Chapter III - Rings

1.1 Def: $(R, +, \cdot)$ ring if:

① $(R, +)$ group

② $x.(y.z) = (x.y).z$
($\cdot$ is ass)

③ $x.(y+z) = x.y + x.z$
$(x+y).z = x.z + y.z$

- R commutative if $x.y = y.x$
- R is a unitary ring if $1 \in R$

ex: ① $(\mathbb{Z}, +, \cdot)$ com. unitary ring
$(\mathbb{Q}, +, \cdot)$ com unitary ring
$(\mathbb{R}, +, \cdot)$ " "

② $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
1- $(\mathbb{Z}/n\mathbb{Z}, +)$ gr
2- $\bar{x}.(\bar{y}.\bar{z}) = (\bar{x}.\bar{y}).\bar{z}$
3- $\bar{x}.(\bar{y}.\bar{z}) = \bar{x}.\bar{y} + \bar{x}.\bar{z}$
4- $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$

1.2 prop: $(R, +, \cdot)$ ring
$\forall a, b, c \in R \quad m, n \in \mathbb{Z}$:

a. $0.a = a.0 = 0$
b. $a.(-b) = (-a).b = -ab$
c. $a.(b-c) = a.b - ac$
$(b-c).a = ba - ca$
d. $(n.a).b = a.(n.b) = n.(a.b)$
e. $m.(n.a) = (m.n).a$

1.3. Def: S subring of R if:
1- $S \subseteq R$
2- $(S,+,\cdot)$ ring

1.4. Prop: The following properties are equiv:
1- S subring of R
2- S subgroup of R for + + S closed under ×
3- $0 \in S$ + S closed under $\boxed{+}$ + $\boxed{\times}$

S subring if:
① $S \subseteq R$
② $\forall x,y \in S$ (for $x,y \in S$) $x-y \in S$

2 nb not zero + in $\mathbb{Z}/4\mathbb{Z}$: $\bar{2}\cdot\bar{2}=\bar{0}$
but result if then = 0

1.5. Def: An element z of R is a zero divisor if $z \neq 0$ & $\exists z' \in R, z' \neq 0$ such that $z.z'=0$ or $z'.z=0$
ex: $\mathbb{Z}/6\mathbb{Z}$: $\bar{2}.\bar{3}=\bar{0}$

1.6. Def: $(R,+,\cdot)$ is an integral ring if:
1- $(R,+,\cdot)$ ring
2- R has no zero divisor
(if $x.y=0 \Rightarrow x=0$ or $y=0$)

ex: $(\mathbb{Z},+,\cdot)$, $\mathbb{Q}$, $\mathbb{R}$

1.7. prop: $(R,+,\cdot)$ integral ring
Every non-zero element is regular for ×
($ax=ay \Rightarrow x=y$)

proof: $\forall a \in R/\{0\}$
$b,c \in R$ s.t $ab=ac$.
$\Rightarrow a.(b-c)=0$
int. $\Rightarrow b.c=0 \Rightarrow b=c$

Rmk: $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ not int in general

- $\mathbb{Z}/6\mathbb{Z}$: $\bar{2}.\bar{3} = \bar{0}$
  $\bar{2}$ zero divisor

- $(\mathbb{Z}/p\mathbb{Z}, +, .)$ p prime

$(\mathbb{Z}/p\mathbb{Z}, +, .)$ integral ring :

proof : $(\mathbb{Z}/p\mathbb{Z}, +, .)$ ring

integral :
$\bar{x}.\bar{y} = \bar{0} \Rightarrow \overline{x.y} = \bar{0}$
$\Rightarrow p \mid x.y$
Prime $\Rightarrow p \mid x$ or $p \mid y$
$\Rightarrow \bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$

- $(R, +, .)$ unitary ring :
  x invertible if $\exists\, x' \in R$ s.t
  $x.x' = x'.x = 1$
- $(\mathbb{Z}, +, .)$: 1 & -1 are the inv elts under $.$

1.9 Def : a A field is : 1. unitary ring
2. every elt is inv
b. A commutative field
(= com)

Ex : $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ } com. field

$(\mathbb{Z}/p\mathbb{Z}, +, .)$ com field

Rk : Every field is integral
1.10 Thm : Every finite integral ring is a field

proof : R field $x, y \in R$ $x.y = 0$ $\Rightarrow x = 0$ or $y = 0$?

If $x \neq 0$ $\xrightarrow{R \text{ field}}$ x invertible

$\Rightarrow \exists x \in R$ s.t $z \cdot x = 1$

2 Ideals $(R, +, .)$ ring

2.1 Def: let $I \subseteq R$ we define:

- I left Ideal

  iff ① I subgroup of $(R, +)$

  ② $\forall r \in R$, $\forall x \in I$: $rx \in I$

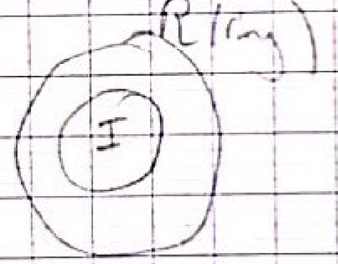
  haw nafs lshi

  $\begin{cases} \forall x, y \in I, r \in R \\ 1\text{-} x + y \in I \\ 2\text{-} rx \in I \end{cases}$ $\Rightarrow$ n7na mnstbil 3a hey

- I right ideal

  $x, y \in I$: $1\text{-} x + y \in I$

  $r \in R$: $2\text{-} xr \in I$



- I ideal : right + left

2.2 prop: 1- if I (left / right) ideal s.t $1 \in I \Rightarrow I = R$

2- if I (left / right) ideal s.t $\exists x \in I$ invertible $\Rightarrow I = R$

Proof: 1. $I \subseteq R$

$R \subseteq I$? $x \in R \Rightarrow x \cdot 1 \in I \Rightarrow x \in I$ (R, $\in I$)

then $R \subseteq I$ + $R = I$

2.4 prop: let L & K left (right) ideal then:

1- $L \cap K$ left (right) ideal

2- $L + K = \{x + y / x \in L, y \in K\}$ is a left (right) ideal.

2.5. prop: The intersection of a non-empty family of left ideals of R is a left ideal of R. (right)

proof: $(L_i)_{i\in X}$ family of left id

Let $L = \bigcap_{i\in I} L_i$ L left id?

1- L subgroup of $(R,+)$ (prop 2.3 chap II)

2- $x\in L$ & $r\in R \Rightarrow r.x \in L$?

$x\in L = \bigcap_{i\in I} L_i \Rightarrow x\in L_i \ \forall i\in I$

$\Rightarrow r.x\in L_i \ \forall i\in I$ (L_i left id)

$\Rightarrow r.x \in \bigcap_{i\in I} L_i = L$

Then L is left id of R.

2.6. prop: $(R,+,.)$ unitary ring $Rx = \{rx / r\in R\}$ $xR = \{x.r / r\in R\}$

$\forall x\in R$, Rx is the smallest left ideal of R containing x

& xR --- right ---

- Rx: left ideal generated by x

2.7. Def:

$(R,+,.)$ unitary ring

1- I is a principle left ideal if $I = Rx$, $x\in R$ (Right $I = xR$).

2- R principle if R integral, com & every ideal is principle

Ex> $(\mathbb{Z},+,.)$ principle ✓ integral ✓ com ✓

$\boxed{I = x\mathbb{Z}}$ every ideal of $\mathbb{Z}$ has the form

2.8. prop: 1. In a field K, we have only two ideals: $\{0\}$ et K

2. A unitary Com ring. R field $\Leftrightarrow$ R has only 2 id: $\{0\}$ et R

Final 2019: $A \subset \mathbb{C}$

Ex 3> Let $A = \{x = a + bi\sqrt{21} \quad a, b \in \mathbb{Z}\}$
et $I = \{x = a + bi\sqrt{21} \in A : a \equiv 0 \pmod 7\}$

1. Show that $(A, +)$ is a unitary com. ring
2. Show that I is an ideal of A
(Recall that $a \equiv b \pmod n \Leftrightarrow n \mid a - b$)

1. $(A, +)$ gp?
a) + ass?
$x + (y + z) \overset{?}{=} (x + y) + z$
$x = a + bi\sqrt{21}$
$y = a' + b'i\sqrt{21}$
$z = a'' + b''i\sqrt{21}$

$x + (y + z) = (a + bi\sqrt{21}) + [(a' + b'i\sqrt{21} + a'' + b''i\sqrt{21})]$

$= (a + bi\sqrt{21}) + [(a' + a'') + (b' + b'')i\sqrt{21}]$

$= (a + a' + a'') + (b + b' + b'')i\sqrt{21}$

$(x + y) + z = \cdots$

2. 0 neutral elt: $0 = 0 + 0i\sqrt{21} \in A$
$\forall x \in A \quad x + 0 = x$ et $0 + x = x$

3. $\forall x \in A$
$x = a + bi\sqrt{21}$
$-x = -a - bi\sqrt{21}$
$\Big\}$ $x + (-x) = 0$
$(-x) + x = 0$

• x is ass?
$x(y.z) = (x.y).z$

$x.(y.z) = (a+bi\sqrt{21}) = (\_\_+\_+\_+\_)$
$= (\quad) + i(\quad)$

$(x.y).z = \_\_\_\_$

• $x(y+z) = x.y + x.z$
$(x+y).z = x.z + y.z$

↳ $(a+bi\sqrt{21})(a'+b'i\sqrt{21} + a''+b''i\sqrt{21})$
$= \_\_\_\_$

• Com?
$x.y = y.x$?
$x = a+bi\sqrt{21}$
$y = a'+b'i\sqrt{21}$

$x.y = (a+bi\sqrt{21})(a'+b'i\sqrt{21})$
$= aa' + b'ai\sqrt{21} + a'bi\sqrt{21}$
$= (aa' - 21bb') + i\sqrt{21}(b'a + a'b)$
$y.x = \_\_\_\_$. com in ¢

$1 = 1 + 0i\sqrt{21} \in A \Rightarrow A$ unitary

2. a) $x, y \in I$
$x = a+bi\sqrt{21} \quad (a \equiv 0 (7))$
$y = a'+b'i\sqrt{21} \quad (a' \equiv 0 (7))$
$x+y \in I$?

$x+y = (a+a') + (b+b')i\sqrt{21} \in A$

$a + \begin{cases} a \equiv 0 (7) \\ a' \equiv 0 (7) \end{cases}$

A Ring
1. (R, +) gr
2. . ass
3. + dist

I id of R
① $\forall x, y \in I$
$x+y \in I$
② $\forall x \in I, r \in R$
$xr \in I$
ma f. fane?
bayn
left & right
2nd Com

$\Rightarrow a + a' \equiv 0 (7)$

then $x + y \in I$

b) $x \in I$, $r \in A$, $r \cdot x \in I$?

$x = a + bi\sqrt{21}$ et $a \equiv 0(7)$

$r = r_1 + r_2 i\sqrt{21}$

$r \cdot x = (r_1 + r_2 i\sqrt{21})(a + bi\sqrt{21})$

$= r_1 a + r_1 bi\sqrt{21} + r_2 a i\sqrt{21} - 21 r_2 b$

$= (r_1 a - 21 r_2 b) + (r_1 b + r_2 a) i\sqrt{21} \in A$.

* $a \equiv 0(7) \longrightarrow 7 | a$

$\Rightarrow$ $r_1 \cdot a \equiv 0(7)$ $\Rightarrow 7 | r_1 a$

* $21 \equiv 0(7)$ $7 | 21$

$r_2 \cdot b(21) \equiv 0(7)$ $\Rightarrow 7 | 21 r_2 b$

$r_1 a - 21 r_2 b \equiv 0(7)$ then $r \cdot x \in I$

ex: True or false

$\mathbb{Z}/5\mathbb{Z}$ is a field ? T 5 is prime

3- Maximal ideal

3.1 Def: A left ideal m of R ($m \neq R$) is a maximal left ideal of R if:

$m \subseteq L \subseteq R \Rightarrow m = L$ or $L = R$

where L is a left ideal of R

ex: $2\mathbb{Z}$ ideal of $\mathbb{Z}$

$4\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq a\mathbb{Z} \subseteq \mathbb{Z} \Rightarrow a | 2$

$\Rightarrow a = 2$ or $a = 1$

$a\mathbb{Z}$ id of $\mathbb{Z}$ $\Rightarrow a\mathbb{Z} = 2\mathbb{Z}$ or $a\mathbb{Z} = \mathbb{Z}$
then $2\mathbb{Z}$ max. id

unitary y3ni
L'J mawjoud
bL Ring

• $p\mathbb{Z}$ (prime) maximal id of $\mathbb{Z}$:
if $a\mathbb{Z}$ is an ideal of $\mathbb{Z}$ s.t.
$p\mathbb{Z} \subseteq a\mathbb{Z} \subseteq \mathbb{Z}$
$\Rightarrow p\mathbb{Z} \subseteq a\mathbb{Z}$
$\Rightarrow a | p$
$\Rightarrow a = p$ or $a = 1$
$\Rightarrow a\mathbb{Z} = p\mathbb{Z}$ or $a\mathbb{Z} = \mathbb{Z}$
then $p\mathbb{Z}$ max id.

3.3 Prop: R unitary Ring
$\{L_i\}_{i\in I}$ non-empty chaine of left ideal of $R (\neq R)$
$\Rightarrow \bigcup_{i\in I} L_i$ is a left ideal of $R (\neq R)$

$(L_i)_{i\in I}$ chaine: let $i,j \in I$: $L_i \subseteq L_j$ or $L_j \subseteq L_i$

Proof: $L = \bigcup_{i\in I} L_i$, $L \neq \phi$

I id of R
(1) if $1 \in I \Leftrightarrow I = R$
(2) if $x \in I$ invertible $\Leftrightarrow I = R$

• Let $x, y \in L$
$\Rightarrow \exists i \in I$ s.t. $x \in L_i$
$\exists j \in I$ s.t. $y \in L_j$
but $L_i \subseteq L_j$ or $L_j \subseteq L_i$
$\Rightarrow x \in L_j$ & $y \in L_j \xRightarrow{\text{by left id}} x + y \in L_j$
$\Rightarrow x + y \in L$

• Let $r \in R$, $x \in L$
$x \in L \Rightarrow \exists j \in I$ st $x \in L_j$
$L_j \xRightarrow{\text{left id}} rx \in L_j$
$\Rightarrow rx \in L$
Then L is a left id of R

* $1 \in L$ since $\boxed{1 \in \bigcup_i V_i}$ since $\bigcup_i \neq R$ $\forall_i$

3.4. Thm: (Krull)
In a unitary ring R, every left ideal distinct from R, is contained in a maximal left ideal of R.

4. Homomorphism + quotient Ring
4.1. Def:
$f: (R, *, T) \longrightarrow (R', *', T')$
ring hom
$\left.\begin{array}{l} f(x+y) = f(x) *' f(y) \\ f(xTy) = f(x)\, T'\, f(y) \end{array}\right\}$ $f: (R, *) \longrightarrow (R', *')$ gp. hom
$f: (R, T) \longrightarrow (R', T')$ gp. hom

4.2 prop: $f: R \longrightarrow R'$ ring hom
1. $f(0) = 0'$ $(R, +, x)$
2. $f(-x) = -f(x)$ $(R', +, x)$
3. S subring of $R \Rightarrow f(S)$ subring of R'
4. L' (l) id of $R' \Rightarrow f^{-1}(L')$ left id of R

4.3. Cor: $f: R \longrightarrow R'$ ring hom
1. Im f subring of R'
2. Ker f id of R

4.4. Def:
- isom : hom + bij
- endo : hom + $R \longrightarrow R$
- autom : isom + $R \longrightarrow R$