Lecture 16: Basics on Rings II

Last Time • $(R,+,\cdot)$ is a ring if (1) $(R,+,0)$ is an abelian group
(2) $(R,\cdot,1)$ is a monoid
(3) Distributive Laws hold.

Note: We always assume $0\neq 1$.

• Left/ Right / 2-sided Ideals $\mathfrak{a}\subset R$ if $\mathfrak{a}$ is a subgroup of $(R,+,0)$ & $R\mathfrak{a}\subset\mathfrak{a}$, resp $\mathfrak{a}R\subseteq\mathfrak{a}$, resp $R\mathfrak{a}R\subseteq\mathfrak{a}$

• $\mathfrak{a}\subset R$ 2-sided ideal $\rightsquigarrow$ $\boxed{R/\mathfrak{a}}$ $=\{x+\mathfrak{a} : x\in R\}$ is a ring with
$(x+\mathfrak{a})+(y+\mathfrak{a})=(x+y)+\mathfrak{a}$, $\underline{0}=0+\mathfrak{a}$
$(x+\mathfrak{a})\cdot(y\cdot\mathfrak{a})=(xy)+\mathfrak{a}$; $\underline{1}=1+\mathfrak{a}$

quotient ring

§1. Homomorphisms:

Def: Let R_1, R_2 be two rings. A map $f:R_1\longrightarrow R_2$ is a homomorphism of rings if:

• f is a group homomorphism between $(R_1,+,0)$ & $(R_2,+,0)$ ie
$$f(a_1+b_1)=f(a_1)+f(b_1)\quad\forall a_1,b_1\in R$$
• f is a homomorphism of monoids between $(R_1,\cdot,1)$ & $(R_2,\cdot,1)$
ie $\quad f(a_1b_1)=f(a_1)f(b_1)\quad$ & $\quad f(1)=1$

NOTATION: $\quad f\in \mathrm{Hom}_{\mathrm{Rings}}(R_1,R_2)$

Obs: $\quad f(0)=0\quad$ & $\quad f(1)=1$.

Example: $\quad\mathfrak{a}\subset R$ ideal, $\quad\pi: R\twoheadrightarrow R/\mathfrak{a}$ is ring hom.

Lemma: Let $f:R_1\longrightarrow R_2$ be a ring homomorphism
Then (i) $\mathfrak{a}=\ker(f)\subset R_1$ is an ideal
(ii) $\mathrm{Im}(f)\subset R_2$ is a subring

Proof: (i) $x\in\mathfrak{a}$, $r,r'\in R$
$$f(rx)=\underbrace{f(r)}_{\in R_2}\underbrace{f(x)}_{=0}=f(r)\cdot 0=0$$
$$f(xr)=f(x)\underbrace{f(r)}_{\in R_2}=0\,f(r)=0$$

(ii) $1=f(1)\in\mathrm{Im}(f)$
$0=f(0)\in\mathrm{Im}(f)$
& $\mathrm{Im}(f)$ is closed under $\cdot$ & it is a subgroup of $(R_2,+,0)$.

Useful remarks: Given $f: R_1 \longrightarrow R_2$ ring homomorphism

① $f^{-1}(\mathfrak{a}_2) \subset R_1$ is an ideal of R_1 for every $\underset{\text{ideal}}{\mathfrak{a}_2 \subset R_2}$

Pf/ $\begin{array}{l} x \in \mathfrak{a}_1 = f^{-1}(\mathfrak{a}_2) \\ r \in R_1 \end{array} \Rightarrow \left.\begin{array}{l} f(rx) = f(r)\overset{\in \mathfrak{a}_2}{f(x)} \in \mathfrak{a}_2 \\ f(xr) = \underbrace{f(x)}_{\in \mathfrak{a}_2} f(r) \in \mathfrak{a}_2 \end{array}\right\} \Rightarrow \begin{array}{l} rx \ \& \ xr \\ \in \mathfrak{a}_1 \end{array}$

② $f(\underset{\substack{\uparrow \\ \text{(multiplicative) units of } R_1}}{R_1^{\times}}) \subset R_2^{\times}$ $\quad (xy = yx = \underset{R_1}{1} \Rightarrow f(x)f(y) = f(y)f(x) = \underset{R_2}{1})$

⚠ The image of an ideal need <u>not</u> be an ideal (need f to be surjective)

Example: $f: \mathbb{Z} \longrightarrow \mathbb{Z}[x]$ is a ring homomorphism

$\mathbb{Z} \supset (n)$ = all multiples of n

$f((n))$ is not an ideal because $f(1) = 1$ so $f(nk) = nk$ gives $f((n)) = n\mathbb{Z}$ & this set is not closed under multiplication by 1.

§2. Basic Isomorphism Theorems

Fundamental Theorem for homomorphisms:

Let $f \in \mathrm{Hom}_{\text{Rings}}(R_1, R_2)$ and $\mathfrak{a} = \ker(f) \subset R_1$ (ideal!)

Then, there exists a unique $\bar{f}: R_1/\mathfrak{a} \longrightarrow R_2$ such that

$$\begin{tikzcd} R_1 \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & R_2 \\ R_1/\mathfrak{a} \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd} \qquad \bar{f} \circ \pi = f$$

Then: $\bar{f}$ is injective

$R_1/\mathfrak{a} \simeq \mathrm{Im}\, f$ under $\bar{f}$

Second Iso Theorem: Let R be a ring and $\mathfrak{a} \subset R$ be an ideal. Set $\overline{R} := R/\mathfrak{a}$. Then, there is a 1-to-1 correspondence:

$$\left\{ \begin{array}{c} \text{Subgroups of } (R,+,0) \\ \text{containing } \mathfrak{a} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Subgroups of} \\ (\overline{R},+,0) \end{array} \right\}$$

$$\begin{array}{ccc} \Downarrow & & \Downarrow \\ A & \longmapsto & \overline{A} = A \bmod \mathfrak{a} \\ \pi^{-1}(A) & \longleftarrow\!\!\!\shortmid & \overline{A} \quad = \pi(A) \text{ under } \pi: R \to \overline{R} \end{array}$$

- A is a subring $\iff$ $\overline{A}$ is a subring
- A is an ideal $\iff$ $\overline{A}$ is an ideal (π is surjective!)

In addition, we get $R/A \simeq \overline{R}/\overline{A}$ as rings.

$\overline{R} = R/\mathfrak{a}$
$\overline{A} = A/\mathfrak{a}$

via
$$\begin{tikzcd} R \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & \overline{R} \arrow[r, "\pi_3"] & \overline{R}/\overline{A} \\ R/A \arrow[rru, dashed] & & \end{tikzcd}$$

$\overline{R}$: $R/\mathfrak{a}$

$\overline{\pi_3 \circ \pi_1}$ is the iso

Third Iso Theorem: Let R be a ring, $S \subset R$ a subring & $\mathfrak{a} \subset R$ be an ideal. Then,

(i) $S \cap \mathfrak{a}$ is an ideal in S

(ii) $S + \mathfrak{a}$ is a subring of R containing $\mathfrak{a}$. , $\mathfrak{a}$ is an ideal of $S+\mathfrak{a}$.

Furthermore $\dfrac{S+\mathfrak{a}}{\mathfrak{a}} \xrightarrow{\sim} \dfrac{S}{S \cap \mathfrak{a}}$ as rings

$$\begin{tikzcd} S \arrow[r, "i"] \arrow[rr, bend left, "f"] \arrow[d, "\pi_1"'] & S+\mathfrak{a} \arrow[r, "\pi"] & (S+\mathfrak{a})/\mathfrak{a} \\ S/\ker f \arrow[rru, dashed, "\overline{f}"'] & & \end{tikzcd}$$

$f = \pi \circ i$
$\ker f = S \cap \mathfrak{a}$
$\overline{f}$ inj
$\operatorname{Im} \overline{f} = S+\mathfrak{a}/\mathfrak{a}$

§3. Algebra of Ideals.

Note: $\mathfrak{a} \cap R^\times \neq \emptyset \implies \mathfrak{a} = R = (1)$ (called the unit ideal)

Let $\mathcal{J}(R)$ = set of all ideals of R.

- Given $\mathfrak{a}, \mathfrak{b} \in \mathcal{J}(R)$, define:

① $\mathfrak{a} + \mathfrak{b} := \{ a+b : a \in \mathfrak{a}, b \in \mathfrak{b} \}$

② $\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{N} a_i b_i \text{ where } N \geq 0 \text{ is arbitrary}, \begin{array}{l} a_1, \dots, a_N \in \mathfrak{a} \\ b_1, \dots, b_N \in \mathfrak{b} \end{array} \right\}$

Easy check: $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a} \cdot \mathfrak{b}$ are again ideals of R.

- $(\mathcal{J}(R), +, (0))$ is an additive monoid.
- $(\mathcal{J}(R), \cdot, (1))$ is a multiplicative monoid.

§4. Ideals generated by sets:

Let R be a ring an $a_1, \dots, a_n \in R$.

Def. The left-ideal generated by $a_1, \dots, a_n$ is $Ra_1 + \dots + Ra_n =: {}_R(a_1, \dots, a_n)$.

The right-ideal ———— is $a_1R + \dots + a_nR =: (a_1, \dots, a_n)_R$.

The ideal generated by $a_1, \dots, a_n$ is $Ra_1R + \dots + Ra_nR =: (a_1, \dots, a_n)$.

- More generally, for any subset $X \subset R$, the ideal generated by X is:

$$\boxed{(X) = \bigcap_{\substack{\mathfrak{a} \in \mathcal{J}(R) \\ X \subset \mathfrak{a}}} \mathfrak{a}}$$

Similarly, we have $(X)_R = \bigcap_{\substack{\mathfrak{a} \subset R \\ \text{right-ideal} \\ X \subseteq \mathfrak{a}}} \mathfrak{a}$ & ${}_R(X) = \bigcap_{\substack{\mathfrak{a} \subset R \\ \text{left-ideal} \\ X \subseteq \mathfrak{a}}} \mathfrak{a}$

[Easy check: These intersections always give left/right/two-sided ideals.]

Definition: An ideal $\mathfrak{a} \subset R$ is said to be **finitely generated** if $\exists\, a_1, \dots, a_m \in \mathfrak{a}$ such that $\mathfrak{a} = (a_1, \dots, a_m)$

- An ideal $\mathfrak{a}$ is **principal** if $\mathfrak{a} = (a) = RaR$ for some $a \in R$
- We say that R is a **principal ideal ring** if every ideal $\mathfrak{a} \subset R$ is principal.

Main examples: $\mathbb{Z}$ is a principal ideal ring (actually domain)
PID
$\mathbb{C}[x]$ is also a principal ideal domain. (PID)

Non-example: $\mathbb{Z}[x]$ $\quad \mathfrak{a} = (2, x)$ is not principal.

Example Ideals in $\mathbb{Z}/N\mathbb{Z}$ $\quad$ By 2^{nd} Iso Theorem.

Ideals in $\mathbb{Z}/N\mathbb{Z}$ $\longleftrightarrow$ ideals in $\mathbb{Z}$ containing N

$= \{(d) : d \text{ divides } N\}$

$\leadsto$ The analogue of 'divisibility of N by d' is the containment '$(N) \subset (d)$'.

§5. Characteristic of a ring:

Remark: Let $f: R_1 \to R_2$ be a homomorphism of rings & $\mathfrak{a}_2 \in \mathcal{I}(R_2)$

$$\begin{tikzcd} R_1 \arrow[r, "f"] \arrow[rr, bend right, "g"'] & R_2 \arrow[r] & R_2/\mathfrak{a}_2 \end{tikzcd}$$

$\ker(g) = f^{-1}(\mathfrak{a}_2) =: \mathfrak{a}_1$

and hence $R_1/\mathfrak{a}_1 \hookrightarrow R_2/\mathfrak{a}_2$

Let R be a ring. We have a natural ring homomorphism:

$$\varphi: \mathbb{Z} \longrightarrow R$$

$$m \longmapsto m \cdot 1_R = \underbrace{1_R + \dots + 1_R}_{m \text{ times}} \quad \text{for } m \geq 0$$

and $\varphi(-n) = -\varphi(n)$ for $n \geq 0$.

$\ker(\varphi) \subset \mathbb{Z}$ is an ideal. Since $1_R \neq 0_R$, then $\ker(\varphi) \neq \mathbb{Z}$

Thus $\ker(\varphi) = (N)$ for some $N \geq 0$, $N \neq 1$.

- If $N = 0$: we say the characteristic of R is zero [$\mathbb{Z}$ is the characteristic subring of R]
- If $N > 0$: $\mathbb{Z}/N\mathbb{Z} \hookrightarrow R$ is the characteristic subring

Obs: If R is a domain, then $\mathrm{char}(R) = 0$ or a prime number.
(because $\mathbb{Z}/N\mathbb{Z}$ cannot have zero divisors since R has none)