3.5 Lecture 14: Maximal and Prime Ideals

The goal of this section is to characterize those ideals of commutative rings with identity which correspond to factor rings that are either integral domains or fields.

Definition 45. *Let* R *be a ring. A two-sided ideal* I *of* R *is called* maximal *if* $I \neq R$ *and no proper two-sided ideal of* R *properly contains* I.

A *proper* ideal of R is an ideal that is not the whole ring R.

EXAMPLES

1. In $\mathbb{Z}$, the ideal $\langle 6 \rangle = 6\mathbb{Z}$ is not maximal since $\langle 3 \rangle$ is a proper ideal of $\mathbb{Z}$ properly containing $\langle 6 \rangle$.
2. In $\mathbb{Z}$, the ideal $\langle 5 \rangle$ is maximal. For suppose that I is an ideal of $\mathbb{Z}$ properly containing $\langle 5 \rangle$. Then there exists some $m \in I$ with $m \notin \langle 5 \rangle$, i.e. 5 does not divide m. Then $\gcd(5, m) = 1$ since 5 is prime, and we can write
$$1 = 5s + mt$$
for integers s and t. Since $5s \in I$ and $mt \in I$, this means $1 \in I$. Then $I = \mathbb{Z}$, and $\langle 5 \rangle$ is a maximal ideal in $\mathbb{Z}$.
3. The maximal ideals in $\mathbb{Z}$ are precisely the ideals of the form $\langle p \rangle$, where p is prime.

The following is a generalization of the statement that $\mathbb{Z}/n\mathbb{Z}$ is a field precisely when n is prime.

Theorem 46. *Let* R *be a commutative ring, and let* M *be an ideal of* R. *Then the factor ring* R/M *is a field if and only if* M *is a maximal ideal of* R.

COMMENT ON PROOF: There are two things to be shown here. We must show that if R/M is a field (i.e. if every non-zero element of R/M is a unit), then M is a maximal ideal of R. A useful strategy for doing this is to suppose that I is an ideal of R properly containing M, and try to show that I must be equal to R.

We must also show that if M *is* a maximal ideal of R, then every non-zero element of R/M is a unit. A strategy for doing this is as follows : if $a \in R$ does not belong to M (so $a + M$ is not the zero element in R/M), then the fact that M is maximal as an ideal of R means that the only ideal of R that contains both M and the element a is R itself. In particular the only ideal of R that contains both M and the element a contains the identity element of R.

Proof of Theorem 46: ($\Longleftarrow$) Suppose that R/M is a field and let I be an ideal of R properly containing M. Let $a \in I$, $a \notin M$. Then $a+M$ is not the zero element of R/M, and so $(a+M)(b+M) = 1 + M$, for some $b \in R$. Then $ab - 1 \in M$; let $m = ab - 1$. Now $1 = ab - m$ and so $1 \in I$ since $a \in I$ and $m \in I$. It follows that $I = R$ and so M is a maximal ideal of R.

($\Longrightarrow$): Suppose that M is a maximal ideal of R and let $a + M$ be a non-zero element of R/M. We need to show the existence of $b + m \in R/M$ with $(a + M)(b + M) = 1 + M$. This means $ab + M = 1 + M$, or $ab - 1 \in M$.

So we need to show that there exists $b \in R$ for which $ab - 1 \in M$. Let M' denote the set of elements of R of the form
$$ar + s, \text{ for some } r \in R \text{ and } s \in M.$$
Then M' is an ideal of R (check), and M' properly contains M since $a \in M'$ and $a \notin M$. Then $M' = R$ since M is a maximal ideal of R. In particular then $1 \in M'$ and $1 = ab + m$ for some $b \in R$ and $m \in M$. Then $ab - 1 \in M$ and
$$(a + M)(b + M) = 1 + M \text{ in } R/M.$$
So $a + M$ has an inverse in R/M as required. □

We will now characterize those ideals I of R for which R/I is an integral domain.

Definition 47. *Let* R *be a commutative ring. An ideal* I *of* R *is called* prime *if* $I \neq R$ *and whenever* $ab \in I$ *for elements* a *and* b *of* R*, either* $a \in I$ *or* $b \in I$.

EXAMPLE: The ideal $\langle 6 \rangle$ is not a prime ideal in $\mathbb{Z}$, since $2 \times 3 \in \langle 6 \rangle$ although neither 2 nor 3 belongs to $\langle 6 \rangle$. However the ideal $\langle 5 \rangle$ *is* prime in $\mathbb{Z}$, since the product of two integers is a multiple of 5 only if at least one of the two is a multiple of 5.

The prime ideals of $\mathbb{Z}$ are precisely the maximal ideals; they have the form $\langle p \rangle$ for a prime p.

Theorem 48. *Let* R *be a commutative ring, and let* I *be an ideal of* R*. Then the factor ring* R/I *is an integral domain if and only if* I *is a prime ideal of* R.

Proof: R/I is certainly a commutative ring, so we need to show that R/I contains zero-divisors if and only if I is not a prime ideal of R. So let $a + I,\ b + I$ be non-zero elements of R/I. This means neither a nor b belongs to I. We have $(a + I)(b + I) = 0 + I$ in R/I if and only if $ab \in I$. This happens for some pair a and b if and only if I is not prime. $\square$

Corollary 49. *Let* R *be a commutative ring. Then every maximal ideal of* R *is prime.*

Proof: Let M be a maximal ideal of R. Then R/M is a field so in particular it is an integral domain. Thus M is a prime ideal of R. $\square$

It is not true that every prime ideal of a commutative ring is maximal. For example

1. We have already seen that the zero ideal of $\mathbb{Z}$ is prime but not maximal.
2. In $\mathbb{Z}[x]$, let I denote the ideal consisting of all elements whose constant term is 0 (I is the principal ideal generated by x). The I is a prime ideal of $\mathbb{Z}[x]$ but it is not maximal, since it is contained for example in the ideal of $\mathbb{Z}[x]$ consisting of all those polynomials whose constant term is even.

Theorem 50. *Let* F *be a field and let* I *be an ideal of the polynomial ring* $F[X]$*. Then*

1. I *is maximal if and only if* $I = \langle p(X) \rangle$ *for some irreducible polynomial* $p(X)$ *in* $F[X]$.
2. I *is prime if and only if* $I = \{0\}$ *or* $I = \langle p(X) \rangle$ *for an irreducible* $p(X) \in F[X]$.

Proof: By Lemma 3.2.3 I is principal, $I = \langle p(X) \rangle$ for some $p(X) \in F[X]$.

1. ($\Longleftarrow$) Assume $p(X)$ is irreducible and let I_1 be an ideal of $F[X]$ containing I. Then $I_1 = \langle f(X) \rangle$ for some $f(X) \in F[X]$. Since $p(X) \in I_1$ we have $p(X) = f(X)q(X)$ for some $q(X) \in F[X]$. Since $p(X)$ is irreducible this means that either $f(X)$ has degree zero (i.e. is a non-zero element of F) or $q(X)$ has degree zero. If $f(X)$ has degree zero then $f(X)$ is a unit in $F[X]$ and $I_1 = F[X]$. If $q(X)$ has degree zero then $p(X) = af(X)$ for some nonzero $a \in F$, and $f(X) = a^{-1}p(X)$; then $f(X) \in I$ and $I_1 = I$. Thus either $I_1 = I$ or $I_1 = F[X]$, so I is a maximal ideal of $F[X]$.
   ($\Longrightarrow$): Suppose $I = \langle p(X) \rangle$ is a maximal ideal of $F[X]$. Then $p(X) \neq 0$. If $p(X) = g(X)h(X)$ is a proper factorization of $p(X)$ then $g(X)$ and $h(X)$ both have degree at least 1 and $\langle g(X) \rangle$ and $\langle h(X) \rangle$ are proper ideals of $F[X]$ properly containing I. This contradicts the maximality of I, so we conclude that $p(X)$ is irreducible. This proves 1.
2. Certainly the zero ideal of $F[X]$ and the principal ideals generated by irreducible polynomials are prime. Every other ideal has the form $\langle f(X) \rangle$ for a reducible $f(X)$. If $I = \langle f(X) \rangle$ and $f(X) = g(X)h(X)$ where $g(X)$ and $h(X)$ both have degree less than that of $f(X)$ then neither $g(X)$ nor $h(X)$ belongs to I but their product does. Thus I is not prime.