AN INTRODUCTION TO RINGS WITH ALGEBRAIC CURVES

LIAM EIFERT

Abstract. We will develop some concepts in ring theory and in classical algebraic geometry so that they are accessible to a reader with no background in algebra. We present an example using the integers and one using polynomials for each new ring theory concept with the first often trying to offer clarity and the second motivation. At the same time, we will try to build up the theory of algebraic curves using ample graphs to emphasize the geometric intuition. We finish with a discussion of the multiplicity of points on a curve and some other interesting techniques that have applications in more advanced topics in algebraic curves.

Contents

1. Rings and Ideals

The purpose of this paper is firstly to introduce ring theory guided by concrete examples. Our two example rings will be the integers and polynomials with coefficients in the field k. As is standard, we refer to the integers as $\mathbb{Z}$ and the polynomials of n variables with the coefficients in the field k as $k[x_1, x_2, \dots x_n]$. When dealing with 2 or 3 variables we will often use $k[x, y]$ or $k[x, y, z]$. Secondly, this paper also seeks to gradually introduce the reader to some basic ideas of classical algebraic geometry which arise naturally when studying polynomial rings. Before proceeding any further we clarify in what way the integers and polynomials are similar: the definition of a ring.

Definition 1.1. A *ring* R is a set endowed with two binary operations, which we call addition, denoted with "+" and multiplication, denoted with "$\cdot$". For those familiar with the field axioms, a ring follows all the field axioms except for the

existence of multiplicative inverses for non-zero elements and the commutivity of multiplication. [1] The ring axioms are therefore as follows for all $r, s, t \in R$:

RA(1) Addition is commutative, so $r + s = s + r$
RA(2) Addition is associative, so $r + (s + t) = (r + s) + t$
RA(3) There exists an additive identity, 0 such that for all $r \in R$, then $r + 0 = r$
RA(4) There exist additive inverses for all $r \in R$, which we denote $(-r)$, such that $r + (-r) = 0$
RA(5) Multiplication is associative, so $r \cdot (s \cdot t) = (r \cdot s) \cdot t$
RA(6) Multiplication distributes with respect to addition, so $r \cdot (s + t) = rs + rt$ and $(s + t) \cdot r = sr + tr$

For our purposes when we refer to a ring in the rest of this paper we will usually mean a commutative ring with identity in which $r \cdot s = s \cdot r$ and there exists a multiplicative identity, 1 for which $r \cdot 1 = 1 \cdot r = r$.

We recognize that $\mathbb{Z}$ is a ring with the regular notions of addition and multiplication. It is the prototypical example of a ring.

To see that $k[x, \dots, x_n]$ is a ring we can once again use the familiar notions of addition and multiplication of polynomials. We can reduce it to the single variable case by considering $k[x_1, \dots x_{n-1}][x_n]$. This is the polynomial ring of one variable, x_n, with coefficients as polynomials in $n - 1$ variables over a field k, $k[x_1, \dots, x_{n-1}]$.[2] This trick will come up again and is important in many inductive arguments. We will not go through the process of verifying each ring axiom for the single variable case since the proof would be quite tedious and overly formal which goes against the spirit of this paper.

In a course on rings, one would follow these axioms carefully and deduce some different classifications and properties of rings (we have already done so by restricting ourselves to commutative rings). The theory developed has powerful, wide-ranging applications, but this might not be obvious to beginners. This paper therefore aims to use plenty of examples to motivate the study of rings. We now present the definition of an ideal along with examples in the integers and polynomials.

Definition 1.2. An *ideal*, I, is a subset of a ring R that satisfies the following two properties:
(1) If $a, b \in I$ then $a + b \in I$
(2) if $r \in R$, and $a \in I$, then $ra \in I$

We note that the concept of an ideal is actually *stronger* than that of a subring. An ideal is a subring which *also* "swallows up" elements of R (which may not be in the ideal) by multiplication such that products remain in the ideal. The simplest ideals of any ring are the ring itself and $\{0\}$.

Example 1.3. We can find ideals of the integers from the common concept of "multiples" of any integer. For example, if we take the positive and negative multiples of 5 then we form an ideal which we denote $5\mathbb{Z}$. It satisfies our two properties

[1] Note that some authors require a ring to contain a multiplicative identity and refer to those that don't as "rngs", and a few do not require the associativity of multiplication.

[2] The observant reader may object here that $k[x_1, \dots, x_{n-1}]$ is not a field, but this is not a necessary condition of a polynomial ring in general, just the type of polynomial ring which we are choosing to study.

of an ideal since the sum of any two multiples of 5 is a multiple of 5 and the product of any integer and a multiple of 5 is a multiple of 5. It turns out that these multiples form all of the ideals of the integers, but this is not important to the paper so we will not prove this.

Before continuing with an example of an ideal of polynomials, we discuss the field k which forms the coefficients. Until otherwise stated it will be perfectly fine for the reader to imagine k as any field and in particular may be helpful to use the real or rational numbers to develop intuition. However, eventually we will require that k is algebraically complete and usually use the complex numbers, $\mathbb{C}$.

Example 1.4. Let us consider the ring $k[x, y]$ and its ideal

$$I((0,0))^{3} = \{p(x,y) \in k[x,y] \mid p(0,0) = 0\}.$$

We are treating our polynomials as *functions* of x and y here in the normal way, so we recognize that

$$\text{if } q(0,0) = 0 \text{ and } p(0,0) = 0, \text{ then } (p+q)(0,0) = p(0,0) + q(0,0).$$

Additionally,

$$\text{if } p(0,0) = 0, \text{ then } p(0,0)q(0,0) = 0(q(0,0)) = 0 \text{ whether or not } q(0,0) = 0.$$

So, we see that $I((0,0))$ is an ideal. However, we also recognize that all the terms of the polynomial with a variable will vanish at $(0,0)$ so the polynomial evaluates to be equal to its constant term there. Therefore, $I((0,0))$ is also just the set of all polynomials composed of only x^i and y^i terms for all $i \in \mathbb{N}$ since the constant term is equal to 0.

We saw in both of our previous examples that we were able to reduce our ideal down to some essential elements. To formalize this, we introduce the following definition.

Definition 1.5. A set S generates an ideal $I \subset R$ if

$$I = \left\{ \sum_i a_i s_i \mid a_i \in R, s_i \in S \right\}$$

In general for any $S \subset R$ then the ideal generated by S is (S), so if S generates I then $(S) = I$.

This is a bit like a spanning set in linear algebra except instead of coefficients in front of each element being from a field, instead they are now elements of the larger ring which the spanning set is a part of.

We can now recognize that our ideals from Example 1.3 and Example 1.4 are generated by $\{5\}$ and $\{x, y\}$ respectively, so $5\mathbb{Z} = (\{5\})$ and $I((0,0)) = (\{x, y\})$. Often we will drop the set notation brackets inside the parenthesis if what we mean is clear. We will have more to say about the ideals and generators later, but we now move to discuss the geometric significance of the ideals of polynomial rings as motivation.

[3]This notation will be formalized and explained in the next section.

2. Algebraic Sets and Ideals

We begin with some of the fundamental ideas of algebraic curves.

Definition 2.1. If $S \subset k[x_1, \dots x_n]$ then

$$V(S) = \{P \in k^n \mid \text{for all } f \in S, f(P) = 0\}$$

we call this the *vanishing set* of S.

Now we consider the reverse direction, taking points to polynomials as we did in Example 1.4.

Definition 2.2. If $A \subset k^n$, we take

$$I(A) = \{f \in k[x_1, \dots, x_n] \mid A \subset V(f)\}.$$

We recognize that for any $A \subset k^n$, $I(A)$ is always an ideal of the ring $k[x_1, \dots, x_n]$ with the same reasoning we went through in Example 1.4. We therefore refer to $I(A)$ as the *ideal* of A.

Definition 2.3. An *algebraic set* or equivalently, a *variety* is some $V \subset k^n$ such that there exists some set $S \subset k[x_1, \dots x_n]$ such that $V(S) = V$.

Example 2.4. For easier visualization, let $k = \mathbb{R}$ and consider S to be the set of points which comprise the unit circle on the plane. So, we have that

$$S = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}.$$

First, since $V(x^2 + y^2 - 1) = S$ we recognize that S is an algebraic set. Let us now consider $I(S)$ and examine some of the polynomials in it. To properly graph them, we will consider them in three variables, so their intersection with the $x - y$ plane will always include the unit circle. The simplest example[4] is, as mentioned, the polynomial $x^2 + y^2 - 1$. Its graph is a paraboloid which we can visualize in 3D space and its vanishing set is its intersection with the plane $z = 0$. We consider a few functions in $I(S)$ on the next page:

[4]This notion of "simplest" will be made more rigorous in section 4

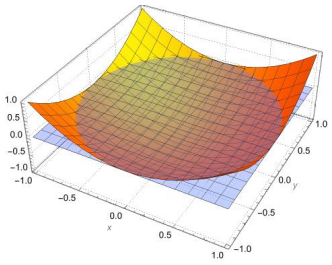

FIGURE 1. A 3D rendering of $x^2+y^2-1=z$

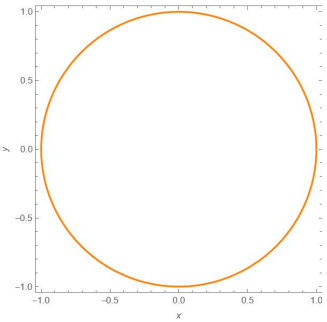

FIGURE 2. $V(x^2+y^2-1)$

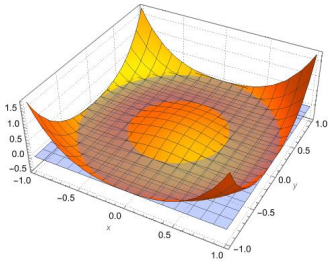

FIGURE 3. A 3D rendering of $(x^2+y^2-1)(x^2+y^2-\frac{1}{4})=z$

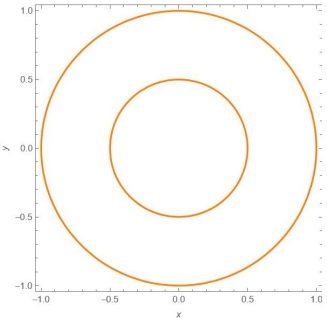

FIGURE 4. $V((x^2+y^2-1)(x^2+y^2-\frac{1}{4}))$

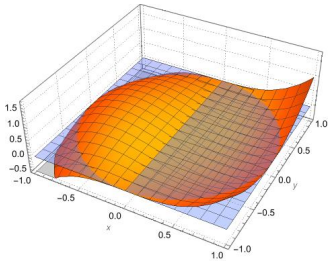

FIGURE 5. A 3D rendering of $(x^2+y^2-1)(x)=z$

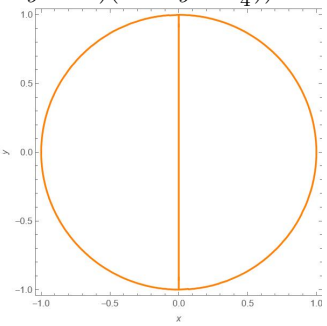

FIGURE 6. $V(x^2+y^2-1)(x)$

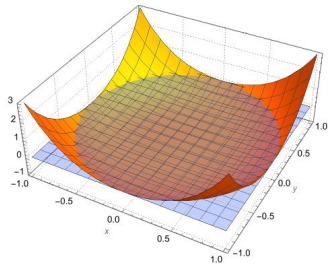

FIGURE 7. A 3D rendering of $(x^2+y^2-1)(x^2+y^2+1)=z$

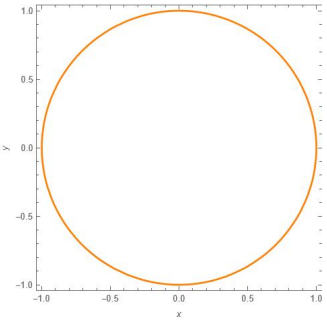

FIGURE 8. $V(x^2+y^2-1)(x^2+y^2+1)$

This geometric intuition from the real numbers is immensely useful in the study of polynomial rings. Notice, however, that in our last example we have another, quite different polynomial, $(x^2+y^2-1)(x^2+y^2+1)$, whose vanishing set is exactly the unit circle. This happens because x^2+y^2+1 has no zeroes over the real numbers. If we choose our field more carefully then we avoid this problem and the correspondence between sets of points and polynomials becomes even stronger. First, however, we need a definition.

Definition 2.5. An *algebraically closed field* is a field, k in which every polynomial in $k[x]$ has a root.

The most commonly used algebraically closed field, both generally and for algebraic curves, is the complex numbers, $\mathbb{C}$.

Theorem 2.6 (Hilbert's Weak Nullstellensatz)**.** *If k is algebraically closed, then if f is a polynomial of n variables then f there exists some $P \in k^n$ such that $f(P) = 0$.*

Proof. The proof of this theorem is beyond the scope of this paper and takes up multiple sections of Fulton's *Algebraic Curves*, one of the main references for this paper. Rather than proving this theorem therefore, we emphasize that when dealing with one variable, the definition of algebraically closed already suffices. The proof is the process of showing that this extending this fact to polynomials with an arbitrary number of variables. □

Before moving on, we return to Example 2.4 and note that if the reals were algebraically closed, then Theorem 2.6 would imply that with C a constant, $C(x^2+y^2-1)$ would be the only polynomials which vanish on just the unit circle. Of course, the reals are not algebraically complete because of polynomials like x^2+y^2+1, but by looking at examples which do have solutions, we can get a geometric intuition for curves on algebraically complete fields which are much harder to visualize.

3. Modular Arithmetic, Coordinate Rings, the Rationals, and Rational Functions

Definition 3.1. Given an ideal I and its ring, R, we can define the following equivalence relation.

$$\text{if } a, b \in R \text{ then } a \sim b \text{ if } a - b \in I.$$

One can verify that this is indeed an equivalence relation using the definition of an ideal and the ring axioms. We can therefore split up R into equivalence classes of elements which are all equal under this equivalence relation. Informally, we refer to this process "modding out" by an ideal. The *quotient ring* is the ring formed by these equivalence classes which we denote R/I. Addition and multiplication in R/I is defined by "lifting" representatives from each class.

So, if $a \in [a] \in R/I$ and $b \in [b] \in R/I$, then $[a]+[b] = [a+b]$ and $[a]\cdot[b] = [ab]$. One can verify that this operation is well defined, meaning that no matter which representative if lifted from each class the sum and product will be the same.

Example 3.2. Recall from Example 1.3 that the multiples of 5 are an ideal in $\mathbb{Z}$ and we denote them by $5\mathbb{Z}$. We can therefore "mod out" $\mathbb{Z}$ by $5\mathbb{Z}$ to get the quotient ring $\mathbb{Z}/5\mathbb{Z}$. We notice that since $0 \in 5\mathbb{Z}$ then if $x \in 5\mathbb{Z}$, $x - 0 \in 5\mathbb{Z}$, so

$x \sim 0$ and $x \in [0]$. We observe that $\mathbb{Z}/5\mathbb{Z}$ contains only the four additional elements:

[1]: if $z = 1 + w$ where $w \in 5\mathbb{Z}$ then $z \in [1]$ since $z - 1 = w \in 5\mathbb{Z}$
[2]: if $z = 2 + w$ where $w \in 5\mathbb{Z}$ then $z \in [2]$ since $z - 2 = w \in 5\mathbb{Z}$
[3]: if $z = 3 + w$ where $w \in 5\mathbb{Z}$ then $z \in [3]$ since $z - 3 = w \in 5\mathbb{Z}$
[4]: if $z = 4 + w$ where $w \in 5\mathbb{Z}$ then $z \in [4]$ since $z - 4 = w \in 5\mathbb{Z}$

We could also consider [5] in this way but it is better to consider it as [0] since it is more clear that it is the additive identity. One could additionally verify that if $z = x + w$ where $w \in 5\mathbb{Z}$ and $x > 5$ or $x < 0$ then we can reduce down to one of the previous cases. Another way to think of these equivalence classes in the integers is with the familiar concept of remainders when dividing. Each class is just what remainder we get when we divide by 5. It is notable that these remainders form a ring. For any $n \in \mathbb{Z}$ we refer to $\mathbb{Z}/n\mathbb{Z}$ as *the integers modulo n*.

Example 3.3. We consider the ring $k[x, y]$ and its ideal, $I((0, 0))$ from Example 1.4. We want to consider $k[x, y]/I((0, 0))$. Consider $f, g \in k[x, y]$. From the definition of a quotient ring, we know that $f \sim g$ if and only if $f - g \in I((0, 0))$. We recall from the definition of $I((0, 0))$ that this implies that $f(0, 0) - g(0, 0) = 0$. So,

$$f \sim g \text{ if and only if } f(0, 0) = g(0, 0).$$

So, for example we see that $x - y + 7 \sim 7$ since they evaluate the same at $(0, 0)$. And in particular that if $f \in k[x, y]$ then there exists some $C \in k$ such that $f \in [C]$ where C is just a constant polynomial.

The previous example motivates the following definition:

Definition 3.4. We define the *coordinate ring* of some algebraic subset $V \subset k^n$ as $k[x_1, \ldots x_n]/I(V)$. We denote the coordinate ring of V as $\Gamma(V)$.

We observe that the coordinate ring on some algebraic subset V can be interpreted as all of the polynomial *functions* from $k^n \to V$ since if some f and g totally agree on V then for all $P \in V$, $(f - g)(P) = 0$. This implies that $f - g \in I(V)$, so $[f] = [g]$. In Example 3.3 V was a single point so this was particularly clear since the output space was just some element of our field (some number).

Definition 3.5. Given any commutative ring with identity where the product of two elements is never 0 we can make it into a field by taking its *fraction field*. The name is suggestive since the construction is much like taking the set of all fractions given a field. A strict definition can be found in [4] but is unnecessary for our purposes.

Example 3.6. We will spare the details of checking this, but if we take the fraction field of $\mathbb{Z}$ then we end up with $\mathbb{Q}$.

Definition 3.7. If we take the fraction field of $\Gamma(V)$ then we end up with the *field of rational functions* on V, $k(V)$. Equivalently, once could consider the fraction field of $k[x_1, \ldots, x_n]$ then mod that out by $I(V)$ to get $k(V)$.

Definition 3.8. We can also consider the set of rational functions on V defined at $P \in k^n$, the *local ring* of V which we denote $\mathcal{O}_P(V)$. This is the set of rational functions defined at P which means that we remove any rational functions which are undefined at P. A rational function being undefined at P has its usual meaning that the denominator evaluates to 0 at P.

Remark 3.9. Note that $\mathscr{O}_P(V)$ is once again a ring and not a field since any polynomial which evaluates to 0 on V will lack a multiplicative inverse. If an element has a multiplicative inverse we say it is a *unit*. Observe therefore that the set of all non units in $\mathscr{O}_P(V)$ is the set that has a numerator in $I(P)$, which in turn is merely the ideal in $\mathscr{O}_P(V)$ generated by $I(P)$.

The local ring is very useful in understanding the behavior of its algebraic set V at a point P. To see why we will need a few more notions about ideals which we develop with the integers.

Definition 3.10. For any ideal I we can raise it to a positive power by defining

$$I^n = \{x \in I \mid x = a_1 a_2 \cdots a_n, \text{ where } a_i \in I \text{ for all } i \leq n\}.$$

Example 3.11. We recognize that $5\mathbb{Z}^2 = 25\mathbb{Z}$ because if a number must have two 5's as factors then it must be a power of 25. We see that we have all of them because for all $x \in 25\mathbb{Z}$, $x = 25a$ where $a \in \mathbb{Z}$, and $25a = (5) \cdot (5a)$ and we know that both 5 and $5a$ are in $5\mathbb{Z}$.

Example 3.12. Now let us consider raising our ideal from Example 1.4, (x, y), to a power. We recognize that the smallest degree terms of $(x, y)^n$ are generated by choosing n x's and y's to multiply together. This gives us all the monomials of degree n. From here we can easily replace an x or y with a higher power to get all monomials of higher degree. So, since the ideal is closed under addition as well, $(x, y)^n$ is all linear combinations of monomials of degree n and higher.

Definition 3.13. A *Prime Ideal* is an ideal, $I \subsetneq R$, in which for all $x \in I$, if $ab = x$ then either $a \in I$ or $b \in I$.

Example 3.14. In the integers, the prime ideals correspond to all the ideals generated by prime numbers. In particular, we observe that $5\mathbb{Z}$ is prime.

The prime ideals in polynomial rings have a particularly nice geometric meaning which we present in the following section.

4. Irreducible Curves

First, we recall that in Example 2.4 we had some different curves which were represented by functions in the ideal of the unit circle. These curves were made by either just the unit circle or the unit circle plus some other algebraic curve. This begs the question, however, are there algebraic curves which we could combine to make the unit circle itself?

Definition 4.1. If for some algebraic set, V, $V = V_1 \cup V_2$ where V_1 and V_2 are also algebraic sets, then V is *reducible*. If, on the other hand, we cannot write V as a union of algebraic sets then V is *irreducible*.

We have some important propositions about irreducible curves.

Proposition 4.2. *An algebraic set $V \subset k^n$ is irreducible if and only if $I(V)$ is prime.*

Proof. First, if V is reducible, then $V = V_1 \cup V_2$ where V_1 and V_2 are algebraic subsets. So, there exists $f, g \in k[x_1, \ldots x_{n+1}]$ such that $V(f) = V_1$ and $V(g) = V_2$. We recognize that $V(fg) = V$, but neither f nor g are in $I(V)$, so $I(V)$ is not prime.

For the reverse direction, if $I(V)$ is not prime then there exists some $h \in I(V)$ such that $h = fg$ with $f, g \notin I(V)$. Recognize that $V \subset V(h) = V(f) \cup V(g)$. Now since V is a subset of $V(f) \cup V(g)$ consider that

$$V = (V(f) \cup V(g)) \cap V = (V(f) \cap V) \cup (V(g) \cap V).$$

We know that $V(f) \cap V$ and $V(g) \cap V$ are both algebraic subsets since they are equal to $V(f, I(V))$ and $V(g, I(V))$ respectively. Additionally, neither are the emptyset because the other cannot itself be V since neither f nor g is in $I(V)$. □

We have another proposition which narrows our focus to k^2.

Proposition 4.3. *If $f, g \in k[x, y]$ have no common factors, then $V(f) \cap V(g)$ is a finite set of points.*

Proof. This can be found in chapter 1, section 6 of Fulton's Algebraic Curves. Although the proposition is somewhat intuitive, the proof uses some techniques that we have not covered so we will assume that it holds. □

The proposition is important for the following corollary.

Corollary 4.4. *The irreducible algebraic sets of k^2 are the empty set, points, the vanishing sets of irreducible polynomials, and k^2 itself.*

Proof. We will check each of our possible forms for an irreducible algebraic set. The distinction between finite and infinite algebraic sets is useful to ensure that this is all of them.

(1) Recognize that $V(1) = \emptyset$. We could also take any other constant or any set containing one.
(2) For any point, $(a, b) \in k^2$, we recognize that $V(x - a, y - b) = (a, b)$. This also shows that a finite collection of more than one point is not irreducible.
(3) We could have $S = k^2$ if $I(S) = (0) = \{0\}$.
(4) The only condition left is that our irreducible algebraic set, S is infinite and that $I(S) \neq \{0\}$. Since S is an algebraic set, consider $I(S)$ and some $f \in I(S)$. If f is not irreducible, then $f = g_1 g_2$. By Proposition 4.2 we recognize that either g_1 or g_2 is in $I(V)$ (or both). So, without loss of generality suppose that $g_1 \in I(V)$ and if g_1 is not irreducible repeat this process. Eventually this process must terminate and yield an irreducible polynomial F since our original polynomial, f, was of finite degree.

    Now suppose that $g \in I(S)$. We know that $V(F) \cap V(g) \supset S$, and since S is infinite this implies that F and g have some common component. Since F is irreducible this in turn implies that $g \in (F)$ and that $(F) = I(S)$ as desired.

□

Now let us examine two reducible algebraic curves. Observe that it is not too difficult to pick out the distinct curves geometrically for simple examples.[5]

And now we present two irreducible algebraic curves in addition to the unit circle which we saw earlier.

[5]We caution here that when visualizing this way we are implicitly working in $\mathbb{R}^n$ so we need to be careful to choose polynomials that do not contain components which vanish nowhere.

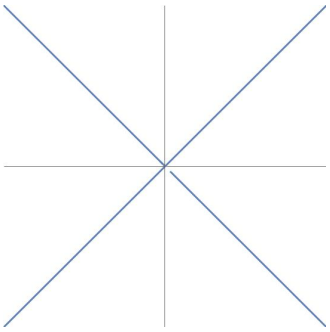

FIGURE 9.
$x^2 - y^2 = 0$

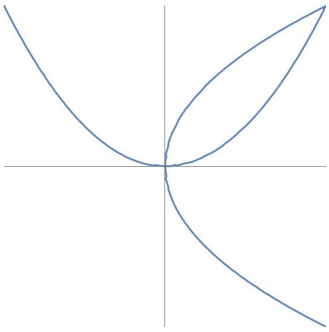

FIGURE 10.
$(y - x^2)(x - y^2) = 0$

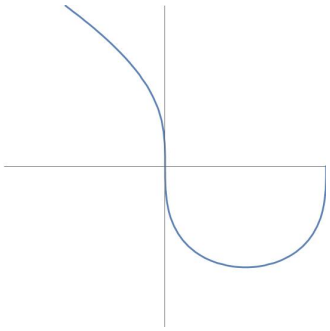

FIGURE 11.
$y^3 - x^2 + x = 0$

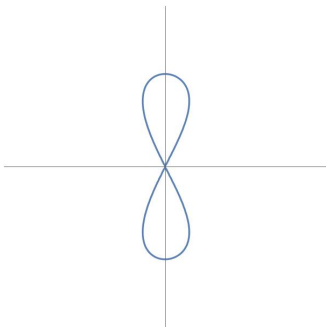

FIGURE 12.
$3y^4 - 2x^3 + 4x^2 - y^2 = 0$

Notice from Figure 12 that even our irreducible algebraic curves can seem to intersect themselves at certain points. This may be suprising since geometrically this might lead one to claim that the top and bottom loops are actually different curves. We will discuss this behavior in section 6 but first we need to develop a bit more machinery.

5. Polynomials As Vector Spaces, Exact Sequences, and Forms

Definition 5.1. A *form* is a polynomial in which all terms are of the same degree.

When a polynomial is of multiple variables then the degree of any one term is the sum of the exponents of each variable.

Example 5.2. We present a few simple examples of forms.

(1) $x^2 + y^2 - 3xy$
(2) $27xyz + \frac{1}{3}z^3$
(3) $x^3y^2 + 2x^5 - 5y^4x$

The following theorem introduces an important property of forms which we will use later.

Theorem 5.3. *If k is an algebraically closed field then if $f \in k[x,y]$ and f is a form of degree n then we can factor f into linear factors g_i where $f = g_1 \cdots g_n$.*

Proof. First, divide f by y^n. When we distribute this out over each term, some we can simplify by cancelling out the powers of y on top. In particular, if y is of degree j in the term, then when we divide by y^n we will get y^{n-j} in the denominator. However, recognize that for each term in f, if y is degree j then x is degree $n-j$ since the exponents must sum to n. Let us take $n-j=i$. This means we now have $\frac{x^i}{y^i} = \left(\frac{x}{y}\right)^i$. If we take $\frac{x}{y} = z$ then this is merely a polynomial equation of one variable which we can factor by Definition 2.5. So, if m is the largest exponent attatched to an x then with a_i for all $i \leq m$ as the zeroes of this polynomial we now have

$$\frac{f}{y^n} = (z-a_1)\cdots(z-a_m) = \left(\frac{x}{y} - a_1\right)\cdots\left(\frac{x}{y} - a_m\right).$$

We now multiply our terms on the right by y^n. We know that $n-m \geq 0$ (since the term with x^m must have exponents summing to n and the exponent for y cannot be negative), so we have at least one y which we can distribute over each term leaving us with

$$f = y^{n-m}(x - a_1 y)\cdots(x - a_m y).$$

The y^{n-m} term poses no problem since it is merely $n-m$ factors of the linear factor of only y. Also note that some a_i's may be 0. □

We recall that we can consider polynomials as a vector space over their field of coefficients, k.[6] This is important in later topics in algebraic curves, so we consider one such important example both because of these applications later on and since it combines many concepts we have seen already.

Lemma 5.4. $\dim_k(k[x,y]/(x,y)^n) = \frac{n(n+1)}{2}$

Proof. First, notice that (x,y) is merely the ideal from Example 1.4, Example 3.3, and Example 3.12. So, $(x,y)^n$ is all linear combinations of the monomials of degree n and higher. We recognize further that $(x,y)^n$ contains all monomials and linear combinations of monomials with degree greater than n.

The number of linearly independent monomials of two variables of arbitrary degree m is $m+1$ since we have a monomial of $x^i y^j$ for all $i \leq m$ including $i = 0$. So, the total number of monomials is $1+2+\cdots+(n-1)+1 = \frac{n(n+1)}{2}$. This is represented in the diagram below.

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & x & & y & & & \\
 & & x^2 & & xy & & y^2 & & \\
 & \iddots & & \vdots & & \vdots & & \ddots & \\
x^{n-1} & & & & \cdots & & & & y^{n-1}
\end{array}$$

[6] If this is new, it is fairly easy to check as long as you are familiar with the axioms of a vector space which can be found in the first few sections of Linear Algebra Done Right.

□

Definition 5.5. An *exact sequence* of vector spaces[7] is a sequence of linear transformations, φ_i such such that for vector spaces V_i,

$$V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \to \cdots \xrightarrow{\varphi_{n-1}} V_n$$

where for all $i \leq n-1$, the image of φ_i is equal to the kernel of φ_{i+1}. Often we will be looking at *short exact sequences* which are of the form

$$0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0.$$

Lemma 5.6. *If we have a short exact sequence of vector spaces*

$$0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0,$$

then $\dim B = \dim A + \dim C$.

Proof. This is a consequence of the rank nullity theorem. One can verify it by applying it to both φ and ψ keeping in mind that $\text{im}\{\varphi\} = \ker\{\psi\}$ because the sequence is exact. Additionally, we can find that φ is injective and ψ must be injective. □

6. Multiplicity

We now return to the problem posed by Figure 12 of an algebraic curve which seemed to cross itself in the middle.

Definition 6.1. A *simple point* is some $P \in V(f)$ such that either $f_x(P) \neq 0$ or $f_y(P) \neq 0$.[8] A *multiple point* is any point on the curve that is not a simple point, so $f_x(P) = 0$ and $f_y(P) = 0$.

Remark 6.2. If P is a simple point then it is not too difficult to find a tangent line to it. If our point is (a, b) then some calculus shows that the line $F_x(P)(x - a) + F_y(P)(y - b)$ is tangent to our curve at P. But when both derivatives are 0 this doesn't work.

Observe that if $P = (0, 0)$, then P is simple on some curve $V(f)$ if an only if there exists some term linear (degree 1) term in f. This motivates the following definition.

Definition 6.3. For all $F \in k[x, y]$, we can consider it as a sum of forms. In particular, with each f_i a form of degree i with $n \geq i \geq m$ and $f_m \neq 0$ we have

$$F = f_n + f_{n-1} + \cdots + f_m.$$

Observe that the largest i such that $f_i \neq 0$ is the degree of F and also that if only $f_m \neq 0$ then F is a form. We define m as the multiplicity of F at $(0, 0)$.

To define the multiplicity of F at some arbitrary $(a, b) \in k^2$ we do the same process but consider the polynomial $F(x - a, y - b)$ where we are merely precomposing a translation to the origin. We denote the multiplicity of f at P as $m_P(f)$.

[7] More generally we could consider exact sequences of other objects, like modules for instance.
[8] by this we mean the derivative at P with respect to x and y respectively

Remark 6.4. Notice that the multiplicity of some point does have something to do with the derivatives. If the multiplicity of $(0,0)$ is m then taking any number of derivatives less than m will always yield 0 at the origin, but there is some way (some combination of derivatives by x and y) such that we can take m derivatives and get a nonzero number at the origin.

Near the origin, a curve takes on much of the behavior of its lowest degree form. In particular, the problem of finding tangents which we encountered in Remark 6.4 is completely resolved.

Observation 6.5. Recognize that if we take some representative point, $(a,b) \neq (0,0)$ from any line through the origin then the whole line, L can be considered as the set

$$L = \{(\lambda a, \lambda b) \mid \lambda \in k\}.$$

Now, if consider $F(x_o, y_o)$ where $(x_o, y_o) \in L$ and $(x_o, y_o) = \lambda_o(a,b)$ and represent F as forms then

$$F(x_o, y_o) = \lambda_o^n f_n(a,b) + \lambda_o^{n-1}(a,b) + \cdots + \lambda_o^m f_m(a,b).$$

As λ goes to 0 and we get closer to the origin, recognize that the f_m term will dominate. In particular, if we are interested in the lines which come most closely to being part of $V(f)$ then we want to look at the lines which f_m vanishes on. By Theorem 5.3 we can find m lines which come closest to being tangent at the origin.

Let us now show some examples. First, in Figure 12 the lowest degree form of $3y^4 - 2x^3 + 4x^3 + 4x^2 - y^2$ is $4x^2 - y^2 = (2x - y)(2x + y)$. If we graphs the lines $y = 2x$ and $y = -2x$ on top of the entire curve then we get the two distinct lines of intersection as pictures below. Additionally, we provide an example where some multiplicities are repeated and its lowest degree form is already factored.

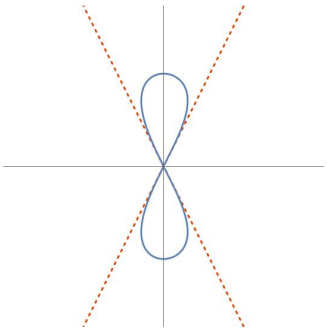

FIGURE 13.
$3y^4 - 2x^3 + 4x^2 - y^2 = 0$

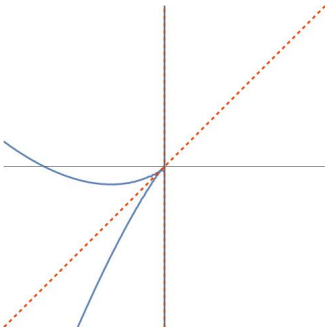

FIGURE 14.
$4x^4 + 3x(x-y)^2 = 0$

We see that one way to think of multiplicity is as the number of tangent lines with some repeat. Another, related intuition is that a curve with multiplicity with multiplicity m at some point P goes through that point m times. In Figure 14 even though there are only 2 tangent lines, the graph still seems to come through the origin 3 distinct times as its multiplicity suggests.

Acknowledgments

Thank you firstly to my mentor, Cameron Chang for recommending this topic and helping me through the material. Having someone to talk and bounce ideas off who had such a firm grasp of the subject already was invaluable. Thank you also to anyone who asked and listened to me explain what I was studying in the REU. There are too many to name individually, but most who knew me these past few months should feel included. Much of the structure of this paper was informed by how I found myself explaining the topic to a beginner, refined from repeated, sometimes convoluted attempts. Finally, thank you to Peter May for giving me this opportunity and organizing the REU. It was a wonderful experience and introduction to math research.

References

[1] https://math.stackexchange.com/questions/3188765/tangent-lines-throught-a-point-in-an-algebraic-curve
[2] William Fulton. Algebraic Curves: An Introduction to Algebraic Geometry. https://dept.math.lsa.umich.edu/ wfulton/CurveBook.pdf
[3] Sheldon Axler. Linear Algebra Done Right. Springer. 2024. https://linear.axler.net/LADR4e.pdf
[4] Davis S. Dummit, and Richard Foote. Abstract Algebra.