Division Algorithm (Theorem 1.1)

Let \( a, b \) be integers with \( b > 0 \). Then there exist unique integers \( q \) and \( r \) such that

\[
a = bq + r \quad \text{and} \quad 0 \leq r < b
\]

\[
\text{dividend} \rightarrow (\text{divisor}) \cdot (\text{quotient}) + (\text{remainder}) \rightarrow \text{remainder}
\]

Proof Let \( a, b \) be fixed integers with \( b > 0 \). Consider the set \( S \) of all integers of the form

\( a - bx \), where \( x \) is an integer,

and \( a - bx \geq 0 \)

Step 1. Show that \( S \) is nonempty. In fact

\( -|a| \in S \).

Proof: \( b > 1 \).

\[
blal \geq |a|
\]

\[
blal \geq -a \quad (\therefore |a| \geq -a)
\]

\[
a + blal \geq 0.
\]
Step 2. Find $q, r$ such that $a = bq + r$, $r \geq 0$.

By Well-Ordering axiom,

( : Every nonempty subset of natural numbers has a least element )

$S$ has a smallest element $r \geq 0$.

Since $r \in S$, $r = a - bx$ for some integer $x = q$. Then $a = bq + r$, $r \geq 0$.

Step 3. Show that $r < b$.

We use a "proof by contradiction".

Assume that $r \geq b$. Then $r - b \geq 0$.

From step 2, $r = a - bq$. Thus

$r > r - b = a - bq - b = a - (q + 1)b \geq 0$.

This shows that $r - b \in S$ and $r - b < r$.

However, $r$ is the smallest element in $S$, which yields a contradiction.

Therefore $r < b$. 
Step 4. Show that \( r, q \) are the only numbers with these properties.

To prove uniqueness, suppose that
\[
a = bq_1 + r_1, \quad 0 \leq r_1 < b
\]
Since \( a = bq + r \), we have
\[
bq + r = bq_1 + r_1
\]
\[
b(q - q_1) = r_1 - r
\]
Since \( 0 \leq r < b \), \(-b < r_1 - r < b\)
Then \(-b < b(q - q_1) < b\)
\[-1 < q - q_1 < 1 \quad (\text{divide by } b)\]
Since \( q, q_1 \) are integers, only possible case is \( q - q_1 = 0 \). This shows \( q = q_1 \)
Consequently, by \( bq + r = bq_1 + r_1 \), we have \( r = r_1 \).
Example, \( a = 4327, \ b = 281 \),
\[
\begin{align*}
4327 &= 281 \cdot 15 + 112 \\
\frac{4327}{281} &= \frac{112}{a}
\end{align*}
\]
\( a = 11432, \ b = 453 \)
\[
\begin{align*}
-11432 &= 453 \cdot (-17) + 269 \\
\frac{-11432}{453} &= \frac{269}{a}
\end{align*}
\]

**Divisibility**

Let \( a, b \) be integers with \( b \neq 0 \). We say that \( b \) divides \( a \) (or that \( b \) is a factor of \( a \)) if \( a = bc \) for some integer \( c \). Denoted by \( b \mid a \) (read: \( b \) divides \( a \)).

If not, write \( b \nmid a \) (read: \( b \) does not divide \( a \)).

Example. \( 3 \mid 6, \ 3 \nmid 5, \ -3 \mid 6 \), \(-3 \nmid -6, \ 3 \mid -6, \ -3 \nmid 5 \).
If $b | a$, we also say that $a$ is a multiple of $b$, and $b$ is a divisor of $a$.

Example. $-6, -3, 0, 3, 6, 9, \ldots$ are multiples of 3.

Definition (Greatest Common Divisor)

Let $a, b$ be integers not both 0.

The greatest common divisor (gcd) of $a$ and $b$ is the largest integer $d$ that divides both $a$ and $b$. i.e.

1) $d | a$ and $d | b$

2) If $c | a$, and $c | b$, then $c \leq d$

We write $d = \text{gcd}(a, b)$ or $d = (a, b)$.

Note. The gcd of any pair $a, b$ exists and unique.

Example, $(12, 30) = 6, (10, 21) = 1, (66, 121) = 11$. 
Theorem 1.2.

Let $a, b$ be integers, not both 0, and $d = (a, b)$. Then there exist integers $u, v$ such that $d = au + bv$.

Proof of Theorem 1.2.

Let $S = \{am + bn \mid m, n \in \mathbb{Z}\}$.

Step 1. Find the smallest positive element of $S$.

Note that $a^2 + b^2 \in S$, $a^2 + b^2 > 0$.

Thus, $S$ contains a positive integer and hence must contain a smallest positive integer $t$ by the Well-Ordering Axiom.

By definition of $S$, there exist $u, v \in \mathbb{Z}$ such that $t = au + bv$.

Step 2. Prove that $t$ is $d = (a, b)$.

Outline: 1. $t | a, t | b$

2. If $c | a, c | b$ then $c \leq t$. 

Let \( S = \{ am + bn | \ m, n \in \mathbb{Z} \} \) and 
\( S^+ = S \cap \mathbb{N}^+ \) 
(elements of \( S \), positive).

We use Well-Ordering axiom to have the least element of \( S^+ \).

But, to do that, we need to show that \( S^+ \) is nonempty.

Consider \( a^2 + b^2 = a \cdot a + b \cdot b \) 
since \( a, b \) are not both 0, \( a^2 + b^2 > 0 \). 
Thus \( a^2 + b^2 \in S^+ \). This shows \( S^+ \) is nonempty.

The least element exists in \( S^+ \) by WO, say \( t \). Then by definition of \( S \), we have \( t = am + bn \) for some integers \( m, n \).
Step 2-1) The least element $t$ from Step 1 divides $a$ and $b$. (common divisor of $a$ and $b$)

By division algorithm, there exist $q, r$ such that $a = tq + r$.

with $0 \leq r < t$.

We use "proof by contradiction".

Assume that $r \geq 0$, then $0 < r < t$.

Since $t = am + bn$ for some $m, n$,

$$r = a - tq = a - (am + bn)q$$

$$= a(1 - mq) + b(-nq).$$

This shows that $r \in S^+$.

This is a contradiction, since $r$ is smaller than the least element of $S^+$.

Then we see that $r = 0$, consequently $t | a$. Similarly we can show that $t | b$. 
Step 2-2) Let \( c \) be a common divisor of \( a \) and \( b \). So, \( a = ck \), \( b = cs \) for some integers \( k \) and \( s \).

Consequently

\[
t = am + bn = ck \cdot m + csn \\
= c(ekm + sn)
\]

This shows that \( c | t \).

Since \( t \) is positive, we have \( c \leq t \).

Corollary) \( S = \{ am + bn \mid m, n \in \mathbb{Z} \} = d \mathbb{Z} \)

where \( d = (a, b) \)

proof) We saw that the least positive member of \( S \) is \( d \). Any number in \( S \) can be written as a multiple of \( d \).

In fact, \( d | a \), \( d | b \), shows \( a = dk \), \( b = dl \), for some integers \( k \), \( l \).

Then for any \( m, n \in \mathbb{Z} \),

\[
amt + bn = d(km + ln) = d(km + ln). \quad \text{Thus} \quad S \subseteq d\mathbb{Z}.
\]
Conversely, if $s \leq dZ$, then $s = dz$ for some integer $z$.

Since there exist $u, v$ (integers) such that $d = au + bv$, we have

$$dz = d \cdot z = (au + bv) \cdot z = a \cdot (uz) + b \cdot (vz) \in S.$$

Thus, $dZ \subseteq S$. Hence $S = dZ$.

Exercise) Find a positive integer $d$ such that

$$\{ 6u + 15v \mid u, v \in \mathbb{Z} \} = dZ.$$

Corollary 2) Let $a, b$ be integers not both 0. The following are equivalent:

1) $(a, b) = 1$

2) There exist $u, v \in \mathbb{Z}$ such that $au + bv = 1$. 
Proof) \(1 \Rightarrow 2\) Let \(S = \{a + mb | m \in \mathbb{Z}\}\)

Then \(S = d\mathbb{Z}\) where \(d = (a, b)\).

Since \(d = 1\), we have \(S = \mathbb{Z}\).

Obviously \(1 \in \mathbb{Z}\), so \(1 = au + bv\)

for some integers \(u, v\).

\(2 \Rightarrow 1\) If there exist \(u, v \in \mathbb{Z}\) such that \(au + bv = 1\), then the set \(S^+ = S \cap \mathbb{N}^+\)

\[= \{a + mb | m \in \mathbb{Z}\} \cap \mathbb{N}^+\]

has the least element 1.

This least element is the \(gcd\) of \(a, b\) as we have seen in the proof of theorem 1.2.
Congruence in \( \mathbb{Z} \) and Modular Arithmetic

Definition Let \( a, b, n \) be integers with \( n > 0 \). Then \( a \) is congruent to \( b \) modulo \( n \), provided that \( n \mid (a-b) \).

Also written as \( a \equiv b \pmod{n} \).

In short, \( a \equiv b \pmod{n} \) if and only if \( n \mid (a-b) \).

Example: \( 17 \equiv 5 \pmod{6} \) (\( \because 6 \mid 17 - 5 = 12 \) )

\( 6 \equiv -4 \pmod{5} \)

Theorem 2.1

1. \( a \equiv a \pmod{n} \)
2. If \( a \equiv b \pmod{n} \), then \( b \equiv a \pmod{n} \).
3. If \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \), then \( a \equiv c \pmod{n} \).

This shows that \( \equiv \pmod{n} \) is an equivalence relation.
Theorem 2.2. If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then

1. \( a + c \equiv b + d \pmod{n} \)
2. \( ac \equiv bd \pmod{n} \)

Proof of 2.1) (1) \( n \mid (a-a) = 0 \)

(2) If \( n \mid (a-b) \) then \( n \mid (b-a) \).

(3) If \( n \mid (a-b) \) and \( n \mid (b-c) \), then

\[ n \mid (a-b) + (b-c) = a-c \]

Proof of 2.2) (1) We have \( n \mid (a-b) \), \( n \mid (c-d) \).

\[ (a+c)-(b+d) = (a-b) + (c-d) \]

Then \( n \mid (a-b) + (c-d) \). Thus

\[ n \mid (a+c)-(b+d) \]

(2) From \( n \mid (a-b) \), \( n \mid (c-d) \), we see that

\[ ac-bd = ac+0-bd \]

\[ = ac-bc+bc-bd \]

\[ = (a-b)c+b(c-d) \]

Thus, \( n \mid ac-bd \).
Definition: Let \( a, n \) be integers with \( n > 0 \).

The congruence class of \( a \) modulo \( n \) (denoted \([a]\)) is the set of all integers that are congruent to \( a \) modulo \( n \), that is \([a] = \{ b \mid b \in \mathbb{Z} \text{ and } b \equiv a \pmod{n} \}\).

Note: \([a] = \{ b \mid b \equiv a \pmod{n} \}\)  
= \{ b \mid b = a + kn \text{ with } k \in \mathbb{Z} \}\)  
= \{ a + kn \mid k \in \mathbb{Z} \}\)  
= \( a + n\mathbb{Z} \)

\( \text{ex} \) \([9] = \{ 9 + 5k \mid k \in \mathbb{Z} \} = \{ 4 + 5k \mid k \in \mathbb{Z} \} = [4] \)

Theorem 2.3 \( a \equiv c \pmod{n} \) if and only if \([a] = [c] \)

Proof in p29.

Corollary 2.4 Two congruence classes modulo \( n \) are either disjoint or identical.

Proof in p29.

Corollary 2.5 Let \( n > 1 \) be an integer and consider congruence modulo \( n \).

1. If \( a \) is any integer and \( r \) is the remainder when \( a \) is divided by \( n \), then \([a] = [r] \)

2. There are exactly \( n \) distinct congruence classes, namely, \([0], [1], \ldots, [n-1] \).
Proof. (1) Let \(a \in \mathbb{Z}\). By the Division Algorithm, 
\[ a = nq + r, \text{ with } 0 \leq r < n. \]
Thus, 
\[ a - r = qn, \text{ so that } a \equiv r \pmod{n}. \]
By Theorem 2.3, \([a] = [r]\).

(2) If \([a]\) is any congruence class, then (1) shows that \([a] = [r]\) with \(0 \leq r < n\).
Hence \([a]\) must be one of \([0], [1], \ldots, [n-1]\).

To complete the proof, we must show that these \(n\) classes are all distinct. To do this, we first show that no two of \(0, 1, 2, \ldots, n-1\) are congruent modulo \(n\). Suppose \(s\) and \(t\) are distinct integers in \(0, 1, 2, \ldots, n-1\).

We can assume \(0 \leq s < t < n\). Then \(0 < t - s < n\). Hence \(n\) does not divide \(t - s\), which means \(t \not\equiv s \pmod{n}\). Therefore, by Theorem 2.3, the classes \([0], [1], \ldots, [n-1]\) are all distinct.
ex). Prove that if \( x \) is an integer, then \( x^2 \equiv 0 \pmod{4} \) or \( 1 \pmod{4} \).

ex). Prove that if \( x \equiv 1 \pmod{2} \), \( x \equiv 2 \pmod{3} \), then \( x \equiv 5 \pmod{6} \).

cf. Chinese Remainder Theorem (Sec. 14.1)

Consider congruence classes modulo \( n > 0 \)

Definition:
\[
[a] + [c] = [a + c] \\
[a] \cdot [c] = [ac]
\]

in \( \mathbb{Z}_n = \{ [0], [1], \ldots, [n-1] \} \)

ex). In \( \mathbb{Z}_5 \), \([1] + [4] = [0]\)

\([2] \cdot [3] = [6] = [1]\)

| \(\oplus\) | \([0]\) | \([1]\) | \([2]\) | \([3]\) | \([4]\) |
|---|---|---|---|---|
| \([0]\) | \([0]\) | \([1]\) | \([2]\) | \([3]\) | \([4]\) |
| \([1]\) | \([1]\) | \([2]\) | \([3]\) | \([4]\) | \([0]\) |
| \([2]\) | \([2]\) | \([3]\) | \([4]\) | \([0]\) | \([1]\) |
| \([3]\) | \([3]\) | \([4]\) | \([0]\) | \([1]\) | \([2]\) |
| \([4]\) | \([4]\) | \([0]\) | \([1]\) | \([2]\) | \([3]\) |

| \(\otimes\) | \([0]\) | \([1]\) | \([2]\) | \([3]\) | \([4]\) |
|---|---|---|---|---|
| \([0]\) | \([0]\) | \([0]\) | \([0]\) | \([0]\) | \([0]\) |
| \([1]\) | \([0]\) | \([1]\) | \([2]\) | \([3]\) | \([4]\) |
| \([2]\) | \([0]\) | \([2]\) | \([4]\) | \([1]\) | \([3]\) |
| \([3]\) | \([0]\) | \([3]\) | \([1]\) | \([4]\) | \([2]\) |
| \([4]\) | \([0]\) | \([4]\) | \([3]\) | \([2]\) | \([1]\) |
properties of \( \mathbb{Z} \)

1. If \( a, b \in \mathbb{Z} \) then \( a + b \in \mathbb{Z} \)
   \([\text{Closure for } +]\)

2. \( a + (b + c) = (a + b) + c \)
   \([\text{Associative for } +]\)

3. \( a + b = b + a \)
   \([\text{Commutative for } +]\)

4. \( a + 0 = 0 + a = a \)
   \([\text{Additive identity}]\)

5. For each \( a \in \mathbb{Z} \), the equation \( a + x = 0 \) has a solution \( x \in \mathbb{Z} \).

6. If \( a, b \in \mathbb{Z} \), then \( ab \in \mathbb{Z} \).
   \([\text{Closure for } \cdot]\)

7. \( a(bc) = (ab)c \)
   \([\text{Associative for } \cdot]\)

8. \( a(b + c) = ab + ac \)
   \([\text{Distributive laws}]\)

\((a + b)c = ac + bc\)
9. $ab = ba$ [commutative \(*\)]
10. $a \cdot 1 = 1 \cdot a = a$ [multiplicative identity]

11. If $ab = 0$, then $a = 0$ or $b = 0$  
    [Integral Domain]

$p$ is not necessarily $\neq 11$.


ex) In $\mathbb{Z}_5$, $[a] \circ [b] = [0]$ implies $[a] = [0]$ or $[b] = [0]$.
    (See the table)

Exponents $[a] \circ \ldots \circ [a] = [a]^k = [a^k]$

k times

Multiplicative Inverse in \( \mathbb{Z}_n \)

If \( [a] \circ [x] = [1] \)
and \( [x] \circ [a] = [1] \), then we say that \([a]\) has an inverse in \( \mathbb{Z}_n \) (multiplicative).

and \([x]\) is the inverse of \([a]\) in \( \mathbb{Z}_n \).

In \( \mathbb{Z}_n \), if \( a \neq \pm 1 \), \( a \) does not have a multiplicative inverse.

In \( \mathbb{Z}_n \), some elements have inverses.

\( \text{ex}) \) In \( \mathbb{Z}_5 \), \([1],[2],[3],[4]\) have multiplicative inverses.

\( \text{ex}) \) In \( \mathbb{Z}_6 \), \([2],[3],[4]\) do not have multiplicative inverse, but \([1],[5]\) have multiplicative inverse.

We will get back to this with complete characterization of existence of multiplicative inv.
Primes and Unique Factorization

Definition: An integer $p$ is said to be prime if $p \neq 0, \pm 1$, and the only divisors of $p$ are $\pm 1$ and $\pm p$.

Example: $2, 3, -5, 7, -11, 13, -17$ are prime, but $15$ is not. $4567$ is prime.

Remark: 1. $p$ is prime if and only if $-p$ is prime.

2. If $p$ and $q$ are prime and $p \mid q$, then $p = \pm q$.

Theorem 1.5: Let $p$ be an integer with $p \neq 0, \pm 1$. Then $p$ is prime if and only if $p$ has the property "Whenever $p \mid bc$, then $p \mid b$ or $p \mid c$.”

\[ \Rightarrow \] Let $p$ be a prime, consider $bc$ with $p \mid bc$. We prove that $p \mid b$ or $p \mid c$.

Consider $(b, p)$. This is a divisor of $p$. Since $p$ is prime, $(b, p) = 1$ or $p$. If $(b, p) = 1$, then by Thm 1.4, $p \mid c$.

If $(b, p) = p$, then $p \mid b$. 
Exercise 14. (HW1)

Corollary 1.6,

If \( p \) is a prime and \( p \mid a_1 a_2 \cdots a_n \),
then \( p \) divides at least one of the \( a_i \).

\( \text{or} \)

We know that \( 3 \mid 6 \cdot 20 = 120 \)
we have \( 3 \mid 6 \) or \( 3 \mid 20 \) since
3 is a prime. Obviously \( 3 \mid 6 \) is true.

Theorem 1.7

Every integer \( n \neq 0, \pm 1 \) is a product
of primes.

\( \text{proof} \)
We need proving this only when \( n > 1 \),
Let \( S \) be the set of all integers \( > 1 \)
that are not a product of primes.

We prove that \( S = \emptyset \).

Assume \( S \neq \emptyset \), then by WLOG,
there is the least element \( m \in S \).
m itself is not a prime, so
\[ m = ab \] for some \( a, b \) with
\[ 1 < a < m, \quad 1 < b < m. \]

Then \( a \not\in S \) (smaller than least element
of \( S \), so does not
belong to \( S \)),
and \( b \not\in S \).

Thus \( a \) is a product of \( r \) primes
\[ a = p_1 \cdots p_r \] and
\( b \) is also a product of \( r \) primes.
\[ b = q_1 \cdots q_s. \]

Then \( m = ab = p_1 \cdots p_r q_1 \cdots q_s \)
is a product of \( r \) primes, so that \( m \not\in S \).

We have a contradiction.

Therefore \( S = \emptyset \).
\[ 45 = 3 \cdot 3 \cdot 5 \]
\[ = -3 \cdot -3 \cdot 5 \]
\[ = 3 \cdot 3 \cdot -5 \]  

(Unique Factorization)

Theorem 1.8. (The Fundamental Theorem of Arithmetic.) Every integer \( n \neq 0, \pm 1 \) is a product of primes. This prime factorization is unique in the following sense: if

\[ n = p_1 \cdots p_r \quad \text{and} \quad n = q_1 \cdots q_s \]

with each \( p_i, q_j \) prime, then \( r = s \) and \( p_1 = \pm q_1, \ldots, p_r = \pm q_r \) after reordering and relabeling \( q \)'s.

Proof. Suppose \( n \) has two factorizations

\[ n = p_1 \cdots p_r \quad \text{and} \quad n = q_1 \cdots q_s \]

Then \( p_1 \mid q_1 \cdots q_s \). By Cor 1.6, \( p_1 \) must divide one of \( q_s \).

After reordering and relabeling, we may assume that \( p_1 = \pm q_1 \).
Consequently, 
\[ \pm q_1, P_2 \ldots P_r = q_1 \ldots q_s \]

Dividing both sides by \( q_1 \) shows that 
\[ P_2 (\pm P_3 \ldots P_r) = q_2 \ldots q_s \]

By Cor 1.6, \( P_2 \) must divide one of \( q_j \) \((2 \leq j \leq s)\); as before, we may assume that \( P_2 \mid q_2 \). Hence \( P_2 = \pm q_2 \)
\[ \pm q_2, P_3 \ldots P_r = q_2 \ldots q_s \]

Dividing both sides by \( q_2 \) shows that 
\[ P_3 (\pm P_4 \ldots P_r) = q_3 \ldots q_s \]

We continue in this manner, repeatedly using Cor 1.6 and eliminating one prime on each side at every step.

If \( r > s \), this process will lead to 
\[ \pm P_{s+1} \ldots P_r = 1 \quad (\text{when } r > s) \]

This equation says that \( P_r = \pm 1 \). This is a contradiction. Thus, we must have \( r = s \), as desired.
Corollary 1.9.

Every integer \( n > 1 \) can be written as

\[
  n = p_1 \cdots p_r, \quad \text{where} \quad p_i : \text{prime}
\]

\[
  p_1 \leq \cdots \leq p_r.
\]

Or, this is preferred.

\[
  n = p_1^{e_1} \cdots p_s^{e_s}
\]

where \( p_i : \text{prime}, \quad e_i \geq 1 \)

\[
  p_1 < \cdots < p_s.
\]

\( \text{e.g.} \)

\[
  45 = 3 \cdot 3 \cdot 5
  = 3^2 \cdot 5^1
  = 3^2 \cdot 5
\]

\[
  68 = 2 \cdot 2 \cdot 17
  = 2^2 \cdot 17^1
  = 2^2 \cdot 17
\]

\[
  60 = 2 \cdot 2 \cdot 3 \cdot 5
  = 2^2 \cdot 3^1 \cdot 5^1
\]
Primality Testing (p21)

Let \( n \geq 1 \). If \( n \) has no positive prime factor less than or equal to \( \sqrt{n} \), then \( n \) is prime.

Ex. To show 137 is prime, try dividing \( n \) by the integers \( \leq \sqrt{137} = 11.7 \).

So, divide 137 by 2, 3, 5, 7, 11.

You can verify that they do not divide it.

Thus, 137 is a prime.

Proof. The proof is by contradiction. Suppose that \( n \) is not prime. Then \( n \) has at least two positive primes \( p_1, p_2 \) dividing \( n \).

Then \( n = p_1 p_2 k \) for some positive integer \( k \). By hypothesis, \( p_1 > \sqrt{n}, p_2 > \sqrt{n} \).

Which says \( n = p_1 p_2 k > \sqrt{n} \cdot \sqrt{n} k = nk \), so \( n > n \). Since the assumption that \( n \) is not prime led to a contradiction, \( n \) must be prime.
The Structure of \( \mathbb{Z}_p \) when \( p \) is Prime.

Theorem 2.8.

If \( p > 1 \) is an integer, then TFAE

1. \( p \) is prime
2. For any \( a \neq 0 \) in \( \mathbb{Z}_p \), the equation \( ax = 1 \) has a solution in \( \mathbb{Z}_p \)
3. Whenever \( bc = 0 \) in \( \mathbb{Z}_p \), then \( b = 0 \) or \( c = 0 \).

Proof. (1) \( \Rightarrow \) (2) Suppose \( p \) is prime and \( a \neq 0 \) in \( \mathbb{Z}_p \). Then in \( \mathbb{Z} \), \( a \neq 0 \) (mod \( p \)). Hence \( p \mid a \) by definition of congruence. Since \( (a,p) \mid a \) and \( p \mid a \), we must have \( (a,p) = 1 \). By Theorem 1.2, \( au + pv = 1 \) for some integers \( u, v \). Hence \( au - 1 = p(-v) \) so that \( au \equiv 1 \) (mod \( p \)). Hence \( au = 1 \) in \( \mathbb{Z}_p \). Then \( x = u \) in \( \mathbb{Z}_p \) is a solution of \( ax = 1 \).
(2) \Rightarrow (3) Suppose \( ab = 0 \) in \( \mathbb{Z}_p \). If \( a = 0 \), there is nothing to prove. If \( a \neq 0 \), then by (2) there exists \( u \in \mathbb{Z}_p \) such that \( au = 1 \). Then

\[
0 = u \cdot 0 = u \cdot (ab) = (ua) \cdot b = (au) \cdot b = 1 \cdot b = b.
\]

Therefore we have \( a = 0 \) or \( b = 0 \).

(3) \Rightarrow (1) "If \( bc = 0 \) in \( \mathbb{Z}_p \) then \( b = 0 \) or \( c = 0 \)."

This property is precisely,

"If \( p \mid bc \), then \( p \mid b \) or \( p \mid c \)."

This is the property in Theorem 1.5.

By Theorem 1.5, \( p \) is a prime.
Structure of \( \mathbb{Z}_n \). (Theorem 2.9)

Let \( a, n \) be integers with \( n > 1 \). Then \( ax \equiv 1 \pmod{n} \) has a solution in \( \mathbb{Z}_n \) if and only if \((a,n) = 1\) in \( \mathbb{Z} \).

**Proof.** Recall that TFAE

1. There exist integers \( u, v \) such that \( au + nv = 1 \).
2. \((a,n) = 1\).

We need to check if the existence of \( x \) in the equation \( ax \equiv 1 \pmod{n} \) is equivalent to 1. above.

Indeed this is clear; If 1 is true then \( au - 1 = n(-v) \), \( au \equiv 1 \pmod{n} \) so, \( ax = 1 \) has a solution \( x = u \) in \( \mathbb{Z}_n \).

If \( ax = 1 \) has a solution in \( \mathbb{Z}_n \), then there is an integer \( k \) such that

\[ ax - 1 = nk \quad (\text{since } ax \equiv 1 \pmod{n}) \]

Then \( ax + n(-k) = 1 \). With \( x, k \) integers.
Units and Zero Divisors

Definition (Units)

If the equation $ax = 1$ in $\mathbb{Z}_n$ has a solution, then we say that $a$ is a unit in $\mathbb{Z}_n$.

Definition (Zero Divisors)

If $a \neq 0$, $b \neq 0$ in $\mathbb{Z}_n$, but $ab = 0$ in $\mathbb{Z}_n$, then we say that, $a$, $b$ are zero divisors in $\mathbb{Z}_n$.

ex) $2 \cdot 3 \equiv 0 \pmod{6}$, 2, 3 are zero divisors in $\mathbb{Z}_6$.

1, 5 are units in $\mathbb{Z}_6$.

ex) $2 \cdot 2 \equiv 0 \pmod{4}$ so 2 is a zero divisor in $\mathbb{Z}_4$.

1, 3 are units in $\mathbb{Z}_4$.

ex) In $\mathbb{Z}_p$ ($p$: prime), any nonzero element is a unit.
Notation) \((\mathbb{Z}_n)^*\) or \(\mathbb{Z}_n^*\)

These are the group of units in \(\mathbb{Z}_n\).

In fact, by Theorem 2.9,

\[ \mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n | (a, n) = 1 \} \]

Euler's Totient Function.

The function \(\phi: \mathbb{N} \to \mathbb{Z}\) is defined by

\[ \phi(n) = |\mathbb{Z}_n^*|\] (The number of units in \(\mathbb{Z}_n^*\))

Then this function has the property,

\[ \phi(n) = n \cdot \prod_{\text{all prime divisors of } n} \left(1 - \frac{1}{p}\right) \] (The product is over all prime divisors of \(n\))

In particular, \(\phi(p) = p - 1\) for primes \(p\),

\[ \phi(p^n) = p^n - p^{n-1} \] if \(n \geq 1\), and \(p\) is prime.

Moreover, \(\phi(mn) = \phi(m) \phi(n)\) if \((m, n) = 1\).
2. If \( ax = b \) has a solution in \( \mathbb{Z}_n \),
    (not necessarily unique)
    then \( (a, n) \mid b \),  \( \text{(Exercise 12, in HW2)} \)
    Conversely, if \( (a, n) \mid b \), then \( ax = b \)
    has a solution in \( \mathbb{Z}_n \) \( \text{(Exercise 13, in HW2)} \)

3. If \( d = (a, n) \mid b \), then \( ax = b \) has
    \( d \) distinct solutions in \( \mathbb{Z}_n \) \( \text{(Exercise 14, in HW2)} \)

ex) The equation \( 4x = 3 \) in \( \mathbb{Z}_6 \)
    does not have solution in \( \mathbb{Z}_6 \) since
    \( (4, 6) = 2 \mid 3 \).

ex) The equation \( 4x = 2 \) in \( \mathbb{Z}_6 \)
    has 2 solutions in \( \mathbb{Z}_6 \) since
    \( (4, 6) = 2 \mid 2 \).

What are the solutions? \( x = 2, 5 \) in \( \mathbb{Z}_6 \).
The equation $ax = b$ in $\mathbb{Z}_n$ (Exercise 11-14)

1. If $a$ is a unit, then the equation $ax = b$ has a solution in $\mathbb{Z}_n$, and the solution is unique. (Exercise 11) 

proof) Since $a$ is a unit, there is an integer $u$ such that $au = 1 \pmod{n}$.

Then $a \cdot ax \equiv b \pmod{n}$ gives 

$$u(ax) \equiv ub \pmod{n}$$

$$(ua) x \equiv ub \pmod{n}$$

$$x \equiv ub \pmod{n}$$

This shows the existence in $\mathbb{Z}_n$.

To prove uniqueness, let $x_1$ and $x_2$ be two solutions to $ax = b$ in $\mathbb{Z}_n$.

Then $ax_1 \equiv ax_2 \pmod{n}$

This gives $U(ax_1) \equiv U(ax_2) \pmod{n}$

$$(ua)x_1 \equiv (ua)x_2 \pmod{n}$$

$$x_1 \equiv x_2 \pmod{n}$$

Therefore $x_1 = x_2$ in $\mathbb{Z}_n$, which shows the uniqueness.
Rings

A ring is a nonempty set \( R \) equipped with two operations (usually written as \( +, \cdot \)) that satisfy the following axioms. For all \( a, b, c \in R \):

1. If \( a \in R \), \( b \in R \), then \( ab \in R \) [Closure for \( \cdot \)]
2. \( a + (b + c) = (a + b) + c \) [Associative \( + \)]
3. \( a + b = b + a \) [Commutative \( + \)]
4. There is an element \( 0_R \in R \) such that \( a + 0_R = 0_R + a = a \) for every \( a \in R \) [Additive identity]
5. For each \( a \in R \), the equation \( a + x = 0_R \) has a solution in \( R \) [Additive inverse]
6. If \( a \in R \) and \( b \in R \), then \( ab \in R \) [Closure for \( \cdot \)]
7. \( a(bc) = (ab)c \) [Associative \( \cdot \)]
8. \( a(b + c) = ab + ac \) \( (ab)c = ac + bc \) [Distributive Laws]
Definition (Commutative Ring)

A commutative ring is a ring \( R \) that satisfies this axiom

9. \( ab = ba \) for all \( a, b \in R \)

[Commutative \( \cdot \)]

Definition (Ring with identity)

If \( 1 \) \( \in R \) satisfies

10. \( a1 = 1a = a \) for all \( a \in R \)

[Multiplicative Identity]

Then \( R \) is said to be a ring with identity.

(cf) Some books call that a "unital ring".

Examples

1. \( \mathbb{Z}, \mathbb{R}, \mathbb{Q} \) are commutative rings with identity.

2. \( \mathbb{Z}_n \) is a commutative ring with identity.

3. \( 2\mathbb{Z} \) (the set of even integers) is a commutative ring, but not with identity.

4. The set of odd integers is not a ring (with usual \( +, \cdot \)).
Units and Zero Divisors (\(\mathbb{Z}_n\) replaced by \(\mathbb{R}\)) with some changes

Definition (Units)
If the equation \(ax = 1\) in \(\mathbb{R}\) has a solution \(x = a^{-1}\), then we say that \(a\) is a unit in \(\mathbb{R}\).

Definition (Zero Divisors)
If \(a \neq 0\) and \(b \neq 0\), but \(ab = 0\) in \(\mathbb{R}\), then we say that \(a, b\) are zero divisors in \(\mathbb{R}\).

ex) The units in \(\mathbb{Z}\) : \(\pm 1\).

ex) There are no zero divisors in \(\mathbb{Z}\).

ex) Let \(M_2(\mathbb{Z})\) be the set of \(2 \times 2\) matrices over \(\mathbb{Z}\), with usual addition and matrix multiplication. To be included in HW2

1. Verify that \(M_2(\mathbb{Z})\) is a ring.
2. Find \(A, B \in M_2(\mathbb{Z})\) with \(AB \neq BA\) (other than Example 4.47).
   (\(M_2(\mathbb{Z})\) is not a commutative ring)
3. Show that there are infinitely many units.
4. Find a zero divisor in \(M_2(\mathbb{Z})\).
   (other than Example 4.48)
Definition (Integral Domain)

A commutative ring $R$ with identity $1_R \neq 0_R$ that satisfies

11. Whenever $a, b \in R$ and $ab = 0_R$, then $a = 0_R$ or $b = 0_R$. [Cancellation property]

ex) $\mathbb{Z}$, $\mathbb{Z}_p$ ($p$: prime).

Definition (Field)

A field is commutative ring $R$ with identity $1_R \neq 0_R$ that satisfies

12. For each $a \neq 0_R$ in $R$, the equation $ax = xa = 1_R$ has a solution in $R$. [Every nonzero element is a unit.]

ex) $\mathbb{R}$, $\mathbb{Z}_p$, $\mathbb{Q}$, not $\mathbb{Z}$.

ex) The set $C = \{a + bi \mid a, b \in \mathbb{R}\}$ with $i^2 = -1$.

Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Then $\mathbb{Z}[i] \subseteq C$, and $C$ is a field, while $\mathbb{Z}[i]$ is not. $\mathbb{Z}[i]$ is an integral domain.
Properties

1 - 8 : Ring
1 - 9 : Commutative ring
1 - 10 : Commutative ring with identity
1 - 11 : Integral Domain
1 - 12 : Field.
Ring

\( M_2(\mathbb{Z}) \)

Commutative ring

\[ \mathbb{Z}_6 \]

Integral domain

Field

\[ \{0, 2\} \text{ of } \mathbb{Z}_4 \]

with identity

without identity

Optional

Ring with identity

\( \mathbb{Z} \times \mathbb{Z} \)

Integral domain

\[ \mathbb{Z} \]

Property 12

\[ \mathbb{Q}, \mathbb{R}, ... \]

\( M_2(\mathbb{Z}) \)

Commutative

Non-commutative

11-1: Real quaternion
This is a division ring. (Properties 1-8, 10, 12)

See Ex 43 in p58.
Cartesian Product of two rings \( R, S \).
Let \( R, S \) be rings, define
\[
+ : (a, b) + (c, d) = (a+c, b+d) \\
\cdot : (a, b) \cdot (c, d) = (a \cdot c, b \cdot d)
\]
Then \( R \times S \) is a ring under the above +, \( \cdot \).
Note that + and \( \cdot \) are componentwise.

ex) Let \( R = \mathbb{Z} \), \( S = \mathbb{Z} \), and \( T = R \times S \).

\[
(3, 5) + (4, 9) = (1, 14) \\
(3, 5) \cdot (4, 9) = (0, 45)
\]

Is this an integral domain? No.
\[
(3, 1) \cdot (2, 0) = (0, 0)
\]
This is a ring with identity, the identity is \((1, 1)\).

\( \mathbb{Z} \times \mathbb{Z} \) is commutative ring with identity but not an integral domain.
\[
(1, 0) \cdot (0, 1) = (0, 0)
\]
Subrings.

Definition) Let $R$ be a ring, and $S \subseteq R$.
If $S$ forms a ring under the $+$ and $\cdot$ in $R$, then $S$ is called a subring of $R$.

ex) $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring of $\mathbb{Q}$.
$\mathbb{Q} \subseteq \mathbb{R}$ is a subfield of $\mathbb{R}$.
$\mathbb{R} \subseteq \mathbb{C}$ is a subfield of $\mathbb{C}$.
ex) $M_2(\mathbb{Z})$ is a subring of $M_2(\mathbb{R})$.

Theorem 3.2

Let $R$ be a ring, and $S \subseteq R$.

If
i) $S$ is closed under $+$
ii) $S$ is closed under $\cdot$
iii) $0_R \in S$
iv) If $a \in S$, then the solution of the equation $a + x = 0_R$ is in $S$.

Then $S$ is a subring of $R$.

Proof: Axioms 2, 3, 7, 8 hold for all elements of $R$. Axioms 1, 4, 5, 6 hold by i ~ iv).
Ex) \( \mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \) is a subring of \( \mathbb{R} \).

Ex) \( S = \langle 0, 2 \rangle \) of \( \mathbb{Z}_4 \). Check that \( S \) is a subring of \( \mathbb{Z}_4 \).

\( S \) is a commutative ring without identity, finite.

Ex) Ex 10 in p 55.

Is \( S = \{(a, b) \mid a + b = 0\} \) a subring of \( \mathbb{Z} \times \mathbb{Z} \)?

No. \((1, -1) \cdot (1, -1) = (1, 1) \notin S,\)

Arithmetic in Rings

Theorem 3.3.

For any element \( a \in \mathbb{R} \), the equation \( a + x = 0 \) has a unique solution, \( x = -a \).

Proof. By Axiom 5, existence is guaranteed.

To prove uniqueness, let \( a + x_1 = 0 + x_2 = 0 \).

We have \((a + a) + x_1 = (x_1 + a) + x_2 \) (Associative +)

\( 0 + x_1 = 0 + x_2 \) (Commutative +)

\( x_1 = x_2 \).
We write the unique solution of $a + x = 0_R$ as 
"$-a$".

**Theorem 3.14.**

If $a + b = a + c$ in a ring $R$, then $b = c$.

**Proof.** Add $-a$ both sides.

$\begin{align*}
-a + (a + b) &= -a + (a + c) \\
(-a + a) + b &= (-a + a) + c \\
0 + b &= 0 + c \\
b &= c.
\end{align*}$

**Notation.**

$a^n = a \cdot a \cdots \cdot a$

\[\vdash_{n \text{ times.}}\]

$na = a + a + \cdots + a$

\[\vdash_{n \text{ times.}}\]

It is easy to verify that $a^m a^n = a^{m+n}$ for positive integers $m, n$. Also $(a^m)^n = a^{mn}$.

**Warning.** $(ab)^n = a^n b^n$ is not true in general. When is it true?
Theorem 3.5

For any elements \( a \) and \( b \) of a ring \( R \),

1) \( a \cdot 0_R = 0_R = 0_R \cdot a \)

2) \( a(-b) = -ab \), \((-a)b = -ab\)

3) \(-(-a) = a\)

4) \(-a + b = (-a) + (-b)\)

5) \(-a - b = -a + b\)

6) \((-a)(-b) = ab\)

If \( R \) has an identity, then

7) \((-1_R) a = -a\)

Proof: P 61-62

\( \alpha \) Let \( R \) be a ring satisfying

\( a^2 = a \) for all \( a \in R \).

Prove that \( 2a = 0 \) for all \( a \in R \).

Solution: \( a = a^2 = (-a)^2 = -a \)

So, \( a = -a \), equivalently \( 2a = 0 \).
\[(a+b)^2 = a^2 + ab + ba + b^2\]

**proof:**
\[
\begin{align*}
(a+b)(a+b) & = a(a+b) + b(a+b) \\
& = a^2 + ab + ba + b^2
\end{align*}
\]

\[(a+b)^3 = a^3 + a^2b + ab^2 + ba^2 + b^2a + b^3
\]

If \( R \) is commutative, these become

\[(a+b)^2 = a^2 + 2ab + b^2
\]

\[(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3
\]
Theorem 3.6 (Criterion for Subring - Simplified)

Let $S$ be a nonempty subset of a ring $R$ such that

1. $S$ is closed under subtraction
   (i.e., if $a, b \in S$, then $a - b \in S$)
2. $S$ is closed under multiplication

Then $S$ is a subring of $R$.

Proof. Recall i - iv from Theorem 3.2.

1. implies iii)
   since $c - c = 0 \in S$ for $c \in S$.
   implies i), iv)
   since $0 - b \in S$ for $b \in S$
   a - (-b) = a + b \in S

2. is the same as iii).

Therefore by Theorem 3.2, $S$ is a subring of $R$.

Ex) Ex#7 in p67. $R$: a ring, $S = \{n | n \in \mathbb{Z}^\ast\}$.

Then $S$ is a subring of $R$.

Proof. Let $a, b \in S$, then $a - b = k1_R$ for some integer $k$, thus $a - b \in S$.

Also, $ab = l1_R$ for $l \in \mathbb{Z}$. By Theorem 3.6 $S$ is a subring of $R$. 
Theorem 3.9

Every finite integral domain is a field.

Proof) Let \( R \) be a finite integral domain. We only need to show that for each \( a \in R \), the equation \( ax = 1_R \) has a solution. Let \( a_1, \ldots, a_n \) be the distinct elements of \( R \) and suppose \( a_1 \neq 0_R \). To show that \( a_1 x = 1_R \) has a solution, consider

\[
S = \{ a_1 a_1, a_1 a_2, \ldots, a_1 a_n \}
\]

By cancellation property, we have

\[
a_1 a_i = a_1 a_j \quad \text{if} \quad i \neq j.
\]

Therefore the set \( S \) is \( R \) since \( R \) is finite. Thus, some element in \( S \) must be \( 1_R \), this shows the existence of solution in \( a_1 x = 1_R \).
Homomorphisms.

Definition Let $R, S$ be rings. A function $f: R \rightarrow S$ is said to be a homomorphism if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Ex. $g: IR \rightarrow M(IR)$ given by

$$g(r) = \begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix}$$

is a homomorphism.

For any $r, s \in IR$,

$$g(r) + g(s) = \begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ -s & s \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -r - s & r + s \end{pmatrix} = g(r + s)$$

and

$$g(r)g(s) = \begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix}\begin{pmatrix} 0 & 0 \\ -s & s \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -rs & rs \end{pmatrix} = g(rs).$$

The homomorphism $g$ is injective but not surjective.
Let \( R, S \) be rings.

a) \( f: R \times S \to R \) given by \( f((r,s)) = r \) is a surjective homomorphism.

Proof: \( f((r_1+r_2, s_1+s_2)) = r_1 + r_2 \) (by definition)

\( = f((r_1,s_1)) + f((r_2,s_2)) \)

for any \((r_1, s_1), (r_2, s_2) \in R \times S.

\( f(r_1 r_2, s_1 s_2) = r_1 r_2 \) (by definition)

\( = f((r_1,s_1)) \cdot f((r_2,s_2)) \)

Thus, \( f \) is a homomorphism.

To prove that \( f \) is surjective let \( r \in R \) (any element in \( R \)). Take \( 0 \in S \).

We have \( f((r, 0)) = r \).

Isomorphisms

Definition) Homomorphism, and a bijection

Ex) \( f: \mathbb{C} \rightarrow \mathbb{C} \) complex conjugation.

\[
f((a+bi) + (c+di)) = f(a+c + (b+d)i)
= a+c - (b+d)i
= a-bi + c-di
= f(a+bi) + f(c+di)
\]

\[
f((a+bi)(c+di)) = f(ac-bd + (bc+ad)i)
= ac-bd - (bc+ad)i
= c(a-bi) - d;(a-bi)
= (c-di)(a-bi)
= f(a+bi) f(c+di)
\]

For any \( atbi \in \mathbb{C} \), \( f(a-bi) = atbi \)

so \( f \) is surjective,

To check if \( f \) is injective, check if \( atbi \neq ctdi \Rightarrow f(atbi) \neq f(c+di) \)

If \( f(atbi) = f(c+di) \), then \( a = c \) and \( -b = -d \).

Then \( a = c \) and \( b = d \), this shows \( atbi = ctdi \).
Ex.) Ex. 2 in p. 73.

The field \( k \) of all \( 2 \times 2 \) matrices of the form \( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \) where \( a, b \in \mathbb{R} \).

Then \( k \) is isomorphic to \( \mathbb{C} \).

Define \( f: k \to \mathbb{C} \) by

\[
f \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi
\]

It is easy to check that \( f \) is bijective. (see p. 73)

To show that \( f \) is homomorphism

\[
f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}) = f\left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) + f\left( \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right)
\]

\[
= a + c + (b + d)i
\]

\[
= a + bi + c + di
\]

\[
= f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) + f(\begin{pmatrix} c & d \\ -d & c \end{pmatrix})
\]

\[
f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix})(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}) = f\left( \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & bd + ac \end{pmatrix} \right)
\]

\[
= ac - bd + (ad + bc)i
\]

\[
= (a + bi)(c + di)
\]
Ex 5. \( z : R \rightarrow S \) \( z(r) = 0 \) for all \( r \in R \),
This is called the \textbf{zero map}.
This is a \textbf{homomorphism}.

Ex 6. \( f : \mathbb{Z} \rightarrow \mathbb{Z}_6 \) given by \( f(a) = [a] \)
is a \textbf{surjective homomorphism}.

\textbf{Theorem 3.10.} Let \( f : R \rightarrow S \) be homomorphism of rings. Then

1) \( f(0_R) = 0_S \)
2) \( f(-a) = -f(a) \) for all \( a \in R \)
3) \( f(a+b) = f(a) + f(b) \) for all \( a, b \in R \)

If \( R \) is a ring with identity and \( f \) is surjective, then

4) \( S \) is a ring with identity \( f(1_R) \)
5) Whenever \( u \) is a unit in \( R \), then \( f(u) \) is a unit in \( S \) and \( f(u^{-1}) = f(u)^{-1} \)

\textit{Proof:} p.777
Definition (Equivalence Relation, Equivalence Class)

Let \( S \) be a set. An equivalence relation is a relation \( \sim \) on \( S \) such that for all \( a, b, c \in S \),

1. \( a \sim a \) (Reflexivity)
2. If \( a \sim b \) then \( b \sim a \) (Symmetry)
3. If \( a \sim b \) and \( b \sim c \) then \( a \sim c \) (Transitivity)

The equivalence class of \( a \) under \( \sim \), denoted by \([a]\)

\[ [a] = \{ b \in S \mid a \sim b \} \]

Properties

1. \([a] = [b]\) if and only if \( a \sim b \)
2. For any \( a, b \in S \), \([a] \neq [b]\) or \([a] \cap [b] = \emptyset\)
3. Equivalence classes form a partition of \( S \).

\[ S = \cup \{ [a] \mid a \in S \} \]

\( ^\dagger \)

disjoint union

**Ex:** Let \( n \geq 1 \). The relation \( \equiv \) (mod \( n \)) is an equivalence relation on \( \mathbb{Z} \).
Proof of $p | \binom{p}{k}$ for $0 < k < p$

1. (Algebraic)

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$$

and this is an integer (number of ways to choose $k$ elements from a $p$-element set).

We know that $p | p!$, but $p \nmid k!$ and $p \nmid (p-k)!$ since $0 < k < p$. (*)

By the Fundamental Theorem of Arithmetic, the integer has a unique prime factorization

$$\binom{p}{k} = \prod_{i=1}^{k} p_i^{e_i}, \quad e_i \in \mathbb{Z}^+.$$

By (*), we see that one of the prime factor must be $p$, hence $p | \binom{p}{k}$. 
2. (Proof using equivalence relation)

Let \( N_k \) be a set of \( k \)-element subset of \( \{1, 2, \ldots, p\} \). We define a relation \( \sim \) on \( N_k \) by

\[
S \sim T \text{ if } T = S + d \pmod{p}
\]

for some \( d = 0, \ldots, p-1 \).

Then \( \sim \) is an equivalence relation on \( N_k \).

(Here \( A \equiv B \pmod{p} \) means \( A \) and \( B \) are identical as sets modulo \( p \).)

(1) \( \{2, 3\} \) of \( N_2 \) where \( p = 5 \)

and \( \{7, 13\} \) are identical modulo 5

In fact, 1. \( S \sim S \) since \( S \equiv S + 0 \pmod{p} \),

2. \( S \sim T \) implies \( T \sim S \) since

\[
T = S + d \pmod{p} \quad \text{implies}
\]

\[
S = T + p - d \pmod{p}
\]

\[
\equiv T + (-d) \pmod{p}
\]
3. $S - T$ and $T - U$ imply

$$T \equiv S + d_1 \pmod{p}$$

$$U \equiv T + d_2 \pmod{p}$$

and

$$U \equiv S + (d_1 + d_2) \pmod{p}$$

Since $\sim$ is an equivalence relation, the equivalence classes form a partition of $\mathbb{Z}_k$.

Now, we prove that any equivalence class has $p$ elements. Let $[S]$ be an equivalence class. Consider the following map:

$$f : \{0, 1, \ldots, p-1\} \rightarrow \mathbb{Z}_k$$

$$d \rightarrow S + d \pmod{p}$$

and if we prove that $f$ is injective. Then we prove the class $[S]$ has exactly $p$ elements.

To prove this, define $\Sigma S$ by the sum of all elements in $S$. 
If $S \sim T$, then $\Sigma S \equiv \Sigma T \pmod{p}$

Let $d \in \{0, 1, \ldots, p-1\}$ be satisfying

$$T \equiv S + d \pmod{p}$$

Then $\Sigma T \equiv \Sigma S + dk \pmod{p}$.

Then $0 \equiv dk \pmod{p}$ so that $p \mid dk$. Thus, $p \mid d$ or $p \mid k$.

However, $p \mid k$ is impossible ($0 \leq k < p$), we have $p \mid d$. This proves injectivity of the map $f$, and completes the proof.

Using the property of equivalence relation, we have a partition of $\mathcal{N}_k$ with each member of partition is equivalence class.

Let $\mathcal{N}_k = \bigcup_{j=1}^{s} [A_j]$, then

$$1_{\mathcal{N}_k} = \sum_{j=1}^{s} |[A_j]|, \quad \text{and} \quad |[A_j]| = p$$

for all $j = 1, \ldots, s$. Thus, $1_{\mathcal{N}_k} = ps$.

This proves $p \mid 1_{\mathcal{N}_k} = \binom{p}{k}$. 
Further equivalence class examples:

**Ex)** $\mathcal{N} = \mathbb{N} \times \mathbb{N},$

$$(a, b) \sim (c, d) \text{ if } a + d = b + c$$

Explain why the equivalence classes can represent an "integer".

**Ex)** $\mathcal{N} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$

$$(a, b) \sim (c, d) \text{ if } ad = bc$$

Explain why the equivalence class can represent a "rational number".

**Ex)** Let $f$ be a ring homomorphism on two rings $R, S. \quad (f : R \to S)$

Define for $a, b \in R$, $a \sim b$ by $f(a) = f(b)$. Then $\sim$ is an equivalence relation.

(Reflexivity) For $a \in R$,

we have $f(a) = f(a)$ in $S$.

(Symmetry) For $a, b \in R$, let $a \sim b$, so $f(a) = f(b)$.

Then $f(b) = f(a)$. 

(Transitivity) Let \( a, b, c \in R \), \( a \equiv b \) and \( b \equiv c \). So that \( f(a) = f(b) \), and \( f(b) = f(c) \). Then \( f(a) = f(c) \), so \( a \equiv c \).

Remark: \( f \) does not have to be a ring homomorphism. This relation is an equivalence relation for sets \( R, S \) and a function \( f: R \to S \).

In this ring homomorphism case, we call \( [0] \) the kernel of \( f \). In fact,

\[
[0] = \{ b \in R \mid f(0) = f(b) \}.
\]

Since \( f(0) = 0 \), we have

\[
[0] = \{ b \in R \mid f(b) = 0 \}.
\]

ex) Find \( \text{Ker } f \) for \( f: \mathbb{Z} \to \mathbb{Z}_5 \)
given by \( f(x) = [x]_5 \)

Answer: \( [x]_5 = 0 \) if \( x \equiv 0 \pmod{5} \)

so \( \text{Ker } f = 5\mathbb{Z} \).
We can prove injectivity of a ring homomorphism by showing that $\text{Ker } f = \{0\}$.

**Theorem.** Let $f : R \rightarrow S$ be a ring homomorphism. Then

1) $\text{Ker } f$ is a subring of $R$

2) $f$ is injective $\iff \text{Ker } f = \{0\}$

**Proof of 1)**: $\text{Ker } f$ is nonempty, since $f(0) = 0$, $0 \in \text{Ker } f$.

For $a, b \in R$, with $f(a) = 0$, $f(b) = 0$, we have $f(a - b) = f(a) - f(b) = 0 - 0 = 0$.

Thus, $a - b \in \text{Ker } f$.

Now, $f(ab) = f(a) f(b) = 0 \cdot 0 = 0$.

So $ab \in \text{Ker } f$.

Thus, $\text{Ker } f$ is a nonempty subset of $R$ satisfying closure for subtraction and closure for multiplication.

Hence, $\text{Ker } f$ is a subring of $R$. 
2) \( \Rightarrow \) Let \( f \) be an injective ring homomorphism. Let \( b \in \ker f \). We have \( f(b) = 0 \). Since \( f(0) = 0 \), \( f(b) = f(0) \). Since \( f \) is injective, this shows \( b = 0 \). Thus \( \ker f = \{0\} \).

\( \Leftarrow \) Let \( f \) be a ring homomorphism satisfying \( \ker f = \{0\} \). We prove injectivity showing that \( f(a) = f(b) \) implies \( a = b \). For, let \( a, b \in R \) with \( f(a) = f(b) \). Then by \( f(a-b) = f(a) - f(b) \), we see that \( f(a-b) = 0 \). Then \( a-b \in \ker f \). By assumption that \( \ker f = \{0\} \), we must have \( a-b = 0 \). Equivalently \( a = b \). This completes the proof.
ex) Prove that the ring homomorphism

\[ f: \mathbb{C} \rightarrow \mathbb{C} \text{ defined by} \]

\[ f(a + bi) = a - bi , \]

is injective.

**Solution** Let \( x \in \mathbb{C} \) with \( f(x) = 0 \), so that \( x \in \ker f \). Then we have

\[ a - bi = 0. \]

Then \( a = 0, -b = 0 \). Therefore \( a = 0 \) and \( b = 0 \).

This shows \( \ker f = \{ 0 \} \).

ex) The ring homomorphism \( f: \mathbb{Z} \rightarrow \mathbb{Z}_5 \) given by \( f(z) = [z]_5 \), is not injective because \( \ker f = 5 \mathbb{Z} \neq \{ 0 \} \).
1. Problems

- Let $R$ be a ring with $x^3 = x$ for all $x \in R$. Then $R$ is commutative.
- Let $R$ be a ring with $x^4 = x$ for all $x \in R$. Then $R$ is commutative.

**Proof.**

- Let $x$ be an element such that $x^2 = 0$, then $x = 0$.
  We have $x^n = x$ for some $n \geq 3$. Then $x^n = x^2x^{n-2} = 0$. Thus, $x = 0$.
- Let $e$ be an idempotent (i.e. $e^2 = e$). Then $xe = ex$ for all $x \in R$.
  We have $(xe - exe)^2 = (xe - exe)^2 = 0$. Since $e$ is an idempotent, we have
    $$(xe - exe)^2 = xexe - xexe - exeex + exeex = 0.$$ 
  Similarly,
    $$(ex - exe)^2 = exe - exe - exeex + exeex = 0.$$ 
  Then we have $xe - exe = ex - exe = 0$. This implies that $xe = ex$.

For the first problem, we use the following equations.

$$ (x^2 + x)^2 = 2(x^2 + x) $$
$$ (x^2 + x)^3 = 4(x^2 + x) = x^2 + x $$

Thus, we have $(x^2 + x)^2 + x^2 + x = 0$. Since $x^2$ is idempotent for any $x \in R$, $(x^2 + x)^2 + x^2$ commutes with any elements in $R$. Hence,

$$ y((x^2 + x)^2 + x^2 + x) = (x^2 + x)^2y + x^2y + yx = 0 $$

Also,

$$ ((x^2 + x)^2 + x^2 + x)y = (x^2 + x)^2y + x^2y + xy = 0 $$

This implies $xy = yx$.

For the second problem, we have $x = x^4 = (-x)^4 = -x$, therefore $2x = 0$. Then, we have the following.

$$ (x^2 + x)^2 = x^2 + x $$

This implies that $y(x^2 + x) = (x^2 + x)y$. Now, we use

$$ (x + y)^2 + x + y + x^2 + x + y^2 + y = xy + yx $$

to show that $xy + yx$ commutes with every elements in $R$. Hence, $x(xy + yx) = (xy + yx)x$, and this shows that $xy = yx$. 

\qed
Real ring homomorphism

July 7, 2015

**Problem 1** Let \( f : \mathbb{R} \to \mathbb{R} \) be a nonzero ring homomorphism on real numbers. Show that \( f(x) = x \) for all \( x \in \mathbb{R} \).

**Solution.** We work on one of a construction of real number (Dedekind Cuts). For details in the construction, refer to Math 131. We use \( x^2 \geq 0 \) for all \( x \in \mathbb{R} \) without proof. Also, remark that we use the fact that \( \mathbb{R} \) is a field.

We show that \( f(1) = 1 \) first. Since \( 1^2 = 1 \), we have \( f(1^2) = f(1)^2 = f(1) \). Thus, \( f(1) \) is an idempotent. Since the only idempotents in real numbers are 0 or 1, we have \( f(1) = 0 \) or \( 1 \). However, we cannot have \( f(1) = 0 \), since this would imply \( f(x) = f(x \cdot 1) = f(x)f(1) = f(x) \cdot 0 = 0 \) for all \( x \in \mathbb{R} \). Since \( f \) is a nonzero ring homomorphism, we have \( f(1) = 1 \).

Then we show that \( f(n) = n \) for all positive integers \( n \). This is clear by

\[
 f(n) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = 1 + \cdots + 1 = n,
\]

where all the summations have \( n \) terms.

Clearly, \( f(0) = 0 \). (Prob 2 of practice problems)

It is easy to show \( f(n) = n \) for all integers \( n \). Since we have the result when \( n \) is positive integer, we prove this for negative integer. Let \( n = -m \) with positive integer \( m \). We have \( 0 = f(m + (-m)) = f(m) + f(-m) \). Then \( f(-m) = -f(m) = -m \). Thus, \( f(n) = n \).

Then we show that \( f(q) = q \) for all positive rational numbers \( q \). Assume that \( q = \frac{m}{n} \) where \( m, n \) are positive integers. We have

\[
 m = f(m) = f\left(n \cdot \frac{m}{n}\right) = nf\left(\frac{m}{n}\right) = nf(q).
\]

Thus, \( f(q) = \frac{m}{n} = q \).

For negative rationals \( s = -q \) where \( q \) is positive rational. Then we see that

\[
 0 = f(q + (-q)) = f(q) + f(-q) = q + f(-q).
\]

Thus, \( f(-q) = -q \), equivalently \( f(s) = s \).

Therefore, we established \( f(x) = x \) for all rational numbers \( x \).

To have \( f(x) = x \) for irrational numbers, we need the following lemma.

**Lemma 1** Let \( f \) be a nonzero real ring homomorphism, then \( f \) is order-preserving. In fact, \( f(a) \geq f(b) \) if \( a \geq b \). Moreover, the inequality is strict if \( a > b \).

To prove this, we need

\[
 f(x) \geq 0 \quad \text{if } x \geq 0.
\]

Once we achieve this, then the lemma is clear by taking \( x = a - b \). For \( x \geq 0 \), there exist \( y \in \mathbb{R} \) such that \( x = y^2 \). Then

\[
 f(x) = f(y^2) = f(y)^2 \geq 0.
\]
This proves Lemma 1 in the case \( a \geq b \). To prove the strict inequality case, we need the following fact

\[
f(x) \neq 0 \quad \text{if} \quad x \neq 0.
\]

We use proof by contradiction. Assume that \( f(x) = 0 \) with \( x \neq 0 \). For any \( z \in \mathbb{R}, z = xy \) for some \( y \in \mathbb{R} \). Then

\[
f(z) = f(xy) = f(x)f(y) = 0f(y) = 0.
\]

Since \( f \) is nonzero, this is impossible.

Now, we prove \( f(x) = x \) for irrational number \( x \). To prove this, we use the following fact from the construction of real numbers. (Requires Math 131 to understand)

**Lemma 2** For any irrational number \( x \), there is a partition \( A_x, B_x \) of rational numbers such that, \( A_x = \{ q \in \mathbb{Q} | q < x \} \), and \( B_x = \{ q \in \mathbb{Q} | q > x \} \). Furthermore, \( x \) is the only number such that it is greater than any element in \( A_x \), and less than any element in \( B_x \).

Let \( q \in A_x \), and \( r \in B_x \). We have \( q < x < r \). Since \( f \) is order-preserving by Lemma 1, we have \( f(q) < f(x) < f(r) \). Since \( f(q) = q \) and \( f(r) = r \), we have \( q < f(x) < r \). Thus, \( f(x) \) has the property: It is greater than any element in \( A_x \), and less than any element in \( B_x \). By Lemma 2, we must have \( f(x) = x \).

Hence, \( f(x) = x \) for all \( x \in \mathbb{R} \) as desired.
Characteristic of a ring

Definition (see Ex 41-43 p. 70)

Let $R$ be a ring with identity. If there is a smallest positive integer $n$ such that

$$n \cdot 1_R = 0_R,$$

then $R$ is said to have characteristic $n$.

If no such $n$ exists, $R$ is said to have characteristic zero.

ex) $\mathbb{Z}$ has characteristic zero.

(ex HW3) $\mathbb{Z}_n$ has characteristic $n$.

$\mathbb{Z}_4 \times \mathbb{Z}_6$ has characteristic 12.

ex) A finite ring with identity has characteristic $n$ for some $n > 0$.

ex) If $R$ is an integral domain, then

(#43 b) $\text{char } R = 0$ or $p$ (prime).

ex) $\mathbb{Z}_p$ has characteristic $p$.

$\mathbb{Z}_{p^2}$ “ $p^2 \not\mid \text{ same order,}$

$\mathbb{Z}_p \times \mathbb{Z}_p$ “ $p \mid \text{ different characteristic}$
Chinese Remainder Theorem (#41-42, p. 83)

41. Let $m, n \in \mathbb{Z}$ with $(m, n) = 1$ and let $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ be the function given by $f([a]_{mn}) = ([a]_m, [a]_n)$.

a) Show that $f$ is well-defined, that is, show that if $[a]_{mn} = [b]_{mn}$ in $\mathbb{Z}_{mn}$, then $[a]_m = [b]_m$ in $\mathbb{Z}_m$ and $[a]_n = [b]_n$ in $\mathbb{Z}_n$.

Proof: If $[a]_{mn} = [b]_{mn}$, then $a \equiv b \pmod{mn}$. Since $m \mid mn$ and $n \mid mn$, we have $m \mid a - b$ and $n \mid a - b$. Then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. This shows that $[a]_m = [b]_m$ in $\mathbb{Z}_m$ and $[a]_n = [b]_n$ in $\mathbb{Z}_n$.


Prob. 1. Chinese Remainder (General Case)

p. 94: 7-8.
We use the following $x$:
\[ x \equiv a \cdot n \cdot n^* + b \cdot m \cdot m^* \pmod{mn} \]
where $n^*$ is the inverse of $n$ modulo $m$, and $m^*$ is the inverse of $m$ modulo $n$, (i.e. $n \cdot n^* \equiv 1 \pmod{m}$ and $m \cdot m^* \equiv 1 \pmod{n}$).

Finding these inverses is possible by the assumption $(m,n) = 1$.

Then $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

For the first, $x \equiv a \cdot n \cdot n^* \pmod{m}$ and by $n \cdot n^* \equiv 1 \pmod{m}$, we have $x \equiv a \pmod{m}$.

For the second, $x \equiv b \cdot m \cdot m^* \pmod{n}$ and by $m \cdot m^* \equiv 1 \pmod{n}$, we have $x \equiv b \pmod{n}$.

Thus $f(\{x\}_{mn}) = ([a]_m, [b]_n)$. 


b) Prove that $f$ is an isomorphism.

1. Injectivity

   We show this by proving that $\text{Ker } f = \{0\}$.

   Let $a \in \mathbb{Z}$ with $[a]_m = 0$ and $[a]_n = 0$, so that $[a]_{mn} \in \text{Ker } f$. Then $a \equiv 0 \pmod{m}$ and $a \equiv 0 \pmod{n}$.

   Without loss of generality, we have $a \equiv m \pmod{n}$. Then it follows that $mn | a$.

   (See #26, p16 or Thm 1.4 p14).

   This shows that $[a]_{mn} = 0$ in $\mathbb{Z}_{mn}$.

   Thus $\text{Ker } f = \{0\}$.

2. Surjectivity.

   Let $[a]_m \in \mathbb{Z}_m$ and $[b]_n \in \mathbb{Z}_n$, so that $( [a]_m, [b]_n )$ is any element in $\mathbb{Z}_m \times \mathbb{Z}_n$.

   We need to find an $[c]_{mn} \in \mathbb{Z}_{mn}$ such that $f([c]_{mn}) = ([a]_m, [b]_n)$.

   Then, this will show that $f$ is surjective.

3. $f$ is a homomorphism (Check!)
If \((m, n) \neq 1\), prove that \((\text{in HW3})\) \(\mathbb{Z}_{mn}\) is not isomorphic to \(\mathbb{Z}_m \times \mathbb{Z}_n\).

Chinese Remainder Theorem (General case) \((\text{in HW3})\)

\[ f: \mathbb{Z}_{m_1 \cdots m_k} \rightarrow \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \]

is given by \(\left[ x \right]_{m_1 \cdots m_k} \rightarrow \left( \left[ x \right]_{m_1}, \cdots, \left[ x \right]_{m_k} \right)\)

1. Show that \(f\) is an isomorphism if \((m_i, m_j) = 1 \text{ for } i \neq j\).

i) Check that \(f\) is well-defined.

ii) Show that \(f\) is a homomorphism

iii) Show that \(f\) is injective.

iv) Show that \(f\) is surjective.

(Hint: Use

\[ x \equiv \sum_{i=1}^{k} x_i \left(\prod_{j \neq i} m_j\right) \left(\prod_{j \neq i} m_j\right)^{-1} \mod \left(\prod_{i=1}^{k} m_i\right) \]

where \(\left( \right)^{-1}\) is the inverse of the corresponding modulus \(m_i\). \]
Arithmetic in \( \mathbb{F}[x] \)

**Definition.** \( R[x] \).

Let \( R \) be a ring, we write
\[
R[x] = \left\{ a_0 + a_1 x + \ldots + a_n x^n \mid a_i \in R \right\}
\]
the "polynomial ring over \( R \)."

The \( x \) is called an indeterminate.

The meaning of \( x \) is ambiguous, to remove the ambiguity, we use the following theorem.

**Theorem 4.1.** Let \( R \) be a ring, then there exists a ring \( T \) containing an element \( x \) that is not in \( R \) \( (x \notin R) \) and has the properties

i) \( R \) is a subring of \( T \)

ii) \( xa = ax \) for every \( a \in R \)

iii) The set \( R[x] \) of all elements of \( T \) of the form
\[
a_0 + a_1 x + \ldots + a_n x^n \quad (n \geq 0, \ a_i \in R)
\]
is a subring of \( T \) that contains \( R \).
\[
( R \subseteq R[x] \subseteq T )
\]
(v) If \( n \leq m \) and
\[
a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m
\]
then \( a_i = b_i \) for \( i = 1, 2, \ldots, n \) and \( b_i = 0 \) (typo in the text) for each \( i > n \).

(v) \( a_0 + a_1 x + \cdots + a_n x^n = 0 \) if and only if \( a_i = 0 \) for every \( i \).

ex) \( \mathbb{Z}[x] \): Polynomials with integer coefficients.
\( \mathbb{Q}[x] \): rational
\( \mathbb{R}[x] \): real

ex) Let \( E \) be the ring of even integers. Then \( 4 - 6x + 4x^3 \in E[x] \), but \( x \not\in E[x] \).

So we have the following inclusion
\[
E \subset E[x] \subset T
\]
where \( T \) is in the Theorem 4.1.
Arithmetics of Polynomials

Addition
\[
(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_m x^m)
= (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_n + b_n) x^n
\]

Multiplication
\[
(a_0 + a_1 x + \cdots + a_n x^n) \cdot (b_0 + b_1 x + \cdots + b_m x^m)
= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots + a_n b_m x^{n+m}
\]

For each \( k \geq 0 \), the coefficient of \( x^k \) is
\[
a_0 b_0 + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0
= \sum_{i=0}^{k} a_i b_{k-i}.
\]

where \( a_i = 0 \) if \( i > n \), \( b_j = 0 \) if \( j > m \).

Definition (Leading Coefficient, Degree)
If \( f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x] \) with \( a_n \neq 0 \), then \( a_n \) is called the leading coefficient of \( f \), and \( n \) is called the degree of \( f \).
Remark 1. If $a_0 \neq 0$, $f(x) = a_0$ is of degree 0.

2. The constant polynomial $0 \text{R}$ does not have a degree.

With the addition and multiplication as above, $\mathbb{R}[x]$ is commutative if $\mathbb{R}$ is commutative. Furthermore, if $\mathbb{R}$ has identity, then $\mathbb{R}[x]$ has identity, which is the constant polynomial 1R. (Exercise 7, 8 in HW3)

Theorem 4.2

If $\mathbb{R}$ is an integral domain and $f(x), g(x)$ are nonzero polynomials in $\mathbb{R}[x]$, then
\[ \text{deg } [f(x)g(x)] = \text{deg } f(x) + \text{deg } g(x) \]

Proof. Suppose $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and $g(x) = b_0 + b_1 x + \ldots + b_m x^m$ with $a_n \neq 0 \text{R}$, $b_m \neq 0 \text{R}$.

Then
\[ f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \ldots + a_n b_m x^{n+m} \]

Since $\mathbb{R}$ is an integral domain, $a_n b_m \neq 0$. Thus, the degree of $f(x)g(x)$ is $n+m$. 
Corollary 4.3

If $R$ is an integral domain, then so is $R[x]$.

Proof. Since $R$ is a commutative ring with identity, so is $R[x]$. Theorem 4.2 shows that the product of nonzero polynomials in $R[x]$ is nonzero. Therefore, $R[x]$ is an integral domain.

Corollary 4.4.

Let $R$ be a ring. If $f(x)$, $g(x)$ and $f(x)g(x)$ are nonzero in $R[x]$, then

\[
\deg [f(x)g(x)] \leq \deg [f(x)] + \deg [g(x)].
\]

Example 6.

In $\mathbb{Z}_6[x]$, let $f(x) = 2x^4$, $g(x) = 5x$.

Then $f(x)g(x) = 2x^4 \cdot 5x = 4x^5$ so

\[
\deg fg = \deg f + \deg g.
\]

However if $g(x) = 1 + 3x^2$, then

\[
f(x)g(x) = 2x^4 (1 + 3x^2)
= 2x^4 + 2\cdot3x^6 = 2x^4.
\]

so $\deg fg < \deg f + \deg g$. 
Corollary 4.5

Let $R$ be an integral domain and $f(x) \in R[x]$. Then $f(x)$ is a unit in $R[x]$ if and only if $f(x)$ is a constant polynomial that is a unit in $R$.

Proof. First, assume that $f(x) \in R[x]$ is a unit. Then $f(x)g(x) = 1_R$ in $R[x]$ for some $g(x) \in R[x]$. By Theorem 4.2,
\[ \deg f(x) + \deg g(x) = \deg (f(x)g(x)) = \deg 1_R = 0. \]

Since $\deg f, \deg g \geq 0$, we have
\[ \deg f(x) = 0, \quad \deg g(x) = 0. \]

Therefore $f, g$ are nonzero constant polynomials. Since $f(x)g(x) = 1_R$, $f, g$ must be units in $R$.

The converse is clear.
Ex 7. Units in \( \mathbb{Z}[x] \): \( \pm 1 \)
Units in \( \mathbb{Q}[x] \): \( q \in \mathbb{Q} - \{0\} \)
Units in \( \mathbb{R}[x] \): \( r \in \mathbb{R} - \{0\} \)

Ex 8. \( 5x + 1 \) is a unit in \( \mathbb{Z}_{25}[x] \) since
\[
(5x + 1)(20x + 1) = 100x^2 + 25x + 1
= 1 \quad \text{in} \ \mathbb{Z}_{25}[x]
\]

However, \( 5x + 1 \) is not a constant polynomial.

If \( F \) is a field, then the units in \( F[x] \) are nonzero constants in \( F \).

Ex) Units in \( \mathbb{Z}_p[x] \): \( \{1, [2], \ldots, [p-1]\} \)
The Division Algorithm in $\mathbb{F}[x]$:

Let $\mathbb{F}$ be a field, and fix $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Example:

$$2x^2 + 3 \cdot \frac{\frac{1}{2}x}{x^3 + x + 1}$$

in $\mathbb{Q}[x]$.

which shows

$$x^3 + x + 1 = \left(2x^2 + 3\right) \frac{\frac{1}{2}x}{x^3 + x + 1} - \frac{1}{2}x + 1$$

$$f(x) \quad g(x) \quad q(x) \quad r(x)$$
Proof of the Division Algorithm

Existence)

Case 1: \( f(x) = 0 \) , or \( \deg f(x) < \deg g(x) \)

then the theorem is true with

\[
\frac{f(x)}{g(x)} = \frac{g(x) \cdot 0 + f(x)}{g(x)}
\]

Case 2: If \( f(x) \neq 0 \) and \( \deg g(x) \leq \deg f(x) \)

we use induction on \( \deg (f(x)) \)

Base case \( \deg f = 0 \) : Then \( \deg (g(x)) = 0 \)

\[ f(x) = a, \quad g(x) = b \quad \text{for} \quad \text{nonzero} \quad a, b \quad \text{of} \quad F. \]

Then

\[ a = b(c^{-1}(a) + 0). \]

Assume that we have the theorem

for \( \deg f(x) \leq n-1 \). Let

\[ f(x) = a_n x^n + \ldots + a_0, \quad a_n \neq 0 \]

\[ g(x) = b_m x^m + \ldots + b_0, \quad b_m \neq 0 \]

Consider

\[ f(x) - a_n b_m x^{n-m} g(x) \]
Then \( \deg(f(x) - a_n b m^{-1} x^{n-m} g(x)) \leq n-1 \), since we cancelled out the \( x^n \) term in \( f(x) \).

Since we have the theorem for polynomials of degree \( \leq n-1 \), there are \( q_i(x), r(x) \) such that

\[
f(x) - a_n b m^{-1} x^{n-m} g(x) = g(x) q_i(x) + r(x)
\]

with \( r(x) = 0 \) or \( \deg r < \deg g \).

Then \( f(x) = g(x) \left( a_n b m^{-1} x^{n-m} + q_i(x) \right) + r(x) \)

and \( r(x) = 0 \) or \( \deg r < \deg g \).

Thus the theorem is true for polynomials of degree \( n \). The proof of existence is complete by induction.
Uniqueness.

Suppose we have two expressions

\[ f(x) = g(x) q(x) + r(x) \]

with \( r(x) = 0 \) or \( \deg r < \deg g \)

and

\[ f(x) = g(x) q_2(x) + r_2(x) \]

with \( r_2(x) = 0 \) or \( \deg r_2 < \deg g \).

Then

\[ g(x) q(x) + r(x) = g(x) q_2(x) + r_2(x) \]

\[ g(x)(q(x) - q_2(x)) = r_2(x) - r(x) \]

If \( q(x) \neq q_2(x) \), then the LHS has degree \( \geq \deg g \). However, \( r_2(x) - r(x) \) has degree \( < \deg g \). (It cannot be zero.)

This is a contradiction. We must have \( q(x) = q_2(x) \), consequently \( r_2(x) = r(x) \).

Thus \( q(x), r(x) \) are unique.
Let $F$ be a field, $f(x), g(x) \in F[x]$, and $g(x) \neq 0$. We write $g(x) \mid f(x)$ if $f(x) = g(x) \cdot h(x)$ for some $h(x) \in F[x]$.

This is the case $r(x) = 0$ in the Division Algorithm.

Example: $x \mid x^2$ in $\mathbb{Z}_2[x]$

$x \mid \frac{1}{2}x^2$ in $\mathbb{Q}[x]$

$x-1 \mid x^3-1$ in $\mathbb{Q}[x]$

**Theorem 4.7**

Let $F$ be a field, $a(x), b(x) \in F[x]$ with $b(x)$ nonzero.

1. If $b(x) \mid a(x)$, then $c \cdot b(x) \mid a(x)$ for each $c \in F - \{0\}$

2. Every divisor of $a(x)$ has degree less than or equal to $\deg a(x)$
Definition (GCD)

Let \( F \) be a field, let \( a(x), b(x) \in F[x] \) not both 0. The GCD of \( a(x) \) and \( b(x) \) is the monic polynomial of highest degree that divides both \( a(x) \) and \( b(x) \). I.e.

1. \( d(x) \mid a(x) \), \( d(x) \mid b(x) \)
2. If \( c(x) \mid a(x) \) and \( c(x) \mid b(x) \) then \( \deg c(x) \leq \deg d(x) \)
3. \( d \) is monic (leading coefficient is 1)

Ex 3.

\( a(x) = 2x^4 + 5x^3 - 5x - 2 \in \mathbb{Q}[x] \)
\( b(x) = 2x^3 - 3x^2 - 2x \in \mathbb{Q}[x] \)

They have the following factorization:

\( a(x) = 2x^4 + 5x^3 - 5x - 2 = (2x + 1)(x+2)(x+1)(x-1) \)
\( b(x) = 2x^3 - 3x^2 - 2x = (2x+1)(x-2)x \)

The common factor of \( a, b \) is \( 2x+1 \), since GCD is monic polynomial, it must be \( x + \frac{1}{2} \).
Theorem 4.8 (Polynomial version of Theorem 1.2)

Let \( F \) be a field, \( a(x), b(x) \in F[x] \) not both 0. Then there is unique \( g(x) \in F[x] \) such that
\[
d(x) = a(x) u(x) + b(x) v(x).
\]

(Omitting proof, interested reader must compare the proof in p. 97–98 with the proof of Theorem 1.2)

Corollary 4.9. Let \( F \) be a field, \( a(x), b(x) \in F[x] \) not both 0. A monic polynomial \( d(x) \in F[x] \)
is the GCD of \( a(x), b(x) \) if and only if
1) \( d(x) \mid a(x), \ d(x) \mid b(x) \)
2) if \( c(x) \mid a(x) \) and \( c(x) \mid b(x) \), then \( c(x) \mid d(x) \).

Theorem 4.10. Let \( F \) be a field, \( a(x), b(x), c(x) \in F[x] \).
If \( a(x) \mid b(x)c(x) \) and \( a(x), b(x) \) are relatively prime then \( a(x) \mid c(x) \).
Irreducibles and Unique Factorization.

Note that \((F[x])^x = F^x = F - \{0\}\) if \(F\) is a field.

For a commutative ring with identity \(R\), elements \(a, b\) are called "associate" if 
\[ a = bu \text{ for some unit } u. \]

ex) In \(\mathbb{Z}[x]\), \(x\) and \(-x\) are associated.

In \(\mathbb{Z}_{25}[x]\), \(x\) and \(x + 5x^2\) are associated, since \(1 + 5x\) is a unit.

For a field \(F\), elements \(a(x), b(x)\) in \(F[x]\) are associated if and only if \(a(x) = cb(x)\) for some \(c \in F - \{0\}\).

ex) In \(\mathbb{R}[x]\), \(x + 2\), \(\pi x + 2\pi\) are associated. \(x + 2\) is an associate of \(\pi x + 2\pi\).
Definition (Irreducible)

Let $F$ be a field. A nonconstant polynomial $p(x) \in F[x]$ is said to be irreducible if its only divisors are its associates and the nonzero constant polynomials (units). A nonconstant polynomial that is not irreducible is called reducible.

ex) Every polynomial of degree 1 in $F[x]$ is irreducible in $F[x]$.

ex) $x+2$ is irreducible in $\mathbb{Q}[x]$,

$x^2-4$ is reducible in $\mathbb{Q}[x]$.

$x^2-2$ is irreducible in $\mathbb{Q}[x]$

$x^2-2$ is reducible in $\mathbb{R}[x]$

$x^2+1$ is irreducible in $\mathbb{R}[x]$

$x^2+1$ is reducible in $\mathbb{C}[x]$
Theorem 4.11 (Reducible)
Let $F$ be a field. A nonzero polynomial $f(x)$ is reducible in $F[x]$ if and only if $f(x)$ can be written as the product of two polynomials of lower degree.

Theorem 4.12
Let $F$ be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then TFAE

1. $p(x)$ is irreducible
2. If $b(x), c(x) \in F[x]$ with $p(x) \mid b(x)c(x)$, then $p(x) \mid b(x)$ or $p(x) \mid c(x)$
3. If $r(x), s(x)$ are any polynomials such that $p(x) = r(x)s(x)$, then $r(x)$ or $s(x)$ is a nonzero constant polynomial.

Remark) prime numbers $\subseteq$ integers 
irreducible polynomials $\subseteq F[x]$. 
Proof \ (1) \Rightarrow (2) \quad \text{Adapt the proof of Theorem 1.5.}

Let \( b(x), c(x) \in \mathbb{F}[x] \) such that

\[ p(x) \mid b(x) c(x) \]

Consider \( d(x) = \gcd \left( p(x), b(x) \right) \). Then \( d(x) \) is a divisor of \( p(x) \). Since \( p(x) \)

is irreducible, \( d(x) \) is either an associate of \( p(x) \) or a nonzero constant.

Case 1: If \( d(x) \) is an associate of \( p(x) \)

then \( d(x) \mid b(x) \) shows \( p(x) \mid b(x) \).

Case 2: If \( d(x) \) is a nonzero constant,

then \( \gcd \left( p(x), b(x) \right) \) must be a

monic nonzero constant, which is 1.

Then by Theorem 4.10, \( p(x) \mid c(x) \).

\( (2) \Rightarrow (3) \quad \text{If} \quad p(x) = r(x)s(x) \quad \text{then} \quad p(x) \mid r(x) \) or \( p(x) \mid s(x) \) by \( (2) \). Say \( r(x) = p(x)v(x) \).

then \( p(x) = r(x)s(x) = p(x)v(x)s(x) \)

Since \( \mathbb{F}[x] \) is an integral domain,

we have \( 1 = v(x)s(x) \) by cancellation.
Then \( V, S \) are units in \( F[x] \), hence nonzero constants. Then \( S \) is a non-zero constant polynomial. If \( p(x) \mid S(x) \), similar argument shows \( r \) is a constant polynomial.

(3) \implies (1) This is clear, since it is just a re-written definition of irreducibility.

Corollary 4.13.

Let \( F \) be a field, \( p(x) \) is an irreducible polynomial in \( F[x] \). If \( p(x) \mid q_1(x) \cdots q_n(x) \)
then \( p(x) \) divides at least one of the \( q_i(x) \).

\( \diamond \) Theorem 4.14 (Unique Factorization)

Let \( F \) be a field. Every non-constant polynomial in \( F[x] \) is a product of irreducible polynomials in \( F[x] \). This factorization is unique in the following sense:

If \( f(x) = p_1(x) \cdots p_r(x) \), and \( f(x) = q_1(x) \cdots q_s(x) \)
with \( p_i, q_j \) irreducible. Then \( r = s \) and
after re-order and relabeling, \( p_i \) is an associate of \( q_i \).
The proof is almost identical to that of Theorem 1.7 (Unique factorization for integers).

Polynomial Functions on commutative ring

For \( f(x) \in R[x] \), the function

\[ r \in R \mapsto f(r) \in R \]

is a function 'induced' by a polynomial.

This is called a polynomial function.

Roots of Polynomials

Let \( R \) be a commutative ring and \( f(x) \in R[x] \).

An element \( a \in R \) is said to be a root (zero) of the polynomial \( f \) if \( f(a) = 0_R \), that is, the 'induced function' \( f : R \to R \) maps \( a \) to \( 0_R \),

ex) \( f(x) = x^2 - 3x + 2 \in R[x] \)

1, 2 are roots of \( f(x) \).
Theorem 4.15 (The Remainder Theorem)

Let \( F \) be a field, \( f(x) \in F[x] \), and \( a \in F \). The remainder when \( f(x) \) is divided by \( x-a \) is \( f(a) \). That is,

\[
f(x) = (x-a)q(x) + f(a)
\]

in the Div. Alg.

Proof. By the Division Algorithm,

\[
f(x) = (x-a)q(x) + r(x)
\]

where \( r(x) = 0 \) or \( \deg r < \deg (x-a) \).

Thus, either \( r(x) = 0 \) or \( \deg r = 0 \).

In either case \( r(x) = c \in F \). Hence

\[
f(x) = (x-a)q(x) + c,
\]

so that

\[
f(a) = (a-a)q(a) + c,
\]

which gives

\[
c = f(a).
\]
Theorem 4.16 (The Factor Theorem)

(Indeed this is a corollary of Theorem 4.15)

Let \( F \) be a field, \( f(x) \in F[x] \), \( a \in F \).

Then \( a \) is a root of the polynomial \( f(x) \) if and only if \( x-a \) is a factor of \( f(x) \) in \( F[x] \).

Proof. Assume that \( a \) is a root of \( f(x) \). Then

\[
f(x) = (x-a) q(x) + r(x) \quad \text{[Div. Alg]}
\]

\[
= (x-a) q(x) + f(a) \quad \text{[Remainder Thm]}
\]

\[
= (x-a) q(x) \quad \text{[a is a root of } f(x)]
\]

\[
f(a) = 0
\]

Therefore \( x-a \mid f(x) \).

Conversely, if \( x-a \) is a factor of \( f(x) \) in \( F[x] \), then

\[
f(x) = (x-a) q(x) \quad \text{for some } q(x) \in F[x]
\]

Then \( f(a) = (a-a) q(a) = 0 \)

Thus \( a \) is a root of \( f(x) \) in \( F[x] \).
Corollary 4.17
Let $F$ be a field, $f(x) \in F[x]$ a nonzero polynomial of degree $n$. Then $f(x)$ has at most $n$ roots in $F$.

Corollary 4.18
Let $F$ be a field, $f(x) \in F[x]$ with $\deg f \geq 2$. If $f$ is irreducible in $F[x]$, then $f$ has no roots in $F$.

Corollary 4.19
Let $F$ be a field, $f(x) \in F[x]$ with $\deg f = 2$ or $3$. Then $f$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in $F$.

Corollary 4.20
Let $F$ be an infinite field and $f(x), g(x) \in F[x]$. Then $f, g$ induce the same function from $F$ to $F$ if and only if $f(x) = g(x)$ in $F[x]$.
Proof of 4.17) If \( f(x) \) has a root \( a_i \) in \( F \) then by Factor Theorem, \( f(x) = (x-a_i) h_i(x) \) for some \( h_i(x) \in F[x] \). If \( h_i(x) \) has a root \( a_2 \) in \( F \), then by Factor Theorem

\[
f(x_2) = (x-a_1)(x-a_2) h_2(x) \text{ for some } h_2(x) \in F[x].
\]

Repeat until we have one of

1. \( f(x) = (x-a_1) \cdots (x-a_n) h_n(x) \)
2. \( f(x) = (x-a_1) \cdots (x-a_k) h_k(x) \) and \( h_k(x) \) has no root in \( F \).

In case (1), by Theorem 4.12, we have

\[
\deg f = \deg (x-a_1) + \cdots + \deg (x-a_n) + \deg h_n
\]

\[
n = 1 + \cdots + 1 + \left\lfloor \frac{\deg h_n}{n} \right\rfloor \text{ Times}
\]

\[
\deg h_n = 0, \quad \text{so} \quad h_n = c \neq 0
\]

\[
f(x) = c (x-a_1) \cdots (x-a_n).
\]
In case (2), we have \( n = \deg f = k + \deg h k \).
So \( k \leq n \).

In any case we have at most \( n \) roots in \( F \).

Proof of 4.18) If \( f \) is irreducible, then it has no factor \( x - a \) in \( F[x] \) for any \( a \in F \). Therefore, \( f(x) \) has no roots in \( F \) by Factor Theorem.

Remark) Converse is not true.

\( \end{proof} \)

\( x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1) \) has no roots in \( \mathbb{R} \).

Proof of 4.19) \( \Rightarrow \) by 4.18.

\( \Leftarrow \) If \( f \) has no roots in \( F \), then \( f \) does not have \( x - a \) as factor for any \( a \in F \). So, \( f \) does not have any factor of degree 1. Then any factor of \( f \) must be of degree as \( f \).

the same
Irreducibility in \( \mathbb{Q}[x] \).

The following fact will be used frequently.

If \( f(x) \in \mathbb{Q}[x] \), then \( cf(x) \) has integer coefficients for some nonzero integer \( c \).

Example:

\[
f(x) = x^5 + \frac{2}{3}x^4 + \frac{3}{4}x^3 - \frac{1}{6}
\]

The \( \text{lcm} \) of \( 3, 4, 6 \) is \( 12 \), and

\[
12f(x) = 12\left(x^5 + \frac{2}{3}x^4 + \frac{3}{4}x^3 - \frac{1}{6}\right) = 12x^5 + 8x^4 + 9x^3 - 2 \in \mathbb{Z}[x].
\]

Theorem 4.21. (Rational Root Test)

Let \( f(x) = a_nx^n + \cdots + a_1x + a_0 \) be a polynomial with integer coefficients. If \( r \in \mathbb{Q} \) and the rational number \( \frac{r}{s} \) (in lowest terms) is a root of \( f(x) \), then \( r \mid a_0 \) and \( s \mid a_n \).

Proof: Consider

\[
an\left(\frac{r^n}{s^n}\right) + an-1\left(\frac{r^{n-1}}{s^{n-1}}\right) + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0
\]

\[
an r^n + an s r^{n-1} + \cdots + a_1 s^{n-1} r + a_0 s^n = 0 \quad (\text{multiply})
\]

We see that \( s \mid an r^n \) and \( r \mid a_0 s^n \).

Since \( \frac{r}{s} \) is of lowest terms, \( (r, s) = 1 \), and \( s \mid an \) and \( r \mid a_0 \).
Example 1. \( f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12 \)

The possible roots \( \frac{r}{s} \) in \( \mathbb{Q} \) satisfy:

\[ r \mid 12, \quad s \mid 2. \]

Thus \( r = \pm 1, \pm 2, \ldots, \pm 12 \) (divisors of 12)

\[ s = \pm 1, \pm 2 \] (divisors of 2)

Thus \( \frac{r}{s} \) is one of the numbers in the following list:

\[ 1, -1, 2, -2, \quad 3, -3, 4, -4, 6, -6, 12, -12, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2} \]

Among those numbers, only \( -3 \) and \( \frac{1}{2} \) are roots.

By the Factor Theorem, both \( x+3 \) and \( x-\frac{1}{2} \) are factors of \( f(x) \). Division shows that:

\[ f(x) = (x+3)(x-\frac{1}{2})(2x^2-4x-8) \]

\[ 2x^2 - 4x - 8 = 2(x^2 - 2x - 4) \]

\[ x^2 - 2x - 4 = (x-1)^2 - 5 \]

The roots of \( x^2 - 2x - 4 \) are \( 1 \pm \sqrt{5} \) \& \( \mathbb{Q} \).

Thus \( x^2 - 2x - 4 \) is irreducible in \( \mathbb{Q}[x] \), hence so is \( 2x^2 - 4x - 8 \).
Example 2. The only possible rational roots of
g(x) = x^3 + 4x^2 + x - 1 \quad \text{in } \mathbb{Q}\text{ are}
1 \quad \text{and} \quad -1 \quad (\text{Why? The } \frac{r}{s} \text{ satisfy } r|1, s|1)

However, \(1^3 + 4 \cdot 1^2 + 1 - 1 = 5 \neq 0\)

and \((-1)^3 + 4 \cdot (-1)^2 + (-1) - 1 = 1 \neq 0\)

Thus, \(g(x)\) does not have any rational roots. Hence \(g(x)\) is irreducible in \(\mathbb{Q}[x]\)
by corollary 4.19. (degree 3, does not have rational root)

Lemma 4.22. Let \(f(x), g(x), h(x) \in \mathbb{Z}[x]\) with
\(f(x) = g(x) \cdot h(x)\). If \(p\) is a prime that divides every coefficient of \(f(x)\), then either \(p\) divides every coefficient of \(g(x)\) or \(p\) divides every coefficient of \(h(x)\). The converse is also true.

Notation). For a prime \(p\), denote by \(\overline{f(x)}\)
the reduction of \(f(x)\) modulo the prime \(p\).
If \(f(x) = a_n x^n \ldots + a_0 \in \mathbb{Z}[x]\), then
\(\overline{f(x)} = [a_n] x^n \ldots + [a_0] \in \mathbb{Z}_p [x]\).
Proof of Lemma 4.22.

The assumption for \( f \in \mathbb{Z}[x] \) shows that \( \bar{f}(x) \in \mathbb{Z}_p[x] \) is zero-polynomial.

Also, it is easy to see that whenever \( f(x) = g(x)h(x) \) in \( \mathbb{Z}[x] \), we have \( \bar{f}(x) = \bar{g}(x) \bar{h}(x) \) in \( \mathbb{Z}_p[x] \).

We have \( \bar{f}(x) = 0 \) in \( \mathbb{Z}_p[x] \). Thus,

\[
0 = \bar{g}(x) \bar{h}(x) \quad \text{in} \quad \mathbb{Z}_p[x].
\]

Since \( \mathbb{Z}_p \) is a field, (hence integral domain)
we also have \( \mathbb{Z}_p[x] \) is an integral domain.

Then we must have \( \bar{g}(x) = 0 \) or \( \bar{h}(x) = 0 \) in \( \mathbb{Z}_p[x] \).

If \( \bar{g}(x) = 0 \) in \( \mathbb{Z}_p[x] \), then all coefficients is divisible by \( p \).
If \( \bar{h}(x) = 0 \) in \( \mathbb{Z}_p[x] \), then all coefficients is divisible by \( p \).

Thus, the proof is complete.

The converse is obvious. If \( p \) divides every coefficient of one of \( g, h \), then \( p \) does so for \( f \)
Theorem 4.23. Let \( f(x) \) be a polynomial with integer coefficients. Then \( f(x) \) factors as a product of polynomials of degree \( m \) and \( n \) in \( \mathbb{Q}[x] \) if and only if \( f(x) \) factors as a product of polynomials of degrees \( m \) and \( n \) in \( \mathbb{Z}[x] \).

Proof. Obviously, if \( f(x) \) factors in \( \mathbb{Z}[x] \), it factors in \( \mathbb{Q}[x] \). Conversely, suppose \( f(x) = g(x) h(x) \) in \( \mathbb{Q}[x] \). Let \( c, d \) be nonzero integers such that \( \{ c g(x) \} \) has integer coefficients. Then

\[
\text{cd} f(x) = \{ c g(x) \} \{ d h(x) \} \text{ in } \mathbb{Z}[x].
\]

Let \( p \) be any prime divisor of \( \text{cd} \), say \( \text{cd} = p \text{d} \). Then \( p \mid \text{every coefficient of } \text{cd} f(x) \).

Then by Lemma 4.22, either \( p \) divides every coefficient of \( c g(x) \) or every coefficient of \( d h(x) \), say the former. Then \( c g(x) = p c_1(x) \) with \( \{ c_1(x) \} \in \mathbb{Z}[x] \) and \( \deg c_1(x) = \deg g(x) \). Therefore \( p \text{d} f(x) = \text{cd} f(x) = (c g(x)) \{ d h(x) \} = (p c_1(x)) \{ d h(x) \} \). Canceling \( p \), we have \( tf(x) = k(x) dh(x) \) in \( \mathbb{Z}[x] \).
We repeat this process until we exhaust all prime factors of \( cd \). Then the LHS becomes \( \pm f(x) \), and the RHS is a product of polynomials of degree \( m \) and \( n \) having integer coefficients.

(Alternative Proof of Theorem 4.23) Using "Content"

If \( f(x) \) has factors in \( \mathbb{Q}(x) \) and at least one coefficient of \( g \) and at least one coefficient of \( h \) is not rational, so that

\[
f(x) = g(x) h(x), \text{ but } g(x) \notin \mathbb{Z}[x] \text{ and } h(x) \notin \mathbb{Z}[x].
\]

We find positive integers \( c, d \) such that \( c \) is the smallest positive integer such that \( c9(x) \) is in \( \mathbb{Z}[x] \), and \( d \) is the smallest positive integer such that \( dh(x) \) is in \( \mathbb{Z}[x] \).

Then \( c(9g(x)) = c(dh(x)) = 1 \). Thus

\[
c( cd f(x) ) = c( 9g(x)) c( dh(x) ) = 1
\]

Since \( c( cd f(x) ) = cd c(f(x)) \mid 1 \), we have \( c = d = 1 \). This is contradiction.
Definition) Content of a polynomial in \( \mathbb{Z}[x] \)

Let \( f(x) \in \mathbb{Z}[x] \) be a nonzero polynomial.

The content of \( f \), denoted by \( c(f) \), is defined by the g.c.d of all coefficients.

If \( f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x] \), \( f(x) \neq 0 \)

then \( c(f) = (a_n, \ldots, a_0) \).

Lemma 4.22

Let \( f, g \in \mathbb{Z}[x] \) be nonzero polynomials.

Then \( c(fg) = c(f) \cdot c(g) \).

Proof) Let \( p^m \) be the exact power of \( p \) that divides \( c(fg) \). Let \( h = fg \in \mathbb{Z}[x] \).

Consider \( \overline{h} = \overline{f} \cdot \overline{g} \). Since \( \overline{h} = 0 \) in \( \mathbb{Z}_p[x] \), either one of \( \overline{f}, \overline{g} \) is \( 0 \) in \( \mathbb{Z}_p[x] \).

Say \( \overline{f} \). Then we have \( \overline{h} = \overline{f} \cdot \overline{g} \). Since \( \overline{h} = 0 \) in \( \mathbb{Z}_p[x] \), \( \overline{g} = 0 \) in \( \mathbb{Z}_p[x] \).

With \( \frac{h}{p^m}, \frac{f}{p} \in \mathbb{Z}[x] \), continue this process \( n \) times, then \( \frac{h}{p^n} = \frac{f}{p^i} \cdot \frac{g}{p^j} \) with \( i + j = n \) and
\[ \frac{f}{p^i}, \frac{g}{p^j} \in \mathbb{Z}[x]. \]

Then \[ \left( \frac{h}{p^n} \right) = \left( \frac{f}{p^i} \right) \left( \frac{g}{p^j} \right) \text{ in } \mathbb{Z}_p[x]. \]

The LHS is nonzero in \( \mathbb{Z}_p[x] \) by assumption. Thus, neither one of \( \left( \frac{f}{p^i} \right) \) and \( \left( \frac{g}{p^j} \right) \) is zero in \( \mathbb{Z}_p[x] \). Then \( p^i, p^j \) are the exact powers of \( p \) that divide \( \text{c}(f) \) and \( \text{c}(g) \) respectively. Therefore \( p^n \) is the exact power of \( p \) that divides \( \text{c}(f) \text{c}(g) \).
Example 3  
Degree = 4  \Rightarrow \text{ Cor 4.19 is not available}

\[ f(x) = x^4 - 5x^2 + 1 \]

Rational Root Test \Rightarrow \text{ roots } = \pm 1

Plug in \Rightarrow \text{ They are not.}

\Rightarrow \text{ no roots.}

If it factors, then we have

\[ f(x) = x^4 - 5x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d) \]

with \( a, b, c, d \in \mathbb{Z} \).

We show that this is impossible.

First, \( 1 = bd \), \( b = d = 1 \) or \( b = d = -1 \).

Next, \( a + c = 0 \). By comparing coeff of \( x^3 \),
we have \( b + ac + d = -5 \) by coeff of \( x^2 \).

Also, \( ad + bc = 0 \) by comparing coeff of \( x \).

If \( b = d = 1 \), then \( ac = -7 \), cannot have \( a + c = 0 \)

If \( b = d = -1 \), then \( ac = -3 \), also cannot

Therefore \( f(x) \) is irreducible. Have \( a + c = 0 \),
in \( \mathbb{Q}[x] \).
Eisenstein's Criterion

Thm 4.24. Let \( f(x) = a_n x^n + \cdots + a_1 x + a_0 \)
be a nonconstant polynomial with integer coefficients. If there is a prime \( p \) such that \( p | a_0, p | a_1, \ldots, p | a_{n-1}, \) but \( p^2 \nmid a_0, p \nmid a_n \), then \( f(x) \) is irreducible in \( \mathbb{Q}(x) \).

Proof: Suppose not, then \( f(x) = g(x) h(x) \)
for \( g(x), h(x) \in \mathbb{Z}[x] \) non-constant
(by Theorem 4.23)

Consider \( \overline{f}(x) = \overline{g}(x) \overline{h}(x) \) in \( \mathbb{Z}_p [x] \).
By assumption, \( \overline{f}(x) = [a_n] x^n \) in \( \mathbb{Z}_p [x] \).
The polynomial \( x \) in \( \mathbb{Z}_p [x] \) is irreducible
and \( \overline{f}(x) \) is an associate of \( x^n \) in \( \mathbb{Z}_p [x] \).

By the unique factorization, (Theorem 4.14)
and that \( \overline{g} \) and \( \overline{h} \) are divisors of \( \overline{f} \),
we have \( \overline{g}(x) = a x^i, \overline{h}(x) = b x^j \) with \( i+j = n \), \( ab = [a_n] \), and \( i, j \geq 1 \).
This is contradiction, because the above implies
constants of \( g, h \) are divisible by \( p \), then \( p^2 \mid a_0 \).
Ex 4. \( x^7 + 6x^3 - 15x^6 + 3x^2 - 9x + 12 \)

is irreducible in \( \mathbb{Q}[x] \).

Proof) Take \( p = 3 \) in Eisenstein's Criterion.

Ex 5. \( x^n + 5 \) is irreducible in \( \mathbb{Q}[x] \) for each \( n \geq 1 \). Thus

"there are irreducible polynomials of every degree in \( \mathbb{Q}[x] \)."

Theorem 4.25

Let \( f(x) = a_k x^k + \ldots + a_0 \) be a polynomial with integer coefficients, and let \( p \) be a positive prime that does not divide \( a_k \).

If \( f(x) \) is irreducible in \( \mathbb{Z}_p[x] \), then \( f(x) \) is irreducible in \( \mathbb{Q}[x] \).

Proof) By 4.23, if \( f \) is reducible in \( \mathbb{Q}[x] \), then \( f(x) = g(x) h(x) \) for some \( g, h \in \mathbb{Z}[x] \), with \( g, h \) nonconstant. Then

\[
\overline{f}(x) = \overline{g}(x) \overline{h}(x) \quad \text{in} \quad \mathbb{Z}_p[x].
\]

Since \( p | a_k \), the leading coefficients of \( g \) and \( h \) are not divisible by \( p \). Thus \( \deg g = \deg \overline{g} \) and \( \deg h = \deg \overline{h} \). Then \( \overline{g}, \overline{h} \) are nonconstants in \( \mathbb{Z}_p[x] \).
Prove that for \( p \) prime, 
\[
    f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \quad \text{is irreducible in } \mathbb{Q}[x].
\]

Proof: We need a lemma.

Lemma: \( f(x) \) is irreducible in \( \mathbb{Q}[x] \) if and only if \( f(x+1) \) is irreducible in \( \mathbb{Q}[x] \).

Consider 
\[
    \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 = f(x).
\]

We have 
\[
    \frac{(x+1)^p - 1}{(x+1) - 1} = f(x+1).
\]

By the Binomial Theorem, we have 
\[
    f(x+1) = \frac{\sum_{k=0}^{p} \binom{p}{k} x^k - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} \in \mathbb{Z}[x]
\]

Since \( p \mid \binom{p}{k} \) for \( k = 1, \cdots, p-1 \),
\( p \) divides all coefficients except the leading one, and
\[ p^2 \nmid (p^i) = p. \]

The Eisenstein Criterion with this prime \( p \) shows that \( f(x+1) \) is irreducible in \( \mathbb{Q}[x] \).

By Lemma, \( f(x) \) is irreducible in \( \mathbb{Q}[x] \).
Ex 4. \[ x^9 + 6x^3 - 15x^4 + 3x^2 - 9x + 12 \]
is irreducible in \( \mathbb{Q}[x] \).

Proof. Take \( p = 3 \) in Eisenstein's criterion.

Ex 5. \( x^n + 5 \) is irreducible in \( \mathbb{Q}[x] \) for each \( n > 1 \). Thus
"there are irreducible polynomials of every degree in \( \mathbb{Q}[x] \)".

Theorem 4.25
Let \( f(x) = a_n x^n + \ldots + a_0 \) be a polynomial with integer coefficients, and let \( p \) be a positive prime that does not divide \( a_n \).

If \( f(x) \) is irreducible in \( \mathbb{Z}_p[x] \), then \( f(x) \) is irreducible in \( \mathbb{Q}[x] \).

Proof. By 4.23, if \( f \) is reducible in \( \mathbb{Q}[x] \), then \( f(x) = g(x) h(x) \) for some \( g, h \in \mathbb{Z}[x] \), with \( g, h \) nonconstant. Then
\[ f(x) = \overline{f}(x) = \overline{g}(x) \overline{h}(x) \in \mathbb{Z}_p[x]. \]

Since \( \deg a_n \), the leading coefficients of \( g \) and \( h \) are not divisible by \( p \). Thus \( \deg g = \deg \overline{g} \) and \( \deg h = \deg \overline{h} \). Then \( \overline{g}, \overline{h} \) are nonconstants in \( \mathbb{Z}_p[x] \).
Irreducibility in \( \mathbb{R}[x] \) and \( \mathbb{C}[x] \)

The Fundamental Theorem of Algebra

Every nonconstant polynomial in \( \mathbb{C}[x] \) has a root in \( \mathbb{C} \).

Cor 4.29

A polynomial is irreducible in \( \mathbb{C}[x] \) if and only if it has degree 1.

Cor 4.28

Every nonconstant polynomial \( f(x) \) of degree \( n \) in \( \mathbb{C}[x] \) can be written in the form
\[ c(x-a_1) \cdots (x-a_n) \] for some \( c, a_1, \ldots, a_n \in \mathbb{C} \).

Lem 4.29.

If \( f(x) \in \mathbb{R}[x] \) and \( f(a+bi)=0 \) then \( f(a-bi)=0 \).

Thm 4.30

A polynomial \( f(x) \) is irreducible in \( \mathbb{R}[x] \) if and only if \( f(x) \) is a first-degree or
\[ ax^2+bx+c \] with \( b^2-4ac<0 \).

Cor 4.31

Every polynomial \( f(x) \) of odd degree in \( \mathbb{R}[x] \) has a root in \( \mathbb{R} \).
Congruence in \( F[x] \), Congruence Class Arithmetic

**Def.** Let \( F \) be a field and \( f, g, p \in F[x] \) with \( p(x) \neq 0 \). Then write \( f(x) \equiv g(x) \pmod{p(x)} \) if \( p(x) \mid f(x) - g(x) \).

**Thm 5.1** \( \equiv \pmod{p(x)} \) is an equivalence relation.

**Thm 5.2** If \( f(x) \equiv g(x) \pmod{p(x)} \) and \( h(x) \equiv k(x) \pmod{p(x)} \) then

\[
\begin{align*}
    f(x) + h(x) &\equiv g(x) + k(x) \pmod{p(x)} \\
    f(x) h(x) &\equiv g(x) k(x) \pmod{p(x)}
\end{align*}
\]

**Def.** Let \( F \) be a field, \( f(x), p(x) \in F[x] \) with \( p(x) \neq 0 \). The congruence class of \( f(x) \), is

\[
    [f(x)] = \{ g(x) \mid g(x) \in F[x], \ g(x) \equiv f(x) \pmod{p(x)} \}
\]

**Thm 5.3** \( f(x) \equiv g(x) \pmod{p(x)} \) if and only if \( [f(x)] = [g(x)] \).

**Cor 5.4** Two congruence classes are either disjoint or identical. (This is true for any equivalence relation & equivalence classes.)

**Cor 5.5** Let \( F \) be a field, \( p(x) \) a polynomial of degree \( n \) in \( F[x] \),

\[
    f(x) = p(x) q(x) + r(x), \ [f(x)] = [r(x)]
\]

**Def.** The set of all congruence class \( \pmod{p(x)} \) is denoted \( F[x]/(p(x)) \).
This is an analogue of $\mathbb{Z}/n\mathbb{Z}$, which is
\[ \frac{\mathbb{Z}}{n\mathbb{Z}} \text{, or } \mathbb{Z}/(n) \]

The notation $(p(x))$ is for the set of all multiples of $p(x)$ in $F[x]$, so that \[ (p(x)) = \{ g(x) \in F[x] \mid p(x) \mid g(x) \} \]

Also, in the previous notation, this is $[0]$. 

Ex 5. Consider $p(x) = x^3 + 1 \in \mathbb{R}[x]$. Then \[ \mathbb{R}[x]/(x^3 + 1) = \{ [ax + b] \mid a, b \in \mathbb{R} \} \]

This is naturally isomorphic to $\mathbb{C}$. Construct the isomorphism.

Ex 6. Consider $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. \[ \mathbb{Z}_2[x]/(x^2 + x + 1) = \{ [0], [1], [x], [x+1] \} \]

Later (in the subsequent courses), we see that this is a finite field of order 4.
Congruence Class Arithmetic.

Theorem 5.6 Let F be a field, \( p(x) \) a nonconstant polynomial in \( F[x] \). Addition, multiplications are defined in \( F[x]/(p(x)) \) by

\[
[f(x)] + [g(x)] = [f(x) + g(x)]
\]

\[
[f(x)] \cdot [g(x)] = [f(x)g(x)]
\]

Example 1. Consider \( \mathbb{R}[x]/(x^2+1) \). What is \( [x] \cdot [x] \)? It is \( i \in \mathbb{C} \).

How is it related to \( \mathbb{C} \)? It is \( \mathbb{C} \).

Example 2. What is \( [x] \cdot [x+1] \) in \( \mathbb{Z}_2[x]/(x^2+x+1) \)?

\[
[x] \cdot [x+1] = [x^2+x] = [x^3+1-1] = [-1] = [1]
\]

So, \( [x+1] \) is a multiplicative inverse of \( [x] \). Check Ex3 +, \cdot tables for further examples.
Theorem 5.8

Let \( F \) be a field, \( p(x) \) a nonconstant polynomial in \( F[x] \). Then \( F[x]/(p(x)) \) is a commutative ring with identity that contains \( F \).

The structure of how \( F[x]/(p(x)) \) contains \( F \):

Recall \( F[x]/(p(x)) = \left\{ [a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}] \mid a_0, \ldots, a_{n-1} \in F \right\} \)

in case \( \deg p = n \geq 1 \).

This contains \( [a_0] \) for any \( a_0 \in F \),

so we have

\[
\begin{array}{ccc}
F[x]/(p(x)) & \uparrow & [a_0] \in F[x]/(p(x)) \\
\downarrow & & \downarrow \\
F & & a_0 \in F
\end{array}
\]
Theorem 5.9

Let $F$ be a field and $p(x)$ a nonconstant polynomial in $F[x]$. If $f(x) \in F[x]$ and $f(x)$ is relatively prime to $p(x)$, then $[f(x)]$ is a unit in $F[x]/(p(x))$.

Proof: Since $f, p$ are relatively prime, there are polynomials $u(x), v(x)$ such that $f(x)u(x) + p(x)v(x) = 1$. Hence

$$f(x)u(x) = 1 - p(x)v(x) \equiv 1 \pmod{p(x)}$$

Thus $[f(x)][u(x)] = [1]$ in $F[x]/(p(x))$.

Ex. 4. $x^2 - 2$ and $2x+5$ are irreducible polynomials in $\mathbb{Q}[x]$, hence $2x+5, x^2 - 2$ are relatively prime. Then $[2x+5]$ is a unit in $\mathbb{Q}[x]/(x^2 - 2)$.

$$(2x+5)\left(-\frac{2}{7}x + \frac{5}{17}\right) + (x^2 - 2)\frac{4}{17} = 1$$

(use Div. alg.)

Therefore $\left[-\frac{2}{7}x + \frac{5}{17}\right]$ is the inverse of $[2x+5]$ in $\mathbb{Q}[x]/(x^2 - 2)$. 
The Structure of $\mathbb{F}(x)/\langle p(x) \rangle$ when $p(x)$ is Irreducible

Recall that when $p$ is a prime number,

$$\mathbb{Z}_p = \mathbb{Z}/(p)$$

is a field.

Theorem 5.10

Let $F$ be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then TFAE

1. $p(x)$ is irreducible in $F[x]$
2. $F[x]/\langle p(x) \rangle$ is a field
3. $F[x]/\langle p(x) \rangle$ is an integral domain

Proof: (1) $\Rightarrow$ (2) By Theorem 5.9, $F[x]/\langle p(x) \rangle$ is a commutative ring with identity. (Axioms 1-10)

To prove that $F[x]/\langle p(x) \rangle$ is a field, we need to find an inverse of nonzero element:

Let $[a(x)] \neq [0]$ in $F[x]/\langle p(x) \rangle$. Then by Theorem 5.3, $a(x) \not\equiv 0$ (mod $p(x)$), $p(x) \not| a(x)$.

Since $p(x)$ is irreducible, $\gcd(a(x), p(x))$ is either $1_F$ or a monic associate of $p(x)$.

It cannot be a monic associate of $p(x)$ since $a(x)$ is not a multiple of $p(x)$.
Then we have \( \gcd(ac(x), p(x)) = 1 \). By Theorem 5.9, \([a(x)]\) is a unit in \( \mathbb{F}[x]/(p(x)) \). Hence \( \mathbb{F}[x]/(p(x)) \) satisfies Axiom 12, it is a field.

(2) \( \Rightarrow \) (3) This is clear because a field is an integral domain.

(3) \( \Rightarrow \) (1) We shall verify (2) of Theorem 4.12.

Let \( b(x), c(x) \) be any polynomials with \( p(x) \mid b(x)c(x) \). Then \( b(x)c(x) \equiv 0 \pmod{p(x)} \), so \([b(x)] [c(x)] = [0]\) in \( \mathbb{F}[x]/(p(x)) \)

Since \( \mathbb{F}[x]/(p(x)) \) is an integral domain, either \([b(x)] = [0]\) or \([c(x)] = [0]\).

Thus \( p(x) \mid b(x) \) or \( p(x) \mid c(x) \).

Therefore \( p(x) \) is irreducible by Thm 4.12.
Theorem 5.11. Let $F$ be a field and $p(x)$ an irreducible polynomial in $F[x]$. Then $F[x]/(p(x))$ is an extension field of $F$ that contains a root of $p(x)$.

Proof. Let $K = F[x]/(p(x))$. This is a field by previous theorem. We saw that $K$ contains $F$. Thus, $K$ is an extension field of $F$.

This contains a root of $p(x)$ since $\bar{x} \in F[x]/(p(x))$ is a root of $p(x)$. For, let \[ x = \bar{x}, \] and $p(x) = a_n x^n + \cdots + a_0$

\[ p(x) = a_n x^n + \cdots + a_0 \]

\[ = a_n \bar{x}^n + \cdots + a_0 \]

\[ = [a_n x^n + \cdots + a_0] \]

\[ = [p(x)] = [0] \quad \text{in } K. \]

Therefore $x \in K$ is a root of $p(x)$. 

Cor. 5.12

Let $F$ be a field, for a nonconstant polynomial in $F[x]$. Then there is an extension field $K$ of $F$ that contains a root of $f(x)$.

Proof) Consider an irreducible $p(x)$ that divides $f(x)$. Then $F[x]/(p(x))$ is one of the desired extension field.
Ideals and Congruence.

**Def** A subring $I$ of a ring $R$ is an ideal provided:

Whenever $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$.

Examples 1. For any $n \in \mathbb{Z}$, $(n)$ is an ideal.
2. For any polynomial $f(x) \in \mathbb{F}[x]$, $(f(x))$ is an ideal.
3. Of course, $(0_R)$ is an ideal in any ring $R$.
4. In $\mathbb{Z}[x]$, polynomials with even constant term form an ideal.
5. In $T$ : the ring of all functions from $IR$ to $IR$, let $I$ be the subset consisting of functions $g$ s.t.
   
   $g(2) = 0$.

Then $I$ is an ideal.

Non-examples) $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring but not an ideal.
Theorem 6.1.

A nonempty subset $I$ of a ring $R$ is an ideal if and only if

(i) If $a, b \in I$, then $a - b \in I$

(ii) If $r \in R$, $a \in I$, then $ra \in I$ and $ar \in I$.

Proof) Every ideal has these two properties. Conversely, suppose $I$ has these properties we need to prove that $I$ is a subring, then we would have all properties of ideal.

Since by (i), $I$ is closed under subtraction. Also, by (ii), $I$ is closed under multiplication.

Thus, $I$ is a subring, absorbing products.

Finitely Generated Ideals

Theorem 6.2. Let $R$ be a commutative ring with identity, $c \in R$, and $I = \{rc | r \in R\}$.

Then $I$ is an ideal, denoted by $(c)$.

ex. 1. $(1R) = R$.

2. Let $a, b \in R$, then $(ab) \subseteq (a)$.

Theorem 6.2 is a special case of Theorem 6.3.
Theorem 6.3.
Let \( R \) be a commutative ring with identity, \( c_1, \ldots, c_n \in R \). Then
\[
I = \{ r_1 c_1 + \cdots + r_n c_n \mid r_1, \ldots, r_n \in R \}
\]
is an ideal in \( R \).

Proof.
If \( a, b \in I \), then there are \( r_1, \ldots, r_n \in R \) and \( s_1, \ldots, s_n \in R \) such that \( 0 \in R \). \( a = r_1 c_1 + \cdots + r_n c_n \) and \( b = s_1 c_1 + \cdots + s_n c_n \).

Then \( a - b = (r_1 - s_1)c_1 + \cdots + (r_n - s_n)c_n \).

Since \( r_i - s_i \in R \), for all \( i = 1, \ldots, n \), we have \( a - b \in I \).

If \( r \in R \), \( a \in I \) with
\[
a = r_1 c_1 + \cdots + r_n c_n \quad \text{and} \quad r_1, \ldots, r_n \in R,
\]
then \( ra = r(r_1 c_1 + \cdots + r_n c_n) \)
\[
= (rr_1)c_1 + \cdots + (rr_n)c_n.
\]

Since \( rr_i \in R \) for all \( i = 1, \ldots, n \), we have \( ra \in I \). (This is enough.

Therefore \( I \) is an ideal. [because \( R \) is commutative] )
\[ I = \langle r_1, \ldots, r_n \mid r_i \in \mathbb{R} \rangle \]

is sometimes denoted by \( (c_1, \ldots, c_n) \).

(\( c \)) is called a principal ideal. \( (c) = \langle c \rangle \).

\( (c_1, \ldots, c_n) \) is called a finitely generated ideal.

**Ex. 9.** \( I = \{ f(x) \in \mathbb{Z}[x] \mid f(0) \in 2\mathbb{Z} \} \)

We have seen that \( I \) is an ideal.

This \( I \) can be also written as

\[ I = (x, 2) \]

**Proof.** Let \( f(x) \in \mathbb{Z}[x] \) with \( f(0) \in 2\mathbb{Z} \).

Then \( f(x) = a_n x^n + \cdots + a_1 x + a_0 \), with \( a_i \in \mathbb{Z} \) for all \( i = 0, \ldots, n \), and \( a_0 \in 2\mathbb{Z} \).

Consider \( f(x) = (a_n x^{n-1} + \cdots + a_1) x + a_0 \).

Since \( a_n x^{n-1} + \cdots + a_1 \in \mathbb{Z}[x] \) and \( a_0 \in \mathbb{Z}[x] \) as constant polynomials, we have \( f(x) \in (x, 2) \).
Conversely, let \( f(x) \in (x, 2) \), then there are \( g(x), h(x) \in \mathbb{Z}[x] \) \( \text{s.t.} \)
\[
f(x) = g(x) \cdot x + h(x) \cdot 2
\]
Plug in \( x = 0 \), then \( f(0) = g(0) \cdot 0 + h(0) \cdot 2 \)
so that \( f(0) = 2h(0) \in 2\mathbb{Z} \).

Thus, \( (x, 2) \subseteq I \). Hence \( I = (x, 2) \).

Congruence.

Def. Let \( I \) be an ideal in a ring \( R \).

Then \( a \equiv b \pmod{I} \) provided that \( a - b \in I \).

Recall \)
\[
f(x) \equiv g(x) \pmod{p(x)} \iff p(x) | f(x) - g(x)
\]
\( \iff \)
\[
f(x) \equiv g(x) \pmod{p(x)} \iff f(x) - g(x) \in (p(x))
\]
\( \iff \)
\[
f(x) - g(x) = p(x)q(x) \text{ for some } q(x) \in F[x]
\]
\( \iff \)
\[
[f(x)] = [g(x)], \text{ in } F[x]/(p(x))
\]
Thm 6.4, \( a \equiv b \pmod{I} \) is an equivalence relation.

Thm 6.5 (Arithmetic) Let \( I \) be an ideal in \( \mathbb{Z} \), \( R \).

\[
\begin{align*}
\text{If } & a \equiv b \pmod{I}, \ c \equiv d \pmod{I} \\
& \text{then } a + c \equiv b + d \pmod{I} \\
& ac \equiv bd \pmod{I}
\end{align*}
\]

Congruence Class

\[ [a] = \{ b \in \mathbb{R} \mid b \equiv a \pmod{I} \} \] as usual, but we avoid \([a]\) from now on.

We write instead, \( \overline{a + I} \) (a coset of \( I \) in \( R \))

because \( [a] = \{ a + i \mid i \in I \} \).

Thm 6.6 Let \( I \) be an ideal in \( \mathbb{Z} \), \( a, c \in \mathbb{Z} \).

Then \( a \equiv c \pmod{I} \) if and only if \( a + I = c + I \).

Change of Notations

Ex1. Consider \([0], [1], [2]\) in \( \mathbb{Z}_3 \), they are now \( 0 + (3), 1 + (3), 2 + (3) \).

or \( 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z} \).
Example 2. \([0], [1], [x], [x+1] \) in \( \mathbb{Z}_2[x]/(x^2+x+1) \)

They are \(0+I, 1+I, x+I, x+1+I\)

where \(I = (x^2+x+1)\)

Operations on Ideals

1. Intersection

If \(I, J\) are ideals in \(R\)

\(I \cap J\) is an ideal \(\) (Exercise 17)

2. Sum

If \(I, J\) are ideals in \(R\)

\(K = \{a+b \mid a \in I, b \in J\}\)

is an ideal in \(R\).

Denoted by \(I + J\). \(\) (Exercise 20)

3. Product

If \(I, J\) are ideals in \(R\)

\(IJ = \{a_ib_i + \cdots + a_nb_n \mid n \geq 1, a_i \in I, b_i \in J\}\)

is an ideal in \(R\).
Def  Let \( f: R \to S \) be a ring homomorphism. Then

\[ \ker f = \{ r \in R \mid f(r) = 0_S \} \]

is an ideal of \( R \).

and

\[ \text{Im} f = \{ f(r) \mid r \in R \} \]

is a subring of \( S \). (check both)

Tho  (First Isomorphism Theorem)

Let \( f: R \to S \) be a ring homomorphism. Then

\[ R / \ker f \cong \text{Im} f. \]

In particular, if \( f \) is surjective, then \( R / \ker f \cong S \).

proof) We prove that \( R / \ker f \cong \text{Im} f \).

Define \( \overline{f}: R / \ker f \to S \) by

\[ \overline{f}(r + \ker f) = f(r). \]

Then

1. \( \overline{f} \) is well-defined: if \( r_1, r_2 \in R \), and

\[ r_1 - r_2 \in \ker f, \]

then

\[ f(r_1 - r_2) = f(r_1) - f(r_2) = 0 \]

so

\[ f(r_1) = f(r_2). \]

2. \( \overline{f} \) is a ring homomorphism: If \( r_1, r_2 \in R \)

\[ \overline{f}(r_1 + \ker f + (r_2 + \ker f)) = \overline{f}(r_1 + r_2 + \ker f) = f(r_1 + r_2) = f(r_1) + f(r_2) = \overline{f}(r_1 + \ker f) + \overline{f}(r_2 + \ker f). \]
\[
\overline{f}((r_1 + \ker f)(r_2 + \ker f)) = \overline{f}(r_1 r_2 + \ker f)
\]
\[
= f(r_1 r_2)
\]
\[
= f(r_1)f(r_2)
\]
\[
= \overline{f}(r_1 + \ker f)\overline{f}(r_2 + \ker f)
\]

3. \(\overline{f}\) is injective: We check that \(\ker \overline{f} = (0)_{\mathbb{R}/\ker f}\)

Let \(r \in \mathbb{R}\) with \(\overline{f}(r + \ker f) = 0\).

Then \(f(r) = 0\), so \(r \in \ker f\).

Thus \(r + \ker f = 0 \mod {\ker f}\), hence \(\ker \overline{f} = (0)_{\mathbb{R}/\ker f}\).

4. \(\overline{f}\) is surjective: Let \(s \in \text{Im} \overline{f}\). Then \(s = f(r)\) for some \(r \in \mathbb{R}\).

We show that there is an element in \(\mathbb{R}/\ker f\) that maps to \(s\). Simply, take the \(r + \ker f\). Then we see that \(\overline{f}(r + \ker f) = f(r) = s\).
Prime and Maximal Ideals

**Def** P : ideal in a commutative ring R. P \subseteq R.

Whenever b \in P then b \in P or c \in P.

**Thm 6.14** Let P be an ideal in a commutative ring R with identity. Then P is a prime ideal if and only if the quotient ring R/P is an integral domain.

**Proof** ($\Rightarrow$) Let \( a + P, b + P \in R/P \) with \( a, b \in R \).

**Prop** Suppose that \((a + P)(b + P) = 0_{R/P}\).

Then \( ab + P = 0_{R/P} \), so \( ab \in P \).

Since P is a prime ideal, \( a \in P \) or \( b \in P \).

Thus \( a + P = 0_{R/P} \) or \( b + P = 0_{R/P} \).

**Prop** ($\Leftarrow$) Let \( ab \in P \) with \( a, b \in R \). We have \((a + P)(b + P) = 0_{R/P}\). Since \( R/P \) is an integral domain, \( a + P = 0_{R/P} \) or \( b + P = 0_{R/P} \).

Equivalently \( a \in P \) or \( b \in P \).

For \( R/P \) to be an integral domain, we also need \( 1_{R/P} \neq 0_{R/P} \). This is true by \( P \not\subseteq R \). (check)

In fact, \( 1_{R/P} \neq 0_{R/P} \) ($\Rightarrow$) \( P \not\subseteq R \).
**Def**: An ideal $M$ in a ring $R$ is said to be maximal if $M \neq R$ and whenever $J$ is an ideal such that $M \subseteq J \subseteq R$, then $M = J$ or $J = R$.

**Thm 6.15**: Let $M$ be an ideal in a commutative ring $R$ with identity. Then $M$ is a maximal ideal if and only if the quotient ring $R/M$ is a field.

**Proof**: Let $a + M$ with $a \in R$ be a nonzero element in $R/M$. Then $a + M$.

Consider $J = M + (a)$. This is an ideal of $R$ containing $M$. Then $J = M$ or $J = R$. Since $a + M$, we must have $J = R$. Thus, $M + (a) = R$.

There is $m \in M, b \in R$ such

$$m + a \cdot b = 1_R.$$ 

Then we have $(a + M)(b + M) = 1_{R/M}$. 
Suppose that any nonzero element $a + M \in R/M$ is a unit in $R/M$. Let $J$ be an ideal of $R$ containing $M$ and $J \supseteq M$.

Then $J$ contains an element $j \in M$. We have $j + M \neq 0_{R/M}$. Since this element has a multiplicative inverse, there is an element $b + M$ with $b \in R$ such that $(j + M)(b + M) = 1_{R/M}$. Then for some $m \in M$, $j \cdot b - 1_R = m$.

Since $M \subseteq J$, $m \in J$. Also $j \cdot b \in J$.

Thus $1_R \in J$, which shows that $J = R$.

**Exercise**

Take care of relation between $R \supseteq M$, and $1_{R/M} \neq 0_{R/M}$.

**Cor 6.16.** In a commutative ring with identity, every maximal ideal is prime.
ex) \( \mathbb{Z}[x]/(x) = \mathbb{Z} \), \((x)\) is not maximal.

ex) \( \mathbb{Z}[x]/(2) = \mathbb{Z}_2[x] \), \((2)\) is not maximal.

ex) \( \mathbb{Z}[x]/(x,2) = \mathbb{Z}_2 \), \((x,2)\) is maximal.

General question: What are the maximal ideals in \( \mathbb{Z}[x] \)?

If \( F \) is a field, then \((p(x))\) with \( p \) irreducible
is maximal. \( (F[x]/(p(x)) \) is an extension

\[ \text{field of } F \text{ containing a root of } P(x) \]

In fact, any maximal ideal is of this form.

cf. PF- Ideals Prob 2, Theorem 5.11
Exercise 3 (b), p 166.

In \( F[x] \), Prime Ideals = Maximal Ideals.

(can you prove it?)