Lecture 15: Basics on Ring Theory

Def A ring R is a non-empty set, together with two operations:

$+, \cdot : R \times R \longrightarrow R$ (addition & multiplication)

and two distinct elements $0, 1 \in R$ satisfying:

① $(R, +, 0)$ is an abelian group (0 = neutral element)

② $(R, \cdot, 1)$ is a multiplicative monoid with identity element 1

(closed under $\cdot$, but need not have inverses for all elements in R)

③ Multiplication is distributive over addition:

$$\begin{cases} a \cdot (b+c) = a \cdot b + a \cdot c \\ (b+c) \cdot a = b \cdot a + c \cdot a \end{cases} \qquad \forall\, a, b, c \text{ in } R$$

Example: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Obs: If multiplicative inverses exist, they are unique, so we write the inverse of x by x^{-1}

More Examples

① **Direct Product**: If R_1, R_2 are two rings, then

$$R_1 \times R_2 = \{(x,y) : x \in R_1,\ y \in R_2\}$$

becomes a ring with componentwise addition & multiplication. ⇝ $\mathbb{Z}^2$, $\mathbb{Z} \times \mathbb{R}$ are rings

② $M_{n\times n}(R)$ = $n \times n$ matrices over R (usual + & · for matrices)

③ **Polynomial Rings over R**: Given R ring, x variable,

$$R[x] = \left\{ \sum_{j=0}^{N} a_j x^j \ \ a_j \in R,\ N \geq 0 \right\} \quad \text{is a ring:}$$

- **Addition**: componentwise (degree-by-degree)

$$\sum_{j=0}^{N} a_j x^j + \sum_{k=0}^{M} b_k x^k = \sum_{j=0}^{\max(N,M)} (a_j + b_j) x^j$$

where $a_j = 0$ for $N < j \leq \max(N,M)$.
$b_j = 0$ — $M < j \leq$ —

- **Multiplication**: $\left(\sum_{j=0}^{M} a_j x^j\right)\left(\sum_{k=0}^{N} b_k x^k\right) = \sum_{l=0}^{M+N} \sum_{i+j=l} (a_i b_{l-i}) x^l$ where $a_i, b_k \neq 0$ $\forall i > M$, $k > N$

⇝ Inductively: $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x] \ni f = \sum_{\alpha \in \mathbb{N}_0^n,\ \text{finite}} a_\alpha x^\alpha$ $\quad x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$

$\deg(x^\alpha) = |\alpha| = \alpha_1 + \cdots + \alpha_n$

Obs: $0 \cdot x = 0$ for all $x \in R$ $\quad ((0+1)\cdot x = 0\cdot x + 1\cdot x = \boxed{0\cdot x} + x = x \ \forall x)$

Obs: 0 is never invertible $\quad (0 \cdot x = 0 \neq 1) \rightsquigarrow U(R) \subset R \setminus \{0\}$.

Notation: $R^\times := \{ x \in R$ such that x has a multiplicative inverse, ie $xy = yx = 1$ has a soln $\}$

$\| \quad U(R) =$ group of units of R

Some important subtypes of rings: Let R be a ring

Def: ① R is said to be commutative if $ab = ba \ \forall a, b \in R$.

② R is said to be a division ring (or skew-field) if $R^\times = R \setminus \{0\}$

③ R is a field if it is a commutative, division ring.

④ R is an integral domain if R is commutative &

$\forall a, b$: $\quad ab = 0 \implies a = 0$ or $b = 0$.

[In general, if for $a \in R \setminus \{0\}$ there is $b \neq 0$ in R with $ab = 0$ we say a is a zero divisor. Integral domain = commutative + no zero divisors]

Example: $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring.

- If n is **not** a prime number, say $n = n_1 n_2$, the residue classes of n_1 & n_2 in $\mathbb{Z}/n\mathbb{Z}$ are zero divisors.
- If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{m} : \gcd(m,n)=1\}$.

Why? Euclidean Algorithm gives $am+bn=1$ for some a, b in $\mathbb{Z}$, so $\overline{a}\,\overline{m} = \overline{1}$. Conversely if $am \equiv 1 \bmod n$, we have $n \mid am-1$ so $am-1 = nk$ for some $k \in \mathbb{Z}$ $\rightsquigarrow am+n(-k)=1$ & $\gcd(m,n)=1$ ($d \mid m, d \mid n \Rightarrow d \mid am+n(-k)=1$ so $d = \pm 1$.)

Subrings & Ideals

Def: A subring R' of a ring R is a subset $R' \subset R$ containing 0 & 1 that is closed under addition, additive inverses & multiplication, ie:

$$\text{If } a, b \in R' \text{ then } a+b,\ a-b,\ ab \in R'$$

So R' is a ring with inherited (ring) structure.

Def Let $\mathfrak{a} \subset R$ be a subgroup of the abelian group $(R, +, 0)$. We say $\mathfrak{a}$ is:

1. a left ideal of R if $\forall r \in R,\ a \in \mathfrak{a},\ r \cdot a \in \mathfrak{a}$
2. a right ideal of R if $\forall r \in R,\ a \in \mathfrak{a},\ a r \in \mathfrak{a}$
3. an ideal of R if it is both a left & a right ideal.

Example:

1. All subgroups of $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ are ideals.
2. For $R[x] = \left\{ \sum_{i=1}^{n} f_i g_i h_i : f_i, h_i \in R[x] \right\} = \langle g_1, \dots, g_n \rangle$ is an ideal of $R[x]$ (generated by $g_1, \dots, g_n$).
3. $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{C} \right\}$ is neither left nor right ideal $\begin{cases} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \end{cases}$

Lemma If $\{\mathfrak{a}_j\}_{j\in J}$ is a set of ideals of a ring R, then so is $\bigcap_{j\in J}\mathfrak{a}_j$ (Similar results hold for left or right ideals).

Pf/ Enough to check it's a group, closed under left/right multiplication by elements of R. □

Quotient Rings R ring, $\mathfrak{a}\subset R$ ideal $\rightsquigarrow R/\mathfrak{a}$ quotient group.

The abelian group $R/\mathfrak{a}$ has a multiplication structure:

$$\boxed{(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}}$$

Well-defined: $a+\mathfrak{a} = a'+\mathfrak{a} \rightsquigarrow a' = a+x$ for some $x\in\mathfrak{a}$

$b+\mathfrak{a} = b'+\mathfrak{a} \rightsquigarrow b' = b+y$ for some $y\in\mathfrak{a}$

$$\Rightarrow a'b' = (a+x)(b+y) = (ab) + \underbrace{xb}_{\in\mathfrak{a}\text{ (right ideal)}} + \underbrace{ay}_{\in\mathfrak{a}\text{ (left ideal)}} + \underbrace{xy}_{\in\mathfrak{a}} \in ab+\mathfrak{a}$$

$$\Rightarrow a'b'+\mathfrak{a} = ab+\mathfrak{a}$$

Def: $R/\mathfrak{a}$ quotient ring $(0 = 0+\mathfrak{a},\ 1 = 1+\mathfrak{a})$

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 $(R_1, +, 0)$ & $(R_2, +, 0)$ i.e.
$$f(a_1 + b_1) = f(a_1) + f(b_1) \quad \forall a_1, b_1 \in R$$

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

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

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

Example: ① $\mathfrak{a} \subset R$ ideal, $\pi : R \longrightarrow\!\!\!\!\rightarrow R/\mathfrak{a}$ is ring hom.

② $\mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ $\quad m \longmapsto (m, m)$. (diagonal map)

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

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

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

Proof: (i) $x \in \mathcal{A}$, $r, r' \in R$ $\quad f(rx) = \underbrace{f(r)}_{\in R_2} \underbrace{f(x)}_{=0} = f(r) \cdot 0 = 0$.

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

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

$0 = f(0) \in \mathrm{Im}(f)$

& $\mathrm{Im}(f)$ is closed under $\cdot$ &

$\mathrm{Im}(f)$ is a subgroup of $(R_2, +, 0)$, so closed under $+$.

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

Pf/ $x \in \mathcal{A}_1 = f^{-1}(\mathcal{A}_2)$, $r \in R_1$ $\Rightarrow$ $f(rx) = f(r)\underbrace{f(x)}_{\in \mathcal{A}_2} \in \mathcal{A}_2$, $f(xr) = \underbrace{f(x)}_{\in \mathcal{A}_2} f(r) \in \mathcal{A}_2$ $\Rightarrow$ rx & $xr \in \mathcal{A}_1$

② $f(R_1^{\times}) \subset R_2^{\times}$ ($xy = yx = 1_{R_1} \Rightarrow f(x)f(y) = f(y)f(x) = 1_{R_2}$)

⚠ 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) = all multiples of n

$f((n))$ is not an ideal because $f(1) = 1$ so $f(nk) = nk$ gives

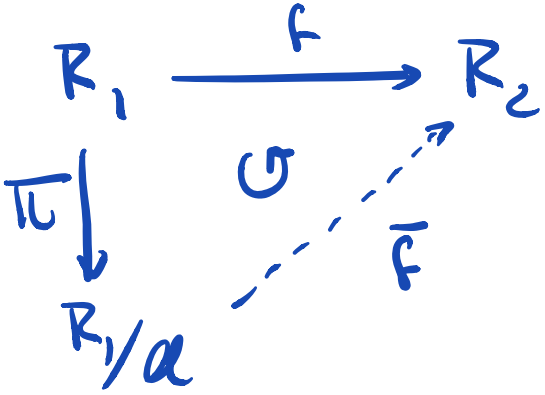
$f((n)) = n\mathbb{Z}$ & this set is not closed under multiplication by 1.

Basic Isomorphism Theorems

Fundamental Theorem for homomorphisms:

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

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



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

Then: $\bar{F}$ is injective

$R_1/\alpha \simeq \mathrm{Im} f$ via $\bar{F}$.

Pf/ Same as with groups:

Show $\bar{F}$ is well-defined; ring hom + bij = iso of rings. □

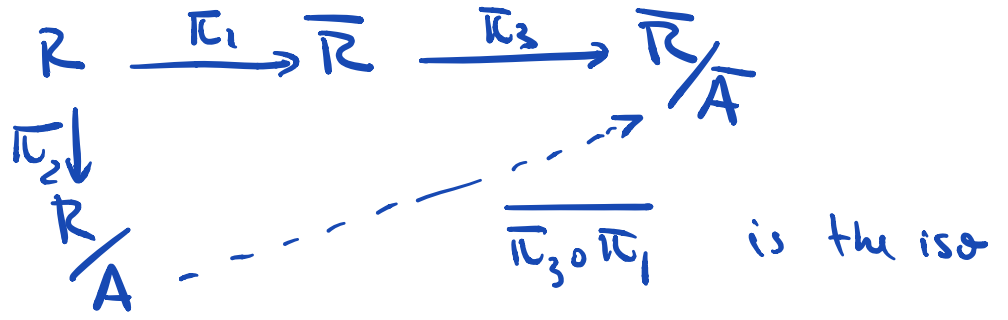
Second Iso Theorem: Let R be a ring and $\mathfrak{a} \subset R$ be an ideal. Set $\overline{R} := R/\mathfrak{a}$. Then, there is a 1-to-1 correspondence:

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

$$\begin{array}{ccc} \cup & & \cup \\ A & \longmapsto & \overline{A} = A \bmod \mathfrak{a} \\ & & = \pi(A) \text{ under } \pi: R \to \overline{R} \end{array}$$

- A is a subring $\iff$ $\overline{A}$ is a subring
- A is an ideal $\iff$ $\overline{A}$ is an ideal. In this situation we get $R/A \simeq \overline{R}/\overline{A}$ as rings.

via



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

$$\begin{array}{ccccc} S & \xrightarrow{i} & S+\mathfrak{a} & \xrightarrow{\pi} & \dfrac{S+\mathfrak{a}}{\mathfrak{a}} \\ {\scriptstyle \pi_1}\downarrow & & & \nearrow_{\bar{F}} & \\ \dfrac{S}{\ker f} & & & & \end{array}$$

$f = \pi \circ i$

$\bar{F}$ inj & surj.

Pf/ Same as with groups

$\ker f = S \cap \mathfrak{a}$, $\operatorname{Im} \bar{F} = S+\mathfrak{a}/\mathfrak{a}$, $\bar{F}$ ring hom + bij $\Rightarrow$ isomorphisms.