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:

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

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

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,

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

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 $(0 \cdot x = 0 \neq 1)$ $\rightsquigarrow U(R) \subset R \setminus \{0\}$.

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

$\quad \parallel$

$U(R)$ = 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 $b = 0$.

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

Subrings & Ideals

Def: A <u>subring</u> R' of a ring 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 <u>left ideal</u> of R if $\forall r \in R$, $a \in \mathfrak{a}$, $r \cdot a \in \mathfrak{a}$
2. a <u>right ideal</u> of R ________________, $ar \in \mathfrak{a}$
3. an <u>ideal</u> of R if it is both a left & a right ideal.

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 & right ideals).

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:

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

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 $\quad f(a_1 b_1) = f(a_1) f(b_1) \quad$ & $\quad f(1) = 1$

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

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

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

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 $\mathfrak{a}_2 \subset R_2$ ideal

2. $f(R_1^\times) \subset R_2^\times$

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

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

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

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:

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

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

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

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

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

$\overline{\pi_3 \circ \pi_1}$ 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

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

$f = \pi \circ i$

$\bar{f}$ inj & surj.

($\bar{f}$ is an iso)