Lecture 15: Basics on Ring Theory

§1 Definitions

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:

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

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

$$R^{\times} = \mathcal{U}(R) = \text{group of units of } R$$

Obs: If multiplicative inverses exist, they are unique, so we write x^{-1} for the inverse of $x \in \mathcal{U}(R)$.

Obs: 0 is never invertible ($0\cdot x = 0 \neq 1$) $\leadsto \mathcal{U}(R) \subset R \smallsetminus \{0\}$.

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

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

- 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.

More examples ① $M_{n\times n}(R)$ = $n\times n$ matrices over R (usual $+$ & $\cdot$ for matrices)

② Polynomial Rings over R

Given R ring x variable, $R[x] = \{ \sum_{j=0}^{N} a_j x^j \ \ a_j \in R \ N \geq 0 \}$ is a ring:

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

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

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

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

with the understanding that $a_i = 0 \ \forall i > M$ & $b_k = 0 \ \forall k > N$
(this rule is imposed by distributive property & definition of $+$)

Inductively $R[x_1, \ldots, x_n] = \underbrace{R[x_1, \ldots x_{n-1}]}_{\text{coefficient ring}}[x_n]$

$$\| $$

$$\Big\{ \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ \text{finite}}} a_\alpha \underline{x}^\alpha \Big\} \qquad \underline{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

degree $(\underline{x}^\alpha) = |\alpha| = \alpha_1 + \cdots + \alpha_n$.

§2. 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 $am \equiv 1 \mod n$, 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 $d = \pm 1$.)

§3. Subrings & Ideals

Fix R a ring.

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

If $a,b \in R'$ 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 ________________, $ar \in \mathfrak{a}$

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 $R[x] = \{ \sum_{i=1}^{n} f_i g_i \quad f_i \in R[x] \} = \langle g_1, \ldots, g_n \rangle$ is a left ideal of $R[x]$ (generated by $g_1, \ldots, g_n$).

③ $\mathfrak{a}$ = Upper Triangular 2x2 matrices / $\mathbb{C}$ = $\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \quad a, b, d \in \mathbb{C} \}$

- $\mathfrak{a}$ is not a left ideal

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{\in \mathfrak{a}} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \notin \mathfrak{a}$$

- $\mathfrak{a}$ is not a right ideal:

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{\in \mathfrak{a}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \notin \mathfrak{a}$$

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. □

§3 Quotient Rings

Let R be a ring & $\mathfrak{a} \subset R$ be an ideal. We consider the set $R/\mathfrak{a}$ (viewed as a quotient of groups) with inherited abelian gp structure.

We endow this set with a multiplication:

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

Obs: This is well-defined:

If $a + \mathfrak{a} = a' + \mathfrak{a}$, meaning $(a' - a) \in \mathfrak{a}$, so $a' = a + \underset{\in \mathfrak{a}}{x}$

$b + \mathfrak{a} = b' + \mathfrak{a}$, ——— $(b' - b) \in \mathfrak{a}$ so $b' = b + \underset{\in \mathfrak{a}}{y}$

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

so $a'b' - ab \in \mathfrak{a}$, meaning $a'b' + \mathfrak{a} = ab + \mathfrak{a}$, as we wanted.

Def: $R/\mathfrak{a}$ with $+$ & $\cdot$ as defined above is a ring, called the <u>quotient ring</u> (or <u>residue ring</u>) of R modulo $\mathfrak{a}$.

- $0_{R/\mathfrak{a}} = 0 + \mathfrak{a}$
- $1_{R/\mathfrak{a}} = 1 + \mathfrak{a}$

Distributive Laws are valid because they reflect those in R.

§4. 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 $\quad f(a_1 b_1) = f(a_1) f(b_1) \quad$ & $\quad f(1)=1$

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

<u>Obs</u>: $f(0)=0$ & $f(1)=1$.

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

<u>Lemma</u>: 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

<u>Proof</u>: (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 $f: R_1 \to R_2$ ring homomorphism

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

Pf/ $x \in \mathfrak{a}_1 = f^{-1}(\mathfrak{a}_2)$, $r \in R_1$ $\Rightarrow$

$$\left.\begin{aligned} f(rx) &= f(r)\overset{\in \mathfrak{a}_2}{f(x)} \in \mathfrak{a}_2 \\ f(xr) &= \underbrace{f(x)}_{\in \mathfrak{a}_2} f(r) \in \mathfrak{a}_2 \end{aligned}\right\} \Rightarrow rx \,\&\, xr \in \mathfrak{a}_1$$

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

⚠ The image of an ideal need not 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.

§5. Basic Isomorphism Theorems

Fundamental Theorem for homomorphisms:

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

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

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

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:

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

$$\begin{array}{ccc} \uplus & & \uplus \\ A & \longmapsto & \overline{A} = A \bmod \mathfrak{a} \end{array}$$

$$= \pi(A) \text{ under } \pi : R \to \overline{R}$$

- A is a subring $\Longleftrightarrow$ $\overline{A}$ is a subring
- A is an ideal $\Longleftrightarrow$ $\overline{A}$ is an ideal. In this situation

we get $\quad R/A \simeq \overline{R}/\overline{A}$ as rings.

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

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

via

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

$\overline{R}$ ${}^{''}$ $R/\mathfrak{a}$

$\overline{\pi_3 \circ \pi_1}$ 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 $\quad S+\mathfrak{a}/\mathfrak{a} \xrightarrow{\sim} S/S\cap\mathfrak{a}$ as rings

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

$f = \pi \circ i$

$\ker f = S \cap \mathfrak{a}$

$\overline{f}$ inj

$\operatorname{Im} \overline{f} = S+\mathfrak{a}/\mathfrak{a}$