Chapter 14

Ideals and factor Rings

Defn:- An ideal I of a ring R is a subring of R such that $\forall a \in A$ and $\forall r \in R$

ar and ra are in A.

that is $r \cdot A \subseteq A$ and $A \cdot r \subseteq A$.

Defn:- An ideal A is proper ideal if $A \subset R$

i.e proper subset.

Ideal Test:-

A nonempty subset A of a ring R is an ideal of R if

1) $\forall a, b \in A$, $a - b \in A$.
2) $\forall a \in A, \forall r \in R$, ar and $r.a \in A$.

Examples: 1) $\{0\}$ and R are ideals of R (Trivial ideals)

2) $n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n\}$ is an ideal of $\mathbb{Z}$

3) let R be Commatative ring with unity let $a \in R$, then $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called principle ideal generated by a

proof: 1) let $ra, sa \in \langle a \rangle$ then $ra - sa = (r-s)a = r'a \in \langle a \rangle$

2) let $r \in R$ and $sa \in \langle a \rangle$ then $r.(sa) = (rs)a = r'a \in \langle a \rangle$.

so by ideal test $\langle a \rangle$ is an ideal of R.

④ Let $R = \mathbb{R}[x]$ = all polynomials with real coefficients.

Let $A = \{ f \in R \mid f(0) = 0 \}$ then A is an ideal of R and $A = \langle x \rangle$.

⑤ Let R be commutative ring with unity

Let $a_1, a_2 \in R$.

Define $I = \{ r_1 a_1 + r_2 a_2 \mid r_1, r_2 \in R \}$ then R is an ideal. (satisfies conditions 1,2 of ideal test)

since

1) if $r_1 a_1 + r_2 a_2$, $s_1 a_1 + s_2 a_2 \in I$ then

$$(r_1 a_1 + r_2 a_2) - (s_1 a_1 + s_2 a_2) = (r_1 - s_1) a_1 + (r_2 - s_2) a_2$$
$$= r' a_1 + s' a_2 \in I.$$

2) if $r_1 a_1 + r_2 a_2 \in I$ and $r' \in R$ then

$$r'(r_1 a_1 + r_2 a_2) = (r' r_1) a_1 + (r' r_2) a_2$$
$$= r^{*} a_1 + s a_2 \in I$$

wher $r = r' r_1$, $s = r' r_2$

I is written $\langle a_1, a_2 \rangle$ called the ideal generated by a_1, a_2.

<u>Notice</u> We can generalize last example to if $a_1, a_2, \dots, a_n$ then $I = \{ r_1 a_1 + \dots + r_n a_n \mid r_i \in R \}$ written $\langle a_1, a_2, \dots, a_n \rangle$

⑥ Let $R = \mathbb{Z}[x]$ all polynomials with Integer Coefficients

Let $I = \{ p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z} \}$ all polynomials with even constant terms.

say $p(x) = x^2+5x+2$, $q(x) = x^5+4x^2+7x+8$

i.e the contant term is even or $p(0) = q(0) \in 2\mathbb{Z}$

then I is ideal of $\mathbb{Z}[x]$ and

$$I = \langle x, 2 \rangle$$

⑦ $R \neq$ ~~$\mathbb{R}[x]$~~ All real valued functions as $\sin x$, e^x, x^2, $|x|$, ...

$S =$ all differentiable functions

then S is a subring of R since

1) if $f, g \in S$ then $f - g \in S$

i.e difference of differentiable is differentiable

2) if $f, g \in S$ then $f \cdot g \in S$ since product of diff is diff.

But S is not ideal of R since

condition (2) of ideal test is not satisfied

Ex:- $f(x) = 2 \in S$, $g(x) = |x| \in R$

but $g(x) \cdot f(x) = 2|x| \notin S$.

Factor Rings:

Def: Let R be a ring, I an ideal of R then $R/I = \{r+I, r \in R\}$ is the set of all left cosets of I.

Th:- if R is a ring, I ideal of R then $(R/I, +, \cdot)$ is a ring with respect to $+, \cdot$ defined as

$(r+I)+(s+I) = (r+s)+I$ and

$(r+I)\cdot(s+I) = r.s+I$

this ring is called factor ring.

proof:- See text (Excercise). page 26.4

Examples: ① $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$ defined as above is a ring w.r. to $+$ and $\cdot$

for example
$$(2+4\mathbb{Z})+(3+4\mathbb{Z}) = (2+3)+4\mathbb{Z} = 5+4\mathbb{Z} = (1+4)+4\mathbb{Z} = 1+(4+4\mathbb{Z}) = 1+4\mathbb{Z}.$$

$$(2+4\mathbb{Z})\cdot(3+4\mathbb{Z}) = 6+4\mathbb{Z} = 2+(4+4\mathbb{Z}) = 2+4\mathbb{Z}.$$

we will rite $\mathbb{Z}/4\mathbb{Z}$ as $\mathbb{Z}_4$.

(5) Let $\mathbb{R}[x]$ = all polynomials with real coefficients.

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

then $\mathbb{R}[x]/\langle x^2+1\rangle = \{ g(x) + \langle x^2+1\rangle \mid g(x)\in\mathbb{R}[x]\}$

as example (4) above this factor ring can be simplified more.

<u>First:-</u> any $g(x)\in\mathbb{R}[x]$ by division algorithm can be written as $g(x) = q(x)(x^2+1) + r(x)$ where $r(x)=0$ or degree $r(x) < \deg x^2+1$

and $q(x)$ is the quotient

so $r(x)=0$ or $r(x) = ax+b$ where $a,b\in\mathbb{R}$

$$\text{So } \mathbb{R}[x]/\langle x^2+1\rangle = \{ r(x) + q(x)(x^2+1) + \langle x^2+1\rangle \}$$
$$= \{ r(x) + \langle x^2+1\rangle \}$$
$$= \{ a+bx + \langle x^2+1\rangle \mid a,b\in\mathbb{R}\}$$

and also $x^2+1 + \langle x^2+1\rangle = 0 + \langle x^2+1\rangle$

$$\Rightarrow x^2 + \langle x^2+1\rangle = -1 + \langle x^2+1\rangle.$$

<u>for example:-</u> $(2+3x + \langle x^2+1\rangle) + (5+6x + \langle x^2+1\rangle)$

$$= (2+5) + (3+6)x + \langle x^2+1\rangle = 7 + 9x + \langle x^2+1\rangle$$

also $(2+3x + \langle x^2+1\rangle)\cdot(5+6x + \langle x^2+1\rangle)$

$$= (2+3x)(5+6x) + \langle x^2+1\rangle$$
$$= 10 + 12x + 15x + 9x^2 + \langle x^2+1\rangle$$
$$= (10-9) + 27x + \langle x^2+1\rangle$$
$$= -1 + 27x + \langle x^2+1\rangle$$

since $9x^2 + \langle x^2+1\rangle$
$= (9 + \langle x^2+1\rangle)\cdot(x^2 + \langle x^2+1\rangle)$
$= 9 + \langle x^2+1\rangle \cdot (-1 + \langle x^2+1\rangle)$
$= -9 + \langle x^2+1\rangle.$

② $2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$

notice that $6+6\mathbb{Z} = 0+6\mathbb{Z}$

$$14+6\mathbb{Z} = 2+12+6\mathbb{Z}$$
$$= 2+6\mathbb{Z}.$$

and $+, \cdot$ are mod 6 so $(2\mathbb{Z}/6\mathbb{Z}, \oplus_6, \otimes_6)$

is a ring For example.

$$(2+6\mathbb{Z}) + (4+6\mathbb{Z}) = 6+6\mathbb{Z} = 0+6\mathbb{Z}$$
$$(2+6\mathbb{Z}) \cdot (4+6\mathbb{Z}) = 8+6\mathbb{Z} = 2+6+6\mathbb{Z}$$
$$= 2+6\mathbb{Z}.$$

③ Let $R = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i \in \mathbb{Z} \right\}$, $I = \left\{ \begin{bmatrix} x & y \\ z & w \end{bmatrix} \;\; x,y,z,w \in 2\mathbb{Z} \text{ even.} \right\}$

then I is an ideal of R (see ideal test).

and $R/I = \left\{ \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I \mid r_i \in \{0,1\} \right\}$

for example $\begin{bmatrix} 5 & 17 \\ 2 & 12 \end{bmatrix} + I = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 4 & 16 \\ 2 & 12 \end{bmatrix} + I$

$$= \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + I.$$

since $\begin{bmatrix} 4 & 16 \\ 2 & 12 \end{bmatrix} \in I$ so $\begin{bmatrix} 4 & 16 \\ 2 & 12 \end{bmatrix} + I = I$.

so R/I is a ring containing 16 element.

④ the ring $\mathbb{Z}[i]/\langle 2-i\rangle$.

- any element of this factor ring has the form $a+bi+\langle 2-i\rangle$ by definition.

since $2-i \in \langle 2-i\rangle$ so in particular

$2-i+\langle 2-i\rangle = 0+\langle 2-i\rangle$ or

$2+\langle 2-i\rangle = i+\langle 2-i\rangle$. ---- (1)

so $4+5i+\langle 2-i\rangle = 4+\langle 2-i\rangle+(5+\langle 2-i\rangle)\cdot(2+\langle 2-i\rangle)$

$= 4+\langle 2-i\rangle + 10+\langle 2-i\rangle$

$= 14+\langle 2-i\rangle$.

<u>so far</u> $\mathbb{Z}[i]/\langle 2-i\rangle = \{a+\langle 2-i\rangle \mid a\in\mathbb{Z}\}$.

Furthermore $i+\langle 2-i\rangle = 2+\langle 2-i\rangle$

so $(i+\langle 2-i\rangle)^2 = (2+\langle 2-i\rangle)^2$

i.e $-1+\langle 2-i\rangle = 4+\langle 2-i\rangle$

Hence $5+\langle 2-i\rangle = 0+\langle 2-i\rangle$

So $\mathbb{Z}[i]/\langle 2-i\rangle = \{a+\langle 2-i\rangle \mid a=0,1,2,3,4\}$

Furthermore all these 5 elements in $\mathbb{Z}[i]/\langle 2-i\rangle$ are distinct since $|1+\langle 2-i\rangle| = 1$ or 5.

$|1+\langle 2-i\rangle| \neq 1$ since if $1+\langle 2-i\rangle = 0+\langle 2-i\rangle$

$\Rightarrow 1 \in \langle 2-i\rangle \Rightarrow 1 = (2-i)(a+bi)$

$= (2a+b)+(-a+2b)i$

$\Rightarrow \left.\begin{array}{l} 2a+b=1 \\ -a+2b=0 \end{array}\right\} \Rightarrow b=\frac{1}{5}\notin\mathbb{Z}$ ※.

Prime and maximal ideals.

Def^n:- 1) An ideal A of a commutative ring R is prime if A is proper ideal and

$a \cdot b \in A \Rightarrow a \in A$ or $b \in A$.

2) An ideal A of a commutative ring R is maximal if A is proper such that if B is any other ideal with $A \subseteq B \subseteq R$ then $A = B$ or $B = R$.

Ex:- 1) $n\mathbb{Z}$ is prime iff $n = p$ is prime

2) in $\mathbb{Z}_{36}$, $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximals.

3) $\langle x^2+1 \rangle$ in $\mathbb{Z}[x]$ is maximal.

proof:- suppose that A is an ideal of $\mathbb{R}[x]$ and

$$\langle x^2+1 \rangle \subseteq A \subseteq R[x].$$

if $A = \langle x^2+1 \rangle$ we have done.

if $A \neq \langle x^2+1 \rangle \Rightarrow$ let $f(x) \in A$ and $f(x) \notin \langle x^2+1 \rangle$

$\Rightarrow f(x) = q(x)(x^2+1) + r(x)$, $r(x) \neq 0$ and $\deg r(x) < 2$

so $r(x) = ax+b$ a, b not both zeros.

$ax+b = r(x) - q(x)(x^2+1) \in A$.

[illegible]

Ex:- $\langle x^2+1 \rangle$ is not prime in $\mathbb{Z}_2[x]$

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

but $x+1 \notin \langle x^2+1 \rangle$.

Th:- Let R be a commutative ring with unity.

Let A be an ideal then

R/A is integral domain iff A is a prime ideal.

proof:- see text.

Ideals & Factor rings

Ex $\langle x^2+1\rangle$ is not maximal ideal in $\mathbb{Z}_2[x]$

Since $\left((x+1)+\langle x^2+1\rangle\right)\cdot\left((x+1)+\langle x^2+1\rangle\right)$

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

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

$$= 0 + \langle x^2+1\rangle \in \langle x^2+1\rangle$$

but $x+1 + \langle x^2+1\rangle \notin \langle x^2+1\rangle$.

Th:- Let R be commutative ring with unity. Let A be an ideal of R then R/A is an integral domain iff A is prime.

proof:- $\boxed{\Rightarrow}$ suppose R/A is integral domain and suppose that $ab \in A$.

$\Rightarrow (a+A)(b+A) = ab+A = 0+A$

$\Rightarrow a+A = A$ or $b+A = A$ (since R/A is integral domain).

$\Rightarrow a\in A$ or $b\in A$. so A is prime

$\boxed{\Leftarrow}$ R/A is commutative ring with unity since A is an ideal.

so need to prove R/A is integral domain i.e has no zero divisors.

so let $(a+A)(b+A) = 0+A \Rightarrow ab+A = 0+A$

$\Rightarrow ab\in A$ but A is prime so $a\in A$ or $b\in A$

$\Rightarrow a+A = 0+A$ or $b+A = 0+A$

so R/A has no zero divisors so integral domain

Th 14.4 Let R be commutative ring with unity.
Let A be an Ideal of R. then
R/A is a field iff A is maximal.

proof:- $\boxed{\Rightarrow}$ suppose R/A is a field, and let B be an ideal of A; $\{0\} \subseteq A \subset B \leq R$.

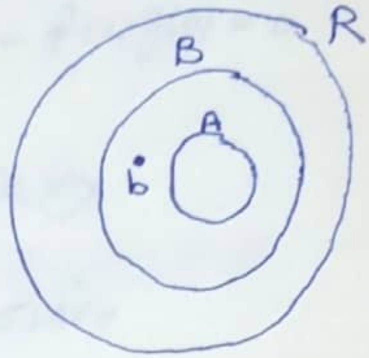
Let $b \in B$, $b \notin A$

$\Rightarrow b+A \neq 0+A \in R/A$.

but R/A is a field so

$\exists\ c+A \in R/A$;

$(b+A)(c+A) = bc+A = 1+A$.



$\Rightarrow 1-bc \in A \subseteq B$

$\Rightarrow (1-bc)+bc = 1 \in B \Rightarrow B = R$

$\boxed{\Leftarrow}$ Suppose A is maximal, let $b \in R$, $b \notin A$.
Need to show $b+A$ is a unit in R/A.
since all other properties (commutative ring with unity are trivialy satisfied).

so let $B = \{br+a \mid r \in R, a \in A\}$
B is an ideal of R containing A.
but A is maximal so $B = R$
so $1 \in B \Rightarrow 1 = b\cdot c + a'$, $a' \in A$.
Now $1+A = bc+a'+A = bc+A = (b+A)(c+A)$.

Corollary : if R is commutative ring with unity then any maximal ideal is prime

Solution of H.W of Chapter 14

④ $A = \{(a,a) \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} + \mathbb{Z}$ since

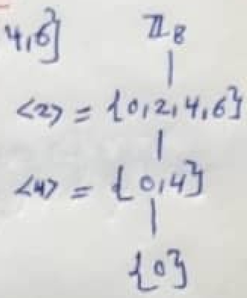
* $A \neq \phi$ since $(0,0) \in A$.
* closed under subtraction let $(a,a) \in A$, $(b,b) \in A$ then
  $(a,a) - (b,b) = (a-b, a-b) \in A$
* closed under multiplication since if $(a,a) \in A$, $(b,b) \in A$ then
  $(a,a) \cdot (b,b) = (ab, ab) \in A$.

But A is not ideal of $\mathbb{Z} \oplus \mathbb{Z}$

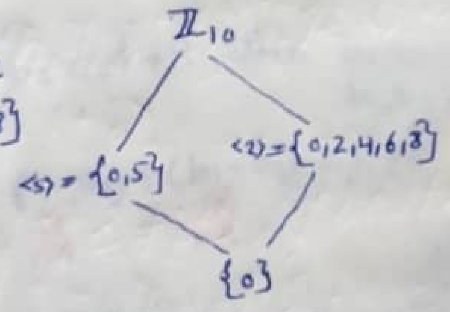
let $(2,5) \in \mathbb{Z} \oplus \mathbb{Z}$, $(6,6) \in A$ then
$(2,5) \cdot (6,6) = (12,30) \notin A$.

---

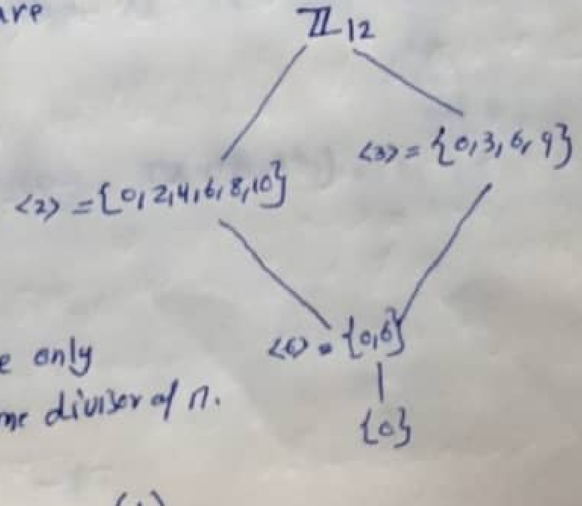
⑥ * maximal ideals in $\mathbb{Z}_8$ only $\langle 2 \rangle = \{0,2,4,6\}$



* maximal ideals in $\mathbb{Z}_{10}$ are
  $\langle 2 \rangle = \{0,2,4,6,8\}$
  $\langle 5 \rangle = \{0,5\}$



* maximal ideals of $\mathbb{Z}_{12}$ are
  $\langle 2 \rangle = \{0,2,4,6,8,10\}$
  $\langle 3 \rangle = \{0,3,6,9\}$



* maximal ideals of $\mathbb{Z}_n$ are only
  $\langle p \rangle$ where p is a prime divisor of n.

Let A_i, $i \in I$ be an indexed family of ideals of R then $\bigcap_{i\in I} A_i$ is an ideal of R since

* $\bigcap_{i\in I} A_i \neq \phi$ since $0 \in \bigcap_{i\in I} A_i$

* Let $a, b \in \bigcap_{i\in I} A_i \Rightarrow a, b \in A_i \ \forall i \in I$.
$\Rightarrow a-b \in A_i \ \forall i \in I$
$\Rightarrow a-b \in \bigcap_{i\in I} A_i$.

* Let $a \in \bigcap_{i\in I} A_i$ and suppose let $x \in R$. then

for every $i \in I$, $a \in A_i$, $x \in R \Rightarrow ax$ and $xa \in A_i$
since A_i is an ideal

then ax and $xa \in \bigcap_{i\in I} A_i$.

) If A, B are ideals of R then $A+B = \{a+b \mid a \in A, b \in B\}$ is an ideal of R since

* $0 = \underset{\in A}{0} + \underset{\in B}{0} \in A+B$

* Let $x = a_1 + b_1$, $y = a_2 + b_2 \in A+B$ where $a_1, a_2 \in A$
$b_1, b_2 \in B$.

$\Rightarrow x-y = (a_1+b_1)-(a_2+b_2) = \underset{\in A}{(a_1-a_2)} + \underset{\in B}{(b_1-b_2)} \in A+B$

* Let $x = a_1+b_1$, $r \in R$ then $xr = x(a_1+b_1) = \underbrace{xa_1}_{\in A} + \overset{\in B \text{ since } x\in R, b_1 \in B}{xb_1} \in A+B$

since $x \in R$, $a_1 \in A$ and A is ideal

similarly $rx = r(a_1+b_1) = ra_1 + rb_1 \in A+B$

(12) Let A, B be ideals of R. Let $A \cdot B = \{a_1b_1 + \dots + a_nb_n \mid a_i \in A, b_i \in B\}$

Show that AB is an ideal of R.

* $0 = \underset{\in A}{0} \cdot \underset{\in B}{0} \in A \cdot B$

* suppose $x = a_1b_1 + \dots + a_nb_n \in A \cdot B$, $y = a_1'b_1' + \dots + a_m'b_m' \in A \cdot B$

then $x - y = (a_1b_1 + \dots + a_nb_n) - (a_1'b_1' + \dots + a_n'b_n')$

$= a_1b_1 + \dots + a_nb_n + (-a_1')b_1' + \dots + (-a_n')b_n' \in A \cdot B.$

* suppose $r \in R$, $x = a_1b_1 + \dots + a_nb_n \in AB$ then

$rx = \underbrace{(ra_1)}_{= a_1' \in A} b_1 + \dots + \underbrace{(ra_n)}_{= a_n' \in A} b_n = AB.$

(14) if A, B ideals, show $AB \subseteq A \cap B$.

Let $x \in AB \Rightarrow x = a_1b_1 + \dots + \underbrace{a_nb_n}_{\in A \cap B \text{ similarly}} \in A \cap B$.

a_1b_1: $\in A$ since $a_1 \in A, b_1 \in R$; $\in B$ since $a_1 \in R, b_1 \in B$

$\in A \cap B$

(15) Let $1 \in A$ show $A = R$

Let $x \in R \Rightarrow x = \underset{\in R}{x} \cdot \underset{\in A}{1} \in A$ (since A is ideal)

so $R = A$.

(16) from (14) above $AB \subseteq A \cap B$ for the other inclusion

Let $x \in A \cap B$, $1 = a + b \in A + B$ (given) then

$x = x \cdot 1 = xa + xb = \underset{\in A}{a}\underset{\in B}{x} + \underset{\in A}{x}\underset{\in B}{b} \in AB.$

(17) if A is ideal of R and $x \in A$ (x is a unit) show $A=R$.

since $x \in A$ then $\forall y \in R$

$\underbrace{y = y \cdot x^{-1}}_{\in R} \cdot \underbrace{x}_{\in A} \in A$ so $A=R$.

(19) $\mathbb{Z}_6$ has exactly two maximal ideals $\langle 2 \rangle$ and $\langle 3 \rangle$.

see #6 (above)

(20) if R is a ring with $|R|=30$, A ideal with $|A|=10$ show A is maximal.

since if B is a proper ideal of R such that

$A \subseteq B \subseteq R$ then

$(R,+)$, $(A,+)$, $(B,+)$ are groups and $A \subseteq B \subseteq R$

so if $|B|=x$ then $\left.\begin{array}{l} |A| \,/\, |B| = x \\ |B| = x \,/\, |R| \end{array}\right\} \Rightarrow x = 10 \text{ or } 30$

so B can't be proper subset of R and A proper in B

i.e either $B=A$ or $B=R$ so R is maximal.

(22) $I[x]$ is not maximal since

$I[x] \subset \langle x \rangle \subset \mathbb{Z}[x]$.

(26) since A is proper ideal of R then $1 \notin A$ (see 17 above)

then it is trivially that R/A is commutative ring

since $(x+A)\cdot(y+A) = xy+A = yx+A = (y+A)(x+A)$

the other properties of ring are easy to show

this ring has the unity $1+A$.

(7) $\{0\}$ and F are ideals of F

let A be ideal such that $\{0\} \subseteq A \subseteq F$

if $A \neq \{0\}$ then $\exists\, x \neq 0, x \in A \Rightarrow 1 = \underbrace{x^{-1}}_{\in R} \underbrace{x}_{\in A} \in A$

$\Rightarrow A = F$ using (by #15 - above)

or

A ideal of F containing a unit $x \neq 0$, since $F \neq \{0\}$ so by (#17) above.

---

(28) Since $\langle x^2+1 \rangle$ is maximal in $\mathbb{R}[x]$ (see noted)

So by theorem 14.4 $\mathbb{R}[x]/\langle x^2+1 \rangle$ is maximal.

---

(30) $\mathbb{Z} \oplus \mathbb{Z}/A = (\{(0,0)+A, (1,0)+A, (2,0)+A\}, +, \cdot)$

since for example $(5,17)+A = (2,0)+A + (3,17)+A$

$= (2,0)+A + (0,0)+A$

$= (2,0)+A.$

$\mathbb{Z} \oplus \mathbb{Z}/A \cong (\mathbb{Z}_3, +, \cdot)$ which is a field so by th 14.3 A is maximal. and in general A is maximal when n is prime

---

(31) let ~~$A \trianglelefteq B \trianglelefteq \mathbb{R}[x]$~~, let $f(x)+A \neq A$

$\Rightarrow f(0) \neq 0$

$\Rightarrow f + A = f(0) + A,\ f(0) \neq 0$

so $(f(x)+A)^{-1} = \frac{1}{f(0)} + A$

$\Rightarrow \mathbb{R}[x]/A$ is a field so A is maximal by th 14.4

say $f(x) = x^2+2x+5$

$f(x)+A = 5+x^2+2x+A$

$= (5+A)+\underbrace{(x^2+2x)}_{\in A}+A$

$= 5+A+0+A$

$= 5+A$

---

(32) $\langle 1 \rangle \oplus \langle 2 \rangle = \mathbb{Z}_8 \oplus \{0,2,4,\dots,28\}$ R/A of order 2.

$\langle 2 \rangle \oplus \langle 1 \rangle = \{0,2,4,6\} \oplus \mathbb{Z}_3$ and R/A is of order 2

$\langle 1 \rangle \oplus \langle 3 \rangle = \mathbb{Z}_8 \oplus \{0,3,6,\dots,27\}$ and R/A is of order 3

$\langle 1 \rangle \oplus \langle 5 \rangle = \mathbb{Z}_8 \oplus \{0,5,10,\dots,125\}$ and R/A " " " 5

(34)

$I \subset B \subset \mathbb{Z}[x]$

where $B = \{ f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even} \}$

(35)

$\mathbb{Z} \oplus \mathbb{Z} / I = \{ (a,b) + I \ / \ a,b \in \mathbb{Z} \}$

but $(a,b) + I = (0,b) + (a,0) + I$

$= (0,b) + I$ since $(a,0) \in I$.

So $\mathbb{Z} \oplus \mathbb{Z} / I = \{ (0,b) + I \ / \ b \in \mathbb{Z} \}$

and $(\mathbb{Z} \oplus \mathbb{Z} / I, +, \cdot)$ is isomorphic to $(\mathbb{Z}, +, \cdot)$

Hence by th 14.3 and 14.4 and since $(\mathbb{Z}, +, \cdot)$ is integral domain but not field so A is prime ideal and not maximal.

(38) $\mathbb{Z}[i] = \{ a+bi \mid a,b \in \mathbb{Z} \}$

$I = \langle 2+2i \rangle \Rightarrow (2 + \langle 2+2i \rangle) \cdot ((1+i) + \langle 2+2i \rangle) =$

$= 2(1+i) + \langle 2+2i \rangle$

$= 2+2i + \langle 2+2i \rangle$

$= 0 + \langle 2+i \rangle$.

but $2 + \langle 2+2i \rangle$, $1+i + \langle 2+2i \rangle$ are nonzero so $\mathbb{Z}[i] / \langle 2+2i \rangle$ has zero divisors so not integral domain

Next $2+2i + \langle 2+2i \rangle = 0 + \langle 2+2i \rangle$

$2+2i + \langle 2+2i \rangle = -2 + \langle 2+2i \rangle$ .... (1)

$\Rightarrow 2i + \langle 2+2i \rangle = -2 + \langle 2+2i \rangle$

squaring both sides $\Rightarrow -4 + \langle 2+2i \rangle = 4 + \langle 2+2i \rangle$

so $8 + \langle 2+2i \rangle = 0$

$\Rightarrow \mathbb{Z}[i] / \langle 2+2i \rangle = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{i}, \overline{1+i}, \overline{2+i}, \overline{3+i} \}$ 8 elements

and characteristic of this ring 4,

notice $\overline{1+i}$ means $1+i + \langle 2+2i \rangle$.

(41) $\mathbb{Z}$ is principal ideal domain since every ideal in $\mathbb{Z}$ has the form $\langle m \rangle$ $m \in \mathbb{Z}$.

(45) $Ann(A) = \{ r \in R \mid ra = 0 \ \forall a \in A \}$.

to show $Ann(A)$ is ideal.

* $Ann(A) \neq \phi$ since $0 \in Ann\,A$ since $0 \cdot a = 0$ for every $a \in A$

* suppose $x, y \in Ann(A)$ then $xa = 0$ and $ya = 0$ $\forall a \in A$

$(x-y)a = x \cdot a - y \cdot a = 0 - 0 \quad \forall a \in A$.

* Suppose $x \in Ann(A)$ and $r \in R$ then

$r \cdot x \cdot a = r \cdot (xa) = r \cdot 0 = 0 \quad \forall r \in R$

(58) in $\mathbb{Z}_5[i] / \langle 1+i \rangle$

notice that $1+i + \langle 1+i \rangle = 0 + \langle 1+i \rangle$

$\Rightarrow 1 + \langle 1+i \rangle = -i + \langle 1+i \rangle$

$\Rightarrow 1 + \langle 1+i \rangle \cdot 1 + \langle 1+i \rangle = -i + \langle 1+i \rangle \cdot -i + \langle 1+i \rangle$

$\Rightarrow 1 + \langle 1+i \rangle = -1 + \langle 1+i \rangle$

$\Rightarrow 2 + \langle 1+i \rangle = 0 + \langle 1+i \rangle$

so $\mathbb{Z}[i] / \langle 1+i \rangle = \{ 0 + \langle 1+i \rangle, 1 + \langle 1+i \rangle \}$

commutative ring with unity of order 2

so is a field.

Chapter 15
Ring homomorphisms

Def^n: A ring homomorphism from a ring R to a ring S is a mapping $\phi : R \to S$ such that
$\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$
for all $a, b \in R$. and if ϕ is 1-1 and onto then ϕ is called an isomorphism.

Examples: ① $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ is a homomorphism $\forall n$.
$k \longmapsto k \pmod n$

② $\phi : \mathbb{C} \longrightarrow \mathbb{C}$ is a homomorphism since
$a+bi = z \longmapsto a-bi = \bar{z}$

$\phi(z_1+z_2) = \overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2 = \phi(z_1) + \phi(z_2)$

and $\phi(z_1 z_2) = \overline{z_1 . z_2} = \bar{z}_1 . \bar{z}_2 = \phi(z_1) . \phi(z_2)$.

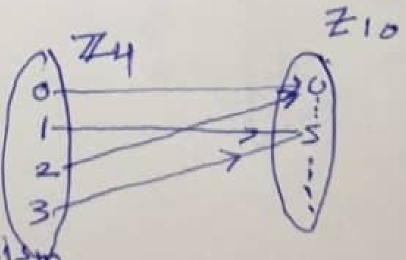
for all $z_1, z_2 \in \mathbb{C}$.

③ $\phi : \mathbb{R}[x] \longrightarrow \mathbb{R}$ is a homomorphism. since
$p(x) \longmapsto p(1)$

$\phi(p(x)+q(x)) = (p(x)+q(x))(1)$
$= p(1) + q(1) = \phi(p(x)) + \phi(q(x))$
$\forall p(x), q(x) \in \mathbb{R}[x]$

$\phi(p(x) q(x)) = (p(x) . q(x))(1) = p(1) . q(1)$
$= \phi(p(x)) \phi(q(x))$.

④ $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}$
$x \longmapsto 5x$



is a ring homomorphism

(5) To determine all homomorphism from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$

since $\mathbb{Z}_{12} = \langle 1 \rangle$ so we determin $\phi(1)$

from groups we know.

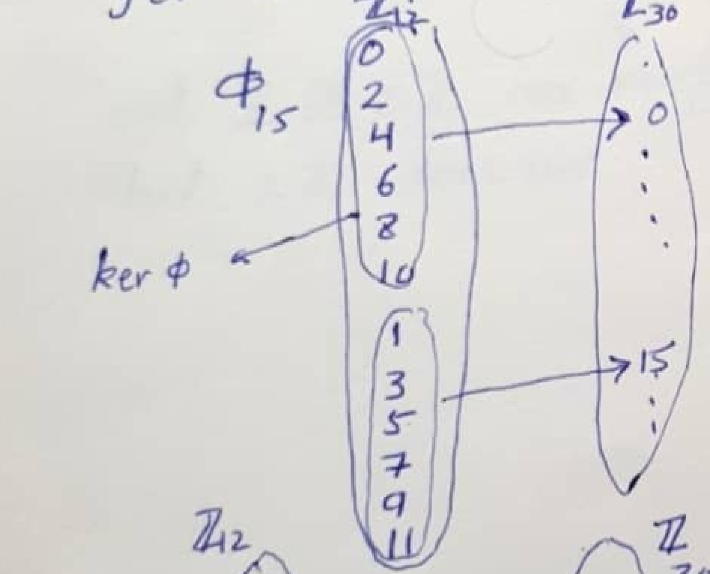
$|\phi(1)| / 12$ and $|\phi(1)| / 30$

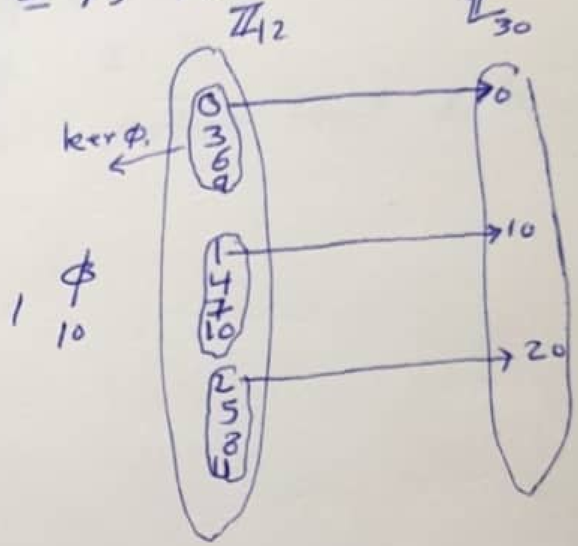
so $|\phi(1)| = 1 \;,\; 2 \;,\; 3 \;,\; 6$

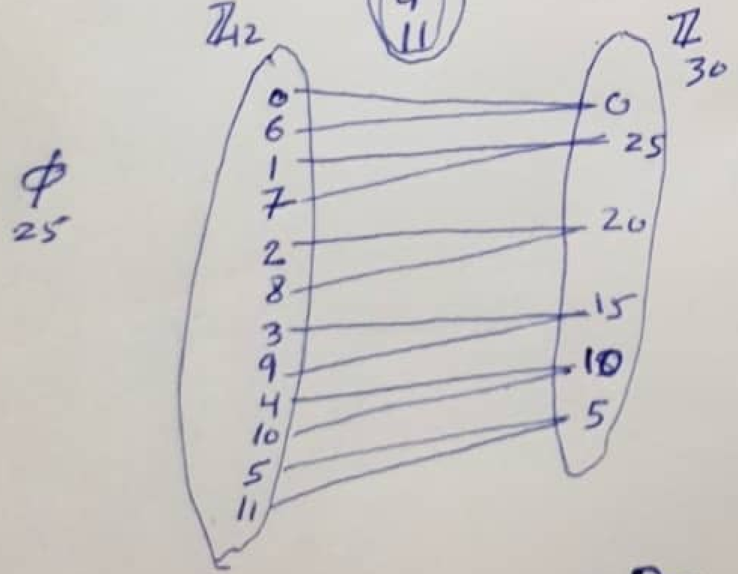
so $\phi(1) = 0 \;,\; 15 \;,\; 10, 20 \;,\; 5, 25$

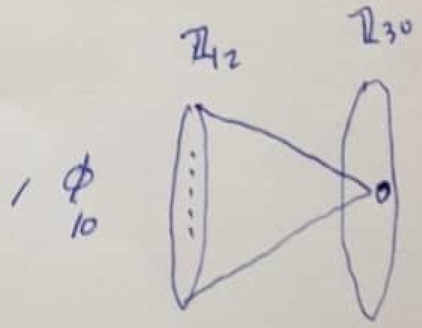
But $\phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$ and the element from $0, 15, 20, 10, 5, 25$ that satisfies $a = a \cdot a$ are $0, 15, 10, 25$ so we have 4 homomorphisms.

for example if $\phi(1) = 15$ then









(6) Let R be a commutative ring with characteristic of $R = 2$

then $\phi : R \longrightarrow R$ is a homomorphism since.
$x \longmapsto x^2$

$\phi(a+b) = (a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2 = \phi(a)\phi(b)$
$\phi(ab) = (ab)^2 = a^2 b^2 = \phi(a)\phi(b)$.

(7) $\phi : \mathbb{Z} \longrightarrow 2\mathbb{Z}$ is not an isomorphism
$x \longmapsto 2x$

since $\phi(1) = \phi(1.1) \neq \phi(1)\phi(1)$
$2 \neq 2 \cdot 2$.

and $\mathbb{Z} \not\cong 2\mathbb{Z}$ as rings. notice that $\mathbb{Z}$ has unity but $2\mathbb{Z}$ does not.

Theorem 15.1 Let $\phi : R \to S$ be a ring homomorphism and let A be a subring of R and B an ideal of S then

① $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$ $\forall r \in R$ $\forall n \in \mathbb{Z}$

② $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.

③ if A is an ideal and ϕ is onto then $\phi(A)$ is an ideal

④ $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.

⑤ If R is commutative then $\phi(R)$ is commutative

⑥ if R has a unity 1 and $S \neq \{0\}$ and ϕ is onto then $\phi(1)$ is the unity of S.

⑦ ϕ is an isomorphism iff ϕ is onto and $\ker\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$

⑧ if ϕ is an isomorphism from R onto S then ϕ^{-1} is an isomorphism from S onto R.

proof:- similar to the proofs in th 10.1 and th 10.2 and left as excercise.

Theorem 15.2:- Let $\phi: R \to S$ be a homomorphism then $\ker\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

proof $*$ $0 \in \ker\phi$ since $\phi(0) = 0$ so $\ker\phi \neq \phi$

$*$ Let $a, b \in \ker\phi \Rightarrow \phi(a) = \phi(b) = 0$
$\Rightarrow \phi(a-b) = \phi(a) - \phi(b) = 0 - 0 = 0$ so $a-b \in \ker\phi$

$*$ Let $a \in \ker\phi$ and $r \in R$ then
$\phi(r.a) = \phi(r)\phi(a) = \phi(r).0 = 0$ so $r.a \in \ker\phi$
the same is thrue for $\phi(ar) = \phi(a)\phi(r) = 0.\phi(r)$
so $ar \in \ker\phi$.

Th 15.3 | 1st isomorphism theorem for rings
suppose $\phi: R \to S$ be a homomorphism then

$$\psi: R/\ker\phi \longrightarrow \phi(R)$$
$$r + \ker\phi \longmapsto \phi(r)$$

is an isomorphism.

that is $R/\ker\phi \cong \phi(R)$.

proof: ① ψ is 1-1 since suppose $\psi(r_1 + \ker\phi) = \psi(r_2 + \ker\phi)$
$\Rightarrow \phi(r_1) = \phi(r_2) \Rightarrow \phi(r_1 - r_2) = 0 \Rightarrow r_1 - r_2 \in \ker\phi$
$\Rightarrow r_1 + \ker\phi = r_2 + \ker\phi$.

② ϕ is onto since if $s \in \phi(R) \Rightarrow \exists r \in R;\ \phi(r) = s$
$\Rightarrow \psi(r + \ker\phi) = \phi(r) = s$.

Now $\psi(r_1 + \ker\phi + r_2 + \ker\phi) = \psi(r_1 + r_2 + \ker\phi)$
$= \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = \psi(r_1 + \ker\phi) + \psi(r_2 + \ker\phi)$

also $\psi(r_1+\ker\phi \cdot r_2+\ker\phi) = \psi(r_1r_2+\ker\phi)$

$= \phi(r_1r_2)$

$= \phi(r_1)\,\phi(r_2)$

$= \psi(r_1+\ker\phi)\cdot\psi(r_2+\ker\phi).$

So ψ is isomorphism.

theorem 15.4 Every ideal A of a ring R is the kernel of a ring homomorphism of R.

proof:- Let A be an ideal of R then

$\phi: R \longrightarrow R/A$ is a ring homomorphism of R

$r \longmapsto r+A.$

since * $\phi(r_1+r_2) = (r_1+r_2)+A = r_1+A+r_2+A$
$= \phi(r_1)+\phi(r_2)$

also * $\phi(r_1r_2) = r_1r_2+A = (r_1+A)\cdot(r_2+A)$
$= \phi(r_1)\cdot\phi(r_2).$

and * $\ker\phi = \{r\in R \mid \phi(r) = 0+A\}$
$= \{r\in R \mid r\in A\} = A.$

Chapter 18

Divisibility in Integral Domains

Def^n: * Let D be an integral domain, let $a, b \in D$ then a, b are associates iff $a = ub$ where u is a unit in D.

* Let D be an integral domain, let $a \in D$ then a is irreducible if $a \neq 0$, a is not a unit and $a = b.c$ with $b, c \in D$ implies b or c is a unit.

* Let D be an integral domain, let $a \in D$, $a \neq 0$ a is not a unit. then a is prime if a/bc implies a/b or a/c.

Notice that 1) $a \in D$ is prime iff $\langle a \rangle$ is prime ideal.
2) if $D = \mathbb{Z}$ then a is irreducible iff a is prime.
but in general it is not true.

Def^n: Let $d \neq 1$ and d is not divisible by the squre of a prime then
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

Def^n: Let $N : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}^+ \cup \{0\}$

$$a + b\sqrt{d} \longmapsto a^2 - b^2 d.$$

N called norm.

Theorem:- $N: \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}^+ \cup \{0\}$ has the following

* $N(x) = 0$ iff $x = 0$
* $N(xy) = N(x)N(y) \quad \forall x, y.$
* $N(x) = 1$ iff x is a unit.
* $N(x)$ is prime $\Rightarrow x$ is irreducible in $\mathbb{Z}[\sqrt{d}]$.

Proof:- Excercise

Example:- Consider $\mathbb{Z}[\sqrt{-3}]$. where $N(a+b\sqrt{-3}) = a^2+3b^2$.

Let $u = 1+\sqrt{-3}$. then is irreducible. since

suppose $u = x \cdot y$ where x, y are not units.

$\Rightarrow N(u) = 4 = N(x)N(y)$

$\Rightarrow N(x) = 2 \Rightarrow \exists\, a, b \in \mathbb{Z}$; $N(x) = N(a+b\sqrt{-3}) = a^2+3b^2 = 2$

a contradiction. so x or y is a unit and u is irreducible.

Next:- u is not prime since otherwise $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$

So $1+\sqrt{-3} \,/\, 2 \cdot 2 \Rightarrow 1+\sqrt{-3} \,/\, 2$

$\Rightarrow 2 = (1+\sqrt{-3})(a+b\sqrt{-3})$

$\Rightarrow 2 = (a-3b) + (a+b)\sqrt{-3}$

$\Rightarrow a-3b = 2, \; a+b = 0$ $\times$ no solutions in $\mathbb{Z}$.

Ex:- Let $D = \mathbb{Z}[\sqrt{5}]$, let $u = 7 \in \mathbb{Z}[\sqrt{5}]$ then u is irreducible.

Suppose $7 = x \cdot y$, x, y are not units.

$\Rightarrow 49 = N(xy) = N(x)N(y)$ but $N(x) \neq 1$ since x is not a unit

So $N(x) = 7$,

if $x = a+b\sqrt{5} \Rightarrow |a^2-5b^2| = 7$

$\Rightarrow$

$\Rightarrow a^2 - 5b^2 = \mp 7$

$a^2 + 2b^2 = 0 \pmod 7$

$\Rightarrow a = b = 0 \mod 7.$

$\Rightarrow a, b$ are divisible by 7.

but $|a^2 - 5b^2| = 7 \,/\, 49$ ✗.

Th:- In an integral domain, every prime is an irreducible.

Proof:- Suppose a is a prime in an integral domain and $a = bc$.

$\Rightarrow a/b$ or a/c

$\Rightarrow at = b$

$\Rightarrow 1 \cdot b = b = at = (bc)t = b(ct)$

$\Rightarrow 1 = ct \Rightarrow c$ is a unit.

Th:- In a principal ideal domain, an element is irreducible if and only if it is a prime

proof:- ($\Rightarrow$) previous th

($\Leftarrow$) let a be irreducible in D. and suppose a/bc, let $I = \{ax + by \mid x, y \in D\}$, let $I = \langle d \rangle$

$a \in I \Rightarrow a = dr$ but a is irreducible

$\Rightarrow d$ is a unit or r is a unit.

if d is a unit then $I = D$ and $1 = ax + by$

$\Rightarrow c = acx + bcy \Rightarrow a/c.$

if r is a unit then $\langle a \rangle = \langle d \rangle = I.$

but $b \in I \Rightarrow b = at$ so $a/b.$