1 Prime Ideals and Maximal Ideals

Definition 1.1: Prime Ideals

A **prime ideal** A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.

Consider the following examples:

- Consider $R = \mathbb{Z}$. The ideals of $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ for $n = 1, 2, \ldots$. We know that $2\mathbb{Z}$ is prime. So, if $nm \in 2\mathbb{Z}$, then $nm = 2k$, which is even. This implies that one of n or m is even, so $n \in 2\mathbb{Z}$ or $m \in 2\mathbb{Z}$.

  This is true in general. If p is prime, then $p\mathbb{Z}$ is a prime ideal. Recall that if $p|ab$, then $p|a$ or $p|b$ by Euclid's Lemma.

- Consider $6\mathbb{Z}$, which is not prime. We want to show that this is not a prime ideal. To do this, we want to find an $n, m \in \mathbb{Z}$ such that $nm \in 6\mathbb{Z}$ but $n, m \notin 6\mathbb{Z}$. An obvious example is $n = 2$ and $m = 3$.

  In general, if $n = st$ is composite, then $st \in n\mathbb{Z}$ but $s, t \notin n\mathbb{Z}$.

- Consider $R = \{0\}$. This is a prime ideal. Suppose $n, m \in \mathbb{Z}$ with $nm \in R$. Then, $nm = 0$ means that one of n or m is 0, which implies that $n \in R$ or $m \in R$.

Fact: $\{0\} \subseteq R$ is a prime ideal if and only if R is an integral domain.

Definition 1.2: Maximal Ideals

A **maximal ideal** of a commutative ring R is a proper ideal of R such that, when B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Put it another way, a maximal ideal I of a commutative ring R is a proper ideal which is not contained in any other proper ideals, i.e. if $I \subseteq A \subseteq R$ for some ideal A, then $A = I$ or $A = R$.

Theorem 1.1

Let R be a commutative ring with unity and $I \subseteq R$ an ideal. Then, R/I is an integral domain if and only if I is prime.

Proof. Suppose R/I is an integral domain. Suppose then that $a, b \in R$ with $ab \in I$. Then, $ab + I = 0 + I$. This further implies that $(a + I)(b + I) = 0 + I$. This implies that $a + I = 0 + I$ *or* $b + I = 0 + I$ by integral domain definition. By the definition of a coset, $a \in I$ or $b \in I$. Thus, I is prime.

Suppose now that I is prime. Suppose $a, b \in R$ with $(a + I)(b + I) = 0 + I$ with $ab + I = 0 + I$. This implies that $ab \in I$, which further means that $a \in I$ or $b \in I$ by prime. Thus, $a + I = 0 + I$ or $b + I = 0 + I$. Thus, R/I is an integral domain. □

Theorem 1.2

Let R be a commutative ring with unity and $I \subseteq R$ an ideal. Then, R/I is a field if and only if I is maximal.

Proof. Suppose R/I is a field. We want to show that if $I \subseteq A \subseteq R$, then $A = I$ or $A = R$.[a] Suppose $A \subseteq R$ is an ideal satisfying $I \subseteq A$ and $A \neq I$. The fact that $A \neq I$ implies that we can choose some $b \in A \setminus I$. This implies that $b + I \neq 0 + I$ and so $b + I \in R/I$ is a unit. This implies that there exists some $c + I \in R/I$ with $(b + I)(c + I) = 1 + I$, which further implies that $bc + I = 1 + I$. Thus, ... We know that $1 - bc \in A$, but $b \in A \setminus I \subseteq A$ so $bc \in A$ and thus $1 = (1 - bc) + bc \in A$. So, $R = R \cdot 1 \subseteq A$ so that $A = R$. Thus, I is maximal.

Suppose that I is maximal. We want to show that any $b + I \neq 0 + I$ is a unit in R/I. Choose some $b + I \in R/I$ with $b + I \neq 0 + I$, i.e. choose some $b \in R \setminus I$. Consider $B = \{rb + a \mid r \in R, a \in I\}$. Thus, $B = R$ by $I \subseteq B \subseteq R$ and $b \neq I$ $(b \in B, b \in I)$.[b] From there, $1 \in B$ which means that $1 = rb + a$ for some $r \in R$ and $a \in I$, which finally implies that $1 + I = (r + I)(b + I)$. □

[a] We can prove the fact that $I \subsetneq A \subseteq R$ and $A \neq I$ *implies that* $A = R$.

[b] Exercise: Show that B is an ideal with contains I

Corollary 1.1

All maximal ideals are prime ideals.

Proof. Suppose $I \subseteq R$ is maximal.

$$\begin{aligned} &R/I \text{ is a field.} \\ &\implies R/I \text{ is an integral domain.} \\ &\implies R/I \text{ is prime.} \end{aligned}$$

So, we are done. □

Remark: The converse is not true. Consider $\langle x \rangle \subseteq \mathbb{Z}[x]$. This is not maximal by $\langle x \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$.

$$\mathbb{Z}[x]/\langle x \rangle \longleftrightarrow \mathbb{Z}$$

$$f(x) + \langle x \rangle \longleftrightarrow f(0)$$

$$f(x) + \langle x \rangle = h(x) + \langle x \rangle \iff f(x) - h(x) = g(x)x \text{ for some } g(x) \iff f(0) - h(0) = 0$$

Thus, this ideal $\langle x \rangle$ is prime.