Lecture 9

Ideals and algebraic functions

9.1 Goals

1. Recall what it means to restrict functions to a subset.
2. (Definitional.) Understand what algebraic functions are on an algebraic set
3. Understand that a single algebraic function may have many different polynomial extensions
4. (Definitional.) Become familiar with the algebraic definition of ideal
5. Become familiar with the main example of an ideal: The set of all polynomial functions that vanish on a given algebraic set

9.2 Recollection: Restriction of functions, and extensions of functions

In what follows, we fix a set Y. In many examples, Y will be some Euclidean space $\mathbb{R}^n$.

9.2.1 Definition of restriction of functions

Let $g : Y \to \mathbb{R}$ be a function, and let $S \subset Y$ be any subset. Then, of course, g defines a function on S: Any element $s \in S$ is an element of Y, so $g(s)$ makes sense. When we consider g as a function on S, we will write the notation

$$g|_S.$$

We call this “g restricted to S,” or “the restriction of g to S.” To make the domain and codomain clear, one can also write:

$$g|_S : S \to \mathbb{R}.$$

Example 9.2.1. Two very different functions may restrict to the same function on S! For example, if $S = \{0\} \subset \mathbb{R}$, then all the following functions on $\mathbb{R}$ restrict to the same function on S:

$$g(s) = x^2, \qquad h(s) = x, \qquad j(s) = \sin(x), \qquad k(s) = e^0 - 1.$$

So even though $g \neq h$, it is true that $g|_S = h|_S$ in the above examples.

9.2.2 Extensions

Sometimes, we want to ask if a function on a subset extends to a function on a big set.

Definition 9.2.2. Fix $S \subset Y$, and a function $f : S \to \mathbb{R}$. We say that a function $g : Y \to \mathbb{R}$ is an *extension of f* if $g|_S = f$. In other words, g is an extension of f if for every $x \in S$, we have $g(x) = f(x)$.

What we saw in Example 9.2.1 is that a single function on S may have many different extensions to Y.

9.2.3 Restriction is a ring homomorphism

Given a set S, the collection of real-valued functions on S is a ring. For example, given two functions $f_1, f_2 : S \to \mathbb{R}$, we can define a new function $f_1 + f_2$ by declaring

$$(f_1 + f_2)(x) = f_1(x) + f_2(x).$$

Then the constant function sending every $x \in S$ to $0 \in \mathbb{R}$ is the additive identity, and given a function f, its additive inverse is the function sending x to $-f(x)$.

Likewise, one can define a new function $f_1 f_2$ by declaring

$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

Then the function sending every element of S to the number 1 is a multiplicative identity. In fact, the set of all functions on S is a commutative ring. This is a fancy way of articulating an intuition you already had: You can add and multiply functions.

Proposition 9.2.3. Let Y be a set and fix a subset $S \subset Y$. Restriction

$$\{\text{Functions } Y \to \mathbb{R}\} \to \{\text{Functions } S \to \mathbb{R}\}, \qquad g \mapsto g|_S$$

is a ring homomorphism. In other words, for any two functions $g, h : Y \to \mathbb{R}$, we have

$$(g+h)|_S = g|_S + h|_S, \qquad (gh)|_S = g|_S h|_S; \qquad \text{and} \qquad 1|_S = 1.$$

9.3 Algebraic functions

So far we've defined what *algebraic sets* are—these are subsets of $\mathbb{R}^n$ that can be realized as the common zero set of some collection of functions. These algebraic sets are the kinds of shapes I'd like to study for the moment. I mentioned in Section 7.2 that fields of math can be divided into the kinds of spaces, and the kinds of functions between these spaces, one decides to contemplate. So let me tell you what kinds of functions I want to study.

Definition 9.3.1. Let $X \subset \mathbb{R}^n$ be an algebraic set. Then a function $f : X \to \mathbb{R}$ is called an *algebraic function* if f extends to some polynomial function on $\mathbb{R}^n$. Put another way, f is algebraic if there exists a polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ so that, for every $x \in X$, we have $f(x) = p(x)$.

Notation 9.3.2. Let $X \subset \mathbb{R}^n$ be an algebraic set. We let

$$\mathcal{O}_X(X)$$

denote the set of algebraic functions on X.

Remark 9.3.3. The notation $\mathcal{O}_X(X)$ is a bit funny. One might be tempted to simply write $\mathcal{O}_X$ or $\mathcal{O}(X)$, but I promise that $\mathcal{O}_X(X)$ is a notation used widely enough that people will know what you mean.

Remark 9.3.4. There is a generalization to any commutative ring: Fix a commutative base ring R, and an algebraic set $X \subset R^n$. Then a function $f : X \to R$ is also called algebraic if there exists a polynomial function $p \in R[x_1, \dots, x_n]$—which one can think of as a function $R^n \to R$—so that p agrees with f at all points of X.

Remark 9.3.5. So the word "algebraic" is an adjective that can be used for two kinds of objects: Subsets of $\mathbb{R}^n$ (Definition 8.3.8), and functions on subsets of $\mathbb{R}^n$ (Definition 9.3.1).

Example 9.3.6. Let $X = \mathbb{R}^n$. Then $\mathcal{O}_X(X) = \mathbb{R}[x_1, \dots, x_n]$.

Example 9.3.7. Let $X = \{a_1, \dots, a_n\} \subset \mathbb{R}$ be any finite collection of n points on the real line. Then a function $f : X \to \mathbb{R}$ is just a choice of n real numbers:

$$t_1 =: f(a_1), \qquad \dots, \qquad t_n =: f(a_n).$$

Moreover, we can find a polynomial in one variable, $p(x)$, so that for all elements $a_i \in x$, we have that $p(a_i) = t_i$. For example, take:

$$p(x) = \sum_{i=1}^{n} \left(((x - a_i) + t_i) \prod_{j \neq i} \frac{x - a_j}{a_i - a_j} \right).$$

So, if X is any algebraic subset of $\mathbb{R}$, then *any* function on X is algebraic. But the situation is very different for algebraic subsets in higher dimensions. There are many functions on an algebraic set that are not algebraic.

So, if X is a set of n distinct points in $\mathbb{R}$, we have a bijection

$$\mathcal{O}_X(X) \cong \mathbb{R}^n.$$

Example 9.3.8. Let $X \subset \mathbb{R}^2$ be the x-axis. Then the function $f(x) = x^2$ on the x-axis has many extensions to $\mathbb{R}^2$. For example, $g(x, y) = x^2 + y$ restricts to f along X. So does the function $h(x, y) = x^2 + e^y - 1$. It turns out g is polynomial, while h is not. Regardless, the existence of g means that f is an algebraic function on X.

Example 9.3.9. Let $X \subset \mathbb{R}^2$ be the x-axis. Then the function $f(x) = \sin(x)$ is *not* algebraic. The reason is as follows: Any polynomial function $g(x, y)$ must either (i) have only finitely many 0s along X, or (ii) be identically equal to 0 along X.

Here is why: The set X is defined by the equation $y = 0$, so the restriction of $g(x, y)$ to X is computed by plugging in $y = 0$. Writing $g(x, y) = \sum_{i,j} a_{i,j} x^i y^j$, we see that $g|_X(x, 0) = g(x, 0) = \sum_{i,j} a_{i,j} x^i 0^j = \sum_{i,j} a_{i,0} x^i$. (Because if $j \geq 1$, we see $y^j = 0^j = 0$.) In paticular, $g|_X$ is a polynomial in one variable, which means it must satisfy either (i) or (ii) above.

So f could not be the restriction of any polynomial g. This shows f is not an algebraic function on X.

Remark 9.3.10. Fix an algebraic set $X \subset \mathbb{R}^n$. By definition, given any polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ restricts to an algebraic function on X. Thus, we have a restriction map

$$\mathbb{R}[x_1, \ldots, x_n] \to \mathcal{O}_X(X).$$

More generally, if $Y \subset \mathbb{R}^n$ and $X \subset \mathbb{R}^n$ are both algebraic sets, and if $X \subset Y$, then we have a restriction map

$$\mathcal{O}_Y(Y) \to \mathcal{O}_X(X).$$

9.4 Algebraic functions can have different polynomial extensions

Let $X = \{(x, y) \,|\, y^2 - x = 0\}$. (This is a parabola inside $\mathbb{R}^2$.) Let f be the function that sends every point $(x, y) \in X$ to the number x.

Then f has many different algebraic extensions:

1. Define $g : \mathbb{R}^2 \to \mathbb{R}$ to be the function $g(x, y) = x$. Then, of course, $g|_X = f$.

2. Define $h : \mathbb{R}^2 \to \mathbb{R}$ to be the function $h(x, y) = x + 7y^2 - 7x$. Of course, g does not equal h as a function on $\mathbb{R}^2$. But what about their restrictions to X? If $(x, y) \in X$, we know that $y^2 - x = 0$. Thus, if $(x, y) \in X$, we have:

   $$h(x, y) = x + 7y^2 - 7x = x + 7(y^2 - x) = x + 7 \cdot 0 = x = g(x, y).$$

   In other words, $h|_X = g|_X$.

3. Fix any polynomial $p \in \mathbb{R}[x, y]$. Consider the function $j = g + p \cdot (y^2 - x)$. Then if $(x, y) \in X$, we have:

   $$j(x, y) = g(x, y) + p(x, y)(y^2 - x) = g(x, y) + p(x, y) \cdot 0 = g(x, y).$$

9.5 Functions that restrict to zero (i.e., functions that extend zero)

So fix an algebraic set X inside $\mathbb{R}^n$. In general, it may be very hard to identify every algebraic function on X. Here's another (in general, difficult) question to ask: Can we identify all the polynomial function son $\mathbb{R}^n$ that restrict to 0 on X?

Example 9.5.1. Let $X = \{3\} \subset \mathbb{R}$ be the set containing exactly one element of $\mathbb{R}$ called 3. Can we say exactly what polynomials in one variable restrict to the 0 function on X? Tautologically, the set of such polynomials is exactly the set of polynomials that vanish at $x = 3$. For example, the set of functions that vanish at $x = 3$ contains the following polynomials:

$$x - 3, \qquad (x-3)^2, \qquad x(x-3), \qquad (7 - x + x^2)(x-3)$$

and more.

Because this notion will be important to us, we give it some notation:

Notation 9.5.2. Let $X \subset \mathbb{R}^n$ be an algebraic set. We let $I(X)$ denote the set of all polynomials $g \in \mathbb{R}[x_1, \ldots, x_n]$ for which $g|_X = 0$. In other words, $I(X)$ is the set of all polynomials g satisfying the following property:

$$x \in X \implies g(x) = 0.$$

Remark 9.5.3. Put another way, $I(X)$ is the set of all functions $p \in \mathbb{R}[x_1, \ldots, x_n]$ that get sent to zero under the restriction map $\mathbb{R}[x_1, \ldots, x_n] \to \mathcal{O}_X(X)$ (Remark 9.3.10).

As usual in math, if we cannot identify an answer on the nose, we can at least try to identify some useful *properties* that an answer would satisfy.

Proposition 9.5.4. Let $X \subset \mathbb{R}^n$ be an algebraic set. Then $I(X)$ satisfies the following properties:

1. If $g, h \in I(X)$, then $g + h \in I(X)$. (In other words, $I(X)$ is closed under addition.)

2. If $g \in I(X)$ and $p \in \mathbb{R}[x_1, \ldots, x_n]$, then $gp \in I(X)$. (In other words, $I(X)$ is closed under scaling by elements of $\mathbb{R}[x_1, \ldots, x_n]$.)

Proof. (1) It suffices to show that if $g|_X = h|_X = 0$, then $(g+h)|_X = 0$. Well, to see this, take any $x \in X$. Then $(g+h)(x) = g(x) + h(x) = 0 + 0$. (The last equality is because both g and h equal 0 on X.) So we conclude $(g+h)(x) = 0$, meaning $g + h \in I(X)$.

(2) It suffices to show that for all $x \in X$, we have $(gp)(x) = 0$. Well, $(gp)(x) = g(x)p(x) = 0 \cdot p(x)$, where the last equality is by the assumption that $g \in I(X)$. Of course, for any value of $p(x)$, we have that $0 \cdot p(x) = 0$, so we conclude $(gp)(x) = 0$ for every $x \in X$. This shows $gp \in I(X)$. □

9.6 Ideals

In short, $I(X)$ is a subset of the ring $\mathbb{R}[x_1, \ldots, x_n]$ that is closed under addition and under scaling. And regardless of the algebraic set X, $I(X)$ satisfies these properties. Such subsets are so important that we give them a name:

Definition 9.6.1 (Ideals)**.** Let R be a commutative ring. A subset $I \subset R$ is called an *ideal* of R if:

1. I is non-empty.

2. For all $x, y \in I$, we have that $x + y \in I$.

3. For all $x \in I$ and $r \in R$, we have that $rx \in I$.

Put another way, Proposition 9.5.4 says that—for any algebraic set $X \subset \mathbb{R}^n$—the set $I(X)$ is an ideal of $\mathbb{R}[x_1, \ldots, x_n]$.

Remark 9.6.2. We thus see that every algebraic subset $X \subset \mathbb{R}^n$ defines an ideal $I(X) \subset \mathbb{R}[x_1, \ldots, x_n]$. So one may ask a question: Does *every* ideal of $\mathbb{R}[x_1, \ldots, x_n]$ arise from an algebraic subset of $\mathbb{R}^n$?

The answer turns out to be no, but this answer leads to a deep innovation. Perhaps we should think of ideals not as not only coming from geometrically significant things like algebraic sets, but we should explore a way in which every ideal does define a geometrically significant object more general than an algebraic set. This mode of thought gains us huge mileage in the field of algebraic geometry, though we won't be able to explore it much in this course.

9.7 Examples of proofs involving ideals

Let's see some properties of ideals. I emphasize that the properties in the following proposition are not part of the definition of "ideal," but are consequences of the definition of "ideal."

Proposition 9.7.1. Let R be a commutative ring and let $I \subset R$ be an ideal. Then the following hold:

(a) $0 \in I$. (Ideals always contain the additive identity.)

(b) If $1 \in I$, then $I = R$. (Ideals almost never contain the multiplicative identity; when they do, they are equal to the ring itself.)

(c) If $x \in I$, then $-x \in I$. (Ideals are closed under additive inverses.)

Proof. (a) Because I is an ideal, it is non-empty. So fix $x \in I$. Because I is closed under scaling, $rx \in I$ for any $r \in R$. So choose $r = 0$. Then by Proposition 2.4.4, $rx = 0x = 0$. This shows $0 \in I$.

(b) By assumption, $I \subset R$. So we must show that $R \subset I$. Fix $r \in R$. Because $1 \in I$ by assumption, we know that $r \cdot 1 \in I$ because I (being an ideal) is closed under scaling by elements of R. But of course, $r \cdot 1 = r$, so this shows $r \in I$.

(c) Again because I is closed under scaling by elements of R, if $x \in I$, we know that $-1 \cdot x \in I$. By Proposition 2.4.5, we conclude $-x \in I$.

□

Proposition 9.7.2. Fix a commutative ring R and let I and J be ideals of R. Then $I \cap J$ is an ideal of R.

Proof. We must show that $I \cap J$ satisfies the two defining properties of ideals.

(Closure under addition.) Suppose that $x, y \in I \cap J$. Then $x, y \in I$, so $x+y \in I$ because I is an ideal. Likewise, $x, y \in J$ by definition of intersection, so $x + y \in J$ because J is an ideal. As $x + y$ is in I and in J, we conclude $x + y \in I \cap J$.

(Closure under scaling.) Suppose that $x \in I \cap J$, and let $r \in R$. Well,

$$x \in I \cap J \implies x \in I \implies rx \in I$$

where the last implication is because I is an ideal. Likewise,

$$x \in I \cap J \implies x \in J \implies rx \in J.$$

Thus rx is an element of both I and of J, showing $rx \in I \cap J$. □

9.8 Examples of ideals

9.8.1 The two "trivial" ideals

Let R be a commutative ring. Then the set $I = \{0\}$ consisting only of the additive identity is an ideal. This is obvious: $0 + 0 = 0 \in I$, and for any $r \in R$, we have $r \cdot 0 = 0$. This choice of I is often called the *zero ideal*.

Likewise, the set $I = R$ consisting of the entire ring is also an ideal. This ideal rarely comes up, but it is an ideal that could be called a "trivial ideal." (The other thing that could be called the trivial ideal is the zero ideal.)

These two ideals only coincide if R is the zero ring—the ring consisting of one element.

9.8.2 Ideals of $\mathbb{Z}$

The ring of integers $\mathbb{Z}$ has very concrete ideals.

Notation 9.8.1. Fix any integer $n \in \mathbb{Z}$. We let

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

denote the set of all integers obtained by multiplying n by some integer. In other words, $n\mathbb{Z}$ is the set of all multiples (negative and positive) of n. Sometimes, we will also write

$$(n)$$

instead of $n\mathbb{Z}$.

Example 9.8.2. (a) $0\mathbb{Z} = \{0\}$ is the zero ideal.

(b) $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$.

(c) $1\mathbb{Z} = \mathbb{Z}$.

(d) $-3\mathbb{Z} = 3\mathbb{Z}$.

(e) $6\mathbb{Z} = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}$.

9.8.3 Principle ideals

Notation 9.8.3. Let R be a commutative ring and fix an element $f \in R$. We let

$$(f)$$

denote the smallest ideal of R containing f. We say that (f) is the *ideal generated by f*.

It is not a priori obvious that such a "smallest" ideal exists, or what it means to be "smallest." Let's make it precise:

Proposition 9.8.4. Let R be a commutative ring and fix an element $f \in R$. Let I denote the set of all elements in R that can be factored by f. That is, $x \in I$ if and only if there exists some $x' \in R$ for which $x = fx'$. Then

(a) I is an ideal, and I contains f.

(b) If J is any other ideal containing f, then $I \subset J$. (This shows that I is the smallest ideal containing f.) In other words, (f) is precisely the set of all elements of R that can be factored by f.

(c) In fact, I is the intersection of all ideals containing f.

Proof. (a) Suppose that x and y are in I, so that $x = fx'$ and $y = fy'$. Then $x + y = fx' + fy' = f(x' + y')$, meaning that $x + y$ is factored by f. This shows $x + y \in I$. Now, if $x \in I$ and $r \in R$, then $xr = (fx')r = f(x'r)$, showing that xr can also be factored by f. This shows I is an ideal. Finally, note that $f = f1$, so f is factored by itself; this shows that $f \in I$.

(b) We must show that if $x \in I$, then $x \in J$. Well, if $x \in I$, then we know that $x = fx'$ for some $x' \in R$. But J is an ideal, so if $f \in J$, then $fx' \in J$.

(c) The previous proof shows that I is contained in the intersection of all ideals having f as an element. So now we must show that the intersection of all such ideals is contained in I—but this is trivial. After all, I is an ideal containing f, so the intersection of I with anything else is a subset of I.

□

Definition 9.8.5. Let R be a commutative ring and I an ideal of R. We say that I is a *principal ideal* if there exists an element $f \in R$ for which $I = (f)$.

Example 9.8.6. Let $R = \mathbb{R}[x, y]$, and choose a polynomial f. For example, choose $f(x, y) = y - x^2$. Then the ideal generated by f is the set of all polynomials divisible by f. In other words, (f) is the set of all polynomials of the form pf where p is some polynomial.

Though it is not obvious, it turns out that not all ideals are principal.

9.8.4 Functions vanishing along a fixed set

Finally, let me just remind you that if $X \subset \mathbb{R}^n$, then the set of all functions that vanish along X is an ideal. See Proposition 9.5.4. Though we will not see a proof, very few ideals of the form $I(X)$ are principal. For example, if $X \subset \mathbb{R}^2$ consists of a single point, $I(X)$ is not principal (though we do not prove this fact).

9.9 Exercises

Exercise 9.9.1. Show that the polynomial given in Example 9.3.7 indeed satisfies the property that $p(a_i) = t_i$.

Exercise 9.9.2. Here are two facts about the set of all integers that you may have seen before: (1) *The well-ordering principle*: If $A \subset \mathbb{Z}$ is a subset consisting of only *positive* integers (meaning $a \in A \implies a > 0$) then A contains a least element (meaning an element a_0 so that $a \in A \implies a_0 \leq a$).

(2) *The Euclidean algorithm*: If m and n are two integers, then you can find integers a, b so that $am + bn = gcd(m, n)$ where $gcd(m, n)$ is the greatest common divisor of m and n. (This implies in particular that $gcd(m, n) \leq m$ and $gcd(m, n) \leq n$.)

You may take the above two facts for granted. Doing so, prove that *every* ideal of $\mathbb{Z}$ is a principal ideal.

Exercise 9.9.3. Let R be a commutative ring. Suppose that r, s, x are elements of R for which $rx = s$. Prove that $(s) \subset (r)$.

Exercise 9.9.4. Let R be a commutative ring and fix $r, s \in R$. Show that if $(r) = (s)$, then there exists some $x \in R$ satisfying the following properties: (i) $rx = s$, and (ii) There exists some $y \in R$ so that $xy = 1$.

9.10 Extra credit

(a) Let $X \subset \mathbb{R}^n$ be a finite set. Prove that X is algebraic. (You may have done this in a previous exercise.)

(b) Let $f : X \to \mathbb{R}$ be any function. Prove that f is algebraic.