1 Ring Homomorphisms

Theorem 1.1

Let $\varphi : R \mapsto S$ be a ring homomorphism. Then, $\ker\varphi = \{r \in R \mid \varphi(r) = 0\}$ is an ideal of R.

Proof. If $a, b \in \ker\varphi$, then $\varphi(a-b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$, which implies that $a - b \in \ker\varphi$. Now, if we check $a \in \ker\varphi$ and $r \in R$, then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Therefore, $ra \in \ker\varphi$. Thus, $\ker\varphi$ is an ideal by the ideal test. □

1.1 First Isomorphism Theorem

Theorem 1.2: First Isomorphism Theorem

Let $\varphi : R \mapsto S$ be a ring homomorphism. Then, the map

$$\overline{\varphi} = R/\ker\varphi \mapsto \varphi(R)$$

defined by the mapping

$$r + \ker\varphi \mapsto \varphi(r)$$

is an isomorphism.

Proof. We already know that $\overline{\varphi} : R/\ker\varphi \mapsto \varphi(R)$ is an isomorphism of additive groups; in particular,

$$(R/\ker\varphi, +) \mapsto (\varphi(R), +)$$

by the First Isomorphism Theorem for groups. Thus, it suffices to check that:

$$\overline{\varphi}(xy) = \overline{\varphi}(x)\overline{\varphi}(y)$$

So, it suffices to check:

$$\begin{aligned}
\overline{\varphi}((r + \ker\varphi)(s + \ker\varphi)) &= \overline{\varphi}(rs + \ker\varphi) \\
&= \varphi(rs) \\
&= \varphi(r)\varphi(s) \\
&= \overline{\varphi}(r + \ker\varphi)\overline{\varphi}(s + \ker\varphi)
\end{aligned}$$

And so we are done. □

Remark: If $I \subseteq R$ is an ideal, then $I = \ker q$ where $q : R \mapsto R/I$, defined by the mapping $r \mapsto r + I$, is the quotient homomorphism.

1.2 Examples

1. Consider the homomorphism $\varphi : \mathbb{Z}[x] \mapsto \mathbb{Z}$ defined by the mapping $f(x) \mapsto f(0)$. φ is a surjective[1] homomorphism. By the First Isomorphism Theorem:

   $$\mathbb{Z}[x]/\ker\varphi \cong \mathbb{Z}$$

   Here, we define $\ker\varphi = \{a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}\}$ because $f(0)$ is a constant term. However, we can factor x out to get:

   $$\ker\varphi = \{x(a_1 + a_2x^1 + \cdots + a_nx^{n-1}) \mid a_i \in \mathbb{Z}\} = \langle x\rangle$$

[1] If $a \in \mathbb{Z}$, then $(x + a) \xrightarrow{\varphi} 0 + a = a$

And so it follows that:

$$\boxed{\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}}$$

2. Consider the homomorphism $\varphi : \mathbb{R}[x] \mapsto \mathbb{C}$ defined by the mapping $f(x) \mapsto f(i)$. φ is surjective because $f(a+bx) = a+bi$ for any $a, b \in \mathbb{R}$. We also know that $x^2+1 \in \ker\varphi$ by $i^2+1=0$. This implies that:

$$\langle x^2+1\rangle \subseteq \ker\varphi \subset \mathbb{R}[x]$$

Fact: $\langle x^2+1\rangle$ is maximal, which implies that $\langle x^2+1\rangle = \ker\varphi$.

Proof. (Of fact.) We prove that $\mathbb{R}[x]/I$ for $I = \langle x^2+1\rangle$ is a field for any $a+bx+I$ with a, b not both zero, then $(a+b+I)^{-1} = \frac{a-bx}{a^2+b^2} + I$. ☐

Therefore, $\boxed{\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}}$ by the First Isomorphism Theorem.

1.3 Rings with Unity

Proposition. *If R has unity, then $\varphi : \mathbb{Z} \mapsto \mathbb{R}$ defined by*

$$\varphi(n) = n\cdot 1 = \begin{cases} \underbrace{1+\cdots+1}_{n\ times} & n>0 \\ 0 & n=0 \\ \underbrace{-1-1-\cdots-1}_{-n\ times} & n<0 \end{cases}$$

is a homomorphism.

Proof. Left as an exercise. ☐

Proposition. *If R is a ring with unity, then:*

(a) If $\operatorname{char} R = n > 0$*, then R contains a subring isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

(b) If $\operatorname{char} R = 0$*, then R contains a subring isomorphic to $\mathbb{Z}$.*

Proof. Let $\varphi : \mathbb{Z} \mapsto \mathbb{R}$ with $\varphi(n) = n\cdot 1$. Then, $\operatorname{char} R$ is the additive order of 1. This implies that if $\operatorname{char} R = n > 0$, then $\ker\varphi = n\mathbb{Z}$ so $\mathbb{Z}/n\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq R$ by the First Isomorphism Theorem. Likewise, if $\operatorname{char} R = 0$, then $\ker\varphi = \{0\}$ and it follows that $\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq R$ by the First Isomorphism Theorem. ☐

1.4 Fields

Definition 1.1: Prime Subfield

The subfield of a field isomorphic to $\mathbb{F}_p$ or $\mathbb{Q}$ is called the **prime subfield**.

Theorem 1.3

- If F is a field of characteristic p, then F contains a subfield isomorphic to $\mathbb{F}_p$.
- If F is a field of characteristic 0, then F contains a subfield isomorphic to $\mathbb{Q}$.

Proof. We prove both parts.

- By the previous proposition, $\operatorname{char} F = p$ implies that the subring is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.
- $\operatorname{char} F = 0$ implies that the subring is isomorphic to $\mathbb{Z}$, given by

  $$\varphi : \mathbb{Z} \mapsto F$$

  which sends $n \mapsto n \cdot 1$. Consider the set

  $$T = \{ab^{-1} \mid a, b \in \varphi(\mathbb{Z}), b \neq 0\} \subseteq F$$

  We claim that T is a subring isomorphic to $\mathbb{Q}$.

  Proof. Define $\overline{\varphi} : \mathbb{Q} \mapsto F$ by $\overline{\varphi}(a/b) = \varphi(a)\varphi(b)^{-1}$.

  - Well-Defined: This is well-defined since $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$, which then implies that $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$ for $\varphi : \mathbb{Z} \mapsto F$. This implies that $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$, which again implies that $\overline{\varphi}(a/b) = \overline{\varphi}(c/d)$.
  - Homomorphism: Addition is left as an exercise. For multiplication, see lecture.

  So, we are done. □

And so on (need to come back). □

Remark: If F is a field and $I \subseteq F$ is an ideal, then $I = \{0\}$ or $I = F$.

Proof. $F/\{0\} \cong F$ is a field. Thus, $\{0\}$ is a maximal ideal of F. This implies that, for all ideals I with $\{0\} \subseteq I \subseteq F$, $I = \{0\}$ or $I = F$. The fact that all ideals satisfy $\{0\} \subseteq I \subseteq F$ concludes the proof. □