

MATH 4/51002
Maximal and Prime Ideals

We provide here proofs for some theorems and examples about maximal and prime ideals using only the relevant definitions. These were all done in class as well, but using more machinery. In particular, the Correspondence Theorem and the fact that a nonzero commutative ring is a field if and only if it has no nonzero proper ideals were used to prove Theorem 1. Theorem 1 and Theorem 2 were used in Example 1 and Example 2, respectively, and were used to prove Theorem 3. The proofs here are longer, but more instructive.

Theorem 1. *Let R be a commutative ring and let M be an ideal of R . The ideal M is a maximal ideal of R if and only if R/M is a field.*

Proof. Suppose first that M is a maximal ideal. In particular, $M \neq R$, so that R/M is a nonzero commutative ring. To show that R/M is a field, it therefore suffices to prove that every nonzero element of R/M is a unit.

Let $a + M$ be a nonzero element of R/M , hence $a + M \neq 0 + M$ and a is not an element of M . This if (a) is the principal ideal of R generated by a , then the sum $M + (a)$ is an ideal of R properly containing M (since $a \in M + (a)$ but $a \notin M$). By the maximality of M , this implies $M + (a) = R$.

In particular, we have $1 \in M + (a)$, so $1 = m + ra$ for some $m \in M$ and $r \in R$. Hence $1 - ra = m \in M$ and so $1 + M = ra + M = (r + M)(a + M)$, and therefore $a + M$ is a unit in R/M . Since every nonzero element of R/M is a unit, it follows that R/M is a field.

Now suppose conversely that R/M is a field, so that R/M is a nonzero commutative ring and $M \neq R$. Let I be an ideal of R properly containing M . Then there is an element $a \in I$ with $a \notin M$.

Since $a \notin M$, $a + M$ is a nonzero element of the field R/M , so $a + M$ has an inverse $r + M$ in R/M . Hence $ra + M = 1 + M$, so $1 - ra \in M \subseteq I$ and $1 - ra = b$ for some $b \in I$. Since I is an ideal and $a \in I$, we have $ra \in I$, and since $b \in I$, it follows that $1 = ra + b$ is in I . Since I is an ideal of R and contains 1, $I = R$. Hence any ideal of R properly containing M must equal R , so M is a maximal ideal of R . \square

Example 1. Maximal Ideals of \mathbb{Z}

We know that every ideal of \mathbb{Z} is principal, so is of the form $(a) = \{ra \mid r \in \mathbb{Z}\}$ for some $a \in \mathbb{Z}$. Since $(0) \subsetneq (2) \subsetneq \mathbb{Z}$, we know (0) is not maximal, and since $(1) = \mathbb{Z}$, we know (1) is not maximal.

Let a be an integer greater than 1. (As $(-a) = (a)$, we need not consider negative integers.) Notice that $(a) \subseteq (b)$ if and only if $a \in (b)$, hence if and only if $a = rb$ for some $r \in \mathbb{Z}$. Thus $(a) \subseteq (b)$ if and only if $b \mid a$.

It follows that the only ideals of \mathbb{Z} containing (a) are those generated by the factors of a . If a is prime, the only ideals containing (a) are therefore $(1) = \mathbb{Z}$ and (a) , and so (a) is maximal. On the other hand, if a is not prime, then $a = mn$ for some m, n with $1 < n < a$, hence $(a) \subsetneq (n) \subsetneq (1) = \mathbb{Z}$, and (a) is not maximal. Therefore, an ideal (a) of \mathbb{Z} is maximal if and only if a is prime.

Theorem 2. *Let R be a commutative ring and let P be an ideal of R . The ideal P is a prime ideal of R if and only if R/P is an integral domain.*

Proof. First suppose that P is a prime ideal. In particular, $P \neq R$, so that R/P is a nonzero commutative ring. To show that R/P is an integral domain, it therefore suffices to prove that R/P has no zero divisors.

Let $a+P, b+P$ be elements of R/P such that $(a+P)(b+P) = 0+P$. Then $ab+P = 0+P$, hence $ab \in P$. Since P is a prime ideal, this implies $a \in P$ or $b \in P$, hence $a+P = 0+P$ or $b+P = 0+P$. Therefore R/P has no zero divisors and so is an integral domain.

Conversely, suppose R/P is an integral domain, so in particular R/P is a nonzero ring and $P \neq R$. Let a, b be elements of R such that $ab \in P$. Then $ab+P = 0+P$ in R/P , and so $(a+P)(b+P) = 0+P$. Since R/P is an integral domain, this implies $a+P = 0+P$ or $b+P = 0+P$, that is, $a \in P$ or $b \in P$. Hence P is a prime ideal. \square

Example 2. Prime Ideals of \mathbb{Z}

Again, we know that every ideal of \mathbb{Z} is principal, so is of the form $(a) = \{ra \mid r \in \mathbb{Z}\}$ for some $a \in \mathbb{Z}$. Also, (0) is prime since for $a, b \in \mathbb{Z}$, we have $ab = 0$ if and only if $a = 0$ or $b = 0$. Suppose now n is a positive integer. (As in Example 1, we need not consider negative integers.)

If n is prime and $a, b \in \mathbb{Z}$ with $ab \in (n)$, then $n \mid ab$. By Euclid's Lemma, $n \mid a$ or $n \mid b$, as n is prime, hence $a \in (n)$ or $b \in (n)$. Hence if n is prime, then (n) is a prime ideal.

Suppose n is not prime. If $n = 1$, then $(n) = \mathbb{Z}$ is not a prime ideal. Otherwise, $n = ab$ with $1 < a < n$ and $1 < b < n$. Thus $ab \in (n)$, but n divides neither a nor b , so neither a nor b is in (n) . Hence (n) is not a prime ideal.

Therefore, an ideal of (n) of \mathbb{Z} is a prime ideal if and only if $n = 0$ or n is a prime number.

Theorem 3. *Let R be a commutative ring. If M is a maximal ideal of R , then M is a prime ideal of R .*

Proof. Let M be a maximal ideal of R , so $M \neq R$ in particular, and let $a, b \in R$ with $ab \in M$. Suppose $a \notin M$ and $b \notin M$. Then the ideals $(a) + M$ and $(b) + M$ properly contain the maximal ideal M , hence $(a) + M = (b) + M = R$.

Now $1 \in R$, so $1 \in (a) + M$ and $1 \in (b) + M$. Hence $1 = ra + m$ and $1 = sb + n$ for some $r, s \in R$ and $m, n \in M$, and we have

$$\begin{aligned} 1 &= (ra + m)(sb + n) \\ &= rasb + ran + msb + mn \\ &= rs(ab) + ran + sbm + mn. \end{aligned}$$

Since M is an ideal and ab, m, n are in M , this implies $1 = rs(ab) + ran + sbm + mn$ is an element of M . But then M is an ideal of R containing 1, hence $M = R$, a contradiction. Therefore, if $ab \in M$, then $a \in M$ or $b \in M$, that is, M is a prime ideal. \square