LECTURE 10: SOME BASIC ALGEBRAIC GEOMETRY

STEPHEN MCKEAN

We recently met the graded ring MF_* of modular forms. Although MF_* is a ring, its objects are analytic objects. In my personal experience, whenever you have a ring of analytic objects, that ring is usually infinitely generated or some other sort of nonsense. Not so for MF_*:

Theorem 0.1. *There is an isomorphism* $\mathrm{MF}_* \cong \mathbb{C}[G_4, G_6]$ *of* $\mathbb{C}$*-algebras.*

Proof. Two good places to see a proof are [Zag08, §2.1] or [Lan95, §2]. Here's the general idea. The $\mathbb{C}$-algebra structure on MF_* comes from viewing each MF_k as a $\mathbb{C}$-vector space. The proof now proceeds via some dimension counting and a check that G_4 and G_6 are algebraically independent. □

Remark 0.2. You should now be saying, "Wait a minute, what about all the other Eisenstein series?" Well, they satisfy a pretty crazy recurrence relation. Let $d_k = (2k+3)k!G_{2k+4}$ for $k \geq 0$. Then

$$d_{n+2} = \frac{3n+6}{2n+9}\sum_{k=0}^{n}\binom{n}{k}d_k d_{n-k}$$

for all $n \geq 0$. We won't prove this, but you might find it to be a fun exercise.

In particular, once you know G_4 and G_6, the remaining Eisenstein series are given by a polynomial in G_4 and G_6. The coefficients of such a polynomial are rational — are they ever integers?

By now, you should be convinced that modular forms are at least somewhat interesting. For example, they played a role in the example of two isospectral but non-isometric tori. In fact, modular forms are extremely interesting, with all sorts of crazy applications in combinatorics, number theory, and even the representation theory of the monster group. These could be fun things to write your semester project on, but we'll have to press on.

Despite being interesting, the ring MF_* is extremely simple. What's more, the two generators G_4, G_6 of MF_* played a central role when we used $\wp(z,\Lambda)$ to write down the equation of the elliptic curve $\mathbb{C}/\Lambda$. So it seems like there should be some close connection between elliptic curves and modular forms. Our next major story arc is to make precise the connection between elliptic curves and MF_*, but this will take us a few lectures. Today, we'll just talk about elliptic curves.

1. Crash course in algebraic geometry

Some of you have expressed some worries about algebraic geometry, so we're going to begin with a very quick introduction to the subject. There is a lot that I won't be able to say here, but hopefully this will give you enough of a bearing to navigate our discussion on elliptic curves.

Historically (and intuitively), algebraic geometry begins with *affine varieties.*

Definition 1.1. Let k be a field. An *affine algebraic variety* is the set

$$\{c = (c_1, \ldots, c_n) \in k^n : f_1(c) = f_2(c) = \cdots = f_m(c) = 0\},$$

where $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$. In short, an affine variety is the solution set to a system of polynomial equations. I will often denote the solution set of $f_1, \ldots, f_m$ by $\mathbb{V}(f_1, \ldots, f_m)$.

Example 1.2. What does $\mathbb{V}(ax^2 + by^2 - 1)$ look like? How does this depend on our choice of field k?

Example 1.3. What does $\mathbb{V}(x^2+y^2-1, y-x)$ look like? What about $\mathbb{V}(x^2+y^2-1, y-1)$?

When $k = \mathbb{C}$, this is a pretty good definition. Points $(a_1, \ldots, a_n) \in \mathbb{C}^n$ are solutions to systems of the form $\{x_1 - a_1, \ldots, x_n - a_n\}$, which are in bijection with maximal ideals of the ring $\mathbb{C}[x_1, \ldots, x_n]$ (this is the *Nullstellensatz*). Even better, the set of solutions inherits a topology from the topology on $\mathbb{C}$, so affine varieties over $\mathbb{C}$ are topological spaces.

When $k = \mathbb{R}$, we still get a topology on our set of solutions, but other features of the definition start to break down a little. For example, the solution set to $x^2 + 1$ is empty, but this same polynomial has two solutions over $\mathbb{C}$. Even more strangely, $(x^2 + 1)$ is a maximal ideal of $\mathbb{R}[x]$, so the desired bijection between points of $\mathbb{R}^n$ and maximal ideals of $\mathbb{R}[x_1, \ldots, x_n]$ really breaks down.

Over an arbitrary field, things are even worse. Most fields don't have a reasonable topology to offer, and we still get all sorts of weird maximal ideals in $k[x_1, \ldots, x_n]$. You can solve both of these issues by introducing the *Zariski topology.* On first pass, the Zariski topology is the topology on k^n generated by sets of the form $\mathbb{V}(f_1, \ldots, f_m)$, which we define to be closed. After ruminating on this idea, you are eventually led to the notion of an *affine scheme*:

Definition 1.4. Let R be a commutative ring. The *spectrum of* R,[1] denote $\operatorname{Spec} R$, is the set of all prime ideals of R. The *Zariski topology* on $\operatorname{Spec} R$ is generated by closed sets, which we define as sets of the form $\mathbb{V}(I) = \{P \in \operatorname{Spec} R : P \subset I\}$. In other words, the *points* of $\mathbb{V}(I)$ are the *prime ideals* contained in I.

[1] We again encounter one of the most overloaded terms in math.

Here, I is an ideal of R, which is the correct formulation of a system of polynomial equations — indeed, if $I = (f_1, \dots, f_m)$, then $c \in k^n$ is a common solution of $f_1, \dots, f_m$ if and only if $g(c) = 0$ for all $g \in I$.

Definition 1.5. An *affine scheme* is the spectrum of some ring, equipped with the Zariski topology. Given an ideal $I \subset R$, the solution set $\mathbb{V}(I)$ is the scheme $\operatorname{Spec}(R/I)$.

To see that this is a good definition, let's think back on our weird $x^2 + 1$ example over $\mathbb{R}$. This didn't have any points as an algebraic variety, but it *does* have a point as a scheme! In particular, $(x^2 + 1)$ is a prime ideal, so this is a point of $\mathbb{V}(x^2 + 1)$.

Example 1.6. What does $\mathbb{V}(ax^2 + by^2 - 1)$ look like? How does this depend on our choice of field k?

Example 1.7. What does $\mathbb{V}(x^2+y^2-1, y-x)$ look like? What about $\mathbb{V}(x^2+y^2-1, y-1)$?

Remark 1.8. When you encounter the term *variety* in algebraic geometry, it generally means a scheme with several adjectives associated to it. These adjectives are meant to rule out some of the more unusual geometric properties that schemes can have.

As geometric objects, schemes should have a good notion of smoothness and dimension. The rough idea for smoothness is that the Jacobian matrix $(\partial f_i / \partial x_j)$ should have full rank on all of $\mathbb{V}(f_1, \dots, f_m)$. The notion of dimension comes from *Krull dimension.*

Definition 1.9. The *Krull dimension* of a commutative ring R is the supremum of the lengths of proper chains of proper ideals. The *Krull dimension* of a scheme $\operatorname{Spec} R$ is the Krull dimension of R.

Exercise 1.10. Compute the Krull dimension of $k[x_1, \dots, x_n]$ and $k[x, y]/(y^2 - ax^3 - bx - c)$.

The next step in the story is to go from affine schemes to projective schemes. I won't describe this carefully, but will instead tell you what you should imagine at the level of solution sets.

Let $\mathbb{P}^n_k$ denote projective n-space over a field k, whose points are $(n+1)$-tuples $[c_0 : \cdots : c_n]$ such that $[c_0 : \cdots : c_n] = [\lambda c_0 : \cdots : \lambda c_n]$ for all $\lambda \in k - \{0\}$. Given a system of homogeneous polynomials $f_1, \dots, f_m \in k[x_0, \dots, x_n]$, the projective variety $\mathbb{V}(f_1, \dots, f_m)$ is the set of solutions in $\mathbb{P}^n_k$ to $f_1, \dots, f_m$. Requiring the f_i to be homogeneous ensures that this solution set is well-defined.

2. What is an elliptic curve?

Now we can talk about elliptic curves. Our first encounter with these was as the complex tori $\mathbb{C}/\Lambda$. As a manifold, this is smooth, compact, and has genus 1. But we can also think about this as an abelian group, where the group operation comes from addition in $\mathbb{C}$, and the identity is the image of Λ. This leads to two plausible definitions of an elliptic curve over $\mathbb{C}$.

Definition 2.1. An *elliptic curve* over $\mathbb{C}$ is a smooth, projective algebraic curve of genus 1.

Definition 2.2. An *elliptic curve* over $\mathbb{C}$ is an abelian variety of dimension 1.

I haven't defined abelian varieties yet – we'll do this more carefully next time. For now, I'll just mention that these two definitions coincide.

Exercise 2.3. Prove that every abelian variety of dimension 1 has genus 1.

Hint: use the group structure to show that every abelian variety has trivial tangent bundle. For curves, the tangent bundle is dual to the canonical bundle. Use the adjunction formula to compute the canonical bundle of a smooth, projective curve of genus g.

Next time: elliptic curves and period integrals.

References

[Lan95] Serge Lang. *Introduction to modular forms.* Vol. 222. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original. Springer-Verlag, Berlin, 1995, pp. x+261.

[Zag08] Don Zagier. "Elliptic modular forms and their applications". In: *The 1-2-3 of modular forms.* Universitext. Springer, Berlin, 2008, pp. 1–103. URL: https://doi.org/10.1007/978-3-540-74119-0_1.

Department of Mathematics, Harvard University

Email address: smckean@math.harvard.edu

URL: shmckean.github.io