Ideals & Quotient Rings

Let \((R, +, \cdot)\) be a ring. Let \(S \subseteq R\) be a subring.

Since \(S \subseteq R\), then we can form the set of left cosets.

\[
R/S = \{ r + S \mid r \in R \}
\]

**Goal:** Create a new ring from \(R, S\) and \(R/S\).

**Question:** How do we give \(R/S\) the ring structure?

**A natural way:**
\[
(a + S) + (b + S) = (a + b) + S
\]
\[
(a + S) \cdot (b + S) = (ab) + S
\]
1. Addition of classes is well-defined because $S \subseteq R$. \checkmark \quad \text{because} \quad (R,+) \quad \text{is an abelian group}.
2. $(R/S, +)$ is an abelian group. \checkmark
3. Multiplication of classes is well-defined \xmark
4. Multiplication of classes is associative \checkmark \quad \text{because} \quad (R,+,:)$ is a ring
5. The distributive laws of classes hold. \checkmark

$$a + S = b + S$$
and
$$c + S = d + S$$

$\Rightarrow (a + S) \cdot (c + S) = (b + S) \cdot (d + S)$

$\iff \forall r \in R. \forall s \in S$

$rs \in S \text{ and } sr \in S$

\! Multiplication of classes is well-defined if and only if \times is true

Observe that not any subring satisfies \times: \quad \text{R is a subring of C. i.e. C and } 2 \in R \text{ but } 2i \notin R.

When a subring satisfies \times, then $R/S$ has a well-defined multiplication and becomes a ring. \(\wink\)
Subrings with property ⋅ deserve a name:

**Def:** A subring $I$ of a ring $R$ is called an ideal of $R$ if $ra \in I$ and $ar \in I$ for all $r \in R$ and $a \in I$.

$I \subseteq R$ is an ideal if $I$ "absorbs" $R$ from the left and the right.

**Ex:**

1. If a ring then $R$ and $\{0\}$ are ideals called trivial ideals.

2. $\mathbb{Z}$: $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all $n \in \mathbb{Z}$.

3. $\mathbb{Z}[x]$:

   \[ I = \left\{ a_1 x^2 + \ldots + a_n x^n \mid a_i \in \mathbb{Z} \text{ and } n = 2, 3, \ldots \right\} \text{ is an ideal of } \mathbb{Z}[x], \]

   \[ J = \left\{ p(x) \in \mathbb{Z}[x] \mid p(0) \in 2 \mathbb{Z} \right\} \text{ is an ideal of } \mathbb{Z}[x]. \]
4. \( F(\mathbb{R}, \mathbb{R}) : S = \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable} \} \) is not an ideal of \( F(\mathbb{R}, \mathbb{R}) \).

**Theorem: Ideal Test**

Let \( I \) a subset of a ring \( R \).

\[
I \text{ is an ideal of } R \iff (1) \ I \neq \emptyset \\
(2) \ a-b \in I \quad \forall a, b \in I \\
(3) \ ra \text{ and } ar \quad \forall r \in R \quad \forall a \in I
\]

**Proof:** \((\Rightarrow) \checkmark\)

\((\Leftarrow)\) From (1) and (2), \( I \) is a subgroup of \( R \). From (3), \( I \) absorbs \( R \) on the left/right.

WTS: \( ab \in I \) for all \( a, b \in I \).

Since \( a \in R \) and \( b \in I \), then \( ab \in I \) by (3).
Theorem 10: A subring $I \subseteq R$ is an ideal $\iff$ (if $a+I = b+I$ and $c+I = d+I$, then

$$(ac)+I = (bd)+I, \quad \forall a, b, c, d \in R$$

Proof:

$(\Rightarrow)$ Suppose $a+I = b+I$ and $c+I = d+I$, i.e., $a-b \in I$ and $c-d \in I$ by Lemma 27.

WTS: $ac-bd \in I$.

$$ac-bd = ac-bc + bc-bd = (a-b)c + b(c-d) \in I$$

$I$ absorbs on the right $I$ on the left

$(\Leftarrow)$ Since $I \subseteq R$ is a subring, we only need to prove that $ra$ and $ar \forall r \in R, a \in I$.

Let $r \in R$ and $a \in I$, then $a+I = I$ and $r+I = r+I$. By hypothesis,

$ar+I = 0r+I$ and $ra+I = r0+I$. Thus, $ar \in I$ and $ra \in I$. $\blacksquare$
Corollary 11: Let \((R, +, \cdot)\) be a ring and let \(I \subseteq R\) be an ideal. Then \(R/I = I/R\) is a ring under the operations\n\[(a + I) + (b + I) := (a + b) + I\quad \text{and} \quad (a + I) \cdot (b + I) := (ab) + I.\]

Moreover,\n\[(1) \text{ If } R \text{ has an identity, then } R/I \text{ has an identity, } 1_{R/I} = 1 + I.\]
\[(2) \text{ If } R \text{ is commutative, then } R/I \text{ is commutative.}\]

Proof: From Thm 10, \(\cdot\) is well-defined.

Def: Let \(I \subseteq R\) be an ideal of \(R\)
\[(1) \text{ } R/I \text{ is called the quotient ring of } R \text{ by } I.\]
\[(2) \text{ The ring homomorphism } \pi: R \rightarrow R/I \text{ given by } \pi(r) = r + I \text{ is called}\]
the natural projection of \(R\) onto \(R/I\).
Examples:

1. \( R/R = \{ R \} \cong \{ 0 \} \) and \( R/I_{01} = \{ \{ r \} \mid r \in R \} \cong R \)

2. \( \mathbb{Z}/n\mathbb{Z} = \{ n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z} \} \)

3. \( \mathbb{Z}[x]/I = \{ p(x) + I \mid p(x) \in \mathbb{Z}[x] \} \) where \( I = \{ a_2x^2 + \ldots + a_nx^n \mid a_i \in \mathbb{Z} \) and \( n = 2, 3, \ldots \} \)

\( \mathbb{Z}[x]/I \leftrightarrow \text{"I and polynomials of poly in } \mathbb{Z}[x] \text{ that fail to belong to } I" \)

\( (a_0 + a_1x) + I = (b_0 + b_1x) + I \iff (a_0 + a_1x) - (b_0 + b_1x) \in I \)

\( \iff (a_0 - b_0) - (a_1 - b_1)x = 0 \)

\( \iff a_0 = b_0 \) and \( a_1 = b_1 \)

Two classes \( p(x) + I, q(x) + I \) are equal iff they have the same constant terms and the same coefficients of \( x \).
\[ \mathbb{Z}[x]/I = \left\{ (a + b \cdot x) + I \mid a, b \in \mathbb{Z} \right\} \]

\[ \mathbb{Z}[x]/I \]

\[
\begin{array}{cccccc}
... & (2 + 2x) + I & (-2 + x) + I & x + I & (1 + 2x) + I & (2 + 2x) + I & ... \\
... & (-2 + x) + I & (-1 + x) + I & x + I & (1 + x) + I & (2 + x) + I & ... \\
... & (2) + I & (-1) + I & a_0 + x^2 + ... + a_n x^n & 1 + I & 2 + I & ... \\
... & (-2) + I & (-1) + I & x + I & (1 - x) + I & (2 - x) + I & ... \\
... & (-2 - x) + I & (-1 - x) + I & (-x) + I & (1 - x) + I & (2 - x) + I & ... \\
... & (-2 - 2x) + I & (-1 - 2x) + I & (-2x) + I & (1 - 2x) + I & (2 - 2x) + I & ... \\
\end{array}
\]

\[ \mathbb{Z}[x]/I \cong \mathbb{Z} \times \mathbb{Z} \]
\[
\mathbb{Z}[x]/J = \left\{ p(x) + J \mid p(x) \in \mathbb{Z}[x] \right\} \quad \text{where} \quad J = \left\{ p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z} \right\}
\]

\[
\mathbb{Z}[x]/J \quad \text{"J and packages of poly in } \mathbb{Z}[x] \text{ that fail to belong to J"}
\]

Let \( n > m \):

\[
\left( \sum_{i=0}^{m} a_i x^i \right) + J = \left( \sum_{i=0}^{n} b_i x^i \right) + J \iff \sum_{i=0}^{n} (a_i - b_i) x^i \in J
\]

\[\iff a_0 - b_0 \in 2\mathbb{Z}\]

\[\iff [a_0] = [b_0] \quad \text{in } \mathbb{Z}/2\]

Two classes \( p(x) + J \), \( q(x) + J \) are equal iff their constant terms are equal \( \text{mod } 2 \).

\[
\mathbb{Z}[x]/J = \{ J, 1 + J \}
\]

\[
\mathbb{Z}[x]/J \approx \mathbb{Z}/2
\]

\[
p(x) \in \mathbb{Z}[x]
\]

\[
p(0) \text{ is even} \]

\[
p(x) \in \mathbb{Z}[x]
\]

\[
p(0) \text{ is odd} \]