# MTHSC 412 Section 6.1 – Ideals and Congruence

Kevin James

## Definition

Suppose that $I$ is a subring of a ring $R$. We say that $I$ is an ideal and write $I \trianglelefteq R$ (or $I \triangleleft R$ if $I \neq R$) if whenever $a \in I$ and $r \in R$, $ra, ar \in I$.

## Example

1. $\{0_R\} \trianglelefteq R$.
2. $3\mathbb{Z} \triangleleft \mathbb{Z}$.
3. For $f \in F[x]$, put $(f) = \{gf \mid g \in F[x]\}$. Then $(f) \trianglelefteq F[x]$.
4. Let $S = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Is $S$ and ideal of $\mathbb{M}_2(\mathbb{R})$.

### Theorem

*Suppose that $R$ is a ring. Then a nonempty set $A \subseteq R$ is an ideal provided*

1. *if $a, b \in I$ then $a - b \in I$.*
2. *if $r \in R$ and $a \in I$ then $ar, ra \in I$.*

### Theorem

*Let $R$ be a commutative ring with identity. Suppose that $c \in R$ and let $(c) = \{cr \mid r \in R\}$. Then $(c) \trianglelefteq R$.*

### Definition

For $R$ a commutative ring with identity and $c \in R$, $(c)$ is called the <u>principal ideal generated by $c$</u>.

## Fact

*Every ideal of $\mathbb{Z}$ is principal.*

## Example

Let $I = \{f \in \mathbb{Z}[x] \mid 3|f(0)\}$. Then, $I \lhd \mathbb{Z}[x]$. However, $I$ is not principal.

### Theorem

*Suppose that $R$ is a commutative ring with identity and that $c_1, \ldots, c_n \in R$. Then the set $I = \{r_1 c_1 + \cdots + r_n c_n \mid r_i \in R\}$. is an ideal of $R$.*

### Definition

The ideal in the previous theorem is called <u>the ideal generated by $c_1, \ldots, c_n$</u> and is denoted by $(c_1, c_2, \ldots, c_n)$. Such an ideal is said to be <u>finitely generated</u>.

### Example

Consider the ideal $(3, x) \trianglelefteq \mathbb{Z}[x]$.

### Definition

Suppose that $R$ is a ring that that $I \trianglelefteq R$; $a, b \in R$. We say that $a$ is congruent to $b$ modulo the ideal $I$ and write $a \equiv b \pmod{I}$ if $(a - b) \in I$.

### Example

1. Let $R = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous}\}$, and let $I = \{f \in R \mid f(1) = 0$. Then $R$ is a commutative ring with identity and $I \trianglelefteq R$. Let $f(x) = x^2 + 2$ and $g(x) = 2x + 1$. Then $f \equiv g \pmod{I}$.
2. Let $R = \mathbb{Z}$ and $I = (3)$ then $a \equiv b \pmod{3}$ if and only if $a \equiv b \pmod{I}$.

**Theorem**

*Let $R$ be a ring and let $I \trianglelefteq R$. Then congruence modulo $I$ is an equivalence relation on $R$.*

**Theorem**

*Suppose that $I \trianglelefteq R$. If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$ then*

$$a + c \equiv b + d \pmod{I} \qquad \text{and} \qquad ac \equiv bd \pmod{I}.$$

## Note

Suppose that $I \trianglelefteq R$.

$$\begin{aligned} \{b \in R \mid b \equiv a \pmod{I}\} &= \{b \in R \mid (b-a) = i \in I\} \\ &= \{(a+i) \mid i \in I\} \end{aligned}$$

## Definition

The <u>congruence class of $a$ modulo $I$</u> is defined as

$$a + I = \{(a+i) \mid i \in I\}.$$

These congruence classes are also called the <u>cosets</u> of $I$.

## Theorem

*Suppose that* $I \trianglelefteq R$ *and* $a, c \in R$. *Then* $a \equiv c \pmod{I}$ *if and only if* $a + I = c + I$.

## Corollary

*Let* $I \trianglelefteq R$ *and* $a, c \in R$. *Then* $a + I$ *and* $c + I$ *are either disjoint or identical.*

## Example

1. Suppose that $R = \mathbb{Z}$ and $I = (4)$. Then the distinct cosets are $0 + (4) = [0], 1 + (4) = [1], 2 + (4) = [2]$ and $3 + (4) = [3]$.
2. Suppose that $R = Z[x]$ and $I = (3, x)$ then the distinct cosets are $0 + I$, $1 + I$ and $2 + I$.

**Definition**

Suppose that $I \trianglelefteq R$. Then the set of distinct cosets is usually denoted by $R/I$. That is,

$$R/I = \{r + I \mid r \in R\}.$$