10 Ideals in Polynomial Rings

10.1 Ideals in a Field

Last class, we looked at ideals in rings, and began discussing ideals in polynomial rings. Today we will consider what such ideals can look like. The following proposition will be useful later, when discussing maximal ideals:

Proposition 10.1
A ring R is a field if and only if it has exactly two ideals.

Any ring has the ideals $(0) = \{0\}$ and $(1) = R$ — these coincide only in the zero ring, which is not a field by definition. So the proposition states that the ring is a field if and only if it has no other ideals.

Proof. Suppose R is a field, so it has at least two ideals (0) and (1). But there are no other ideals, because every element is invertible — if I is an ideal containing some element $x \neq 0$, then $1 = x^{-1}x$ is in I as well, so $I = (1)$.

Conversely, if R is not a field, then either it is the zero ring and only has one ideal, or it contains a nonzero x which is not invertible. Then (x) cannot contain 1, so (0), (x), and (1) are distinct ideals. □

10.2 Polynomial Rings over a Field

We'll first look at ideals in $F[x]$, the ring of polynomials in one variable over a field.

Proposition 10.2
Every ideal in $F[x]$ is principal. More precisely, if $I \subset F[x]$ is a nonzero ideal and P a (nonzero) element of I of minimal degree, with $\deg(P) = n$, then we have $I = (P)$, and the images of 1, x, x^2, …, x^{n-1} form a basis in $F[x]/I$ (as a vector space over F).

Proof. The main idea is to use division of polynomials with remainder.

In order to check that P generates I, take any $Q \in I$; then by polynomial division we can write

$$Q = P \cdot S + R,$$

where S and R are in $F[x]$ and $\deg R < \deg P$. But R must be in I, so if $R \neq 0$ then this contradicts the choice of P as having minimal degree. So $R = 0$, which means $P \mid Q$. So P generates I.

Now consider the quotient $F[x]/(P)$, and let the images of 1, x, …, x^{n-1} be denoted by $\overline{1}$, $\overline{x}$, …, $\overline{x^{n-1}}$. These images must be linearly independent — for any $P, Q \in F[x]$ we have $\deg(PQ) = \deg(P) + \deg(Q)$ (since F is a field, so has no zero divisors), which means a polynomial with degree less than n cannot be divisible by P. Then if $\overline{1}$, …, $\overline{x^{n-1}}$ were linearly dependent with $a_0 \cdot \overline{1} + \cdots + a_{n-1} \cdot \overline{x^{n-1}} = 0$, then $a_0 + \cdots + a_{n-1}x^{n-1}$ would have to be divisible by P, which is a contradiction.

Conversely, these images must span the quotient by using division with remainder again — for any $Q \in F[x]$, we can write $Q = P \cdot S + R$ with $\deg(R) < n$, which means $\overline{Q} = \overline{R}$ for some $\overline{R}$ which is a linear combination of $\overline{1}$, …, $\overline{x^{n-1}}$. □

Recall that to divide a polynomial Q by P with remainder, we subtract a multiple of P from Q to cancel out the leading term of Q; we then repeat until the remaining polynomial has degree less than that of P.

Note 10.3
This doesn't generalize fully to polynomials over an arbitrary ring R, but some parts do. First, it's not always true that

$$\deg PQ = \deg P + \deg Q.$$

For example, in $\mathbb{Z}/4[x]$, $(2x)(2x+1) = 2x$ does not have degree 2.

Division with remainder also does not necessarily work — for example, we can't divide x^2 by $2x+1$ with remainder in $\mathbb{Z}[x]$. This is because when we cancel out the leading coefficient of Q, we need to scale; and here, 2 isn't invertible, so we can't scale by the correct factor.

But both facts remain true for monic polynomials — so we can divide with remainder if P is monic (meaning it has leading coefficient 1; this works the same way if the leading coefficient is a unit). So if P is monic, then it's still true that every element of $R[x]/(P)$ can be written uniquely as

$$a_0\overline{1} + a_1\overline{x} + \cdots + a_{n-1}\overline{x^{n-1}},$$

for $a_i \in R$. We no longer say that the $\overline{x^i}$ form a basis, since $R[x]/(P)$ is not a vector space (vector spaces are defined over a field); but we will later discuss an analog of vector spaces over rings.

Last time, we mentioned that the construction $F[x]/(P)$ is equivalent to adjoining a root of P — for example, $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$. Using Proposition 10.2, we can now make this more precise:

Proposition 10.4
If F is a field and $P \in F[x]$, then $F[x]/(P) \cong F[\alpha]$, where α is a root of P.

Proof. We know that

$$F[x]/(P) = \left\{a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x^{n-1}}\right\},$$

where $n = \deg(P)$, while

$$F[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\right\}$$

(note that we don't need higher powers of α, as the polynomial relation guarantees that we can express them in terms of these powers). To multiply in $F[\alpha]$, it's enough to understand how to multiply by α. We have

$$\alpha(a_0 + \cdots + a_{n-1}\alpha^{n-1}) = a_0\alpha + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1}\alpha^n,$$

and we can expand α^n using the fact that $P(\alpha) = 0$ — if $P(x) = c_n x^n + \cdots + c_0$, then we have

$$\alpha^n = -c_n^{-1}(c_{n-1}\alpha^{n-1} + \cdots + c_0).$$

This is exactly how multiplication works in $F[x]/(P)$; so the two rings have the same additive and multiplicative structure, and are therefore isomorphic, with the isomorphism given by replacing $\overline{x}$ with α. □

Note 10.5
Here we should think of α as a *universal* root of P — an element that satisfies $P(\alpha) = 0$ but no extra conditions. Given a *specific* root, it's possible that α satisfies additional relations (if P is not irreducible), in which case $F[\alpha]$ would instead be isomorphic to a quotient of $F[x]/(P)$.

10.3 Maximal Ideals

We'll now discuss maximal ideals. These will turn out to be quite useful; today we'll see how to use them to connect algebra to geometry.

Definition 10.6 (Maximal Ideals)
An ideal $I \subset R$ is **maximal** if $I \neq R$, and the only ideals of R containing I are R and I itself.

Example 10.7
The maximal ideals in $\mathbb{Z}$ are (p), for p prime. To prove this, we saw earlier that the ideals of $\mathbb{Z}$ are $n\mathbb{Z}$. But $n\mathbb{Z} \subset m\mathbb{Z}$ if and only if $m \mid n$. So understanding the maximal *ideals* of $\mathbb{Z}$ in the poset of ideals ordered by inclusion is equivalent to understanding the minimal *elements* of $\mathbb{Z}$ in the poset of elements ordered by divisibility. These minimal elements are the primes p, so the maximal ideals are (p).

Example 10.8
For a polynomial ring over a field $F[x]$, any ideal is of the form (P). For the same reason as in the case of $\mathbb{Z}$, the ideal (P) is maximal if and only if P does not factor as QR where Q and R have positive degree, or in other words, if P is irreducible.

Example 10.9
In $\mathbb{C}[x]$, the only irreducible polynomials are linear, since by the Main Theorem of Algebra every polynomial can be factored as $c(x - z_1) \cdots (x - z_n)$. So the maximal ideals of $\mathbb{C}[x]$ are exactly the ideals $(x - \alpha)$.

We'll now see how this example generalizes to polynomials in *multiple* variables. The following proposition will be useful:

Proposition 10.10
An ideal $I \subset R$ is maximal if and only if R/I is a field.

Proof. First, R/I is a field if and only if R/I has exactly two ideals (by Proposition 10.1). But by the correspondence theorem for rings, ideals in R/I are in bijection with ideals in R containing I. So R/I is a field if and only if R has exactly two ideals containing I. But this is equivalent to the condition that I is maximal (since I and R are both containing I, so if there are only two such ideals, then there can be no others). □

Example 10.11
In the case of $\mathbb{Z}$, as we've mentioned earlier, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Example 10.12
If F is a field and $P \in F[x]$ is irreducible, then $F[x]/(P)$ is a field as well — this is a construction which can be used to build new fields.

This describes what happens when we look at polynomials in *one* variable over a field, but we can try to consider what happens for polynomials in *multiple* variables as well.

10.4 Ideals in Multivariate Polynomial Rings

Example 10.13
Let $R = F[x_1, \ldots, x_n]$, where F is a field. Fixing scalars $\alpha = (\alpha_1, \ldots, \alpha_n)$ (with $\alpha_i \in F$), we have the evaluation homomorphism $F[x_1, \ldots, x_n] \to F$ defined as

$$\mathrm{ev}_\alpha : P \mapsto P(\alpha_1, \ldots, \alpha_n).$$

This map is clearly onto, as the constants in $F[x_1, \ldots, x_n]$ are sent to themselves, so by the first isomorphism theorem for rings, we have

$$F \cong F[x_1, \ldots, x_n]/\ker(\mathrm{ev}_\alpha).$$

Since F is a field, the kernel is a maximal ideal of R. In fact, this kernel can be explicitly written as

$$\mathfrak{m}_\alpha = (x_1 - \alpha_1, \ldots, x_n - \alpha_n).$$

This provides a way to construct maximal ideals of $F[x_1, \dots, x_n]$; building on this, we can also try to construct maximal ideals of *quotients* of this ring (since many rings can be constructed in this way).

Suppose that $R = F[x_1, \dots, x_n]/J$, with $J = (P_1, \dots, P_m)$. (We'll later see that for *any* J, we can find finitely many polynomials P_i which generate J; but we won't focus on that right now.) Then for any α for which $\mathfrak{m}_\alpha \supset J$, where $\mathfrak{m}_\alpha$ is the maximal ideal of $F[x_1, \dots, x_n]$ as defined above, by the correspondence theorem the image of $\mathfrak{m}_\alpha$ is also a maximal ideal of $F[x_1, \dots, x_n]/J$.

But we know $\mathfrak{m}_\alpha \supset J$ if and only if $\alpha = (\alpha_1, \dots, \alpha_n)$ is a common zero of P_1, ..., P_n (since $\mathfrak{m}_\alpha = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ contains P_i if and only if α is a zero of P_i). This gives the following construction:

Proposition 10.14
Suppose $R = F[x_1, \dots, x_n]/(P_1, \dots, P_m)$. Then any common zero $\alpha = (\alpha_1, \dots, \alpha_n)$ of P_1, ..., P_m yields a maximal ideal of R, which is the image of $\mathfrak{m}_\alpha$ when quotienting out by $(P_1, \dots, P_m)$.

The sets of common zeroes of a list of polynomials are studied in algebraic geometry. Here, we can see that such common zeroes can be used to produce maximal ideals of R. A famous theorem states that in the case $F = \mathbb{C}$, the converse is true as well:

Theorem 10.15 (Hilbert's Nullstelensatz)
Every maximal ideal of $\mathbb{C}[x_1, \cdots, x_n]$ is of the form $\mathfrak{m}_\alpha$ for some $\alpha = (\alpha_1, \cdots, \alpha_n)$.

In the name of the theorem (in German), "null" means zero, "stelen" means place, and "satz" means theorem.

This immediately implies the following corollary (since maximal ideals in $\mathbb{C}[x_1, \cdots, x_n]/(P_1, \cdots, P_m)$ are in correspondence with maximal ideals in $\mathbb{C}[x_1, \dots, x_n]$ containing all the P_i):

Corollary 10.16
The maximal ideals in $R = \mathbb{C}[x_1, \cdots, x_n]/(P_1, \cdots, P_m)$ are in bijection with the common zeroes of the polynomials P_i.

Proof of Theorem 10.15. Let $\mathfrak{m} \subset \mathbb{C}[x_1, \dots, x_n]$ be a maximal ideal; then $F = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{m}$ is a field. This gives a homomorphism from $\mathbb{C}$ to F — taking the quotient by $\mathfrak{m}$ gives a homomorphism from $\mathbb{C}[x_1, \dots, x_n]$ to F, and we can restrict the homomorphism to $\mathbb{C}$. It suffices to show that this map $\mathbb{C} \to F$ is an isomorphism — then the original homomorphism $\mathbb{C}[x_1, \dots, x_n] \to F$ from taking the quotient must map $\mathbb{C}$ isomorphically to F, and we can suppose it maps $x_i \to \alpha_i$ for each i where $\alpha_i \in \mathbb{C}$ (it really maps x_i to some element of F, but F is isomorphic to $\mathbb{C}$). Then it's clear that the kernel of this homomorphism is generated by $x_1 - \alpha_1$, ..., $x_n - \alpha_n$; therefore this kernel is $\mathfrak{m}_\alpha$ where $\alpha = (\alpha_1, \dots, \alpha_n)$, and we have $\mathfrak{m} = \mathfrak{m}_\alpha$. So now we want to show that the map $\mathbb{C} \to F$ is bijective.

But *any* homomorphism between fields is injective — the kernel of the homomorphism must be an ideal, but the only ideals of a field are $\{0\}$ and the entire field. Since the homomorphism cannot map 1 to 0, the kernel cannot be the entire field, so must be $\{0\}$.

So it suffices to show that the homomorphism is surjective. Assume not. Then F strictly contains $\mathbb{C}$ (since we have an injective map $\mathbb{C} \hookrightarrow F$, so $\mathbb{C}$ is isomorphic to its image), so we can pick $z \in F$ with $z \notin \mathbb{C}$. Then consider the elements

$$\left\{ \frac{1}{z - \lambda} \mid \lambda \in \mathbb{C} \right\}.$$

Now we'll use a bit of set theory — $\mathbb{C}[x_1, \dots, x_n]$ is a countable union of finite-dimensional vector spaces $U_1 \subset U_2 \subset \cdots$ over $\mathbb{C}$, where U_i is the vector space of polynomials with degree at most i. Then since F is a quotient of $\mathbb{C}[x_1, \dots, x_n]$, it must also be a countable union of finite-dimensional vector spaces $V_1 \subset V_2 \subset \cdots$, where V_i is simply the image of U_i in this quotient.

On the other hand, $\mathbb{C}$ is not countable, so there are uncountably many terms $1/(z - \lambda)$. Since all such terms are elements of F, one of the finite-dimensional vector spaces that F consists of must contain infinitely many of them.

But then since these terms all belong to the same finite-dimensional vector space, and there's infinitely many of them, we can find a finite set which is linearly dependent — so then we have an identity

$$\sum \frac{a_i}{z - \lambda_i} = 0,$$

where $a_i \in \mathbb{C}$ for all i and there are finitely many terms. But by clearing denominators, we can translate this into a polynomial relation in z — we then have $P(z) = 0$ for some $P \in \mathbb{C}[x]$. Then since all polynomials over $\mathbb{C}$ factor, we can write

$$P(x) = c \prod_i (x - r_i),$$

for some $r_i \in \mathbb{C}$. But $z \notin \mathbb{C}$, so z cannot equal any of the r_i, contradiction (as F is a field, so the product of nonzero terms cannot be zero).

So then the map $\mathbb{C} \to F$ must be an isomorphism, as desired. □

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng