Def/Theorem: Let $R$ be a ring, $I$ an ideal.

\[ R/I = \text{Quotient ring of } R \text{ modulo } I \]

**Thm:** The Factor group $R/I$ is a ring with multiplication given by

\[ (r+I)(s+I) = rs + I \]

(\( \forall r+I, s+I \in R/I \))

**Proof:**

- We know $R/I$ is an Abelian under addition, i.e., $r+I + s+I = (r+s)+I$.

**Show that mul. is well defined.**

Let $s+I, r+I \in R/I$, let $\hat{s} \in r+I \iff r+I = r+I$.

**Show** $\hat{s}\hat{r} = rs + I$

$\hat{r} \in r+I \iff \exists \alpha \in I \text{ s.t. } r = r+\alpha$

$\hat{s} \in s+I \iff \exists \beta \in I \text{ s.t. } s = s + \beta$

$\hat{s}\hat{r} = (r+\alpha)(s+\beta) = rs + rs + rb + ab$

$\because I \text{ is an ideal}$

\[ \hat{s}\hat{r} \in rs + I \]

$\therefore \hat{s}\hat{r} + I = rs + I$

**Distributivity**

Say $r+I, s+I, w+I \in R/I$

**Show**
\[(r+I) \cdot (s+I) + (w+I) = r+I \cdot (s+w+I)\]
\[= r(s+w) + I\]
\[= (rs + rw) + I\]
\[= (rs + I) + (rw + I)\]
\[= (r + I)(s + I) + (r + I)(w + I)\]

Associativity is similar...

**Theorem.** Let \( I \) be an ideal in a ring \( R \).

The map \( \Psi: R \rightarrow R/I \) where \( r \mapsto r+I \) is a ring hom.

and \( \ker(\Psi) = I \).

**Proof:** From groups we know

\[\Psi: R \rightarrow R/I \text{ is a surjective group hom.}\]

Show \( \Psi \) is a ring hom.

\[\Psi(r) \cdot \Psi(s) = (r+I)(s+I) = rs + I = \Psi(rs)\]

From groups \( \ker(\Psi) = I \)

\[\Psi: R \rightarrow R/I \text{ is sometimes called the natural or canonical ring hom.}\]
**Thm.** (First Isomorphism Thm. for rings)

Let \( \phi : R \to S \) be a ring homomorphism.

Let \( \psi : R \to R/\ker(\phi) \) be the canonical hom. Then there exists a unique isomorphism \( \pi : R/\ker(\phi) \to \phi(R) \) such that \( \phi = \pi \circ \psi \).

In particular \( \phi(R) \cong R/\ker(\phi) \)

\[ \begin{array}{c}
R \\ \phi \downarrow \\
\psi \\
\downarrow \exists ! \pi \\
R/\ker(\phi) \\
\end{array} \]

**Proof:** Let \( k = \ker(\phi) \). By the 1st iso. thm. for groups \( \exists \) a unique (well defined) group isomorphism \( \pi : R/k \to \phi(R) \)

\[ r + k \mapsto \phi(r) \]

\( \therefore \) we need only show that \( \pi \) is a ring hom.

\[ \pi((r+k)(s+k)) = \pi(rs+k) = \phi(rs) = \phi(r)\phi(s) = \pi(r+k)\pi(s+k) . \]
**Theorem (Second Isom. Theorem)**

Let $I$ be a subring of a ring $R$, and let $J$ be an ideal of $R$. Then $I + NJ$ is an ideal of $I$ and

$$I/(INJ) \cong (I+J)/J \cong \{a+b \mid a \in I, b \in J\}.$$

**Proof:**

1. Show $I + J$ is a subring of $R$.
   - We know $I + J$ is an abelian subgroup.
   - Let $a, \hat{a} \in I$, $b, \hat{b} \in J$
   - $(a+b)(\hat{a}+\hat{b}) = a\hat{a} + (b\hat{a} + a\hat{b} + b\hat{b}) \\ \in I + J$
   - Hence, $(a+b)(\hat{a}+\hat{b}) \in I + J$

2. Show $J$ is an ideal of $I + J$:
   - Let $a \in I$, $b \in J$.
   - Since $J$ is an ideal of $R$, and also a subring, since $J$ is an ideal of $R$.
   - Show for any $a + b \in I + J$ that $(a + b)c \in J$.
   - $(a+b)c = a(c) + b(c) \in J$
   - Hence, $(a+b)c \in J + J$
   - Thus, $J$ is an ideal of $I + J$.

From Homework we know $INJ$ is an ideal of $I$. 
Now define \( \phi: I \rightarrow (I+J)/J \)
\[
\begin{align*}
\phi & : I \rightarrow (I+J)/J \\
\phi(a) & : a + J \\
& = a + J
\end{align*}
\]

Show \( \phi \) is a hom. of rings

\[
\phi(a_1 + a_2) = a_1 + a_2 + J = (a_1 + J) + (a_2 + J) \\
= \phi(a_1) + \phi(a_2)
\]

\[
\phi(a_1 a_2) = a_1 a_2 + J = (a_1 + J)(a_2 + J) = \phi(a_1) \phi(a_2)
\]

Want \( \phi(I) = I + J/J \), i.e. \( \phi \) to be onto.

\( \phi \) is onto since \( \forall a \in I \) be \( J \)

\[
\begin{align*}
\phi(a) & = (a + J) \\
& \text{any element of } I + J/J
\end{align*}
\]

\[
\text{ker}(\phi) = \{ a \in I \mid \phi(a) = 0 + J \} \\
= \{ a \in I \mid a \in J \} \\
= I \cap J \\
\therefore I \cap J \text{ is an ideal}
\]

\( \therefore \phi: I \rightarrow (I+J)/J \) is an onto ring hom.

By the first isom. Thm., for rings

\[
\phi(I) \cong I/\text{ker}(\phi) \\
I + J/J \cong I/\text{I} \cap \text{J}
\]
**Third Isomorphism**

Let \( R \) be a ring, \( I, J \) ideals where \( J \subseteq I \).
Then
\[
R / I \cong (R / J) / (I / J)
\]

**Correspondence**

Let \( S \) be a subring of \( R \) and \( I \) an ideal of \( R \).
Then \( S \rightarrow S / I \) is a 1-1 correspondence (\( I \subseteq S \))

\[
\begin{cases}
\{ \text{Subrings of } R \text{ s.t. } I \subseteq S \} \\
\{ \text{Subrings of } R / I \}
\end{cases}
\] \( 
\xrightarrow{1-1}
\) \( 
\begin{cases}
\{ \text{Ideals of } R \text{ s.t. } I \subseteq S \} \\
\{ \text{Ideals of } R / I \}
\end{cases}
\]

**Maximal and Prime Ideals**

When is \( R / I \) a field? an integral domain?

Idea: (This week's homework)

The only ideals in a field \( R \) are \( \{0\} \) and \( R \).
Since if \( I \) is an ideal in \( R \) and \( I \neq \{0\} \),
if \( r \in I \), \( r \neq 0 \) \( \Rightarrow r^{-1} \in R \) since \( I \) is an ideal,
\( r^{-1} r \in I \) \( \Rightarrow 1 \in I \)
\( \Rightarrow s \cdot 1 \in I \) \( \forall s \in R \)
\( \Rightarrow I = R \).
**Definition:** A proper ideal \( M \) of a ring \( R \) is called a **maximal ideal** if:

- \( M \) is not a proper subset of any ideal of \( R \) other than \( R \).

Equivalently:

- \( M \) is maximal if for any ideal \( I \) of \( R \) with \( M \subset I \), \( I = R \).

**Theorem:** Let \( R \) be a commutative ring with \( 1 \in R \) and let \( M \) be an ideal of \( R \). \( M \) is maximal if and only if \( R/M \) is a field.

**Proof:**

Let \( M \) be a maximal ideal in \( R \).

\[ R \text{ commutative} \implies R/M \text{ commutative} \]

\[ 1 + M \text{ is the identity in } R/M \]

Show inverses exist for non-zero elements of \( R/M \):

If \( a + M \neq 0 + M \) in \( R/M \), \( a + M \)

Fix \( a + M \neq 0 + M \in R/M \).

Let \( I = \{ ra + M \mid r \in R, m \in M \} \subseteq R \)

Show \( I \) is an ideal:

- \( I \) non-empty since \( 0 + 0 = 0 \in I \).
- Let \( r_1a + M, r_2o + M \in I \)
\[ r_1a + m_1 - (r_2a + m_2) = \underbrace{(r_1 - r_2)}_{\in \mathbb{R}} a + \underbrace{(m_1 - m_2)}_{\in \mathbb{M}} \in I \]

For any \( \tilde{r} \in R \)
\[ \tilde{r}(ra + m) = \tilde{r}ra + \tilde{r}m \in I \]
\( I \) is an ideal.

\( M \) is maximal, and \( M \cap I \) by construction since \( a + m = 0 + m \)
\[ I = \{ ra + m \mid r \in R, m \in M \} \subseteq R \]

\[ \Rightarrow I = R \quad \text{and} \quad I = R \Rightarrow \exists! \in I \]
\[ \therefore \exists! b \in R \text{ s.t. } 1 = ba + m \]
\[ l + m = (ba + m) + M = (ab + m) + M \]
\[ = ab + m = (a + m)(b + m) \]
\[ = (b + m)(a + m) \]
\[ \therefore \text{by def. } (a + m)^{-1} = b + m \text{ in } R/M \]
\[ \therefore R/M \text{ is a field}. \]

Now suppose \( M \) is an ideal and \( R/M \) is a field,
show \( M \) is maximal.
\[ \Rightarrow 0 + M, 1 + m \in R/M \]
\[
: M \not\subset R \quad \text{(since } r \notin M = R \quad R/M = \{0 + m\} \text{)} \\
: \quad M \not\subset R
\]

Let \( I \) be any ideal of \( R \). Show \( I = R \).

Show \( I = R \).

Pick \( a \in I \), \( a + M \neq 0 + M \)

\[\Rightarrow \exists b + M \ \text{s.t.} \quad (a + M)(b + M) = (1 + M) \quad (a + M)^{-1} \quad (ab + M)\]

\[\Rightarrow \exists m \in M \ \text{s.t.} \quad ab + m = 1 \quad \text{since } I \text{ is an ideal} \]

but \( ab + m \in I \quad \text{and } I \text{ is an ideal} \)

\[\therefore 1 \in I \Rightarrow n \cdot 1 = n \in I \quad \forall n \in R \]

\[\Rightarrow I = R \]

\[\therefore M \text{ is a maximal ideal}. \]

Ex 1

\( \mathbb{Z} \) is a maximal ideal in \( \mathbb{Z} \) for \( p \) prime

since \( \mathbb{Z}/p\mathbb{Z} \) is a field

Def 1

A proper ideal \( P \) in a commutative ring \( R \) is called a \textbf{prime ideal} if whenever \( ab \in P \)

then either \( a \in P \) or \( b \in P \).
Example: \( P = \{ 0, 1, \ldots, 10 \} = 2\mathbb{Z} \) in \( \mathbb{Z}_{12} \) is a prime ideal.

**Proposition:** Let \( R \) be a commutative ring with \( 1 \in R, 1 \neq 0 \). Then \( P \) is a prime ideal in \( R \) if and only if \( R/P \) is an integral domain.

**Proof:**
First let \( P \) be an ideal of \( R \), and let \( R/P \) be an integral domain.
Show \( P \) is prime.
Suppose \( ab \in P \) then
\[
ab + P = 0 + P
\]
\[
\Rightarrow (a + P)(b + P) = 0 + P
\]
\[
\therefore \text{since } R/P \text{ is an integral domain}
\]
\[
\Rightarrow \text{Either } a + P = 0 + P \text{ or } b + P = 0 + P
\]
\[
\therefore \text{either } a \in P \text{ or } b \in P
\]
\[
\therefore P \text{ is a prime ideal.}
\]

Now suppose \( P \) is prime, show \( R/P \) has no zero divisors.
Suppose \( (a + P)(b + P) = 0 + P \)
\[
ab + P = 0 + P
\]
\[ a \in P \quad \Rightarrow \quad a \text{ or } b \in P \]

\[ \Rightarrow \quad \text{either } a+P = 0+P \text{ or } b+P = 0+P \]

\[ \therefore \quad R/P \text{ is an integral domain} \]

Every field is in particular an integral domain.

\[ \text{(Cor.) Every maximal ideal in a commutative ring } R \]

\[ \text{with } 1 \in R \text{ is also prime.} \]

\[ \text{Proof:} \quad R/I \text{ a field } \Leftrightarrow I \text{ maximal} \]

\[ \quad \uparrow \quad \text{This is also an integral domain} \]

\[ \quad \therefore \quad I \text{ is prime.} \]

\[ x \equiv r \mod I \Leftrightarrow x + I = r + I \]

\[ \text{Poly nominal Rings} \]

Let \( R \) be a commutative ring with 1\( \in R \)

Any expression

\[ f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n \]

\[ a_i \in R \quad 1 \in R \implies \text{poly nominal with coefficients} \]

\[ \text{in } R \text{ and intermediate } x. \]
\( a_n \) - leading coefficient

\( a_n x^n \) - leading term

If \( a_n = 1 \), call \( f(x) \) monic.

If \( n \) is the largest non-negative integer s.t.

\[ a_n \to 0 \implies \deg(f) = n \]

degree of \( f(x) \) is \( n \).

If no such \( n \) exists \( \implies f \equiv 0 \)

\[ \deg(0) = -\infty \]

\[ a_0 + a_1 x + \ldots + a_n x^n = b_0 + b_1 x + \ldots + b_m x^m \]

If and only if \( a_i = b_i \ \forall \ i \geq 0 \)

\( \mathbb{R}[x] = \) \{ set of polynomials \( f(x) \) in \( \mathbb{R} \) with coefficients in \( \mathbb{R} \) \}

Addition is given by

\[
\begin{align*}
    (a_0 + a_1 x + \ldots + a_n x^n) + (b_0 + b_1 x + \ldots + b_m x^m)
\end{align*}
\]

\[ \text{s.t. } n \geq m \]

\[ \Rightarrow (a_0 + b_0) + (a_1 + b_1) x + \ldots + (a_n + b_n) x^n \]

\( m \geq n \).

\[ p(x) q(x) = \sum_{i=0}^{m+n} \left( \sum_{k=0}^{i} a_k b_{i-k} \right) x^i \]
Example: work in \( \mathbb{Z}_2[x] \)

\[
P(x) = 3 + 3x^3, \quad q(x) = 4 + 4x^2 + 4x^4
\]

\[
P(x) + q(x) = 7 + 4x^2 + 3x^3 + 4x^4
\]

\[
P(x)q(x) = 0
\]

Theorem: Let \( R \) be a commutative ring with \( 1 \). \( R[x] \) is a commutative ring with identity.

Proof:

Show \( R[x] \) is an additive abelian group.

1. \( f(x) = 0 \in R[x] = \text{add. identity} \)

2. Add. inverse of \( p(x) = \sum a_i x^i \) is \( -p(x) = \sum -a_i x^i \)

3. Poly. add is commutative since done in coefficients.

Show mult. properties, i.e. mult. is associative, distributive.

Note \( f(x) = 1 \in R[x] \)

Show mult. is associative like

\[
P(x) = \sum_{i=0}^{n} a_i x^i, \quad q(x) = \sum_{i=0}^{n} b_i x^i, \quad r(x) = \sum_{i=0}^{s} c_i x^i
\]

\[
(p(x) \cdot q(x)) \cdot r(x) = \left[ \left( \sum_{i=0}^{n} a_i x^i \right) \left( \sum_{i=0}^{n} b_i x^i \right) \right] \left( \sum_{i=0}^{s} c_i x^i \right)
\]

\[
= \left[ \sum_{i=0}^{\min(n,s)} \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^i \right] \left( \sum_{i=0}^{s} c_i x^i \right)
\]
\[
\begin{align*}
&= \sum_{i=0}^{m+n+5} \left( \sum_{j=0}^{i} \left( \sum_{k=0}^{j} a_r b_{i-j-k} \right) c_{i-j} \right) x^i \\
&= \sum_{i=0}^{m+n+5} \left( \sum_{j=0}^{i} \left( \sum_{k=0}^{j} b_{i-j-k} c_{i-j} \right) \right) x^i \\
&= \sum_{i=0}^{m+n+5} \left[ \sum_{j=0}^{i} a_r \left( \sum_{k=0}^{j} b_{i-j-k} c_{i-j} \right) \right] x^i \\
&= \left( \sum_{i=0}^{m-a} a_i x^i \right) \left[ \sum_{i=0}^{n-a} \left( \sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right] \\
&= p(x) \left[ q(x) \cdot r(x) \right]
\end{align*}
\]

**Proposition**

Let \( p(x), q(x) \in R[x] \) where \( R \) is an integral domain. Then \( \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) \)

and \( R[x] \) is an integral domain.

**Proof:**

Let \( p, q \in R[x] \), \( p \neq 0, q \neq 0 \)

\[
p = a_m x^m + \cdots + a_1 x + a_0
\]

\[
q = b_n x^n + \cdots + b_0
\]

\( \deg(p) = m, \quad \deg(q) = n \), leading term of \( p(x)q(x) \)

is \( a_m x^m \cdot b_n x^n \) since \( a_m \neq 0, b_n \neq 0 \) and \( R \) is an integral domain.

\( \therefore \) \( \deg(p \cdot q) = m + n \)
and further \( p(x) \neq 0 \) since its leading term is non-zero

\[ \therefore R[x] \text{ is an integral domain.} \]

**Multivariate Polynomial Rings**

i.e. \[ f = x^2 - 3xy + 2y^3 \]

- \( R[x] \) is a commutative ring with 1 (since \( R \) is comm. \& 1 exists)

\[
(R[x])[y] \quad \text{commutative ring with } 1
\]

\[
(R[y])[x] \quad \text{commutative ring with } 1
\]

Show \( (R[x])[y] \cong (R[y])[x] \).