Lecture 11 – Rings

Prop 42 In any ring, the following hold:

- $0 \cdot a = 0 = a \cdot 0$ for all $a \in R$
- $(-a)(b) = (a)(-b) = -(ab)$
- If $1 \in R$, then $-a = (-1)a$
- If $1 \in R$, (& $R \neq \{0\}$) then $1 \neq 0$.

Def $a, b \in R - \{0\}$ are <u>zero divisors</u> if $ab = 0$.

(a is a " " if $\exists\, b \neq 0$ s.t. $ab = 0$)

Ex: $R = M_2(\mathbb{R})$

$$a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad b = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow ab = 0$$

Ex: $R = \mathbb{Z}/n\mathbb{Z}$ & n is composite, then R has zero divisors

$n = a \cdot b \Rightarrow [a] \cdot [b] = [n] = [0]$

Def A ring R is an <u>integral domain</u> if R is unital, commutative, & has no zero divisors.

Ex:
- Any field.
- $\mathbb{Z}$
- Rings inside subfields of $\mathbb{C}$.

Prop 43: A finite integral domain is a field.

Pf: $\phi_a : R \to R$, $b \mapsto ab$

$b + c \longmapsto a(b+c) = ab + ac = \phi_a(b) + \phi_a(c)$

$\ker(\phi_a) = \{b \mid ab = 0\} = \{0\}$ (a not a zero divisor)

$\Rightarrow \phi_a : R - \{0\} \longrightarrow R - \{0\}$ is injective $\Rightarrow$ surjective.

$\Rightarrow \exists\, b$ s.t. $ab = 1$. $\Rightarrow$ a is invertible.

Cor 44: $\mathbb{Z}/p\mathbb{Z}$ is a field for all primes p.

Def Given a unital ring R, the group of units R^* is the set of all invertible elements $(\{a \mid \exists b \in R \ ab = ba = 1\})$.

group under multiplication.

Ex: $(\mathbb{Z})^* = \{\pm 1\}$

$(\mathbb{F})^* = \mathbb{F} - \{0\}$, $\mathbb{F}$ a field

$(\mathbb{D})^* = \mathbb{D} - \{0\}$, $\mathbb{D}$ a division ring / skew field.

$(\ )^*$ is a functor

$(\ )^*: \mathcal{R}ing \longrightarrow \mathcal{G}rp$

Def A homomorphism of Rings is a function $f: R \to S$ s.t.

1) f is a homomorphism of the underlying additive groups
2) $f(ab) = f(a) f(b)$
(3) if R & S are unital, $f(1) = 1$)

$u: \mathcal{R}ng \longrightarrow \mathcal{G}rp$ is a functor.

ring w/o identity

$(\ )^*: \mathcal{R}ing \longrightarrow \mathcal{G}rp$ is a functor

$(f: R \to S$, $a, b \in R^*$, then $f(a), f(b) \in S^*)$

$$ab = 1 \Rightarrow \underset{\underset{f(a)f(b)}{\parallel}}{f(ab)} = f(1) = 1$$

Def A subset I of R is an ideal if

1) I is an additive s.g.
2) $\forall r \in R$, $i \in I$, $ri \in I$, $ir \in I$.

Prop 45: If K is the kernel of $f: R \to S$, then K is an ideal.

Pf: $k \in K$, $r \in R$, then $rk \in K$, $kr \in K$.

$f(rk) = f(r) \cdot f(k) = f(r) \cdot 0 = 0$ by Prop 42.

$f(kr) = f(k) \cdot f(r) = 0 \cdot f(r) = 0$.

If I is an ideal, then there is a ring structure on R/I s.t. $R \longrightarrow R/I$ is a homomorphism.

$R/I = R/\sim$ $\quad a \sim b$ iff $a - b \in I$.

Abelian, additive group $= R/I$: $[a] + [b] = [a+b]$

$[a]\cdot[b] = [a\cdot b]$

$a' = a+i$
$b' = b+j$ $\qquad i,j \in I$

$$(a\cdot b)-(a'\cdot b') \in I$$
$$(a\cdot b) - (a+i)(b+j)$$
$$= \cancel{(ab)} - \cancel{(ab)} - (ib) - (aj) - (ij)$$
$$= -(\underset{I}{\underset{\cap}{i\cdot b}} + \underset{I}{\underset{\cap}{a\cdot j}} + \underset{I}{\underset{\cap}{i\cdot j}}) \in I$$

Def If I is an ideal, then the quotient of R by I is R/I with $[a]\cdot[b]=[a\cdot b]$.

Prop 46: If I is an ideal, then I is the kernel of the map
$$R \to R/I$$
$$a \mapsto [a]$$

Thm 47: If f is a homomorphism $R\to S$, then f induces an isomorphism
$$R/\ker(f) \xrightarrow{\cong} \mathrm{Im}(f) \subseteq S$$

Pf: $R/\ker(f) \xrightarrow{\tilde{f}} \mathrm{Im}(f)$
$\quad [a] \longmapsto f(a)$

$$\tilde{f}([a]\cdot[b]) = \tilde{f}([a\cdot b]) = f(ab) = f(a)\cdot f(b) = \tilde{f}([a])\cdot\tilde{f}([b]).$$

1^{st} Isom thm for groups $\Rightarrow$ $\tilde{f}$ is a 1-1, onto homomorphism of groups, $\tilde{f}$ is a hom of rings $\Rightarrow$ $\tilde{f}$ an iso. $\boxtimes$

Prop 48: R/I has a universal property: If $f: R\to S$ has $\ker(f)\supseteq I$, then there is a unique map $\tilde{f}: R/I \to S$ s.t.

$$\begin{tikzcd} R \arrow[d] \arrow[dr, "f"] & \\ R/I \arrow[r, "\tilde{f}"'] & S \end{tikzcd}$$

Def: If I and J are ideals, then $I\cap J$ is an ideal;
$$I+J = \{ i+j \mid i\in I,\ j\in J\} \text{ is an ideal.}$$
$$IJ = \{ i\cdot j + i'\cdot j' + \dots \mid i^{(\prime)} \in I,\ j^{(\prime)} \in J\} \text{ is an ideal.}$$

Thm 49: $I+J/J \cong I/I\cap J$

Thm 50: $R/I \cong (R/J)/(I/J)$ $J \subseteq I \subseteq R$, I, J ideals.