Ideals & Quotient Rings

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

Since $S \leq R$, 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 $S \trianglelefteq R$. ✓
2. $(R/S, +)$ is an abelian group. ✓

} because $(R,+)$ is an abelian group

Problem ⇝ 3. Multiplication of classes is well-defined ✗

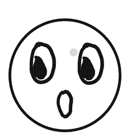
4. Multiplication of classes is associative. ✓
5. The distributive laws of classes hold. ✓

} because $(R,+,\cdot)$ is a ring

$$\boxed{\begin{matrix} a+S = b+S \\ \text{and} \\ c+S = d+S \end{matrix} \Rightarrow (a+S)\cdot(c+S) = (b+S)\cdot(d+S)} \iff \overset{\ast}{\boxed{\begin{matrix} \forall r \in R \quad \forall s \in S \\ rs \in S \quad \text{and} \quad sr \in S \end{matrix}}}$$

⚠ Multiplication of classes is well-defined if and only if $\ast$ is true

Observe that not any subring satisfies $\ast$: $\mathbb{R}$ is a subring of $\mathbb{C}$. $i \in \mathbb{C}$ and $2 \in \mathbb{R}$ but $2i \notin \mathbb{R}$

When a subring satisfies $\ast$, then R/S has a well-defined multiplication and becomes a ring.  wow!

Subrings with property ✱ deserve a name:

Def: A subring I of a ring R is called an ideal of R if

$$ra \in I \quad \text{and} \quad ar \in I \quad \text{for all } r \in R \text{ and } a \in I.$$

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

Ex:

1. R 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. $\mathbb{Z}[x]$: $I := \{a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{Z} \text{ and } n = 2, 3, \dots\}$ is an ideal of $\mathbb{Z}[x]$,

   $J := \{p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$ is an ideal of $\mathbb{Z}[x]$.

4. $\mathcal{F}(\mathbb{R},\mathbb{R})$: $\quad S := \{ f : \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ is differentiable} \}$ is not an ideal of $\mathcal{F}(\mathbb{R},\mathbb{R})$.

Theorem: Ideal Test Let I a subset of a ring R.

I is an ideal of R $\iff$ (1) $I \neq \emptyset$

(2) $a - b \in I \quad \forall a, b \in I$

(3) ra and $ar \quad \forall r \in R \ \forall a \in I$

Proof: $(\Rightarrow)$ ✓

$(\Leftarrow)$ 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 of R $\iff$ $\left(\begin{array}{l} \text{If } a+I = b+I \text{ and } c+I = d+I, \text{ then} \\ (ac)+I = (bd)+I. \quad \forall a,b,c,d \in R \end{array} \right)$

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: $ac - bd \in I$.

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

I absorbs on the right

I absorbs on the left

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

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 $ra \in I$.

Corollary 11: Let $(R,+,\cdot)$ be a ring and let $I \subseteq R$ be an ideal. Then

$R/I = I\backslash R$ is a ring under the operations

$$(a+I)+(b+I) := (a+b)+I \quad \text{and} \quad (a+I)\cdot(b+I) := (ab)+I.$$

Moreover, (1) If R has an identity, then R/I has an identity, $1_{R/I} = 1+I$.

(2) If R is commutative, then R/I is commutative.

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

Def: Let $I \subseteq R$ be an ideal of R

(1) R/I is called the quotient ring of R by I.

(2) The ring homomorphism $\pi : R \longrightarrow R/I$ given by $\pi(r) = r + I$ is called the natural projection of R onto R/I.

Examples:

1. $R/R = \{R\} \cong \{0\}$ and $R/\{0\} = \{\{r\} \mid r \in R\} \cong R$

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

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

$\mathbb{Z}[x]/I \leftarrow$ "I and packages of poly in $\mathbb{Z}[x]$ that fail to belong to I"

$$(a_0 + a_1x) + I = (b_0 + b_1x) + I \iff (a_0 + a_1x) - (b_0 + b_1x) \in I$$
$$\iff (a_0 - b_0) - (a_1 - b_1)x = 0$$
$$\iff a_0 = b_0 \text{ and } a_1 = b_1$$

Two classes $p(x)+I$, $q(x)+I$ are equal iff they have the same constant terms and the same coefficients of x.

$$\mathbb{Z}[x]/I = \{ (a+bx)+I \mid a,b \in \mathbb{Z} \}$$

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

$$\begin{array}{ccccccc}
 & \vdots & \vdots & \vdots & \vdots & \vdots & \\
\cdots & (-2+2x)+I & (-2+x)+I & 2x+I & (1+2x)+I & (2+2x)+I & \cdots \\
\cdots & (-2+x)+I & (-1+x)+I & x+I & (1+x)+I & (2+x)+I & \cdots \\
\cdots & (-2)+I & (-1)+I & \boxed{\begin{array}{c} a_2x^2+\cdots+a_nx^n \\ a_i \in \mathbb{Z} \text{ and } n=2,3,\ldots \end{array}} & 1+I & 2+I & \cdots \\
\cdots & (-2-x)+I & (-1-x)+I & (-x)+I & (1-x)+I & (2-x)+I & \cdots \\
\cdots & (-2-2x)+I & (-1-2x)+I & (-2x)+I & (1-2x)+I & (2-2x)+I & \cdots \\
 & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

$$\mathbb{Z}[x]/I \cong \mathbb{Z} \times \mathbb{Z}$$

4) $\mathbb{Z}[x]/J = \{ p(x) + J \mid p(x) \in \mathbb{Z}[x] \}$ where $J := \{ p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z} \}$

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

Let $n \geq m$.

$$\underbrace{\left(\sum_{i=0}^{m} a_i x^i\right)}_{p(x)} + J = \underbrace{\left(\sum_{i=0}^{n} b_i x^i\right)}_{q(x)} + J \iff \sum_{i=0}^{n} (a_i - b_i) x^i \in J$$

$$\iff a_0 - b_0 \in 2\mathbb{Z}$$

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

Two classes $p(x) + J$, $q(x) + J$ are equal iff their constant terms are equal mod 2

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

$\mathbb{Z}[x]/J$

$\boxed{\begin{array}{l} p(x) \in \mathbb{Z}[x] \\ p(0) \text{ is even} \end{array}}$ $\boxed{\begin{array}{l} p(x) \in \mathbb{Z}[x] \\ p(0) \text{ is odd} \end{array}}$

$\mathbb{Z}[x]/J \cong \mathbb{Z}/2$