Algebraic Geometry I Class Notes

Instructor: Amod Agashe

September 3, 2008

Contents

Chapter 1

Lecture 1: August 25, 2008

Scribe: Jay Stryker

1.1 General class information

[Material on the syllabus was discussed.]

Instructor: Amod Agashe

Email: agashe@math.fsu.edu

Office: 216 LOV

Phone: 644-8704

Webpage: http://www.math.fsu.edu/∼agashe/ag.html

Recommended text: *Algebraic Geometry* by Robin Hartshorne [3]

Parts of Chapters I,II,III and IV will be covered (see syllabus for specifics.)

Class time: 3:35 Mondays and Wednesdays

Prerequisites: The syllabus states that you should have a year long sequence in graduate algebra, but the real requirement is "Algebraic maturity."

You should be comfortable with groups, rings ideals and preferably modules. (Field theory/Galois theory is not necessary.)

Statements such as "I is maximal $\Leftrightarrow$ R/I is a field" should not look strange to you.

Course Description: Classical algebraic geometry (the theory of varieties) will be developed alongside the more modern approach and language of schemes. (More details exist in the syllabus.)

Grading: There will be some homework and class attendance is expected. A scribe system in which notes will be written up in LaTeXwill be implemented and may count toward a homework assignment.

1.2 Motivation for studying algebraic geometry

1.2.1 Finding all pythagorean triples

We wish to find $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = z^2$.

[Dr. Agashe will use the abbreviation s.t. to stand for "such that" when writing on the board.]

By scaling it suffices to consider the case when $gcd(x, y, z) = 1$. (x, y and z should be coprime. Some refer to the set of coprime Pythagorean triples as primitive Pythagorean triples. Parenthesis notation will often be used for gcd as (m, n) is defined to be $gcd(m, n)$ in appropriate contexts.)

If $z = 0$ then $x = y = 0$ which gives us the solution $(0, 0, 0)$

If $z \neq 0$ then

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

Since x/z and y/z are we can rephrase the question as "we want to look for rational solutions to $X^2 + Y^2 = 1$." (Where $X = x/z$ and $Y = y/z$.)

If the point (x_t, y_t) is rational then the slope of the line is rational. However, the converse is also true.

The slope of the line is

$$t = \frac{y - 0}{x - (-1)}.$$

From this we see that $y = t(x + 1)$. Substituting back into $x^2 + y^2 = 1$ we get $x^2 + t^2(x + 1)^2 = 1$

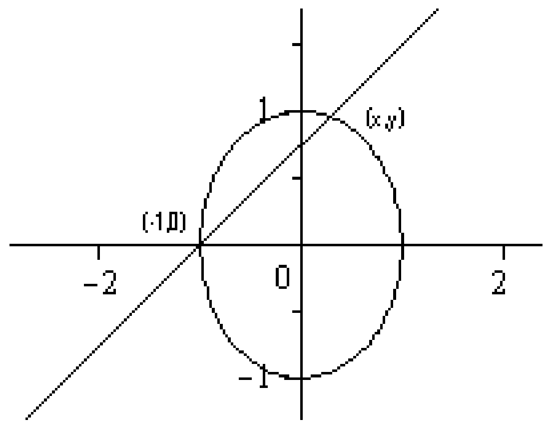

Figure 1.1: [Diagram of circle radius 1 with center at (0,0)and line going from $(-1,0)$ to a point (x_t, y_t) on the circle.]

Through arithmetic manipulations we get

$$(t^2+1)x^2 + 2t^2x + (t^2-1) = 0.$$

Using the sum of the roots[1] we find that

$$\frac{-2t^2}{t^2+1} = -1 + x_t$$

And by simple manipulations and substituting back into our equation we get

$$x_t = \frac{1-t^2}{1+t^2}$$

and

$$y_t = \frac{2t}{1+t^2}.$$

If we choose $t = m/n$ with $(m,n) = 1$ we find that the pythagorean triples are

$$x = m^2 - n^2,$$

$$y = 2mn,$$

[1]Note that $ax^2 + bx + c = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a(x-\alpha)(y-\beta)$ and equating coefficients we see that $-(sum\ of\ roots) = \frac{b}{a}$

and

$$z = m^2 + n^2.$$

for $m, n \in \mathbb{Z}$ and multiples of such.

Moral: We solved an algebra/arithmetic problem using the geometry of some loci of polynomials, but the proof involved algebra.

Something of interest that we will probably see more of later is that we have parameterized the circle by choosing a point on the circle and looking at the slope of the line that passes through this point and every other point on the circle giving us a map $t \mapsto$ circle minus the point (-1,0). [By looking at values of t as they go from $-\infty$ to $+\infty$, we get all points on the circle except (-1,0) which is a limit point. There may be interesting behavior for points as t goes to infinity in such parameterizations.][2]

1.2.2 Elliptic curves

An elliptic curve over a field (of characteristic $\neq$ 2 or 3) is the set of solutions to $y^2 = x^3 + ax + b$ with $a, b \in k$ (and? some extra information... nonsingularity property)

For example, $k = \mathbb{R}, y^2 = x^3 - x$

Fact: There is a group law on the set of solutions. (In fact, it is an abelian variety.)

The coordinates of $P + Q$ are rational functions of the coordinates of $P \& Q$ and the coefficents of the equation.

This works for any k including finite fields ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.)

For example, $y^2 = x^3 - x$ over $\mathbb{P}_5 = \{0, 1, 2, 3, 4\}$

These are used in cryptography and one of the important results that is used is Hasse's theorem (of elliptic curves) which states that

$$|(number\ of\ solutions) - (p + 1)| \leq 2\sqrt{p}$$

The proof uses the number of solutions over $\mathbb{F}_p$ = number of fixed points of $\phi(x, y) \mapsto (x^p, y^p)$ over $\bar{\mathbb{F}}_p$ (The algebraic closure of $\mathbb{F}_p$=number of points in the kernel of $(id - \phi)$

---

[2] It was commented in class that this is essentially a stereographic projection in this case of $\mathbb{P}^1 \backslash p \mapsto \mathbb{R}$.

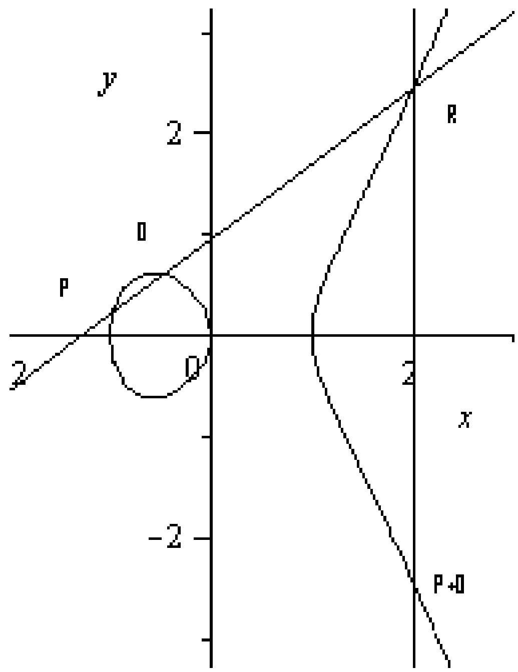

Figure 1.2: [Graph of $y^2 = x^3 - x$ with a two lines illustrating the group law. P and Q on the left component the line passing through them intersects the right component at R and the vertical line down from from R is $P + Q$.]

Moral: We want to consider maps between solutions of polynomials and analogs of geometric properties of such maps. (e.g.[3] coverings, degrees, etc.)

Also, we want to construct invariants of such objects (solutions of polynomials) which come from sheaf cohomology.

More motivation next time...

[3] e.g. means "for example" from the Latin exempli gratia, in case you were curious.

Chapter 2

Lecture 2: August 27, 2008

Scribe: Jay Stryker

2.1 Questions from last time

A question was raised about where $-Q$ would have been on the elliptic curve example.

Back to the elliptic curve example:

(Parallel) vertical lines pass through 0. (Which can be thought of as being a point at infinity. So negative of a point can be found in this curve by looking at the point which is symmetric about the x-axis from a given point.)

Some comments were made about the fact that although the course has a title which includes the word Geometry in the name, there in fact will be few actual pictures. If you wish to see a book that has nice pictures, Dr. Agashe recommends William Fulton's book Algebraic Curves [2]. The older version is available in the library, but it has been recently (in January 2008) been made available online through William Fulton's website.

2.2 Motivation continued

2.2.1 Algebraic sets, ideals and schemes

Last time we talked about the study of the solution of algebraic sets, which we will informally refer to as *algebraic sets*[1], maps between them and properties of such things.

Fact: If $f(x,y)$ is a polynomial with coefficients in an algebrically closed field k,

$$\{(x,y) \in k^2 | f(x,y) = 0\} \leftrightarrow \text{Maximal ideals of } R_f = k[x,y]/f(x,y).$$

Where $\leftrightarrow$ means "is in 1-1 correspondence with."

The correspondence can be seen with the following

$$(a,b) \mapsto (x-a, y-b)$$

and

$$(a_{\mathfrak{m}}, b_{\mathfrak{m}}) \leftarrow\!\shortmid \mathfrak{m}$$

where $R_f/\mathfrak{m} \cong k$ $x \to a_{\mathfrak{m}}$ $y \to b_{\mathfrak{m}}$.

"Geometric properties of algebraic sets and maps between them are reflected algebraically in rings like R_f."

Eventually we want to consider polynomials over rings (like $\mathbb{Z}$ which need not be fields) and more general rings because before 1900 or so the types of Algebraic Geometry that were done primarily utilized this relationship between maximal ideals and algebraic sets. About 1950 or so a different approach arose. Things were turned around:

To any (commutative) ring R we associate a geometric object.

$$\mathrm{Spec} R = \text{set of prime ideals of } R.$$

(Remember that maximal implies prime, but prime does not imply maximal, so we are working with a larger set of objects here.)

We also want to "patch" them together to get analogs of manifolds called *schemes.*

(This is not the end of the story of generalization/abstraction as there are mathematical constructions known as *stacks* and *algebraic spaces* which take this further, but will probably not be mentioned much in this course.)

[1] A more formal definition of algebraic sets will be given later.

[2 minute break in lecture]

2.2.2 Back to the motivation

Goal of this course: Survey the theory of varieties (certain algebraic sets) and schemes in parallel.

To this end we will:

- focus on generality (with motivation and examples,)
- learn the language and important results,
- skip the proofs mostly.

Topics	Sections of Hartshorne
Varieties	I §1-3
Schemes	II §1-8
Sheaf Cohomology	III §1-7
Riemann Roch Theorem (using Serre duality)	IV §1

Alot of commutative algebra will be used in this course. As a nice general reference you can use Atiyah-Macdonald's *Introduction to Commutative Algebra.*[1]

2.3 The course proper

2.3.1 Chapter I §1: Affine Varieties

Remark: We want to view solutions of polynomials as a "geometric" object, but for example $x^2 + y^2 = -1$ in $\mathbb{R}^2$ has no solutions.

So when we are working over a field k we consider solutions over an algebraic closure $\bar{k}$ of k.

Definition: The set of all n-tuples of elements of $\bar{k}$ (i.e. $\bar{k}^n$) is called *affine n space over $\bar{k}$* and is denoted $\mathbb{A}^n_{\bar{k}}$ or $\mathbb{A}^n$ if $\bar{k}$ is implicit.

An element $p = (a_1, \ldots, a_n)$ in $\mathbb{A}^n_{\bar{k}}$ is called a *point* in $\mathbb{A}^n_{\bar{k}}$ and $a_1, \ldots, a_n$ are called the *coordinates* of p.

If L is an algebraic extension of k (so $k \subseteq L \subseteq \bar{k}$) and if $a_1, \ldots, a_n \in L$, then we say that $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\bar{k}}$ is *defined over L* or is a *L-rational point.*

Example: $(-1, 0)$ on $x^2 + y^2 = 1$ is defined over $\mathbb{Q}$.

For simplicity, assume from now on that k is algebraically closed. (i.e. $k = \bar{k}$.)

Let $x_1, \ldots, x_n$ be "free variables."

Then any $f \in k[x_1, \ldots, x_n]$ can be evaluated at a point p in $\mathbb{A}^n$.

(E.g. if $n = 1$ and $f(x) = a_n x^n + \ldots + a_0$ and $p = b$ then $f(b) = a_n b^n + \ldots + a_0$.)

And thus we can define the zero set of f as

$$Z(f) = \{p \in \mathbb{A}^n | f(p) = 0\}.$$

More generally the *zero set of T* is

$$Z(T) = \{p \in \mathbb{A}^n | f(p) = 0 \forall f \in T\}$$

e.g.

$$T = \{x + y, x - y\} \subseteq k[x, y]$$

The zero set would just be $(0, 0)$ (if not in a field of characteristic 2.)

2.4 One more comment (office hours)

Office hours will tentatively be MW 2:30-3:30.

Bibliography

[1] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[2] William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. http://www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf, 2008. Web available version of the classic out of print Addison-Wesley book.

[3] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag, 1977. The standard text in English in this field.