

REBEL ALGEBRAIC GEOMETRY SEMINAR :
LECTURE 1 - THE BASICS

PATRICK DYLAN ZWICK

1. RINGS

Algebraic geometry all begins with rings. No, not jewelry, but mathematical rings. In algebra, a ring R is defined as being a set of elements with two binary operations $(+, \cdot)$ satisfying:

- R is closed under the two operations : So, if $a, b \in R$ we have $a + b \in R$ and $a \cdot b \in R$. We will frequently write $a \cdot b = ab$.
- Associativity under addition : $a + (b + c) = (a + b) + c$.
- Commutativity under addition : $a + b = b + a$.
- Additive identity : There exists an element denoted $0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$.
- Additive inverses : For every $a \in R$ there exists a unique element, denoted $-a \in R$ such that $a + (-a) = 0$.
- Associativity under multiplication : $a(bc) = (ab)c$.
- Distributivity : $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Some examples of rings are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and their associated polynomial rings $\mathbb{Z}[x], \mathbb{Q}[x], \dots$

In pretty much all the rings we deal with we'll have a multiplicative identity, which we'll denote by 1 , and our multiplication will be commutative. Also note that all rings are abelian groups under addition.

- Multiplicative identity : There exists an element denoted $1 \in R$ such that $1a = a = a1$ for all $a \in R$.
- Commutativity under multiplication : For all $a, b \in R$ we have $ab = ba$.

So, from here on out, we'll assume that all of our rings are commutative with a 1 .

Exercises

- 1:** Give an example of a ring that does not contain a 1. Give an example of a ring that is not commutative.
- 2:** Prove that in any ring $0a = 0$ for all $a \in R$.

Now, in a general ring if $ab = 0$ it does not have to be the case that either $a = 0$ or $b = 0$. Rings in which this is the case are called *integral domains* or frequently just *domains*.

2. IDEALS

A subset of a ring $I \subset R$ is called an ideal if:

- (1) I is closed under addition.
- (2) For all $r \in R$ if $a \in I$ then $ra \in I$.

Exercises

- 3:** Prove that $\bigcap_{\lambda \in \Lambda} I_\lambda$ is an ideal. That is to say, an arbitrary intersection of ideals is an ideal.
- 4:** Prove that for any element $a \in R$ the set of elements that can be written as ra for $r \in R$ is an ideal.

For any subset $S \subset R$ we can find the smallest ideal containing S , called $I(S)$. This will be the intersection of all the ideals containing S . It will also be the set of elements that can be written as $r_1s_1 + \cdots + r_ms_m$ for $r_i \in R$ and $s_i \in S$. We call $I(S)$ the ideal generated by S .

Exercise

- 5:** Prove the equivalence of the two definitions of $I(S)$ given above.

Now, obviously if $1 \in S$ then $I(S) = R$. Also, if we have an element $u \in S$ such that there exists a $v \in R$ where $uv = 1$ then $I(S) = R$. An element u satisfying this condition is called a *unit*. If an ideal contains a unit, then it is the entire ring.

Note that a commutative ring in which every non-zero element is a unit is called a *field*.

3. RING HOMOMORPHISMS

A ring homomorphism is a map $\phi : A \rightarrow B$ where A and B are rings and ϕ satisfies:

- $\phi(ab) = \phi(a)\phi(b)$
- $\phi(a + b) = \phi(a) + \phi(b)$.

The set of elements $a \in A$ such that $\phi(a) = 0$ is called the kernel of ϕ .

Exercise

6: Show that $\ker(\phi)$ is an ideal of A .

Now, for any ideal $I \subseteq R$ we can form a new ring called the quotient ring R/I . The elements of this ring are sets of the form $a + I$, called cosets, where this denotes all elements in R that can be written as $a + i$, where $i \in I$. Here we define addition as $(a + I) + (b + I) = (a + b) + I$ and multiplication as $(a + I)(b + I) = ab + I$.

Exercise

7: Explain why this definition of multiplication and division is well defined and makes sense.

Also, for any ideal $I \subseteq R$ this is a natural ring homomorphism $\phi : R \rightarrow R/I$ with kernel I . So, not only is the kernel of a ring homomorphism an ideal, but every ideal is the kernel of some ring homomorphism.

4. SPECIAL RINGS AND IDEALS

There are special types of rings and special types of ideals that take up most of our attention in algebraic geometry. So, let's talk about them.

- *Principal Ideal Domains* - A principal ideal domain (usually abbreviated PID) is an integral domain in which every ideal is generated by only one element. So, all ideals are of the form $I = (a)$. An example of a principal ideal domain is the ring of integers \mathbb{Z} .

Exercise

8: Give another example of a PID.

- *Noetherian Rings* - A noetherian ring is kind of the next step up from a PID¹. A noetherian ring is a ring in which every ideal

¹It's a big step.

is finitely generated. That is to say, for any ideal $I \subseteq R$ we can find a finite set S such that $I = I(S)$.

Exercises

9: (Easy) Give an example of a noetherian ring.

10: (Harder) We say that a ring satisfies the ascending chain condition (ACC) if for every chain of ideals:

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

eventually the chain stabilizes. That is to say for some $N \in \mathbb{Z}^+$ we have $I_n = I_{n+1}$ when $n \geq N$. Prove that a ring satisfies the ACC if and only if it is noetherian.²

- *Prime Ideals* - These are *very* important in algebraic geometry. A prime ideal is an ideal, typically denoted \mathfrak{p} , such that if $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Equivalently, if $a, b \notin \mathfrak{p}$ then $ab \notin \mathfrak{p}$. In other words, the set of elements not in \mathfrak{p} for a *multiplicative system* (a set of elements closed under multiplication). These will be important later.

Exercises

11: Prove that for any prime ideal $\mathfrak{p} \subset R$ that R/\mathfrak{p} is an integral domain.

12: Prove that for any ideal $I \subset R$ if R/I is an integral domain then I is prime. So, we can equivalently define a prime ideal as any ideal I where R/I is an integral domain.

- *Maximal Ideals* - The big ones! A maximal ideal is a proper ideal that is as big as they come. More precisely, a maximal ideal is an ideal, frequently denoted \mathfrak{m} , such that if $I \subseteq R$ is an ideal and $\mathfrak{m} \subseteq I$ then either $\mathfrak{m} = I$ or $I = R$. In other words, a maximal ideal is an ideal that is not contained in any other proper ideal. Please note that we require a maximal ideal to be a proper subset of the ring R , so R itself is not a maximal ideal.

Exercises

13: Prove that a maximal ideal is a prime ideal.

14: Prove that if \mathfrak{m} is a maximal ideal then R/\mathfrak{m} is a field, and vice-versa. Thus, we again have an equivalent definition. Why does knowing this prove that a maximal ideal is a prime ideal?

²This problem was on the January, 2008 algebra prelim.

15: (Hard) Prove that maximal ideals always exist. That is to say, for a ring $R \neq 0$ (so, any ring not equal to the zero ring) there will exist maximal ideals. *Hint : Zorn's lemma.*

- *Radical Ideals* - Useful in mathematics, but can be dangerous in politics.³ A radical ideal is an ideal J where if $a^n \in J$ then $a \in J$. For any ideal I we can define the set \sqrt{I} of all elements $a \in R$ such that $a^n \in I$ for some $n \in \mathbb{Z}^+$.

Exercises

16: Prove that \sqrt{I} is an ideal.

17: Prove that $\sqrt{\sqrt{I}} = \sqrt{I}$.

18: Prove that $\sqrt{\mathfrak{p}} = \mathfrak{p}$ if \mathfrak{p} is a prime ideal. In other words, all prime ideals are radical.

19: (Harder) Prove that \sqrt{I} is the intersection of all prime ideals that contain I .

20: What characterizes the elements in the ideal $\sqrt{0}$? This ideal is called the *nilradical*.

- *Local Rings* - A local ring is a ring with a unique maximal ideal.⁴ As a very easy example, all fields are local rings, as they only have one ideal, namely the zero ideal. Later on we will learn about a process called localization⁵, where using just a ring and a prime ideal you can build a local ring.

Exercise

21: Give an example of a local ring that is not a field.

5. POLYNOMIAL RINGS AND VARIETIES

So why do we call it algebraic geometry and not, say, ring theory? Well, I sometimes wonder this myself, but it all starts with polynomial rings. A polynomial ring over a field R is the ring of polynomials with coefficients in R , usually denoted $R[X_1, \dots, X_n]$ if there are a finite number of variables. We'll frequently be assuming that R is an

³Just ask Grothendieck. On second thought, don't. I hear he's gotten pretty weird.

⁴I call this unique maximal ideal the Lord of the Ring! Sorry.

⁵This is where that multiplicative set stuff comes in.

algebraically closed field⁶, and in this case we'll use k for our ring and write $K[X_1, \dots, X_n]$.

Now, if we have a set of polynomials $F_1, \dots, F_n \in K[X_1, \dots, X_n]$ we can ask the question: "at what points in K^n do all these polynomials simultaneously vanish?" This is the zero-set of our collection of polynomials, and it is known as a variety (or, to be more specific, an affine variety). Algebraic geometry begins as the study of these varieties.

Exercise

22: Prove that if the polynomials F_1, \dots, F_n vanish on the set S , then all the polynomials in the ideal $\langle F_1, \dots, F_n \rangle$ generated by the F_i also vanish on S .

We can also go the other way, and take a set $S \subseteq K^n$ and ask: "which polynomials vanish on all the points of S ?"

Exercise

23: Prove that the set of polynomials vanishing on S forms an ideal.

So, for any ideal $I \subseteq K[X_1, \dots, X_n]$ we have a corresponding set of points, which we'll denote $\mathbf{V}(I)$, upon which all the polynomials in I vanish. Similarly, for any set of points S , we have an ideal, which we'll denote $\mathbf{I}(S)$, of all the polynomials that vanish on S . Thus we have this relationship between *algebraic objects*, namely the ideals, and *geometric objects* (surfaces, planes, curves, lines, points, etc...), namely the zero sets of polynomials. So, we can use algebra to study geometry, and geometry to study algebra, and in fact morph the two of them together Voltron-style to form: ALGEBRAIC GEOMETRY!

Exercise

24: Prove that for any set $S \subseteq k^n$ the ideal $\mathbf{I}(S)$ is radical.

We note in general that $I \subseteq \mathbf{I}(\mathbf{V}(I))$ and $S \subseteq \mathbf{V}(\mathbf{I}(S))$.

Exercise

25: Prove that our correspondence is inclusion reversing. That is to say, if $I \subseteq J$ then $\mathbf{V}(I) \supseteq \mathbf{V}(J)$.

⁶An algebraically closed field is a field in which every polynomial with coefficients in that field has a root in that field. The classic example is \mathbb{C} , the field of complex numbers. In fact, you'll prove \mathbb{C} is algebraically closed in all three of your prelims classes during spring semester, in three very different ways.

6. THE ZARISKI TOPOLOGY

From now on we'll fix an algebraically closed field K and refer to the space of possible values in K^n as \mathbb{A}^n . This is called *affine space*. For the ring $K[X_1, \dots, X_n]$ we note that:

- $\mathbf{V}(1) = \emptyset$
- $\mathbf{V}(0) = \mathbb{A}^n$
- $\mathbf{V}(I_1) \cup \mathbf{V}(I_2) = \mathbf{V}(I_1 \cap I_2)$
- $\bigcap_{\lambda \in \Lambda} \mathbf{V}(I_\lambda) = \mathbf{V}\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$.

In the final relation the term $\sum I_\lambda$ refers to the ideal given by all finite sums of elements from the I_λ . It is the smallest ideal containing each I_λ .

Exercise

26: Prove the above assertions.

Some of you may notice these relations look familiar. In fact, we can use them to define a topology on \mathbb{A}^n called the *Zariski topology*. In the Zariski topology the closed sets are varieties, and the open sets are the complements of the closed sets. It's a very interesting and, if you're used to Euclidean topology, weird topology.

Exercises

27: Prove that the Zariski topology on $\mathbb{C}[z]$ is not Hausdorff!

28: (Harder) Under what circumstances *is* the Zariski topology Hausdorff?

Now, a variety is called *irreducible* if whenever $V = V_1 \cup V_2$, with V_1, V_2 also varieties, we have either $V = V_1$ or $V = V_2$.

Exercise

29: Prove that a variety is irreducible if and only if $\mathbf{I}(V)$ is prime.

Note - Some authors, notably Robin Hartshorne, only call a variety a variety if it's irreducible, and use the term "algebraic set" to refer to a more general variety.

So, we've expanded our algebra-geometry dictionary (correspondence) and now we know:

Radical ideals \Leftrightarrow Varieties

Prime ideals \Leftrightarrow Irreducible varieties

Maximal ideals \Leftrightarrow Points

Wait, we don't know that last one yet, do we? Well...

Exercise

30: Prove that a point $P \in \mathbb{A}^n$ corresponds with a maximal ideal \mathfrak{m}_P in $K[X_1, \dots, X_n]$. The other way, namely that maximal ideals correspond with points, will have to wait until the next lecture.

6.1. The Hilbert Basis Theorem. There's an issue we've been skirting here. How do we know that given an ideal $I \subset K[X_1, \dots, X_n]$ that it's generated by a finite set of ideals $\langle F_1, \dots, F_m \rangle$? Now, if this were not the case things might be very bad, in that calculating the zero set of an infinite number of polynomials might very well make your head explode. But, things are not that bad, and your head is safe, thanks to the Hilbert Basis Theorem.

Hilbert is really the first big name in algebraic geometry, as he was in so many other areas of mathematics. The two "founding proofs" of algebraic geometry, the basis theorem and the Nullstellensatz (great name) belong to him. We'll end this lecture with the basis theorem, and begin our lecture next week with the Nullstellensatz.

Hilbert Basis Theorem - If R is a noetherian ring, then $R[X]$ is also a noetherian ring.

OK, it's time for our first real proof here. So, get ready for it. It turns out to be not that bad. Just some induction and some cleverness.

Proof⁷ - Recall that for a polynomial:

$$F(X) = a_0X^r + a_1X^{r-1} + \dots + a_r, \quad a_i \in R, \quad a_0 \neq 0.$$

r is called the degree of F , and a_0 is its leading coefficient.

⁷More or less lifted straight from Milne's lecture notes.

Let I be an ideal in $R[X]$, and let I_i be the set of elements of R that occur as the leading coefficient of a polynomial in I of degree $\leq i$. Then I_i is an ideal in R , and

$$I_1 \subset I_2 \subset \dots$$

Because R is noetherian, this sequence eventually stabilizes, say $I_d = I_{d+1} = \dots$ (and I_d consists of the leading coefficients of all polynomials in I).

For each $i \leq d$, choose a finite set F_{i1}, F_{i2}, \dots of polynomials in I of degree i such that the leading coefficients a_{ij} of the F_{ij} 's generate I_i .

Let $F \in I$; we shall prove by induction on the degree of F that it lies in the ideal generated by the f_{ij} . When F has degree 1, this is clear.

Suppose that F has degree $s \geq d$. Then $F = aX^s + \dots$ with $a \in I_d$, and so

$$a = \sum_j b_j a_{dj}, \text{ for some } b_j \in R,$$

Now

$$F - \sum_j b_j F_{dj} x^{s-d}$$

has degree $< \deg(F)$, and so lies in (F_{ij}) by our induction hypothesis.

Suppose that F has degree $s \leq d$. Then a similar argument shows that

$$F - \sum_j b_j F_{sj}$$

has degree $< \deg(F)$ for suitable $b_j \in R$, and so lies in (F_{ij}) again by our induction hypothesis. **QED**

Phew! If that didn't make sense, and it would be no shame at all if you didn't understand the proof the first time you saw it during lecture, make sure you go over the proof in your notes until it does.

Exercise

31: Use the Hilbert basis theorem to prove $K[X_1, \dots, X_n]$ is noetherian.

Note that while the basis theorem proves that a finite set of polynomials generates any ideal I , it tells you *nothing* about how to find

these polynomials. This prompted Paul Gordan to say of it: “Das ist nicht Mathematik. Das ist Theologie.”⁸

Also, suppose you’re given a polynomial F and you want to determine if it belongs to the ideal $\langle G_1, \dots, G_m \rangle$, how do you go about doing so? It turns out to be an interesting problem that’s more or less solved using something called Grobner bases. There will be a talk about this at the undergraduate colloquium on Wednesday, September 23rd, 2009. I hear the speaker is fantastic, and good looking too. There will also be pizza.

⁸In English: “This is not mathematics, this is theology.” Gordan had been working on a constructive proof, one in which you could actually calculate the generating set for a given ideal, for decades, so there may have been some sour grapes here. Eventually, even Gordan found some religion and had to admit that Hilbert’s approach had its merits. An interesting account of this is found in the quite good introductory algebraic geometry book “Elementary Algebraic Geometry” by Keith Kendig. A bit too big for this course, but if you want to continue working on this during spring semester I’d definitely recommend checking it out.