

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/z-sided Ideals $\mathcal{a} \subset R$ if \mathcal{a} is a subgroup of $(R, +, 0)$
 & $R\mathcal{a} \subset \mathcal{a}$, resp $\mathcal{a}R \subset \mathcal{a}$,
 resp $R\mathcal{a}R \subset \mathcal{a}$

• $\mathcal{a} \subset R$ z-sided ideal \rightsquigarrow R/\mathcal{a} \Rightarrow $\{x+\mathcal{a} : x \in R\}$ is a ring with
 $(x+\mathcal{a}) + (y+\mathcal{a}) = (x+y)+\mathcal{a}$, $0 = 0+\mathcal{a}$
 $(x+\mathcal{a}) \cdot (y+\mathcal{a}) = (xy)+\mathcal{a}$, $1 = 1+\mathcal{a}$
quotient ring

§1. Homomorphisms:

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

- f is a group homomorphism between $(R_1, +, 0)$ & $(R_2, +, 0)$ i.e.
 $f(a_1 + b_1) = f(a_1) + f(b_1) \quad \forall a_1, b_1 \in R_1$
- f is a homomorphism of monoids between $(R_1, \cdot, 1)$ & $(R_2, \cdot, 1)$
 i.e. $f(a_1 \cdot b_1) = f(a_1) \cdot f(b_1) \quad \& \quad f(1) = 1$

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

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

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

Lemma: Let $f: R_1 \rightarrow R_2$ be a ring homomorphism

Then (i) $\mathcal{a} = \ker(f) \subset R_1$ is an ideal

(ii) $\text{Im}(f) \subset R_2$ is a subring

Proof: (i) $x \in \mathcal{a}, r, r' \in R$

$$f(rx) = \underbrace{f(r)}_{\in R_2} \underbrace{f(x)}_{=0} = f(r) \cdot 0 = 0$$

$$f(xr) = \underbrace{f(x)}_{=0} \underbrace{f(r)}_{\in R_2} = 0 \cdot f(r) = 0$$

(ii) $1 = f(1) \in \text{Im}(f)$
 $0 = f(0) \in \text{Im}(f)$

& $\text{Im}(f)$ is closed under \cdot & it is a subgroup of $(R_2, +, 0)$.

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

① $f^{-1}(\mathcal{A}_2) \subset R_1$ is an ideal of R_1 for every $\mathcal{A}_2 \subset R_2$ ideal

$$\text{Pf/ } \left. \begin{array}{l} x \in \mathcal{A}_1 = f^{-1}(\mathcal{A}_2) \\ r \in R_1 \end{array} \right\} \Rightarrow \left. \begin{array}{l} f(rx) = f(r) f(x) \in \mathcal{A}_2 \\ f(xr) = f(x) f(r) \in \mathcal{A}_2 \end{array} \right\} \Rightarrow \left. \begin{array}{l} rx \text{ \& } xr \\ \in \mathcal{A}_1 \end{array} \right.$$

② $f(R_1^\times) \subset R_2^\times$ ($xy = yx = 1 \Rightarrow f(x)f(y) = f(y)f(x) = 1$)
 (multiplicative) units of R_1 \uparrow \uparrow R_1 \uparrow R_2

⚠ The image of an ideal need not be an ideal (need f to be surjective)

Example: $f: \mathbb{Z} \longrightarrow \mathbb{Z}[x]$ is a ring homomorphism
 \cup
 $(n) = \text{all multiples of } n$

$f((n))$ 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 $f \in \text{Hom}_{\text{Rings}}(R_1, R_2)$ and $\mathcal{A} = \ker(f) \subset R_1$ (ideal!)

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

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ \pi \downarrow & \searrow \bar{f} & \\ R_1/\mathcal{A} & & \end{array}$$

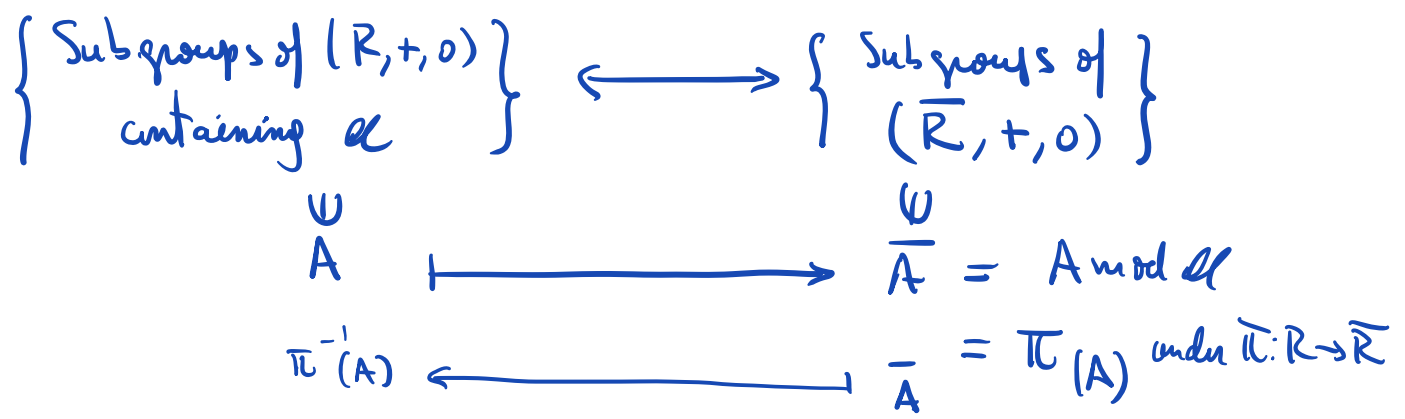
$$\bar{f} \circ \pi = f$$

Then: \bar{f} is injective

$$R_1/\mathcal{A} \cong \text{Im } \bar{f} \text{ under } \bar{f}$$

Second Iso Theorem: Let R be a ring and $\mathcal{A} \subset R$ be an ideal.

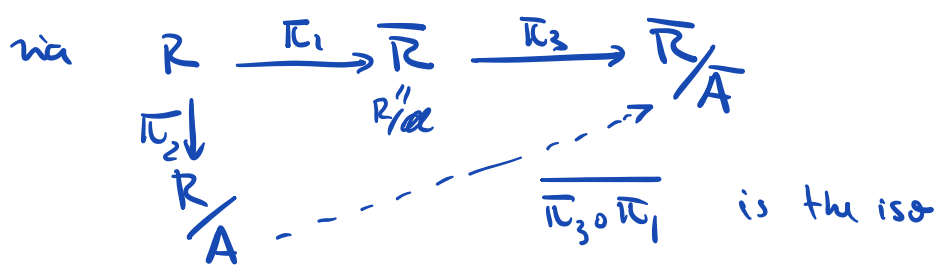
Set $\bar{R} := R/\mathcal{A}$. Then, there is a 1-to-1 correspondence:



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

In addition, we get $R/\mathcal{A} \cong \bar{R}/\bar{\mathcal{A}}$ as rings.

$$\begin{array}{l}
 \bar{R} = R/\mathcal{A} \\
 \bar{\mathcal{A}} = \mathcal{A}/\mathcal{A}
 \end{array}$$

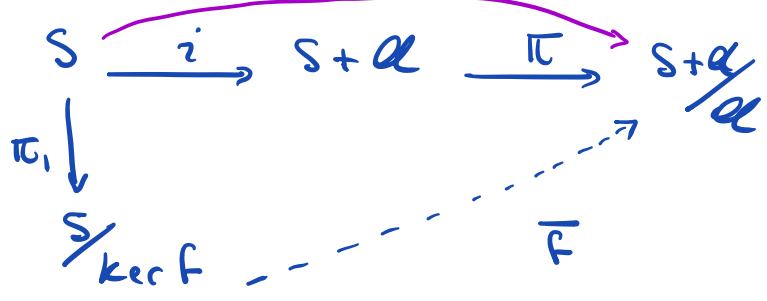


Third Iso Theorem: Let R be a ring, $S \subset R$ a subring

& $\mathcal{A} \subset R$ be an ideal. Then,

- (i) $S \cap \mathcal{A}$ is an ideal in S
- (ii) $S + \mathcal{A}$ is a subring of R containing \mathcal{A} . \mathcal{A} is an ideal of $S + \mathcal{A}$.

Furthermore $\frac{S + \mathcal{A}}{\mathcal{A}} \cong \frac{S}{S \cap \mathcal{A}}$ as rings



$$\begin{array}{l}
 f = \pi \circ i \\
 \ker f = S \cap \mathcal{A} \\
 \bar{F} \text{ ring} \\
 \text{Im } \bar{f} = \frac{S + \mathcal{A}}{\mathcal{A}}
 \end{array}$$

§3. Algebra of Ideals.

Note: $\mathcal{A} \cap \mathcal{R}^* \neq \emptyset \Rightarrow \mathcal{A} = \mathcal{R} = (1)$ (called the unit ideal)

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

• Given $\mathcal{A}, \mathcal{B} \in \mathcal{I}(\mathcal{R})$, define:

① $\mathcal{A} + \mathcal{B} := \{ a+b : a \in \mathcal{A}, b \in \mathcal{B} \}$

② $\mathcal{A} \cdot \mathcal{B} := \left\{ \sum_{i=1}^N a_i b_i \text{ where } N \geq 0 \text{ is arbitrary, } \begin{matrix} a_1, \dots, a_N \in \mathcal{A} \\ b_1, \dots, b_N \in \mathcal{B} \end{matrix} \right\}$

Easy check: $\mathcal{A} + \mathcal{B}$ and $\mathcal{A} \cdot \mathcal{B}$ are again ideals of \mathcal{R} .

• $(\mathcal{I}(\mathcal{R}), +, (0))$ is an additive monoid.

• $(\mathcal{I}(\mathcal{R}), \cdot, (1))$ is a multiplicative monoid.

§4. Ideals generated by sets:

Let \mathcal{R} be a ring and $a_1, \dots, a_n \in \mathcal{R}$.

Def. The left-ideal generated by a_1, \dots, a_n is $\mathcal{R}a_1 + \dots + \mathcal{R}a_n =: {}_{\mathcal{R}}(a_1, \dots, a_n)$.

The right-ideal _____ is $a_1\mathcal{R} + \dots + a_n\mathcal{R} =: (a_1, \dots, a_n)_{\mathcal{R}}$.

The ideal generated by a_1, \dots, a_n is $\mathcal{R}a_1\mathcal{R} + \dots + \mathcal{R}a_n\mathcal{R} =: (a_1, \dots, a_n)$.

• Now generally, for any subset $X \subset \mathcal{R}$, the ideal generated by X

is: $(X) = \bigcap_{\substack{\mathcal{A} \in \mathcal{I}(\mathcal{R}) \\ X \subset \mathcal{A}}} \mathcal{A}$

Similarly, we have $(X)_{\mathcal{R}} = \bigcap_{\substack{\mathcal{A} \subset \mathcal{R} \\ \text{right-ideal} \\ X \subset \mathcal{A}}} \mathcal{A}$ & ${}_R(X) = \bigcap_{\substack{\mathcal{A} \subset \mathcal{R} \\ \text{left-ideal} \\ X \subset \mathcal{A}}} \mathcal{A}$

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

Definition: An ideal $\mathcal{A} \subset R$ is said to be finitely generated if

$$\exists a_1, \dots, a_m \in \mathcal{A} \text{ such that } \mathcal{A} = (a_1, \dots, a_m)$$

. An ideal \mathcal{A} is principal if $\mathcal{A} = (a) = Ra$ for some $a \in R$

. We say that R is a principal ideal ring if every ideal $\mathcal{A} \subset R$ 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: $\mathbb{Z}[x]$ $\mathcal{A} = (2, x)$ is not principal.

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

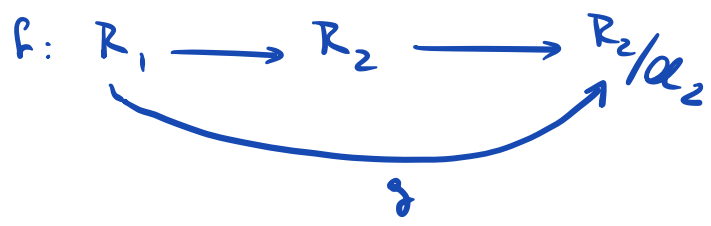
Ideals in $\mathbb{Z}/N\mathbb{Z} \longleftrightarrow$ ideals in \mathbb{Z} containing N

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

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

§5. Characteristic of a ring:

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



$\ker(g) = f^{-1}(\mathcal{A}_2) =: \mathcal{A}_1$
and hence $R_1/\mathcal{A}_1 \xrightarrow{\cong} R_2/\mathcal{A}_2$

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

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

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

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

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

Thus $\ker(\psi) = (N)$ 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 $\text{char}(R) = 0$ or a prime number.

(because $\mathbb{Z}/N\mathbb{Z}$ cannot have zero divisors since R has none)