Last time: Ring homomorphisms

\[ \phi : R \to S \quad R, S \text{ rings} \]

is a ring homomorphism if

- \( \phi(a + b) = \phi(a) + \phi(b) \quad \forall a, b \in R \)
- \( \phi(ab) = \phi(a) \phi(b) \quad \forall a, b \in R \)

**Thm** If \( \phi : R \to S \) is a ring homomorphism, then \( \phi \) induces

\[ \bar{\phi} : R / \ker \phi \to \phi(R) \quad \text{as} \]

\[ \bar{\phi}(r + \ker \phi) = \phi(r) \]

and \( \bar{\phi} \) is a ring isomorphism.

**Example** \( \phi : \mathbb{Z}[x] \to \mathbb{Z} \) as \( f \mapsto f(2) \)

- \( \text{Image} \( \phi \) = \mathbb{Z} \)
- \( \ker \phi = \langle x - 2 \rangle \). \( \text{Pf:} \) Suppose \( f \in \mathbb{Z}[x] \). Then
  \[ f(x) = q(x)(x - 2) + r, \quad r \in \mathbb{Z} \]
  \[ f(2) = r \quad \text{so} \quad f(2) = 0 \iff r = 0 \iff f \in \langle x - 2 \rangle \]

\( \mathbb{Z}[x] / \langle x - 2 \rangle \cong \mathbb{Z} \) by First Isomorphism Thm

Moreover, \( \mathbb{Z} \) is an integral domain \( \implies \langle x - 2 \rangle \) is a prime ideal.
Moreover, \( \mathbb{Z} \) is an integral domain \( \Rightarrow \langle x-2 \rangle \) is a prime ideal.

Recall: \( \langle x-2 \rangle \) is the principal ideal generated by \( x-2 \)

\[
\Rightarrow q \cdot (x-2) : q \in \mathbb{Z}[x] \\
\]

Thm: Suppose \( R \) is a ring with unity. The mapping

\[
\phi: \mathbb{Z} \rightarrow R \text{ given by } n \mapsto n \cdot 1 \text{ is a ring homomorphism.}
\]

Recall: If \( n > 0 \) is a positive integer, then

\[
n \cdot 1 = 1 + 1 + \ldots + 1 \quad \text{(n times)}
\]

If \( n \leq 0 \) is a negative integer, then

\[
n \cdot 1 = -(-n) \cdot 1
\]

Pf: Suppose \( m, n > 0 \), integers.

- \( \phi(m+n) = (m+n) \cdot 1 = m \cdot 1 + n \cdot 1 = \phi(m) + \phi(n) \)
- \( \phi(mn) = (mn) \cdot 1 = (m \cdot 1)(n \cdot 1) = \phi(m) \phi(n) \) \text{ (distributive property)}

Suppose \( m > 0, n > 0, m > n \).

\[
\phi(m+(-n)) = \phi(m-n) = (m-n) \cdot 1 = m \cdot 1 - n \cdot 1 = \phi(m) + \phi(-n)
\]

Suppose \( m \geq 0, n \geq 0, m \leq n \), let \( \phi \) of negative integers.
Suppose \( m > 0, n > 0, m \leq n \) \( \frac{\text{let}}{} \) \( k \) of negative integers

\[
\phi(m + (-n)) = \phi(-(n-m)) = -(n-m) \cdot 1 = m \cdot 1 - n \cdot 1
\]

\[
= \phi(m) + \phi(-n)
\]

\[\blacksquare\]

Corollary: Suppose \( R \) is a ring with unity. If \( \text{char} R = n > 0 \), then \( R \) contains a subring isomorphic to \( \mathbb{Z}/n\mathbb{Z} \). If \( \text{char} R = 0 \), then \( R \) contains a subring isomorphic to \( \mathbb{Z} \).

**Pf:**
- \( 1 \in R \), the unity.
- Define \( S = \{ k \cdot 1 : k \in \mathbb{Z} \} \).

Then \( S \) is a subring of \( R \) and

\[\phi : \mathbb{Z} \rightarrow S\]

\[k \mapsto k \cdot 1\]

is a surjective ring homomorphism.

In case \( \text{char} R = n > 0 \):

\[
\ker \phi = \{ m \in \mathbb{Z} : m \cdot 1 = 0 \} = \mathbb{Z}/n\mathbb{Z}
\]

\[
= \mathbb{Z}/n^R
\]

additive order of \( 1 \) in \( R \)

\[\Rightarrow\text{ First Isom Thm: } \phi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} S \text{ isom.}\]

In case \( \text{char} R = 0 \)

\[
\ker \phi = \{ m \in \mathbb{Z} : m \cdot 1 = 0 \} = \mathbb{Z}/7\mathbb{Z}
\]
\[ \text{Ker } \phi = \{ m \in \mathbb{Z} : m \cdot 1 = 0 \} = \{0\} \]

**First Isom. Thm:** \( \mathbb{Z}/\{0\} = \mathbb{Z} \cong S \). (\( p \) is nec. prime)

**Cor:** If a field \( F \) has char \( p > 0 \), then \( F \) contains a subfield isomorphic to \( \mathbb{Z}/p\mathbb{Z} \). If the field \( F \) has char \( F = 0 \), then \( F \) contains a subfield isomorphic to \( \mathbb{Q} \).

**Pf:** By what we've just proved, if char \( F = p > 0 \), then \( F \) contains a copy of \( \mathbb{Z}/p\mathbb{Z} \) (i.e., a subring isom to \( \mathbb{Z}/p\mathbb{Z} \)).

Now suppose char \( F = 0 \). By above, \( \exists S \subseteq F \) a subring isom to \( \mathbb{Z} \), say \( \psi : S \rightarrow \mathbb{Z} \) is isom.

Now let \( T = \{ a/b^i : a, b \in S, b \neq 0 \} \subseteq F \).

**Claim:** \( T \) is isom to \( \mathbb{Q} \), the rational numbers.

**Pf:** Define \( \tilde{\psi} : T \rightarrow \mathbb{Q} \) so \( \tilde{\psi}(a/b^i) = \frac{\psi(a)}{\psi(b)} \in \mathbb{Q} \).

Because \( b \neq 0 \) and \( \psi \) is isom, \( \psi(b) \neq 0 \) so can write \( \frac{\psi(a)}{\psi(b)} \).
\[ \psi(a) / \psi(b) \]

**\(\tilde{\psi} \) is well-defined:** Suppose \( a, b, a_1, b_1, a_2, b_2 \in S \) with \( a_1, a_2, b_1, b_2 \in S \), \( b_1, b_2 \neq 0 \).

\[ \implies a_1 b_2 = a_2 b_1 \quad \text{in} \quad S \]

\[ \implies \psi(a_1) \psi(b_2) = \psi(a_2) \psi(b_1) \quad \text{in} \quad \mathbb{Z} \]

\[ \implies \frac{\psi(a_1)}{\psi(b_1)} = \frac{\psi(a_2)}{\psi(b_2)} \quad \text{in} \quad \mathbb{R} \]

Therefore, we've constructed a set map \( \tilde{\psi} : T \rightarrow \mathbb{R} \).

**Need to verify:** \( \tilde{\psi} \) is a ring isomorphism.

- \( \tilde{\psi} \) preserves multiplication:
  \[ \tilde{\psi}(a_1 b_2^{-1}) = \tilde{\psi}(a_1) \tilde{\psi}(b_2^{-1}) \]

  \[ \begin{array}{c}
  a_1, b_1, a_2, b_2 \in S \\
  b_1, b_2 \neq 0
  \end{array} \]

  \[ = \frac{\psi(a_1)}{\psi(b_1)} \cdot \frac{\psi(a_2)}{\psi(b_2)} \]

  \[ = \frac{\psi(a_1 b_2^{-1})}{\psi(b_1 b_2^{-1})} \]

  \[ = \frac{\psi(a_1 b_2^{-1})}{\psi(a_2 b_2^{-1})} \]

- \( \tilde{\psi} \) preserves addition:
  \[ \tilde{\psi}(a_1 b_2^{-1} + a_2 b_2^{-1}) \]

  \[ = \tilde{\psi}(a_1 b_2^{-1} + a_2 b_2^{-1})(b_1 b_2)^{-1} \]

  \[ = \frac{\psi(a_1 b_2)}{\psi(b_1 b_2)} \quad \frac{\psi(a_2 b_2)}{\psi(b_1 b_2)} = \frac{\psi(a_1 b_2) + \psi(a_2 b_2)}{\psi(b_1 b_2)} \]
\[ \tilde{\psi} = \frac{\psi(a_1)}{\psi(b_1)} + \frac{\psi(a_2)}{\psi(b_2)} \]
\[ \tilde{\psi} = \tilde{\psi}(a_1 b_1^{-1}) + \tilde{\psi}(a_2 b_2^{-1}) \]

- \( \tilde{\psi} \) is clearly surjective
  
  \[
  \text{If } \psi(a) = m \quad \text{then } \psi(a b^{-1}) = n m \quad \text{if } n \neq 0
  \]

- \( \text{ker } \tilde{\psi} = 0 \): If \( \psi(a b^{-1}) = 0 = \psi(a)/\psi(b) \)
  
  \[
  \Rightarrow \psi(a) = 0 \quad (b/c \quad \psi(b) \neq 0)
  \]
  
  \[
  \Rightarrow a = 0
  \]
  
  \[
  \Rightarrow a b^{-1} = 0.
  \]

\( \Rightarrow \) \( \tilde{\psi} \) is an isomorphism.