Ideals and polynomial rings

Jonas van der Schaaf

First it's probably good to give some concrete examples of prime ideals as I didn't show any.

Example 1. Consider the ring $\mathbb{Z}$ and the ideal $(2) = \{2x : x \in \mathbb{Z}\}$ we discussed last week. Then (2) is a prime ideal so $\mathbb{Z}/2\mathbb{Z}$ is a domain. We prove (2) is a prime ideal:

Suppose $ab \in (2)$: this means that $ab = 2x$ for some $x \in \mathbb{Z}$ so 2 divides ab. Because 2 is a prime number this means that 2 divides either a or b (or both). Therefore, $a \in (2)$ or $b \in (2)$ proving that (2) is a prime ideal.

This proof works more generally: for any prime number p the ideal (p) is a prime ideal. This is where the name "prime" comes from.

The following is also something we'll need:

Lemma 1. *For any ring morphism $f : R \to S$ the kernel $\ker f = \{x \in R : f(x) = 0\}$ is an ideal.*

Proof. The kernel is the kernel of f seen as an additive morphism, so it is definitely a subgroup. We show that $ax \in \ker f$ for all $a \in R$ and $x \in \ker f$:

$$\begin{aligned} f(ax) &= f(a)f(x) \\ &= f(a)0 \\ &= 0. \end{aligned}$$

□

1 Evaluation maps

Proposition 1. *Let k be a field and write $k[x]$ for the polynomial ring. Then any $r \in k$ gives a ring morphism $f_r : k[x] \to k$ determined by $\varphi_r(x) = r$.*

Proof. If $\varphi_r(x) = r$ is true, then by the axioms of ring morphisms for any polynomial $\sum_{i=0}^n a_i x^i$ we must have

$$\begin{aligned} \varphi_r\left(\sum_i a_i x^i\right) &= \sum_i \varphi_r(a_i)\varphi_r(x)^i \\ &= \sum_i \varphi_r(a_i) r^i. \end{aligned}$$

We can define that $a \in k$ we have $\varphi_r(a) = a$, i.e. φ_r does nothing on k itself. Then we get

$$\varphi_r\left(\sum_i a_i x^i\right) = \sum_i a_i r^i = f(r)$$

for any polynomial. The map φ_r just fills in $x = r$ in any polynomial. We show that this defines a ring morphism.

Because φ_r does nothing with k and the $0, 1$ or $k[x]$ are the $0, 1$ from k this means that these are preserved.

Now we show this map is additive: take $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$ two polynomials. Then their sum is defined as $\sum_k (a_k + b_k) x^k$. We apply the evaluation morphism to get

$$\begin{aligned}\varphi_r(f+g) &= \varphi_r\left(\sum_k (a_k + b_k) x^k\right) \\ &= \sum_k (a_k + b_k) \varphi_r(x)^k \\ &= \sum_k a_k r^k + \sum_k b_k r^k \\ &= \varphi_r(f) + \varphi_r(g).\end{aligned}$$

You can do a similar proof for multiplicativity.

Therefore, this is a ring morphism. □

We will look at the ideals of polynomial rings over fields. In order to do this we're going to need a proposition which I will not prove.

Proposition 2. *If k is a field, then all ideals $I \subseteq k[x]$ are of the form (f) for some $f \in k[x]$. You can find such an f by taking the polynomial of lowest degree contained in I.*

Now we can look at the kernel of the evaluation map.

Proposition 3. *If $r \in k$ then the kernel of the evaluation morphism $\varphi_r : k[x] \to k$ is exactly the ideal $(x - r) \subseteq k[x]$.*

Proof. We have that $\varphi_r(x - r) = r - r = 0$. Therefore, the polynomial $x - r$ is contained in the kernel $\ker \varphi_r$. This means that $(x - r) \subseteq \ker \varphi_r$.

Now by the previous unproven proposition there is some $f \in k[x]$ such that $(f) = \ker \varphi_r$ and f is the element of lowest degree in $\ker f$. If $f \neq x - r$ then it must have degree lower than 1, so it has degree 0. This means it is a constant $a_0 \in k^\times = k \setminus \{0\}$. Then $a_0^{-1} a = 1 \in \ker f$ so $\varphi_r(1) = 0$. This is impossible as $\varphi_r(a) = a$ for all $a \in k$ and a field cannot have $1 = 0$.

From this we conclude that $(x - r) = \ker \varphi_r$. □

One can prove that $k[x]/(x - r) = k[x]/\ker \varphi_r$ is naturally isomorphic to k with the natural isomorphism given by $\overline{f} \mapsto \varphi_r(f)$. In this quotient we have essentially set $x - r = 0$ so now x has all the algebraic properties of r. We will now look at what happens when we try to create elements with more complex algebraic properties.

2 Evaluating in elements not in the ring

The idea of creating field extensions is that $x \in k[x]$ is a "generic" element in some sense: there are no algebraic relations it has to anything in k. We can give it some relation to k by taking the quotient by an ideal: $(x - r)$ essentially said that x has exactly the same properties as r: they are equal in the quotient field. Now we look at what happens if we divide by more complex polynomials.

Example 2. We define the ring

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}.$$

We define addition and multiplication by setting $\sqrt{2}^2 = 2$ and expanding expressions using distributivity. This is not only a ring but also a field with inverses $(a + b\sqrt{2})^{-1} = \frac{1}{a^2 - 2b^2}(a - b\sqrt{2})$.

This ring is not isomorphic to $\mathbb{Q}$: $\sqrt{2}$ is irrational and therefore not an element of the fractions. We try to construct this ring using quotients of polynomials.

To do this we construct some ring containing $\mathbb{Q}$ and an element with the algebraic properties of $\sqrt{2}$. The "defining" property of $\sqrt{2}$ is of course that $\sqrt{2}^2 = 2$. We try to emulate this by considering the quotient $k[x]/(x^2-2)$. Here the coset $\overline{x}$ has the property that $\overline{x}^2 = 2$ and this will take on the role of $\sqrt{2}$. It turns out that this quotient ring is exactly the same one as above: the two are isomorphic and there is an isomorphism sending $\overline{x}$ to $\sqrt{2}$. The isomorphism $k[x]/(x^2-2) \to \mathbb{Q}(\sqrt{2})$ is given by the map $\overline{f} \mapsto f(\sqrt{2})$. You can see this as a natural extension of the evaluation maps we saw earlier.

Notice that $\mathbb{Q}$ is still contained in $\mathbb{Q}(\sqrt{2})$. All elements $a + b\sqrt{2}$ with $b = 0$ are just elements of $\mathbb{Q}$.

One can add multiple new "algebraic" elements to a field repeatedly to get larger and larger fields, leading us naturally to the definition of a field extension:

Definition 1. Let k be a field and $k' \subseteq k$ a subring that is also a field. Then we call k a field extension of k'.

Example 3. In the previous example we saw that $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\sqrt{2})$ and therefore $\mathbb{Q}(\sqrt{2})$ is a field extension of $\mathbb{Q}$.

Example 4. You could add $\sqrt[3]{3}$ to $\mathbb{Q}(\sqrt{2})$ by taking the quotient $\mathbb{Q}(\sqrt{2})[y]/(y^3-3)$. This is a field extension of both $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$.