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 $\alpha \subset R$ if $\alpha$ is a subgroup of $(R, +, 0)$ and $R\alpha \subset \alpha$, and $\alpha \subset R\alpha = \{ x + \alpha : x \in R \} = R / \alpha$

- $\alpha \subset R$ 2-sided ideal means

  \[ R / \alpha = \{ x + \alpha : x \in R \} \text{ is a ring with} \]
  \[ (x + \alpha) + (y + \alpha) = (x + y) + \alpha, \quad 0 = 0 + \alpha \]
  \[ (x + \alpha) \cdot (y + \alpha) = (xy) + \alpha, \quad 1 = 1 + \alpha \]

### 3.1. 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 $(R_1, +, 0)$ and $(R_2, +, 0)$ i.e. $f(a + b_1) = f(a) + f(b_1)$ \(\forall a, b_1 \in R_1\)
- $f$ is a homomorphism of monoids between $(R_1, \cdot, 1)$ and $(R_2, \cdot, 1)$ i.e. $f(a \cdot b_1) = f(a) \cdot f(b_1)$ and $f(1) = 1$

**Notation:** $\hom_{\text{Rings}}(R_1, R_2)$

**Obs:** $f(0) = 0$ and $f(1) = 1$.

**Example:** $\alpha \subset R$ ideal, $\pi : R \rightarrow R/\alpha$ is ring hom.

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

Then (i) $\ker f = \{ x \in R_1 : f(x) = 0 \}$ is an ideal
(ii) $\text{Im}(f) \subset R_2$ is a subring

**Proof:** (i) $x \in \ker f, r \in R_1$

\[ f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0 = 0 \]
\[ f(x \cdot r) = f(x) \cdot f(r) = 0 \]
\[ f(x) \cdot f(r) = 0 \in R_2 \]

(ii) $1 = f(1) \in \text{Im}(f)$ \(\Rightarrow 0 = f(0) \in \text{Im}(f) \)
\(\Rightarrow \text{Im}(f) \) is closed under \(\cdot \) and it is a subring of $(R_2, +, 0)$. 

**Useful remarks:** Given \( f: R_1 \rightarrow R_2 \) ring homomorphism

1. \( f^{-1}(a_2) \subset R_1 \) is an ideal of \( R_1 \) for every \( a_2 \subset R_2 \) ideal.

   \[ sf/ x \in a_1 = f^{-1}(a_2) \Rightarrow f(rx) = f(r)f(x) \in a_2 \Rightarrow rx \in a_2 \in a_1 \]

2. \( f(R_1 \times) \subset R_2 \times \) (multiplicative units of \( R_1 \),

\text{The image of an ideal need not be an ideal (need } f \text{ to be surjective.)}

**Example:** \( f: \mathbb{Z} \rightarrow \mathbb{Z}[x] \) is a ring homomorphism

\[ \ker(f) = \text{all multiples of } n \]

\( f(n) \) is not an ideal because \( f(1) = 1 \) so \( f(nk) = nk \) giving \( f(n) = n \mathbb{Z} \) and 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 \( \ker(f) \subset R_1 \) (ideal)

Then, there exists a unique \( \overline{f} : R_1/\ker(f) \rightarrow R_2 \) such that

\[ R_1 \xrightarrow{f} R_2 \]

\[ \ker(f) \xrightarrow{\overline{f}} R_2 \]

Then: \( \overline{f} \) is injective

\[ R_1/\ker(f) \cong \text{Im } f \text{ under } \overline{f} \]
Second Iso Theorem: Let $R$ be a ring and $\alpha \in CR$ be an ideal. Set $\overline{R} := R/\alpha$. Then, there is a 1-to-1 correspondence:

\[
\begin{align*}
\{ \text{Subgroups of } (R, +, 0) \} & \leftrightarrow \{ \text{Subgroups of } (\overline{R}, +, 0) \} \\
\text{containing } \alpha & \leftrightarrow \overline{\alpha} = A \text{ mod } \alpha
\end{align*}
\]

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

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

\[
\begin{array}{ccc}
R & \xrightarrow{\iota} & \overline{R} \\
\downarrow{\pi_2} & & \downarrow{\pi_3} \\
R/\alpha & \xrightarrow{\iota_2} & \overline{R}/\overline{A}
\end{array}
\]

$\pi_3 \circ \pi_1$ is the iso.

Third Iso Theorem: Let $R$ be a ring, $SCR$ a subring, and $\alpha \in CR$ be an ideal. Then,

(i) $S/\alpha$ is an ideal in $S$

(ii) $S + \alpha$ is a subring of $R$ containing $\alpha$, and $\alpha$ is an ideal of $S + \alpha$.

Furthermore, $S + \alpha \overset{f}{\sim} S/\alpha$ as rings.

\[
\begin{array}{ccc}
S & \xrightarrow{\iota} & S + \alpha \\
\downarrow{\iota_1} & & \downarrow{\pi} \\
S/\ker f & \xrightarrow{\overline{f}} & \overline{\alpha}
\end{array}
\]

$f = \text{Bij}$

$\ker f = S/\alpha$

$\overline{f}$ inj

$\text{Im } \overline{f} = S + \alpha / \alpha$
§3. Algebra of Ideals.

Note: \( \alpha \cap R^* \neq \emptyset \Rightarrow \alpha = R = (1) \) (called the unit ideal)

Let \( \mathcal{I}(R) \) = set of all ideals of \( R \).
- Given \( \alpha, \beta \in \mathcal{I}(R) \), define:
  1. \( \alpha + \beta := \{ a + b : a \in \alpha, b \in \beta \} \)
  2. \( \alpha \cdot \beta := \{ \sum_{i=1}^{n} a_i b_i : \text{where } n \geq 0 \text{ is arbitrary}, a_1, \ldots, a_n \in \alpha, b_1, \ldots, b_n \in \beta \} \)

Easy check: \( \alpha + \beta \) and \( \alpha \cdot \beta \) are again ideals of \( R \).
- \( (\mathcal{I}(R), +, (0)) \) is an additive monoid.
- \( (\mathcal{I}(R), \cdot, (1)) \) is a multiplicative monoid.

34. Ideals generated by sets:

Let \( R \) be a ring and \( a_1, \ldots, a_n \in R \).

Def. The left-ideal generated by \( a_1, \ldots, a_n \) is \( R a_1 + \cdots + R a_n \)

\[ =: R(a_1, \ldots, a_n) \]

The right-ideal is \( a_1 R + \cdots + a_n R \)

\[ =: (a_1, \ldots, a_n)_R \]

The ideal generated by \( a_1, \ldots, a_n \) is \( R a_1 R + \cdots + R a_n R \)

\[ =: (a_1, \ldots, a_n) \]

More generally, in any subset \( X \subseteq R \), the ideal generated by \( X \) is:

\[ (X) = \bigcap_{\alpha \in \mathcal{I}(R)} \alpha \]

\[ X \subseteq \alpha \]

Similarly, we have \( (X)_L \) = \( \bigcap_{\alpha \in \mathcal{I}(R)} \alpha \)

\[ X \subseteq \alpha \]

\[ (X)_R \] = \( \bigcap_{\alpha \in \mathcal{I}(R)} \alpha \)

\[ X \subseteq \alpha \]

[Easy check: These intersections always give left/right/two-sided ideals.]
**Definition**: An ideal \( \mathfrak{a} \subseteq R \) is said to be finitely generated if
\[\exists a_1, \ldots, a_m \in \mathfrak{a} \text{ such that } \mathfrak{a} = (a_1, \ldots, a_m).\]
An ideal \( \mathfrak{a} \) is principal if \( \mathfrak{a} = (a) = Ra \) for some \( a \in R \).
We say that \( R \) is a principal ideal ring if every ideal \( \mathfrak{a} \subseteq R \) is principal.

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

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

**Example Ideals in \( \mathbb{Z}/N\mathbb{Z} \)**

By 2nd Iso Theorem:

**Remark**: Let \( f: R_1 \to R_2 \) be a homomorphism of rings and \( \mathfrak{a}_2 \subseteq g(R_2) \).
\[f: R_1 \to R_2 \to R_2/\mathfrak{a}_2 \quad \text{Ker}(g) = f^{-1}(\mathfrak{a}_2) = \mathfrak{a}_1\]
and hence \( R_1/\mathfrak{a}_1 \hookrightarrow R_2/\mathfrak{a}_2 \)

Let \( R \) be a ring. We have a natural ring homomorphism:
\[\Psi: \mathbb{Z} \to R \]
\[m \mapsto m \cdot 1_R = 1_R + \cdots + 1_R \quad \text{for } m \geq 0\]
and \( \Psi(-n) = -\Psi(n) \) for \( n \geq 0 \).

\( \text{Ker}(\Psi) \subseteq \mathbb{Z} \) is an ideal. Since \( 1_R \neq 0_R \), then \( \text{Ker}(\Psi) \neq \mathbb{Z} \).
Thus \( \text{Ker}(\Psi) = (N) \) for some \( N \geq 0 \), \( N \neq 1 \).
If \( N = 0 \) then the characteristic of \( R \) is zero [\( \mathbb{Z} \) is the characteristic subring of \( R \)].

If \( N > 0 \): \( \frac{\mathbb{Z}}{N\mathbb{Z}} \hookrightarrow R \) is the characteristic subring.

Obs: If \( R \) is a domain, then \( \text{char}(R) = 0 \) or a prime number.

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