21MAB143 Rings and Polynomials: Week 9

1 Prime ideals and maximal ideals

This week and next we will study specials kind of ideals, called **prime** and **maximal** ideals, that play important roles in the theory of commutative rings. Roughly speaking, they generalise the notions of prime number in the ring $\mathbf{Z}$ and irreducible polynomial in the ring $K[x]$. The two notions coincide for ideals in $\mathbf{Z}$ and $K[x]$, but not in general: in particular next week we will see that they are different for polynomial rings in more than 1 variable.

Definition 1.1. *Let R be a commutative ring. An ideal $I \subseteq R$ is* **prime** *if for elements $f, g \in R$ we have:*

$$fg \in I \Rightarrow (f \in I \text{ or } g \in I)$$

Definition 1.2. *Let R be a commutative ring. An ideal $I \subseteq R$ is* **maximal** *if $I \neq R$ and for any ideal J such that $I \subseteq J \subseteq R$ we have $J = I$ or $J = R$.*

Proposition 1.3. *In any commutative ring R, a maximal ideal is prime.*

Proof. We will prove the contrapositive of the above statement. Let $I \subsetneq R$ be an ideal which not prime. We will prove it is not maximal.

Since I is not prime, there exists elements f and g, neither belonging to I, such that $fg \in I$. Consider the ideal

$$\begin{aligned} J &= I + \langle f \rangle \\ &= \{a + bf \mid a \in I, b \in R\} \end{aligned}$$

I claim this ideal is not equal to either I or R. To see that $J \neq I$, we just observe that $f \in J$ but $f \notin I$.

To see that $J \neq R$ we argue by contradiction.If we had $J = R$, then in particular we could write

$$1 = a + bf$$

for some $a \in I$ and some $b \in R$. Now multiply this equation by the element g: this gives

$$g = ga + bfg$$

Now $ga \in I$ since $a \in I$ and I is an ideal; also by hypothesis $fg \in I$, therefore $bfg \in I$ also. Therefore the right-hand side is an element of I, whereas the left-hand side is not. This is a contradiction, hence $J \neq R$ as claimed. □

Example Problem Sheet 1 Question 5 showed that when $R = \mathbf{Z}$, the ring of integers, every ideal has the form

$$I = n\mathbf{Z} = \{qn \mid q \in \mathbf{Z}\}$$

for a unique natural number n. Which of these ideals are prime and/or maximal?

First let's consider the case when $n = p$, a prime number, so we are considering the ideal

$$I = p\mathbf{Z} = \{qp \mid q \in \mathbf{Z}\}$$

Suppose a and b are integers and $ab \in I$. So there exists an integer q such that $ab = qp$. Hence p divides ab. This means either a or b must have p among its prime factors, so p divides a or p divides b (or both). But I consists of exactly those integers which are divisible by p, so we have either $a \in I$ or $b \in I$. Therefore I is a prime ideal.

By contrast, if n is a composite number, say $n = kl$ with neither k nor l equal to ± 1, then neither k nor l belongs to the ideal I, while $kl = n$ does. So I is not a prime ideal in this case.

What about maximal ideals? By Proposition 1.3, a maximal ideal in $\mathbf{Z}$ must be prime, so an ideal which is not prime cannot be maximal. Hence if n is composite, the ideal $I = n\mathbf{Z}$ is not maximal.

If $n = p$, a prime, then I claim that $I = p\mathbf{Z}$ is maximal. To see this, suppose J is an ideal such that $I \subsetneq J$. We must shows that $J = \mathbf{Z}$. Let a be an element of J that is not in I. This means that p does not divide a, which since p is prime means in turn that $\gcd(a, p) = 1$. By Bézout's identity, there exist integers x, y such that

$$xp + ya = 1.$$

But $p \in J$ implies that $xp \in J$ and similarly $a \in J$ implies $ya \in J$. So the left-hand side is an element of J, and therefore the right-hand side is too: $1 \in J$. Now any element $m \in \mathbf{Z}$ can be written as $m = m \cdot 1$, and therefore is in J. This shows $J = \mathbf{Z}$ as required.

To summarise, we have shown that for an ideal $I = \langle n \rangle$ in the ring of integers $\mathbf{Z}$:

$$I \text{ is prime} \iff I \text{ is maximal} \iff n \text{ is a prime number.}$$

1.1 Examples

The polynomial ring $\mathbf{Z}[x]$

Let p be a prime number and consider the ideal $\langle p \rangle \subset \mathbf{Z}[x]$, which can be described explicitly as

$$\langle p \rangle = \{pf \mid f \in \mathbf{Z}[x]\}$$

In other words, this is the ideal of all polynomials in $\mathbf{Z}[x]$ whose coefficients are all divisible by p.

Question: Is the ideal $\langle p \rangle$ prime?

To answer this question, suppose that $f, g \in \mathbf{Z}[x]$ are polynomials such that $fg \in \langle p \rangle$. Consider the reduction mod p homomorphism defined in Week 8:

$$\rho_p \colon \mathbf{Z}[x] \to \mathbf{Z}_p[x]$$

Since $fg \in \langle p \rangle$ all its coeffcients are divisble by p, so we have

$$\rho_p(fg) = 0.$$

On the other hand since ρ_p is a ring homomorphism we have

$$\rho_p(fg) = \rho_p(f)\rho_p(g)$$

so the product $\rho_p(f)\rho_p(g)$ equals 0 in $\mathbf{Z}_p[x]$. Since $\mathbf{Z}_p$ is a field, the product of nonzero elements in $\mathbf{Z}_p[x]$ is nonzero, so we conclude that either $\rho_p(f) = 0$ or $\rho_p(g) = 0$, in other words either $f \in \langle p \rangle$ or $g \in \langle p \rangle$. This shows that $\langle p \rangle$ is prime.

Another kind of ideal in $\mathbf{Z}[x]$ is the ideal

$$\langle x \rangle = \{xf \mid f \in \mathbf{Z}[x]\}$$

This is exactly the ideal of all polynomials whose constant term equals 0.

If f has constant term $a \neq 0$ and g has constant term $b \neq 0$, then fg has constant term $ab \neq 0$. So if $fg \in \langle x \rangle$ then either f or g must be in $\langle x \rangle$: that is, $\langle x \rangle$ is prime also.

However, neither $\langle p \rangle$ nor $\langle x \rangle$ is maximal. To see, this consider the ideal $\langle p, x \rangle$. You can check that

$$\langle p \rangle \subsetneq \langle p, x \rangle$$
$$\langle x \rangle \subsetneq \langle p.x \rangle$$

To complete the claim, we must show that $\langle p, x \rangle \neq \mathbf{Z}[x]$. Every polynomial in this ideal has the form $ap + bx$ for some $a, b \in \mathbf{Z}[x]$, and any polynomial of this form has constant term divisible by p. So for example, the constant polynomial 1 is not in $\langle p, x \rangle$. This shows $\langle p, x \rangle \neq \mathbf{Z}[x]$ as required.

In fact the ideal $\langle p, x \rangle$ is maximal. To see this, suppose that J is an ideal such that $\langle p, x \rangle \subsetneq J$. We must show that $J = \mathbf{Z}[x]$.

Choose an element $g \in J$ which is not in $\langle p, x \rangle$. Then we can write g as

$$g = a_0 + xg'$$

where a_o is an integer not divisible by p, and g' is some other polynomial. Rearranging we get that

$$a_0 = g - xg'$$

which shows that a_0 in J.

But now since p is prime and a_0 is not divisible by p, we have $\gcd(a_0, p) = 1$. Bézout's identity (for integers) then says that there exist $m, n \in \mathbf{Z}$ such that

$$ma_0 + np = 1$$

Since a_0 and p are both in J, this equation shows that $1 \in J$ also, therefore $J = \mathbf{Z}[x]$.

The Gaussian integers $\mathbf{Z}[i]$

In this example we will consider the ideals in the ring of **Gaussian integers**

$$\mathbf{Z}[i] = \{a + b\,i \mid a,\, b \in \mathbf{Z}\}$$

Given an integer $n \in \mathbf{Z}$, we can consider the ideal in $\mathbf{Z}[i]$ generated by n:

$$\langle n \rangle = \{na + nb\,i \mid a,\, b \in \mathbf{Z}\}$$

Question: Is $\langle n \rangle$ a prime ideal if n is a prime number?

Example 1: $n = 3$.

I claim that the ideal $\langle 3 \rangle \subset \mathbf{Z}[i]$ is maximal, hence prime. To see this, supppse that J is an ideal such that $\langle 3 \rangle \subsetneq J$. We need to show that $J = \mathbf{Z}[i]$, or equivalently that $1 \in J$.

Chose an element $a + b\,i \in J$ such that $a + b\,i \notin \langle 3 \rangle$. Then at least one of a or b is not divisible by 3.

Consider the product

$$(a + b\,i)(a - b\,i) \in J.$$

The left-hand side equals $a^2 + b^2$. If $3 \nmid a$ then $a^2 = 1 \bmod 3$; if $3 \nmid b$ then $b^2 = 1 \bmod 3$. So $a^2 + b^2 \neq 0 \bmod 3$, in other words $\gcd(3, a^2 + b^2) = 1$.

By Bézout's identity there exist integers x, y such that

$$3x + (a^2 + b^2)y = 1$$

Since $3 \in J$ and $a^2 + b^2 \in J$ we get $1 \in J$, as required.

This shows that the ideal $\langle 3 \rangle \subset \mathbf{Z}[i]$ is maximal, hence prime.

Example 2: $n = 5$.

By contrast, the ideal $\langle 5 \rangle \subset \mathbf{Z}[i]$ is not prime. This is easy to see:

$$(2 + i)(2 - i) = 2^2 + 1^2 = 5$$

but neither $2 + i$ nor $2 - i$ is in the ideal $\langle 5 \rangle$.

In fact there is a general characterisation of odd primes which generate a prime ideal in $\mathbf{Z}[i]$.

Theorem 1.4 (Fermat)**.** *For an odd prime $p \in \mathbf{Z}$, the ideal $\langle p \rangle \subset \mathbf{Z}[i]$ is prime:*

- *if and only if p is not a sum of 2 squares*
- *if and only if $p = 3 \bmod 4$.*

2 Prime and maximal ideals in $K[x]$

In this section we will study the case of ideals in one-variable polynomial rings in more detail. Our main result, Theorem 2.2, will show that in this context, the notions of prime ideals and maximal ideals are the same as each other, and are closely connected to irreducibility of polynomials as studied in Week 8.

Before we begin we recall the following important result from Week 2:

Theorem 2.1 (Week 2 Theorem 2.5)**.** *Let* K *be any field, and* $K[x]$ *the ring of polynomials with coefficients in* K*. If* $I \subseteq K[x]$ *is an ideal, there exists a polynomial* $f \in K[x]$ *such that* $I = \langle f \rangle$*. Moreover two polynomials generate the same ideal if and only if they differ by a nonzero constant multiple:* $\langle f \rangle = \langle g \rangle$ *if and only if* $f = kg$ *for some nonzero* $k \in K$*.*

So every ideal in $K[x]$ is generated by a single polynomial. This leads to a natural question: is there any relationship between the properties of an ideal in $K[x]$ and the properties of a polynomial which generates that ideal? The next theorem provides a complete answer.

Theorem 2.2. *Let* K *be a field and* $K[x]$ *the ring of polynomials in one variable over* K*. For an ideal* $I = \langle f \rangle \subseteq K[x]$ *the following conditions are all equivalent:*

(a) the ideal I *is maximal;*

(b) the ideal I *is prime;*

(c) the polynomial f *is irreducible in* $K[x]$*.*

Note that condition (c) is indeed well-defined thanks to the last part of Theorem 2.1 above: if f and and g are two polynomials which both generate I, then $f = kg$ for some nonzero constant k, and so one is irreducible if and only if the other is too.

Proof of Theorem 2.2. Our strategy of proof will be be prove a "cycle" of implications. We will show that (a) implies (b), that (b) implies (c), and that (c) implies (a).

First, Proposition 1.3 tells us that any maximal ideal is prime, so (a) implies (b). Next, assume (b) is true, so $I = \langle f \rangle$ is a prime ideal. Suppose that $f = gh$ for some elements $g, h \in K[x]$. We want to show that either g or h must be a constant. Now since $gh = f \in I$ and I is prime, we know that either $g \in I$ or $h \in I$. By renaming if necessary, assume $g \in I$. Since $I = \langle f \rangle$, this means that $g = fp$ for some $p \in K[x]$. But then we have

$$\begin{aligned} f &= gh \\ &= fph \end{aligned}$$

which means that both p and h are nonzero constants. This proves (c).

Finally assume (c) is true, so f is irreducible. We want to prove that $I = \langle f \rangle$ is maximal. Suppose $J \subset K[x]$ is an ideal such that $I \subsetneq J$. We want to show that $J = K[x]$.

Notice that since f is irreducible, it has no divisors in $K[x]$ other than constant polynomials and multiples of itself. So for any polynomial $g \in K[x]$ we have $\gcd(f, g) = 1$ or $\gcd(f, g) = \widehat{f}$, and the latter is the case if and only if f divides g.

Now choose a polynomial $g \in J$ such that $g \notin I$. Then f does not divide g, and so $\gcd(f, g) = 1$. Hence by Week 3 Corollary 1.3 (Bézout's identity for polynomials) there are polynomials a, $b \in K[x]$ such that

$$af + bg = 1.$$

But now since both f and g are elements of J, this shows that $1 \in J$ also, which as before means that $J = K[x]$, as required. □

In Week 8 we characterised the irreducible polynomials in the rings $\mathbf{C}[x]$ and $\mathbf{R}[x]$. We can combine these results with Theorem 2.2 above to say the following:

Corollary 2.3. *1. An ideal I in the ring $\mathbf{C}[x]$ is maximal (equivalently, prime) if and only if it is of the form*

$$I = \langle x - z \rangle$$

for some $z \in \mathbf{C}$.

2. An ideal in the ring $\mathbf{R}[x]$ is maximal (equivalently, prime) if and only if it is of one of following forms:

(a) $I = \langle x - r \rangle$ for some $r \in \mathbf{R}$, or

(b) $I = \langle ax^2 + bx + c \rangle$ for a, b, $c \in \mathbf{R}$ such that $b^2 - 4ac < 0$.

By contrast, we saw that there is no such simple description of irreducible polynomials in $\mathbf{Q}[x]$: we introduced tools such as the Gauss Lemma and polynomial reduction to help prove that certain polynomials are irreducible in $\mathbf{Q}[x]$.

2.1 Quotients by prime and maximal ideals

In Week 1 we saw that given a commutative ring R and an ideal I, the set of cosets R/I can be made into a ring by defining addition and multiplication of cosets by the formulas

$$(I + a) + (I + b) = I + (a + b)$$
$$(I + a) \cdot (I + b) = I + (ab)$$

where a, b are elements of R.

We will now show that in the case where the ideal I is prime or maximal, the quotient ring R/I will have good properties. We need the following definition:

Definition 2.4. *A commutative ring R is called a* **integral domain** *if for elements a, $b \in R$ we have*

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Most of the rings we have studied such as $\mathbf{Z}$, any field K, and any polynomial ring $K[x_1, \ldots, x_n]$ over a field, are integral domains. The ring $\mathbf{Z}_6$ is not, since $2 \cdot 3 = 0$ in this ring.

Theorem 2.5. *Let* R *be a commutative ring and* $I \subseteq R$ *an ideal. Then*

(a) The quotient ring R/I *is an integral domain if and only if* I *is prime.*

(b) The quotient ring R/I *is a field if and only if* I *is maximal.*

Sketch of proof. To prove (a), observe that to say R/I is an integral domain means that

$$(I + a) \cdot (I + b) = I \Rightarrow I + a = I \text{ or } I + b = I$$

since the additive identity in R/I is the coset I. But $(I + a) \cdot (I + b) = I + (ab)$, so this equals I if and only if $ab \in I$. Similarly $I + a = I$ if and only if $a \in I$, and $I + b = I$ if and only if $b \in I$. So the above statement is equivalent to

$$ab \in I \Rightarrow a \in I \text{ or } b \in I$$

which is exactly the statement that I is prime.

To prove (b), we want to show that I is maximal if and only if every nonzero element of R/I has a multiplicative inverse. A nonzero element of R/I is a coset $I + a$ where $a \notin I$, and a multiplicative inverse is a coset $I + b$ such that

$$\begin{aligned} (I + a)(I + b) &= I + 1 \quad \text{in other words} \\ I + ab &= I + 1 \quad \text{in other words} \\ ab - 1 &\in I \end{aligned}$$

So we need to show that I is maximal if and only if for every $a \notin I$, there exists b such that $ab - 1 \in I$.

Now I is maximal if and only if $I + \langle a \rangle = R$ for every $a \notin I$, where the sum of ideals is defined as on Problem Sheet 5:

$$I + \langle a \rangle = \{c + ab \mid c \in I,\ b \in R\}$$

An ideal of R equals R itself if and only if it contains the element 1, so $I + \langle a \rangle = R$ if and only if there exist elements $c \in I$ and $b \in R$ such that $c + ba = 1$, equivalently if and only if there exists $b \in R$ such that $ab - 1 \in I$. So we have shown that I is maximal if and only if for every $a \notin I$ there exists b such that $ab - 1 \in I$, which as explained above is true if and only if R/I is a field. □

Note that this Theorem gives another proof of Propostion 1.3, since any field is an integral domain.

2.2 Examples

Let's see what Theorem 2.5 tells us in the case of polynomial rings $K[x]$ where $K = \mathbf{R}$ or $\mathbf{Q}$. Here we know by Theorem 2.2 that prime and maximal ideals are the same, and they are exactly the ideals generated by irreducible polynomials.

Example 1: $K = \mathbf{R}$.

From Week 8, we know that an irreducible polynomial in $\mathbf{R}[x]$ must have degree 1 or 2.

Let $f = ax^2 + bx + c$ be an irreducible quadratic in $\mathbf{R}[x]$, i.e. one for which $b^2 - 4ac < 0$. By Theorem 2.2 we know that the ideal $\langle f \rangle$ is maximal, and by Theorem 2.5 the quotient ring $\mathbf{R}[x]/\langle f \rangle$ is therefore a field. What is this field?

To answer this, let $\alpha \in \mathbf{C}$ be either root of f, so

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Then as we saw in Week 2 we have the "evaluation at α" homomorphism

$$\begin{aligned} \mathrm{ev}_\alpha \colon \mathbf{R}[x] &\to \mathbf{C} \\ p &\mapsto p(\alpha) \end{aligned}$$

We saw in Week 2 the kernel $\mathrm{Ker}(\mathrm{ev}_\alpha)$ is generated by any nonzero polynomial p of minimal degree such that $p(\alpha) = 0$. Similarly to Problem Sheet 2 Question 5, we can show there is no such p of degree 0 or 1. On the other hand $f(\alpha) = 0$, and f has degree 2, so $\mathrm{Ker}(\mathrm{ev}_\alpha) = \langle f \rangle$.

Moreover, the homomorphism ev_α is surjective (onto): we have

$$\mathrm{ev}_\alpha(r_1 + r_2 x) = r_1 + r_2 \alpha$$

and since α is a non-real complex number, it is not hard to check that any $z \in \mathbf{C}$ can be written as $z = r_1 + r_2\alpha$ for appropriate real numbers r_1 and r_2.

So ev_α is a surjective homomorphism with kernel equal to the ideal $\langle f \rangle$. The Homomorphism Theorem for Rings (Week 1 Theorem 2.8) therefore tells us that ev_α induces an isomorphism of rings.

$$\frac{\mathbf{R}[x]}{\langle f \rangle} \cong \mathbf{C}.$$

Example 2: $K = \mathbf{Q}$.

In this case, we saw in Week 8 that $\mathbf{Q}[x]$ contains irreducible polynomials of many different degrees. (In fact Problem Sheet 8 Question 5 shows there are irreducible polynomials of *every* degree in $\mathbf{Q}[x]$.)

As a concrete example let's consider the following polynomial in $\mathbf{Q}[x]$:

$$f = x^4 + 3x^2 + 7.$$

We saw in Week 8 that this polynomial is irreducible in $\mathbf{Q}[x]$. So again the quotient $\mathbf{Q}[x]/\langle f \rangle$ is a field: what does it look like?

Let $\alpha \in \mathbf{C}$ be any root of f. Note that $f(r) > 0$ for all $r \in \mathbf{R}$, so α cannot be real.

As before, we can consider the "evaluation at α" homomorphism

$$\begin{aligned} \mathrm{ev}_\alpha \colon \mathbf{Q}[x] &\to \mathbf{C} \\ p &\mapsto p(\alpha). \end{aligned}$$

I claim that again, the kernel $\mathrm{Ker}(\mathrm{ev}_\alpha)$ is generated by f. If not, there would be a polynomial $g \in \mathbf{Q}[x]$ with $\deg(g) < \deg(f) = 4$ such that $g(\alpha) = 0$. But then consider $d = \gcd(f, g)$. This is a polynomial in $\mathbf{Q}[x]$ such that:

- $d \mid f$
- $\deg(d) \leq \deg(g) < 4$
- $d(\alpha) = 0$ since α is a common root of f and g; in particular d is nonconstant.

So d is a nonconstant polynomial in $\mathbf{Q}[x]$ which divides f and has smaller degree than $\deg(f)$. This contradicts the fact that f is irreducible in $\mathbf{Q}[x]$.

Therefore $\mathrm{Ker}(\mathrm{ev}_\alpha) = \langle f \rangle$, as claimed, and so the Homomorphism Theorem for Rings says that we have an isomorphism

$$\frac{\mathbf{Q}[x]}{\langle f \rangle} \cong \mathrm{Im}(\mathrm{ev}_\alpha)$$

(Note that in this case the image is a countable subset of $\mathbf{C}$, so it cannot be all of $\mathbf{C}$.)

The image $\mathrm{Im}(\mathrm{ev}_\alpha)$ is usually denoted by $\mathbf{Q}(\alpha)$ and called "$\mathbf{Q}$ adjoin α". It is an example of a so-called **algebraic extension** of $\mathbf{Q}$. Fields of this kind are major objects of study in modern number theory.