MA542 Lecture

Timothy Kohl

Boston University

February 21, 2025

Definition

Recall from last time the definitions of prime and maximal ideals.

A prime ideal I of a commutative ring R is a proper ideal such that

$$ab \in I \text{ implies that either } a \in I \text{ or } b \in I$$

A maximal ideal I of a commutative ring R is a proper ideal such that if there is another ideal J such that $I \subseteq J \subseteq R$ then either $I = J$ or $J = R$.

So how do we determine if a given ideal is prime or maximal?

Last time, we discussed prime ideals in $\mathbb{Z}$ as being exactly those of the form $p\mathbb{Z}$ for p a prime integer. And we will discuss more implications of being a prime ideal later on.

As far as maximality is concerned, a standard argument that is used to prove a given ideal $I \subseteq R$ is maximal is to show that any ideal J, that *properly contains* I must be all of R, i.e.

$$I \subsetneq J \subset R \to J = R$$

And the simplest strategy to show that $J = R$ comes from the following small but important fact.

Lemma

Let R be a commutative ring with unity, and $J \subseteq R$ an ideal. If J contains a unit of R then $J = R$.

Proof.

If $u \in J$ is unit with inverse $u^{-1} \in R$ then by the ideal property $u^{-1}u \in J$, but $u^{-1}u = 1$ so $1 \in J$. But now, if $r \in R$ then $r \cdot 1 = r \in J$ (again by the ideal property!) but this implies $R \subseteq J$ and so $J = R$. $\square$

So the application of this is to take the ideal containment $I \subsetneq J \subseteq R$ where I is the ideal we wish to prove is maximal and show that $1 \in J$.

Proposition

The ideal $I = \langle x^2 - 2 \rangle \subseteq \mathbb{Q}[x]$ *is maximal.*

PROOF: Let J be an ideal properly containing I, ie. $\langle x^2 - 2 \rangle \subsetneq J \subseteq \mathbb{Q}[x]$.

So this means there exists $f(x) \in J$ such that $f(x) \notin \langle x^2 - 2 \rangle$, which means that $f(x)$ is *not* a multiple of $x^2 - 2$.

So by the division algorithm there exists $q(x)$ and $r(x)$ such that

$$f(x) = q(x)(x^2 - 2) + r(x)$$

where $deg(r(x)) < deg(x^2 - 2) = 2$ or $r(x) = 0$, but we already know $r(x) \neq 0$.

PROOF (continued)

So we have $f(x) = q(x)(x^2 - 2) + r(x)$ where $r(x) = ax + b$ for some $a, b \in \mathbb{Q}$ where $(a, b) \neq (0, 0)$.

Moreover, since $f(x) \in J$ and $x^2 - 2 \in I \subseteq J$ then $q(x)(x^2 - 2) \in J$ and so $ax + b = r(x) = f(x) - q(x)(x^2 - 2) \in J$.

But now, $(ax - b)(ax + b) = a^2x^2 - b^2 \in J$, and also $a^2(x^2 - 2) = a^2x^2 - 2a^2 \in J$ too.

Putting these two facts together implies $(a^2x^2 - 2a^2) - (a^2x^2 - b^2) = b^2 - 2a^2 \in J$.

But $b^2 - 2a^2 \in \mathbb{Q}$ and $b^2 - 2a^2 \neq 0$ since otherwise $\left(\frac{b}{a}\right)^2 = 2$ which is impossible because... $\sqrt{2} \notin \mathbb{Q}$.

PROOF (continued)

So.... we have that $b^2 - 2a^2$ is a non-zero constant polynomial in J, but this is a **unit** of $\mathbb{Q}[x]$ which means (by the lemma) that $J = \mathbb{Q}[x]$.

Therefore $I = \langle x^2 - 2 \rangle$ is a maximal ideal of $\mathbb{Q}[x]$.

□

Note, we can replace $x^2 - 2$ by something similar like $x^2 - 3$ (since $\sqrt{-3} \notin \mathbb{Q}$) or $x^2 + 1$ (since $i \notin \mathbb{Q}$) and the conclusion (and argument) are virtually the same.

There is another characterization of prime and maximal ideals in terms of the quotient rings they form.

Theorem

Let R be a commutative ring with unity and let I be an ideal of R.
1) R/I is an integral domain iff I is a prime ideal.
2) R/I is a field iff I is a maximal ideal.

PROOF of (1): Suppose R/I is a domain then $(x+I)(y+I) = 0+I$ iff $x+I = 0+I$ or $y+I = 0+I$.

But, since $(x+I)(y+I) = xy+I$ then this is equivalent to saying $xy \in I$ iff $x \in I$ or $y \in I$.

That is R/I is a domain iff $xy \in I$ implies $x \in I$ or $y \in I$.

PROOF of (2):(This is a bit more subtle.)

Suppose R/I is a field, then if J is an ideal such that $I \subsetneq J \subseteq R$ then let $b \in J - I$ which means $b + I \neq 0 + I$.

This implies that $b + I$ is a unit of R/I which means there exists $c + I$ where $(c + I)(b + I) = 1 + I$ so that $bc - 1 \in I$, but also $bc - 1 \in J$.

But since $b \in J$ then $bc \in J$ so $bc - (bc - 1) = 1 \in J$ too, and so $J = R$.

As such, J is a maximal deal.

For the converse, suppose I is maximal in R and consider $\pi : R \to R/I$ where $\pi(x) = x + I$.

We have that if M is an ideal of R/I then $\pi^{-1}(M)$ is an ideal of R that contains I.

So if $x \in R - I$ (i.e. $x + I$ is a non-zero element of R/I) then $\pi^{-1}(\langle x + I \rangle)$ is an ideal of R that contains I,but since I is maximal then $\pi^{-1}(\langle x + I \rangle) = R$, so in particular $\pi(1) = 1 + I \in \langle x + I \rangle$.

So this means there exists $y + I$ such that $(x + I)(y + I) = 1 + I$, which means $y + I = (x + I)^{-1}$, i.e. R/I is a field. $\square$

A very natural consequence of this theorem is the following:

Corollary

If R is a commutative ring with unity, and $I \subseteq R$ is a maximal ideal, then it is automatically a prime ideal.

The proof of this is basically a matter of thinking of the relevant definitions.

If R/I is a field then it is also a domain since a field cannot contain zero divisors.

As such R/I is a domain so I is prime.

We've seen a number of ideas hinted at in this discussion.

In particular, in a ring like $\mathbb{Q}[x]$, an ideal $\langle p(x) \rangle$ which results in a quotient $\mathbb{Q}[x]/\langle p(x) \rangle$ that is a field is tied to the roots of $p(x)$ being numbers α that do *not* lie in $\mathbb{Q}$, e.g. for $x^2 - 2$ it is $\sqrt{2}$.

Concordantly, the resulting field $\mathbb{Q}[x]/\langle p(x) \rangle$ is isomorphic to a field which contains not only $\mathbb{Q}$ but also this very same root α, again with our example from earlier in mind

$$\mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}(\sqrt{2})$$

so the question we have is, what about $p(x)$ specifically makes $\langle p(x) \rangle$ a maximal ideal?

And similarly, for the case of an ideal, say a principal one $I = \langle a \rangle \subseteq R$, what is it about the element 'a' that makes the resulting ideal $I = \langle a \rangle$ prime? (or not prime)

An example to consider (which touches on both questions) is the ideal $I = \langle x^2 - 4 \rangle \subseteq \mathbb{Q}[x]$ and the resulting quotient ring $\mathbb{Q}[x]/I$.

The key feature to note is that this quotient ring is not a domain since $((x-2)+I)((x+2)+I) = (x^2-4)+I$ and of course $(x^2-4)+I = 0+I$ while $(x-2)+I \neq 0+I$ since $x-2 \notin I$.

The reason that $x-2 \notin I$ is that I consists of all multiples of x^2-4 and obviously $x-2$ is not a multiple of x^2-4.

So we have that $(x-2)+I$ and $(x+2)+I$ are zero-divisors in $\mathbb{Q}[x]/I$ which is not too surprising since $I = \langle x^2 - 4 \rangle$ and $x - 2 \mid x^2 - 4$ and $x + 2 \mid x^2 - 4$ and indeed, $x^2 - 4 = (x-2)(x+2)$.

And it is this fact which leads to these zero divisor, namely that $x^2 - 4$ is factorable as a product of lower degree polynomials.

So $I = \langle x^2 - 4 \rangle$ is certainly not a prime ideal (since the quotient ring $\mathbb{Q}[x]/I$ isn't a domain), so I is certainly not a maximal ideal.

In contrast, $I = \langle x^2 - 2 \rangle$ is a prime ideal (and in fact maximal) precisely because $x^2 - 2$ isn't factorable in $\mathbb{Q}[x]$.

Note, it turns out that $\mathbb{Q}[x]/\langle x^2 - 4 \rangle \cong \mathbb{Q} \times \mathbb{Q}$ as rings and the direct product on the right is certainly not a domain since $(1,0)$ and $(0,1)$ are no-zero elements whose product is $(1,0)(0,1) = (0,0)$.

What we shall discuss in the next section is the notion of 'divisibility' in a ring, in particular how to quantify what it means for an element of a ring to be 'irreducible' or 'prime'.

We've seen the term irreducible applied to polynomials, and the term prime is, of course, familiar from basic arithmetic, and it does indeed tie in with the notion of prime ideal.

Also tied in with this discussion is the role of the units in a ring.

In addition, we will be looking at different sub-categories of rings, whose definitions are tied in with these terms, and also those determined by the nature of the ideals of the ring.

Recall we showed earlier that all ideals in $\mathbb{Z}$ have the form $\langle n \rangle$ for some n.

Not all rings have this property. So stay tuned...