date: wednesday, february 28, 2024

Review of Rings II

Homomorphisms

Def^{n}: Let R and S be rings. A ring homomorphism is a function $\varphi: R \to S$ such that
- $\varphi(a+b) = \varphi(a) + \varphi(b)$ <- φ is a group homomorphism + extra
- $\varphi(ab) = \varphi(a)\varphi(b)$

Def^{n}: A homomorphism $\varphi: R \to S$ is an isomorphism if it is bijective. We write $R \simeq S$.

Proposition: Let $\varphi: R \to S$ be a ring homomorphism.
1. $\varphi(0_R) = 0_S$
2. $\varphi(-a) = -\varphi(a)$
3. $\varphi(a^n) = \varphi(a)^n$
4. The image $\varphi(R) = \{\varphi(r) \mid r \in R\} \subseteq S$ is a subring
5. If $1_R \in R$ and $1_S \in S$, and if φ is onto, then $\varphi(1_R) = 1_S$.

Proof

1. Note $0_R = 0_R + 0_R$. So $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Subtract $\varphi(0_R)$ from both sides,
$$0_S = \varphi(0_R) - \varphi(0_R) = (\varphi(0_R) + \varphi(0_R)) - \varphi(0_R) = \varphi(0_R).$$

5. To show $\varphi(1_R) = 1_S$, need to show that $\varphi(1_R)$ "acts like" 1_S. Take $b \in S$. Since φ is onto, exists $a \in R$ such that $\varphi(a) = b$. Now $a = 1_R \cdot a$. So,
$$b = \varphi(1_R \cdot a) = \varphi(1_R)\varphi(a) = \varphi(1_R) b$$
By the same argument,
$$b = \varphi(a \cdot 1_R) = \varphi(a)\varphi(1_R) = b\varphi(1_R).$$
Since multiplicative identities are unique, $1_S = \varphi(1_R)$.

$\square$

eg. $\varphi: \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(n) = 0$ for all n.
We don't have $\varphi(1) = 1$.

Def^n: The kernel of $\varphi: R \to S$ is $\ker\varphi = \{r \in R \mid \varphi(r) = 0_S\}$.

Theorem: ① $\ker\varphi$ is an ideal of R.
② $\ker\varphi = \{0_R\}$ if and only if φ is injective.

Proof

① $\ker\varphi \neq \emptyset$ since $0_R \in R$ and $\varphi(0_R) = 0_S$.
Let $a \in \ker\varphi$ and $r \in R$. Then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0_S = 0_S$. So $ra \in \ker\varphi$.
Let $a, b \in \ker\varphi$. Then $\varphi(a-b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S$. So $a - b \in \ker\varphi$

$\square$

Consequence: Any homomorphism $\varphi: R \to S$ gives us a quotient ring:

$$R/\ker\varphi.$$

Isomorphism Theorems

1st Isomorphism Theorem: Let $\varphi: R \to S$ be a homomorphism. Then,

$$R/\ker\varphi \simeq \varphi(R) \leftarrow \text{image of } R \text{ in } S$$

eg. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}_{2024}$.
Define a ring homomorphism $\varphi: \mathbb{Z} \to \mathbb{Z}_{2024}$ by $\varphi(n) = n \pmod{2024}$.
This is onto. So $\varphi(\mathbb{Z}) = \mathbb{Z}_{2024}$.
By 1st Isomorphism Theorem,

$$\mathbb{Z}/\ker\varphi \simeq \mathbb{Z}_{2024}.$$

Claim: $\ker\varphi = \{2024n \mid n \in \mathbb{Z}\} \leftarrow$ all multiples of 2024

Remark: We can an ideal I of R principal if there exists an $a \in R$ such that $I = \{ra \mid r \in R\}$. We write this as $I = \langle a \rangle$.
↖ ideal generated by a

Return to example: $\ker\varphi = \langle 2024 \rangle$
So $\mathbb{Z}/\langle 2024 \rangle \simeq \mathbb{Z}_{2024}$.

Fact: $\mathbb{Z}/\langle m \rangle \simeq \mathbb{Z}_m$.

2^{nd} Isomorphism Theorem: Let I be a subring of R and J an ideal of R. Then $I \cap J$ is an ideal of I and

$$I/_{I\cap J} \simeq \frac{I+J}{J}.$$

3^{rd} Isomorphism Theorem: Let I, J be ideals of R with $I \subseteq J \subseteq R$. Then,

$$(R/_I)/_{(J/_I)} \simeq R/_J.$$

4^{th} Isomorphism Theorem: Let I be an ideal. Then there is a 1-1 correspondance between the ideals of $R/_I$ and the ideals of R that contain I, ie. $I \subseteq J \subseteq R$.

Maximal and Prime Ideals

R is assumed to be commutative.

Def^n: An ideal M is a maximal ideal of R if for every ideal J such that $M \subseteq J \subseteq R$, then $J = M$ or $J = R$.

Def^n: An ideal P of R is prime if $P \neq R$, and whenever $ab \in P$, $a \in P$ or $b \in P$.

Theorem: M is a maximal ideal if and only if $R/_M$ is a field.

eg. $\langle 2024 \rangle$ in $\mathbb{Z}$ is not maximal since $\mathbb{Z}/_{\langle 2024 \rangle} \simeq \mathbb{Z}_{2024}$ is not a field since it's not a domain (eg. $2 \times 1012 = 0$)
Note that $\langle 2024 \rangle \subseteq \langle 1012 \rangle \subseteq \langle 2 \rangle$.

eg. $\langle m \rangle \subseteq \mathbb{Z}$ is a maximal ideal $\Leftrightarrow$ $\mathbb{Z}/_{\langle m \rangle} \simeq \mathbb{Z}_m$ is a field $\Leftrightarrow$ m is prime.

Theorem: P is a prime ideal if and only if $R/_P$ is an integral domain.

eg. P is a prime ideal of $\mathbb{Z} \iff P = \begin{cases} \langle p \rangle, & p \text{ prime} \\ \langle 0 \rangle \end{cases}$

Note $\mathbb{Z}/\langle 0 \rangle \simeq \mathbb{Z}$ is an integral domain so $\langle 0 \rangle$ is prime.

Theorem: Every maximal ideal is a prime ideal.

<u>Proof</u>

M maximal $\iff R/M$ is a field

$\implies R/M$ is an integral domain

$\iff M$ is a prime ideal.

$\square$

Note: Prime may fail to be maximal (eg. $\langle 0 \rangle$ is prime but not maximal)