one to one

$k_1 = k_2$ ▨

Theorem 8.5: Lagrange's theorem

G finite group. $K \subseteq G$ (subgroup) then $|G| = |K| \cdot [G:K]$

⇐ proof: $[G:K] = r$ "$Ka_1, Ka_2, \cdots Ka_r$ distinct"

$G = Ka_1 \cup Ka_2 \cup Ka_3 \cdots \cup Ka_r$ (disjoint)

$|G| = (\#\text{ element in } Ka_1) + (\#\text{ element } Ka_2) + \cdots + (\#\text{ element in } Ka_r)$

$= |K| + |K| + \cdots + |K|$ "r times"

$= |K| \cdot r = |K| \cdot [G : K]$ ▨

Cor: $|K| \mid |G|$ and $[G : K] = \frac{|G|}{|K|}$

Example: • $|G| = 6$ G have no subgroup of order 5, 4

• $[S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{n!}{(\frac{n!}{2})} = 2$

Cor 8.6: G is finite, $a \in G$ (a) $|a| \mid |G|$

(b) $a^{|G|} = id = e$

proof: (a) as $|a| = |\langle a \rangle|$, $\langle a \rangle$ is subgroup of G

so $|a| \mid |G|$ as $|\langle a \rangle| \mid |G|$

(b) as $|G| = k|a|$, so $a^{|G|} = a^{k|a|} = (a^{|a|})^k = (e)^k = e$

Example: ① $|\mathbb{Z}_4| = 4$, so possible order of elements : 1, 2, 4.

indeed $|0| = 1$

$|3| = |1| = 4$

$|2| = 2$

② $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, so possible order 1, 2, 4

$|(0,0)| = 1$

$|(1,1)| = 2 = |(1,0)| = |(0,1)|$

and we don't have an element of order 4.

③ $|U_p| = |Z_p / \{0\}| = p-1$. so by (b)

for any $a \in U_p$. $a \neq 0 \Longrightarrow a^{p-1} = 1$

$\Downarrow$

$\forall a \in U_p$, $a^p = a$

$\Downarrow$

大师之作 !!! $\forall a \in \mathbb{Z}$ $a^p \equiv a \pmod p$

④ $|Z_5| = 5$ possible order of elements: 1, 5

$|0| = 1$ ← ↓ $|1| = |2| = |3| = |4|$

so $Z_5 = \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$

Them 8.27: if a order of Group $|G| = p$ (prime)

then $G \cong Z_p$

proof: if $0 \neq a \in G$. then by lagon $|a| \mid |G| = p$

so $|a| = p$ so $G = \langle a \rangle$ cyclic $\Rightarrow G \cong Z_p$ ▨

Example: $|U_6| = |\{1, 5\}| = 2 \Rightarrow U_6 \cong \mathbb{Z}$

Them 7.8 if $|G| = 4$. then either $G \cong Z_4$ (✓ cyclic) or $G \cong Z_2 \times Z_2$ (✓ x cyclic)

proof: possible $|a| = 1, 2, 4$

① if $a \in G$, $4 = |a|$, then it is cyclic and $G \cong Z_4$

② if $a \in G$. $|a| \neq 4$. all non-identity elements are order of 2

$G = \{e, a, b, c\}$ $|a| = |b| = |c| = 2$

$\Rightarrow a^{-1}=a\ ;\ b^{-1}=b\ ;\ c^{-1}=c$ (abelian $\to G$)

what is ab? $ab \neq e \leftarrow b=a^{-1}=a$

$ab \neq a \leftarrow b=e$

$ab \neq b \leftarrow a=e$

$ab=c$ ✓

same way $ac=b\ ;\ bc=a$

补充一个 f: so the multiplication operation is just like in $\mathbb{Z}_2\times\mathbb{Z}_2$

ie $G \xrightarrow{\sim} \mathbb{Z}_2\times\mathbb{Z}_2$ "Exp"

$e \longrightarrow (0,0)$

$a \longrightarrow (0,1)$

$b \longrightarrow (1,0)$

$c \longrightarrow (1,1)$

Example: $K_4 = \{id, (12)(34), (13)(24), (14)(23)\} \subseteq A_4$

$|K_4| = 4$

$|(12)(34)| = 2 = |(14)(23)| = |(13)(24)|$

"length" So $K_4 \cong \mathbb{Z}_2\times\mathbb{Z}_2$

abelian $\times$ abelian

Them 8.6 $|G|=6$ then $G \cong \mathbb{Z}_6$ or $G \cong D_3$

Example: • $|\mathbb{Z}_2\times\mathbb{Z}_3| = 6 \Rightarrow \mathbb{Z}_2\times\mathbb{Z}_3 \cong \mathbb{Z}_6$

is of order 6 and abelian

• $|S_3| = 6 \Rightarrow S_3 \cong D_3$

as S_3 is not abelian

• $|U_{16}| = 6 \Rightarrow U_{16} \cong \mathbb{Z}_6$

as U_{16} is abelian

Classification to standard groups

order	isomophic $\Leftrightarrow$ groups
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	(cyclic) $\mathbb{Z}_4$ / $\mathbb{Z}_2 \times \mathbb{Z}_2$ (other)
5	$\mathbb{Z}_5$
6	(abelian) $\mathbb{Z}_6$ / D_3 (otherwise)
7	$\mathbb{Z}_7$

Sec 8.2 normal subgroup.

Recall: Given $K \subseteq G$ subgroup we have $a \equiv b \pmod K$ if $ab^{-1} \in K$, $[a] = Ka = \{ka \mid k \in K\}$.

Can we have operation on the cosets?

for that we need K to be normal.

Def: Subgroup $N \subseteq G$ is normal in G ("Normal Subgroup of G") if: $\forall g \in G : Ng = gN$

equivalently: $\forall g \in G : g^{-1}Ng = N$

$\Leftrightarrow \forall g \in G, n \in N: g^{-1}ng \in N$

Example: ① $\{e\}$. G are normal subgroup of G (N is closed under conjugation by $g \in G$)

($geg^{-1} = gg^{-1} = e \in \{e\}$. $\forall g \in G$)

(gxg^{-1}, $x \in G$. then $gxg^{-1} \in G$. $\forall x \in G$. $g \in G$)

② $\langle r \rangle \subseteq D_4$ is normal

we have two right coset: $\langle r \rangle$ and $\langle r \rangle s$

$\langle r \rangle s = \{s, rs, r^2s, r^3s\}$

$s\langle r \rangle = \{s, sr, sr^2, sr^3\} = \{s, r^3s, r^2s, rs\}$.
"$sr = r^3s$"

③ $\langle s \rangle$ is not normal in D_4.

Take $r^{-1}\langle s \rangle r = r^3\{id, s\}r = \{r^3r, r^3sr\} = \{id, r^2s\} \neq \langle s \rangle$.

④ If G is abelian, all subgroup are normal. !!!

why? $\forall g \in G \quad gN = \{gn \mid n \in N\} = \{ng \mid n \in N\} = Ng$.

Note: if N is abelian, it is not enough !

ex: ($\langle s \rangle \subseteq D_4$)
↓
Abelian

⑤ The center of G: $Z(G) = \{x \in G \mid \forall g \in G : xg = gx\}$.

is a normal subgroup of G.

why? $\forall g \in G, x \in Z(G) : g^{-1}xg = g^{-1}gx = idx = x \in Z(G)$

⑥ $SL(n, R) \subseteq GL(n, R)$ is normal subgroup
||
$\{A : \det A = 1\}$

WTS: $\forall A \in SL(n, R), B \in GL(n, R) : B^{-1}AB \in SL(n, R)$.

$\det(B^{-1}AB) = \det(B^{-1}) \det(A) \det(B)$

$= \det(B^{-1}B) \det(A)$

$= 1 \Rightarrow B^{-1}AB \in SL(n, R)$

① $A_n \subseteq S_n$ is a normal subgroup

WTS: $\forall \sigma \in S_n, \tau \in A_n : \quad \sigma^{-1}\tau\sigma \in A_n$

write $\sigma = \pi_1 \pi_2 \cdots \pi_m$ where π_i are transportation

$$\sigma^{-1} = \pi_m^{-1} \cdots \pi_2^{-1} \pi_1^{-1} = \pi_m \cdots \pi_2 \pi_1$$

Now $\sigma^{-1}\tau\sigma = \overbrace{\pi_m \cdots \pi_1}^{m \text{ time}} \underbrace{\tau}_{\substack{m \\ \text{even}}} \overbrace{\pi_1 \cdot \pi_2 \cdots \pi_m}^{m \text{ time}}$.

"Even" (2m + even number) times transportations $\Rightarrow \sigma^{-1}\tau\sigma \in A_n$.

If $N \subseteq G$ is normal. then we can define an operation of cosets:

$$Na * Nb = Nab$$

(If N additive : $(N+a)+(N+b) = N+(a+b)$)

but we need to show it is well defined

Them 8.1 (operation is well defined)

Let $N \subseteq G$ be normal subgroup. if $\begin{cases} Na_1 = Na_2 \\ Nb_1 = Nb_2 \end{cases}$, then $Nab_1 = Na_2b_2$.

proof $Na_1 = Na_2 \rightarrow n = a_1 a_2^{-1} \in N$

$Nb_1 = Nb_2 \rightarrow n' = b_1 b_2^{-1} \in N$

WTS: $a_1 b_1 (a_2 b_2)^{-1} \in N$

$\Rightarrow a_1 b_1 b_2^{-1} a_2^{-1}$

$\Rightarrow a_1 (n' a_2^{-1})$

$\Rightarrow a_1 a_2^{-1} a_2 n' a_2^{-1}$

$\Rightarrow n(a_2 \underset{\in N}{n'} a_2^{-1})$ as N is normal

$\Rightarrow$ then n (element of N) $\in N$.

$\Rightarrow Na_1b_1 = Na_2b_2$

Def: $G/N = \{Na \mid a \in G\}$ set of all right coset "Sec 8.3"

Them 8.13: If $N \subseteq G$ is normal, then G/N is a group

① $\begin{cases} NaNb = Nab \\ e_{G/N} = Ne = N \end{cases}$

④ $(Na)^{-1} = Na^{-1}$

G/N is called the quotient group of G by N

$$\left|G/N\right| = [G:N]$$

Example:

① $3\mathbb{Z} \subseteq \mathbb{Z}$ "$\mathbb{Z}$ abelian $\Rightarrow 3\mathbb{Z}$ normal"

$$\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}+a \mid a \in \mathbb{Z}\} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$$

$$\cong \mathbb{Z}_3$$

In general $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

② $\langle r \rangle \subseteq D_4$ is normal subgroup

$$D_4/\langle r \rangle = \{\langle r \rangle x \mid x \in D_4\} = \{\langle r \rangle, \langle r \rangle s\} \cong \mathbb{Z}_2$$

"every group of order 2 $\cong \mathbb{Z}_2$"

We can indeed see.

$$(\langle r \rangle s)(\langle r \rangle s) = \langle r \rangle s^2 = \langle r \rangle id = e_{D_4/\langle r \rangle}$$

③ $\langle r^2 \rangle \subseteq D_4$ that is normal subgroup, in fact ($Z(D_4) = \langle r^2 \rangle$)

$\{id, r^2\}$

by lagrange $\left|D_4/\langle r^2 \rangle\right| = [D_4 : \langle r^2 \rangle] = |D_4|/|\langle r^2 \rangle| = 8/2 = 4.$

then $D_4/\langle r^2\rangle \cong Z_2 \times Z_2$ or Z_4

so check order of element in $D_4/\langle r^2\rangle$

- The order of $\langle r^2\rangle$ is 1,
- The order of $\langle r^2\rangle r = 2$.

(the possible order → $\langle r^2\rangle r$ is 1, 2, 4
$(\langle r^2\rangle r)^1 \neq id$, $(\langle r^2\rangle r)^2 = \langle r^2\rangle r^2 = N$)

- The order of $\langle r^2\rangle s = 2$

($\langle r^2\rangle s \neq id$. $(\langle r^2\rangle s)^2 = \langle r^2\rangle id = N$)

- The order of $\langle r^2\rangle rs$ is 2

($\langle r^2\rangle rs \neq N$
$(\langle r^2\rangle rs)^2 = N = \langle r^2\rangle id$)

"$D_4/\langle r^2\rangle$"

Thus $D_4/\langle r^2\rangle \cong Z_2 \times Z_2$. (All element are of order 2)

Ex 4. $SL(n,R) \leq GL(n,R)$ is Normal

$$\frac{GL(n,R)}{\langle SL(n,R)\rangle} = \{ SL(n,R)A \mid A \in GL(n,R) \}$$

$$(SL(n,R)A)(SL(n,R)B) = SL(n,R)AB$$

$$e_{\frac{GL(n,R)}{SL(n,R)}} = SL(n,R)\cdot I = SL(n,R)$$

Execcise : find the order of $\langle 4\rangle + 13$ in $Z_{20}/\langle 4\rangle$

$N = \langle 4\rangle = \{0, 4, 8, 12, 16\}$. possible $1:2:4$

$|N| = 5$ then by lagrange $[\mathbb{Z}_{20} : N]$

"$\mathbb{Z}_{20}/\langle 4\rangle \cong \mathbb{Z}_4$" $\Leftarrow \left|\frac{\mathbb{Z}_{20}}{N}\right| = \frac{20}{5} = 4.$

1. $(N+13) \neq N \rightarrow$ order $\neq 1$
2. $(N+13)^2 = N+26 = N+6 \neq N$

$\Downarrow$

then order of $\langle 4\rangle + 13$ has to be 4.

Remark: $N+13 = N+1$ and we can do calculation this way.

$(N+12)+1$

"N"

In general: $(Na)^n = N \iff a^n \in N$

Dec 5th Note

Sec 8.3 — Cont

Recall: $N \subseteq G$ is a normal subgroup

If $\forall g \in G.\ gN = Ng$

$\forall g \in G\ \ g^{-1}Ng \subseteq N$

$\forall g \in G\ n \in N.\ g^{-1}ng \in N$

1> then $G/N = \{Na \mid a \in G\}$.

is the quotient group.

$(Na = Nb \iff a \equiv b \pmod N \iff ab^{-1} \in N)$

i> $(Na)(Nb) = N(ab)$

ii> $e_{G/N} = Ne = N$

iii> $(Na)^{-1} = Na^{-1}$

Examples: $D_4/\langle r\rangle = \{\langle r\rangle, \langle r\rangle s\}$.

✓ lagrange them

$[D_4 : r] = \frac{8}{4} = 2$

operation table (*)

	$\langle r\rangle$	$\langle r\rangle s$
$\langle r\rangle$	$\langle r\rangle$	$\langle r\rangle s$
$\langle r\rangle s$	$\langle r\rangle s$	$\langle r\rangle$

Properties of G/N:

① Claim: if G is abelian, then G/N is abelian.

"$\Leftarrow$" 不一定正确. "$G/\langle r\rangle \cong \mathbb{Z}_2$, but not abelian"

Them 8.14

G/N is abelian $\iff$ $\forall a, b \in G$, $aba^{-1}b^{-1} \in N$

(commutator's)

pf: "$\Rightarrow$" $Na \cdot Nb = Nb \cdot Na$

$N(ab) = N(ba)$

$\Rightarrow ab \equiv ba \pmod N$

$\Rightarrow ab(ba)^{-1} \in N \Rightarrow aba^{-1}b^{-1} \in N$

"$\Leftarrow$" WTS: $Na \cdot Nb = Nb \cdot Na$

known $aba^{-1}b^{-1} \in N$. then $ab(ba)^{-1} \in N$.

then $Nab = Nba$ so. G/N is abelian.

$$\begin{array}{ccc} Nab & = & Nba \\ \| & & \| \\ NaNb & = & Nb \cdot Na \end{array}$$

Example: $GL(n,R)$:= invertible $n \times n$ matrix

$SL(n,R)$:= "$\det A = 1$"

$V = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ a_{n+1} \end{bmatrix}$

is abelian

"WTS $ABA^{-1}B^{-1} \in SL(n,R)$" ▨

for $\forall A, B \in GL(n,R)$

$$\det(ABA^{-1}B^{-1}) = \det(A)\cdot\det(A^{-1})\cdot\det(B)\cdot\det(B^{-1})$$

$$= \det(I_n) = 1.$$

$\Rightarrow \frac{GL(n,R)}{SL(n,R)}$ is abelian.

Thm 8.15 : If $\frac{G}{Z(G)}$ is cyclic, then G is abelian.

("center")

"Center is always normal subgroup"

proof: let: $\frac{G}{Z} = \langle Zx \rangle$

WTS: G is abelian, $\forall a, b \in G.\ ab = ba$

$$Za = (Zx)^p = Z(x^p)$$

$$Zb = (Zx)^q = Z(x^q)$$

then $a \equiv x^p \pmod N \Rightarrow a = z_1 x^p$ (for some $z_1 \in Z$)

$b \equiv x^q \pmod N \Rightarrow b = z_2 x^q$ (for some $z_2 \in Z$)

$$ab = (z_1 x^p)(z_2 x^q)$$

$$= z_1 x^p z_2 x^q \quad (Z \text{ is commuter})$$

$$= z_2 z_1 x^p x^q \quad \text{ie } "x^p x^q = x^{p+q} = x^q \cdot x^p"$$

$$= (z_2 x^q)(z_1 x^p)$$

$$= ba$$ ▨

Application: Examples

Q: $|G| = 10$ + non-abelian, show Center $Z(G)$ is trival

A: By lagrange the possible $|Z(G)| = 1, 2, 5, 10$

if $|Z_G| = 1$, then it is trival

$|Z_G| \neq 10$, as otherwise. G is abelian

$|Z_G| = 2$. then $|G/Z_G| = 5$ (prime) $\Rightarrow$ $G/Z_G \cong Z_5$ and it's cyclic

$\Rightarrow$ G/ZG is abtliam by Them 8.15

Similary for $|Z_G| = 5$, then $|G/Z_G| = 2$ (prime)

Thus $|Z_G|$ can only be 1, which implies that $Z(G)$ is trival $= \{e\}$.

Sec 8.4. Quotient + Homomorphism.

Them: 8.16:

Let $f: G \longrightarrow H$ be homo!

then $\ker f \leq G$ and is normal.

proof:

$\forall g \in G. \forall x \in \ker f$. WTS $g^{-1}xg \in \ker f$

$f(g^{-1}xg) = f(g^{-1}) \cdot f(x) \cdot f(g)$

$= f(g^{-1}) \cdot e_G \cdot f(g)$

$\| $

$f(g)^{-1}$

$= f(g)^{-1} \cdot f(g) = e_G \in \ker f$