11 More About Rings

11.1 Review: Hilbert's Nullstelensatz

Last time, we proved Hilbert's Nullstelensatz:

Theorem 11.1 (Hilbert's Nullstelensatz)
The maximal ideals in $\mathbb{C}[x_1, \cdots, x_n]$ are exactly the kernels of evaluation homomorphisms, and thus they are in bijection with $\mathbb{C}^n$.

Corollary 11.2
The maximal ideals in $\mathbb{C}[x_1, \cdots, x_n]/(P_1, \cdots, P_m)$ are in bijection with the common zeroes of $P_1, \ldots, P_m$.

It's clear that this corollary follows from the theorem, since maximal ideals in $\mathbb{C}[x_1, \ldots, x_n]/(P_1, \ldots, P_m)$ correspond to maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ containing $(P_1, \ldots, P_m)$, and a maximal ideal $\mathfrak{m}_\alpha$ contains all the P_i if and only if they all evaluate to 0 when plugging in α.

As a brief recap of the ideas seen in the proof of Theorem 11.1:

Proof Sketch. The proof reduces to showing that if F is a field containing $\mathbb{C}$, such that there exists a surjective map $\mathbb{C}[x_1, \ldots, x_n] \twoheadrightarrow F$, then $F = \mathbb{C}$. (In this case, $F = \mathbb{C}[x_1, \ldots, x_n]/\mathfrak{m}$, and the surjective map comes from taking the quotient.)

We first saw that F is a union of countably many finite-dimensional $\mathbb{C}$-vector spaces — it's clear that $\mathbb{C}[x_1, \ldots, x_n]$ is a union of countably many finite-dimensional $\mathbb{C}$-vector spaces $U_1 \subset U_2 \subset \cdots$ (we can take the vector space consisting of polynomials of degree at most d), and then to exhaust F by finite-dimensional $\mathbb{C}$-vector spaces, we can simply take the images V_i of the vector spaces U_i which exhaust $\mathbb{C}[x_1, \ldots, x_n]$. So we can write

$$F = \bigcup_{i=1}^{\infty} V_i,$$

where $\dim_{\mathbb{C}} V_i$ is finite for all i.

Now if $F \neq \mathbb{C}$, we can pick $z \in F$ with $z \notin \mathbb{C}$, and consider $1/(z - \lambda)$ for all $\lambda \in \mathbb{C}$. There are uncountably many such elements (by set theory, $\mathbb{C}$ is not countable), and since there's countably many V_i, infinitely many of these elements must lie in the same space V_i.

But then by linear algebra, there must be a finite sum

$$\sum_{i=1}^{n} \frac{a_i}{z - \lambda_i} = 0$$

with $a_i \in \mathbb{C}$ (since if n is greater than the dimension of the vector space, these elements must be linearly dependent). But clearing denominators, we get

$$\sum_{i=1}^{n} a_i \prod_{i \neq j} (z - \lambda_j) = 0.$$

But the left-hand side is a nonzero polynomial P in z — to see it's nonzero, we can plug in λ_1 and see that $P(\lambda_1) = a_1 \prod_{j>1} (\lambda_1 - \lambda_j) \neq 0$. Since $P \in \mathbb{C}[x]$, it must factor completely over $\mathbb{C}$. But z is not in $\mathbb{C}$, so it cannot equal any of the roots of P; this is a contradiction. □

Note 11.3
In fact, the theorem holds for all fields which are algebraically closed (meaning that every polynomial has a root — here we used the fact that $\mathbb{C}$ was algebraically closed in order to factor P in the final step). For example, it holds for the field of algebraic numbers as well. The specific argument we used here doesn't work in that case, since the algebraic numbers are countable; but there are other proofs as well.

Student Question. *What does it mean to take the union of vector spaces?*

Answer. *In general, this doesn't really make sense (the union of vector spaces may not itself be a vector space). But in this case, we can get vector spaces* $V_1 \subset V_2 \subset \cdots$*, by taking* $V_i = \operatorname{im}(\mathbb{C}[x_1, \ldots, x_n]_{\leq i})$ *(the notation* $\mathbb{C}[x_1, \ldots, x_n]_{\leq i}$ *denotes polynomials of degree at most* i*), and when we have an increasing chain of vector spaces, taking their union* does *make sense.*

This is important because algebraic geometry studies the sets of zeros of a polynomial, and this gives us an algebraic way to think about them.

Definition 11.4
For a ring R, the **maximal spectrum** of R, denoted $\operatorname{MSpec}(R)$, is the set of maximal ideals in R.

The maximal spectrum plays an important role in algebraic geometry and commutative algebra.

For instance, each element $r \in \mathbb{R}$ defines a "function" f_r on $\operatorname{MSpec}(R)$, where f_r sends each maximal ideal $\mathfrak{m}$ to the element $\overline{r}$ in $R/\mathfrak{m}$ (which is a field). If $R = \mathbb{C}[x_1, \ldots, x_n]/I$ is a quotient of a polynomial ring over $\mathbb{C}$, then $R/\mathfrak{m} = \mathbb{C}$ by Hilbert's Nullstelensatz, so f_r is actually a function $\operatorname{Mspec}(R) \to \mathbb{C}$. In fact, this function is given by evaluating the polynomial r at the point corresponding to $\mathfrak{m}$ — so we've recovered the original polynomial function. But in general, there isn't even a guarantee that the fields $R/\mathfrak{m}$ are all isomorphic — they may be different for different $\mathfrak{m}$. This is why "function" is in quotation marks — where the map takes values *depends* on its input.

11.2 Inverting Elements

Last time, we discussed adjoining a root of a polynomial to a ring — in particular, we discussed the structure of $R[x]/(P)$ for a monic polynomial P.

Instead of setting P to be monic, we can set it to be linear, and consider $R[x]/(ax - 1)$, which is denoted by $R_{(a)}$. We've essentially added a variable x and declared it to be the inverse of a; so $R_{(a)}$ is the result of formally inverting a. This construction is known as **localization**.

Example 11.5
We have $\mathbb{Z}_{(2)} = \{a/2^n \mid a, n \in \mathbb{Z}\}$ and $\mathbb{Z}_{(6)} = \{a/2^n 3^m \mid a, n, m \in \mathbb{Z}\}$.

However, we must be careful. In these examples, we were able to simply add a formal inverse of a to R. But it's possible that this might collapse some of R — in particular, if $ab = 0$ for nonzero a and b (which is possible in a general ring), then the image of b in $R_{(a)}$ will vanish. This is because if $ab = 0$ and the image of a is invertible, then the image of b must be 0.

Example 11.6
In $(\mathbb{Z}/6\mathbb{Z})_{(2)}$, the image of 3 vanishes — in particular, $(\mathbb{Z}/6\mathbb{Z})_{(2)} \cong \mathbb{Z}/3\mathbb{Z}$. Meanwhile, $(\mathbb{Z}/4\mathbb{Z})_{(2)}$ is the zero ring — this is because $2 \cdot 2 = 0$, but the image of $2 \cdot 2$ in $(\mathbb{Z}/4\mathbb{Z})_{(2)}$ is invertible.

So when inverting elements, we want to make sure this doesn't happen.

Definition 11.7
An element $a \in R$ is a **zero divisor** if $a \neq 0$, and there exists $b \neq 0$ for which $ab = 0$.

For example, 2 and 3 are zero divisors in $\mathbb{Z}/6\mathbb{Z}$.

Proposition 11.8
If a is *not* a zero divisor, then $R \subset R_{(a)}$.

So we can safely invert elements which are not zero divisors.

We've seen how to invert *one* element a, and this directly generalizes to let us invert finitely many elements; but we can also try to invert *all* (nonzero) elements. For this to make sense, we'd need all elements to not be zero divisors:

Definition 11.9
A ring R is an **integral domain** if R has no zero divisors.

One useful property of integral domains is that we can perform cancellation — if we have $ax = ay$ with $a \neq 0$, then we must have $x = y$.

Definition 11.10
Let R be an integral domain. Then the **fraction field** of R, denoted $\text{Frac}(R)$, is the set $\{(a, b) \mid a, b \in R, b \neq 0\}$ modulo the equivalence relation that $(a, b) \sim (c, d)$ if $ad = bc$.

This is the formal definition, but when we work with a fraction field, it's more intuitive to think of the elements as fractions in the usual sense — we write a/b instead of (a, b). The operations do work in the same way we're used to — we have

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \text{ and } \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

It's clear that $F = \text{Frac}(R)$ is a *field* containing R.

Example 11.11
A familiar example of a fraction field is $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$.

Example 11.12
The fraction field $\text{Frac}(\mathbb{C}[x])$ is called the field of **rational functions** in one variable, and is denoted $\mathbb{C}(x)$; it consists of elements of the form $p(x)/q(x)$, where p and q are polynomials. Each of its elements defines a function on $\mathbb{C}$ (which is defined everywhere except for some number of poles).

This concept can be extended to multiple variables — we can also consider the fraction field of $\mathbb{C}[x_1, \ldots, x_n]$.

Note that for a field F, we have $\text{Frac}(F) = F$ (since all nonzero elements are already invertible).

In general, giving a homomorphism from $\text{Frac}(R)$ to S is the same as giving a homomorphism from R sending nonzero elements of R to S where the image of each nonzero element of R is an invertible element in S. (Invertible elements of a ring are also called *units*.)

11.3 Factorization

Now we will discuss factorization in certain rings. A simple case is polynomials over a field.

Proposition 11.13
For a field F, every polynomial $P \in F[x]$ factors as a product of irreducible polynomials in an essentially unique way (up to rearrangement of the factors or multiplying the factors by scalars).

In order to prove this, we'll use the following lemma:

Lemma 11.14
If P is irreducible and $P \mid QS$, then $P \mid Q$ or $P \mid S$.

Proof. Since P is irreducible and all ideals of $F[x]$ are principal, (P) is a maximal ideal, and therefore $F[x]/(P)$ is a field. So if P divides Q, then the image of Q in the quotient is zero — so the lemma is equivalent to stating that there are no zero divisors in the field, which is true. More explicitly, if $P \mid QS$, then $\overline{Q} \cdot \overline{S} = 0$ (where $\overline{Q}$ denotes Q mod P), which means either $\overline{Q} = 0$ or $\overline{S} = 0$. □

The proposition then essentially follows formally:

Proof of Proposition 11.13. Proving the *existence* of such a factorization is easy — starting with a polynomial, if it isn't irreducible, then we can factor it as a product of polynomials with strictly smaller degree. Since the degree can't keep on decreasing, this process must eventually stop, at which point all our factors are irreducible. (This can be made more formal by using induction on the degree of the polynomial.)

To prove uniqueness, suppose that P factors as $P_1 \cdots P_n = Q_1 \cdots Q_m$, where all of the P_i and Q_i are irreducible. By Lemma 11.14, since P_1 divides $Q_1 \cdots Q_m$, we must have $P_1 \mid Q_i$ for some i. Without loss of generality this means $P_1 = Q_1$ — if $P_1 \mid Q_1$ then we must have $Q_1 = \lambda P_1$ for some scalar λ (since Q_1 is irreducible), and we can rescale the factors to make $\lambda = 1$. Then we have $P_2 \cdots P_n = Q_2 \cdots Q_m$, and we can perform the same argument to keep cancelling out common factors (again this can be made more formal by using induction on degree). □

This argument can be used to prove unique factorization in other situations as well, motivating the following definitions:

Definition 11.15
An integral domain is a **principal ideal domain** (PID) if every ideal is principal.

Definition 11.16
An integral domain is a **unique factorization domain** (UFD) if every element factors as a product of irreducibles in an essentially unique way.

The argument we used to prove Proposition 11.13 more generally proves that every PID is a UFD. The converse is not true — in future classes, we'll see that $\mathbb{Z}[x]$ and $\mathbb{C}[x_1, \ldots, x_n]$ are UFDs but not PIDs.

Resource: Algebra II Student Notes

Spring 2022

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