Last time: If $F$ is an ordered field with the least upper bound property, then $F$ is isomorphic to $\mathbb{R}/I$
($\mathcal{C}$ = Cauchy sequence in $\mathbb{Q}$, $I$ = ideal of sequences converging to 0).

The proof above uses the Homomorphism theorem. Let $f : R \rightarrow S$ be a homomorphism of rings, $I = \ker f$. There exists a unique injective homomorphism $\bar{f} : R/I \rightarrow S$ with $\bar{f}(a + I) = f(a)$ for all $a \in R$.

\[
\begin{array}{c}
R \\
\downarrow f \\
R/I \\
\downarrow \bar{f} \\
S
\end{array}
\]

i.e., the diagram commutes.

Moreover, $\bar{f} : R/I \rightarrow f(R)$ is an isomorphism.

"Recall" A nonzero element $a$ of a (commutative) ring $R$ is a zero divisor if $fa + R \neq 0$ so that $ab = 0$.

Ex. $R = \mathbb{Z}_6$. 
- $[2], [3], [4] \neq 0$ but $[12][37] = 0$, $[3][47] = 0$
- so $[12], [13], [14]$ are zero divisors.

Definition. A commutative ring $R$ (with 1) is an integral domain if it has no zero divisors.

We saw in lecture 3:

If $R$ is an integral domain, $a, b, c \in R$, $a \neq 0$, then $a \cdot b = a \cdot c \Rightarrow b = c$.

Recall. For a commutative ring $R$ the characteristic of $R$ is

\[
\text{char } R = \min \{ k \mid k \text{ is a natural number} \text{ such that } n \cdot 1_R = 0_R \}
\]

Lemma 2.2. Let $R$ be an integral domain. Suppose $\text{char } R > 0$. The characteristic of $R$ is a prime.
Proof Suppose \( \text{char } R > 0 \). Then the homomorphism

\[ f : \mathbb{Z} \rightarrow R, \quad f(n) = n \cdot 1_R \]

is not 1-1 (\( \exists n \in \mathbb{N} \) s.t. \( f(m) = 0 = f(0) \)).

Let \( I = \ker f \). \( I \) is an ideal in \( \mathbb{Z} \) and \( I \neq \{0\} \).

You have proved: if \( I \leq \mathbb{Z} \) is an ideal, then \( I = k \mathbb{Z} \) for some \( k \). In fact, if \( I \neq \{0\} \)

\[ k = \min \left\{ n \in \mathbb{N} \mid n \in I \right\} \]

In our case,

\[ k = \min \left\{ n \in \mathbb{N} \mid f(n) = 0 \right\} = \min \left\{ n \in \mathbb{N} \mid n \cdot 1_R = 0 \right\} = \text{char } R. \]

Homomorphism theorem implies:

\[ \overline{f} : \mathbb{Z}/k\mathbb{Z} \rightarrow f(\mathbb{Z}) \] is an isomorphism.

\( f(\mathbb{Z}) \subseteq k \) is a subring. Since \( R \) has no zero divisors,

\( f(\mathbb{Z}) \) has no zero divisors.

Since \( f(\mathbb{Z}) \) is isomorphic to \( \mathbb{Z}/k\mathbb{Z} \), \( \mathbb{Z}/k\mathbb{Z} \) cannot have zero divisors either.

But if \( k = k \cdot m \) with \( 1 < k, m < k \), then

\( \langle k, \langle m \rangle \rangle \neq \langle 0 \rangle \) in \( \mathbb{Z}_k \) but \( \langle k \mid \langle m \rangle \rangle = \langle k \rangle = \langle 0 \rangle \) in \( \mathbb{Z}_k \),

i.e. \( k \) not a prime then \( \mathbb{Z}_k \) does have zero divisors.

We conclude: \( k = \text{char } R \) must be a prime if \( R \) has no zero divisors (i.e. if \( R \) is an integral domain).

Remark Any field \( F \) is an integral domain:

If \( a \neq 0 \) and \( a \cdot b = 0 \) then

\[ 0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot b = b \]

\( \Rightarrow a \) cannot be a zero divisor.

The set \( \mathbb{R}[x] = \{ a_0 + a_1 x + \ldots + a_n x^n \mid n \geq 0, \ a_0, \ldots, a_n \in \mathbb{R} \} \)
of polynomials with real coefficients form a commutative
Ring under the usual addition and multiplication of polynomials.

You proved in (HW 9, #5):

\[ p(x) \in \mathbb{R}[x], \quad p(x) \mathbb{R}[x] = \{ p(x) q(x) \mid q(x) \in \mathbb{R}[x] \} \]

is an ideal in \( \mathbb{R}[x] \).

\[ \Rightarrow \mathbb{R} = \mathbb{R}[x] / p(x) \mathbb{R}[x] \text{ is a commutative ring.} \]

Our goal:

\[ \mathbb{R}[x] / (x^2 + 1) \mathbb{R}[x] \]

"i.e." the ring of complex numbers.

First, polynomial rings more systematically.

Let \( S \) be a commutative ring (with 1, as usual).

We define

\[ S[x] = \{ a_0 + a_1 x + \ldots + a_n x^n \mid n \geq 0, \quad a_0, \ldots, a_n \in S \} \]

\( S[x] \) is, again, a commutative ring.

\[ \left( \sum_{k=0}^{n} a_k x^k \right) + \left( \sum_{k=0}^{m} b_k x^k \right) = \sum_{k=0}^{n+m} (a_k + b_k) x^k \]

\[ \left( \sum_{i=0}^{n} a_i x^i \right) \cdot \left( \sum_{j=0}^{m} b_j x^j \right) = \sum_{k=0}^{n+m} \left( \sum_{i+j=k} a_i b_j \right) x^k \]

Caution: Every polynomial \( p(x) = \sum_{i=0}^{n} a_i x^i \) defines a function \( p^{\circ}: S \to S \) by

\[ p^{\circ}(s) = \sum_{i=0}^{n} a_i s^i \]

However, different polynomials may define the same function.

\[ \exists \quad p, q \in \mathbb{Z}_2, \quad \begin{cases} p(x) = [1] + [1] x + [1] x^2 & \equiv p(x) = [1] \quad \text{mod} \quad 2 \quad \text{for} \quad x = [1] \\ q(x) = [1] \end{cases} \]

\[ p^{\circ}([0]) = [1] \quad \text{and} \quad q^{\circ}([0]) = [1] \]

\[ p^{\circ}([1]) = [1] + [1] + [1] = [3] = [1] \quad \text{mod} \quad 2 \quad \text{for} \quad x = [1] \]

In fact $|\text{map}(\mathbb{Z}_2, \mathbb{Z}_2)| = 2^2 = 4$
and $|\mathbb{Z}_2[x]|$ is infinite.

In general the map $S[x] \to \text{Map}(S, S)$
$p(x) \mapsto "p"(s)$
need not be 1-1 ($S=\mathbb{Z}_2$) and it need not be onto
(take $S=\mathbb{IR}$).

Def Given a polynomial $p(x) = a_0 + a_1 x + \ldots + a_n x^n \in S[x]$
we define its degree to be $\deg p = \max \{ k \mid a_k \neq 0 \}$.

By convention $\deg 0 = -\infty$

Ex. $p(x) = [1] + [2] x^3 \in \mathbb{Z}_2[x] \, \text{, } \deg p = 3.$

Note For $p + S[x]$ \begin{itemize}
  \item $\deg p = 0 \iff p(x) = a_0 \text{ for some } a_0 \in S,
  \quad a_0 \neq 0.$
\end{itemize}

Lemma 29.1 Let $S$ be a commutative ring, $p, q \in S[x]$.
\begin{enumerate}
  \item $\deg(p+q) \leq \max \{ \deg p, \deg q \}$
  \item if $S$ is an integral domain
    \begin{align*}
      \deg (p \cdot q) &= \deg p + \deg q \\
      \text{(otherwise } \deg (p \cdot q) \leq \deg p + \deg q \text{)}
    \end{align*}
\end{enumerate}

Sketch of proof Suppose $n = \deg p, m = \deg q$. Then
\begin{align*}
  p(x) &= a_0 + \ldots + a_n x^n, \quad a_n \neq 0; \\
  q(x) &= b_0 + b_1 x + \ldots + b_m x^m, \quad b_m \neq 0
\end{align*}
\begin{align*}
  p(x) \cdot q(x) &= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \ldots + a_n b_m x^{n+m}
\end{align*}
If $S$ is an integral domain, $a_n b_m \neq 0$, since $a_n, b_m \neq 0$
\begin{align*}
  \Rightarrow \quad \deg (p \cdot q) &= n + m = \deg p + \deg q.
\end{align*}
Otherwise $\deg (p \cdot q) \leq n + m.$