REU: Rational Curves over Finite Fields

Professor Johan de Jong
Notes by Tabes Bridges

Summer 2012

1 First Lecture, 5/29

Our main object of study is $X \subset \mathbb{P}^5_{\mathbb{F}_2}$, where X is the degree 5 Fermat hypersurface, which we are looking at in $\mathbb{P}^5$ over $\mathbb{F}_2$. X is the zero locus $\{X_0^5 + X_1^5 + ... + X_5^5 = 0\}$. The question is, "what kind of rational curves lie on X?" Since $\mathbb{F}_2$ only has one invertible element, $\mathbb{P}^n(\mathbb{F}_2) = \mathbb{F}_2^{n+1} \setminus 0$, which suggests that the Fermat quintic has the same zero locus as the linear hypersurface $X_0 + X_1 + ... + X_5 = 0$; however, we are interested in field extensions as well, so X is a "thing," not just the space of solutions.

Definition. *A **rational curve** is the image of a morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^5$ which maps into X; it is unlikely that we will ever actually look at the image, instead saying that the morphism is the curve.*

Goal. X has too many rational curves, and they behave differently than we expect. We want to find **(very) free rational curves** on X or prove that they don't exist, i.e. $\varphi^* T_X$ is globally generated or ample.

Definition. *A **morphism** $\varphi : \mathbb{P}^1 \to \mathbb{P}^5$ over a field K is given by $f_0, ..., f_5 \in K[Y_0, Y_1]$ homogeneous and all of the same degree d such that $(a : b) \mapsto (f_0(a : b) : ... : f_5(a : b))$ makes sense (which renders the bit about same degree redundant, and requires them to not have a common zero except $(0, 0)$, equivalently gcd$(f_0, ..., f_5) = 1$.).*

Definition. *We say that φ maps **into** $X = \{F = 0\}$, where F is the Fermat quintic, if and only if $F(f_0, ..., f_5) \equiv 0$ as a polynomial in $K[Y_0, Y_1]$.*

2 Second Lecture, 5/30

We begin with the projective plane. Informally, it is a thing with points and lines and an incidence correspondence, i.e. $P \in L$, together with the axioms

- Any two distinct lines meet in a unique point.
- For any two distinct points, there exists a unique line passing through both of them.

Remark. Swapping the terms “line” and “point” changes nothing, so we have a type of duality.

Exercise. Show that the number of points and the number of lines are equal, assuming that not all points are colinear, and not all lines pass through a single point. If we look at the tautological line bundle over $\mathbb{P}^2$, we can also look at the projection from the total space to the space of lines. It suffices to show that these maps have fibers with the same cardinality. Fix distinct points P, Q. Consider a line L through P but not Q, and a line M through Q but not P. The intersection point $L \cap M$ is neither P nor Q. The set of such pairs (L, M) is in bijection with the points of $\mathbb{P}^2$ not on $\overline{PQ}$. Thus

$$(\#\text{lines thru } P - 1)(\#\text{lines thru } Q - 1) = \#\text{points of } P - \#\text{points on } \overline{PQ}.$$

Thus the number of lines through P is independent of which $P \in \overline{PQ}$ we chose (this only works if $\overline{PQ}$ has at least three points). Because every two points determine a line, we conclude that (modulo boundary cases) the number of points on a line is independent of the choice of line by duality. Now we choose a line L and a point P, assuming $P \notin L$. Choosing any line through P, it intersects L in some Q. Conversely choosing any $Q \in L$, there is a unique line $\overline{PQ}$. We have an explicit bijection of sets $\{\text{lines through } P\} \to \{\text{points on } L\}$ given by $M \mapsto L \cap M$ with inverse given by $Q \mapsto \overline{PQ}$.

Open Question. What are the orders of finite projective planes? There are some exotic ones...

Example. *Let K be a field. We have a projective plane $\mathbb{P}^2_K$ whose points are 1-dimensional K-vector subspaces of $K^{\oplus 3}$. We think of a point as a triple $(a : b : c)$ of elements of K not all zero, taken up to a multiplicative scalar. We might write $\mathbb{P}^2_K = (K^2 \setminus \{0\})/K^*$. A line $L \in \mathbb{P}^2$ is given by an equation $AX_0 + BX_1 + CX_2 = 0$ for $A, B, C \in K$ not all zero. If L' is given by $A'X_0 + B'X_1 + C'X_2 = 0$, then $L = L'$ if and only if $A = \lambda A'$, $B = \lambda B'$, and $C = \lambda C'$ for some $\lambda \in K^*$. The incidence relation is given by saying that $(a : b : c) \in L$ if and only if $Aa + Bb + Cc = 0$.*

Exercise. Show that $\mathbb{P}^2_K$ is a projective plane in the axiomatic sense.

Convention. We will write all scripts over $K = \mathbb{Z}/p\mathbb{Z}$.

Projective Line. We have points of the form $(a : b)$. In the case $\mathbb{P}^2_{\mathbb{F}_p}$, there are $p + 1$ points, which can be counted via the group action or via “affine decomposition.”

Automorphisms of $\mathbb{P}^1$. These will all look like $(x_0 : x_1) \mapsto (a_{00}x_0 + a_{01}x_1 : a_{10}x_0 + a_{11}x_1)$ where $A = (a_{ij} \in GL_2(K)$. If $A = \lambda A'$ for some $\lambda \in K^*$, then A and A' define the same automorphism. We conclude that $Aut_K(\mathbb{P}^1) \cong PGL_2(K) = GL_2(K)/K^*$. These are basically just coordinate changes.

Exercise. Giving the images of three distinct points determines an automorphism of $\mathbb{P}^1$.

Definition. *A **conic** C is an equation $F = 0$ (*not *the zero locus, but the equation itself) where*

$$F = \sum_{0 \le i \le j \le 2} a_{ij} X_i X_j$$

for $a_{ij} \in K$ not all zero. $C = C'$ if and only if $F = \lambda F'$ for $\lambda \in K^*$.

Example. *$F = X_0^2 + X_1^2 + X_2^2$ is a conic.*

Definition. *We say $(a : b : c) \in C$ if $F(a, b, c) = 0$.*

Remark. The example has an empty zero locus over $\mathbb{R}$, though it has many points over $\mathbb{C}$.

Intersections. In affine space, we could have a conic meeting a line in $0, 1$, or 2 points.

Proposition. *Every conic over a finite field K has a point over K.*

Proof. Optional exercise. ■

Definition. *We say $C : F = 0$ is **irreducible** if and only if F is irreducible in $K[X_0, X_1, X_2]$.*

Parametrization. Given a line L and a point $P \notin L$, we can parametrize L by slopes of lines through P intersecting L. We want to do something similar for an irreducible conic. In general, this does not work. The trick is to take a point on C. Since every conic over a finite field has a point, we can do this. Looking at all of the lines through P, we get a bijection with the remaining points on C.

Exercise. Explicitly do the stereographic projection for irreducible, smooth conics.

Example. *Let $K = \mathbb{R}$ and $F = X_0^2 + X_1^2$. This is irreducible since we do not have access to imaginary numbers. It has a single point $(0 : 0 : 1)$ over the reals, which is the intersection point of the two lines which constitute the conic over $\mathbb{C}$ (the lines are conjugate under the action of the Galois group).*

3 Third Lecture, 6/1

In PARI, "Mod(1,p)" returns the integer $1 \mod p$. If we write "Mod(1,p)*A", with A a matrix, we get the matrix with entries $\mod p$.

One way to compute the intersection points of a conic C and a line L is to parametrize the line as $t \mapsto (at + b : ct + d : 1)$, although this misses the point passing through $\{z = 0\}$. Then solve $F(at + b, ct + d, 1) = 0$ in t and substitute back in.

Perhaps more natural is to paramatrize via a morphism $\mathbb{P}^1 \to \mathbb{P}^2$ given by $(y_0 : y_1) \mapsto (ay_0 + by_1 : cy_0 + dy_1 : y_1)$.

Morphisms from $\mathbb{P}^1 \to \mathbb{P}^n$. These are given by $(n + 1)$-tuples $G_0, ..., G_n \in K[Y_0, Y_1]$, homogeneous and all of the same degree, with $gcd(G_0, ..., G_n) = 1$. This last condition makes sense since $K[Y_0, Y_1]$ is a UFD. The map (on points) is then $(a : b) \mapsto (G_0(a, b) : G_1(a, b) : \cdots : G_n(a, b))$.

Explanation of gcd condition. Suppose $K = \bar{K}$. Then if $G \in K[Y_0, Y_1]$ is homogeneous of degree d, it can be factored into linear forms.

Example. *$Y_0^2 + 3Y_0Y_1 + Y_1^2$ de-homogenizes to $T^2 + 3T + 1 = (T - \alpha)(T - \beta$ with α, β given by the quadratic formula. Then our original form factors as $(Y_0 - \alpha Y_1)(Y_0 - \beta Y_1)$.*

So anyway, we can write $G = cY_1^e \prod_{i=1}^{d-e}(Y_0 - \alpha_i Y_1)$, where e is some sufficiently large integer. Call this the **canonical form**

Example. $5Y_0Y_1^2 - Y_1^3 = 5Y_1^2(Y_0 - \frac{1}{5}Y_1)$.

So in this case, the zero locus of G in $\mathbb{P}_K^1$ is the collection consisting of $(1:0)$ with multiplicity e and $(\alpha_i : 1)$ for $i = 1, ..., d-e$ with possible repeats.

Going back to $G_0, ..., G_n$, write each in canonical form. Then take the *gcd* as in the case of integers.

Cool Thing That Happens. A morphism $\mathbb{P}^1 \to \mathbb{P}^2$ should have as its image a curve in $\mathbb{P}^2$. The integer d is the **degree of the morphism**. Multiplying the $(n+1)$-tuple by $\lambda \in K^*$ results in the same morphism.

If $d = 2$, we claim that the "image" is either a line or a conic. Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ be given by the triple G_0, G_1, G_2. We say φ **maps into** a curve $C : F = 0$ if and only if $F(G_0, G_1, G_2) = 0$ in $K[Y_0, Y_1]$. Note that in this case, if φ is not a constant morphism, then φ will be onto C.

4 Fourth Lecture, 6/4

We begin today by trying to solve Exercise 17. Let $G_0, G_1, G_2 \in K[S, T]$ be homogeneous quadratics. We need $a_{ij} \in K$ not all zero such that

$$\sum_{i \leq j} a_{ij} G_i G_j \equiv 0.$$

The terms are elements of a five-dimensional vector space of homogeneous polynomials of degree 4, which has basis $S^4, S^3T, ..., T^4$. There are six polynomials in the sum, hence there is a nontrivial linear dependence.

Suppose now $\deg G_0 = \deg G_1 = \deg G_2 = d$. We want $F \in K[X_0, X_1, X_d]_d$ (the space of homogeneous polynomials od degree d) such that $F(G_0, G_1, G_2) \equiv 0$ in $K[S, T]$. F gives a K-linear map $K[X_0, X_1, X_2]_d \to K[S, T]_{d^2}$. To get a (provably) nonzero kernel, we need

$$\dim(LHS) \binom{d+2}{2} > \dim(RHS) = d^2 + 1.$$

This doesn't work. We could try replacing d on the left with e, giving $\frac{(e+2)(e+1)}{2} > de + 1$, which works for $e >> d$. It always maps into some curve, but it is harder to show that the image is degree d.

In general, cubic curves *cannot* be parametrized by $\mathbb{P}^1$.

Fact. If $C : F = 0$ in $\mathbb{P}^2$ is a cubic, is irreducible even over $\bar{K}$, and is singular, then we can parametrize it.

Warmup. Consider the conic $x^2+y^2=1$ over $\mathbb{R}$. We wish to parametrize it with basepoint $(1,0)$. We have $(1,0)+\lambda(1,t)$, so we get $(1+\lambda)^2+\lambda^2t^2=1$, so $2\lambda+\lambda(1+t^2)=0$. Our basepoint corresponds to $\lambda=0$, so we factor this out and get

$$t \mapsto \left(1+\frac{-2}{1+t^2}, \frac{-2t}{1+t^2}\right).$$

In $\mathbb{P}^2$, this is equivalent to

$$t \mapsto \left(t^2-1:-2t:1+t^2\right).$$

Back to cubics. We can always factor something in just two variables. Consider $C: X^3+Y^3+5XYZ=0$. Dehomogenizing by setting $z=1$, we get $x^3+y^3+5xy=0$. This is most likely a nodal curve. We have the line $\lambda(1,t)$ through the node. Substituting, we get $\lambda^3+(\lambda t)^3+5\lambda(\lambda t)=\lambda^2(\lambda+\lambda t^3+5t)=0$. Thus $\lambda=-5t/(1+t^3)$, and we have the parametrization

$$t \mapsto \left(\frac{-5t}{1+t^3}, \frac{-5t^2}{1+t^3}\right).$$

We now turn to surfaces in $\mathbb{P}^3$. Such a thing is $S: F=0$, where $F \in K[X_0, X_1, X_2, X_3]$. We can again talk about irreducible and singular points.

Dumb Route to Rational Curves. First consider the special case in which S is a quadric or cubic surface (degree of F is 2 or 3). We again have morphisms $\varphi: \mathbb{P}^1 \to \mathbb{P}^3$, this time given by a quadruple of homogeneous polynomials of the same degree. The dumb idea is to just take $X_3=0$, thus passing to a subvariety, which looks like $\mathbb{P}^2$, in which we can look for rational curves; in fact we intersect the ambient subvariety with S. The result of the intersection is a curve. If S is a quadric, we should more or less always be able to parametrize. In the cubic case, we may not be able to parametrize.

Intersecting a quadric with a plane may yield several different types of curves. In the cubic case, we will try to find a plane in $proj^3$ whose intersection with S is singular.

5 Fifth Lecture, 6/6

Definition. *A **rational plane curve** is a morphism $\varphi: \mathbb{P}^1 \to \mathbb{P}^2$ given by $(a:b) \mapsto (G_0(a:b), G_1(a:b), G_2(a:b))$, where the G_i are homogeneous polynomials of degree d.*

Last time, we showed by a dimension count that if

$$\binom{e+2}{2} > de+1,$$

then there exists a curve $C: F=0$ of degree e such that φ maps into C. On the other hand, the general theory says that there exists such a C of degree d. To prove this, begin by dehomogenizing. Take

$$\varphi: (1:t) \mapsto (G_0(1:t):G_1(1:t):G_2(1:t)) = \left(1:\frac{G_1(1:t)}{G_0(1:t)}:\frac{G_2(1:t)}{G_0(1:t)}\right) = (1:f(t):g(t))$$

We want to find $Q \in K[x,y]$ of total degree at most d such that $Q(f,g) = 0$ as a rational function.

"Okay, now we're gonna do something mildly clever..." -Johan

Set $L = K(x)$ and $M = K(t)$, respectively fields of fractions. Consider the map $ev_f : L \to M$ taking $x \mapsto f$, and more generally $h(x) \mapsto h(f)$. One can prove that this is a ring map (in fact a map of K-algebras). Note that there is a potential problem: suppose $h = (x^2 - 5)/(x - 7)$, then $h(f) = (f^2 - 5)/(f - 7)$, and we need $f - 7 \neq 0$ as a rational function. This is OK as long as f is not constant. Since ev_f is a ring map of fields, it is an injective map, so we can think of M as a field extension of L. Since t generates M over K, it also generates M over L. Moreover, we have $x = f(t)$ in M; in other words, $xG_0(1,t) = G_1(1,t)$ is a polynomial equation for t over L of degree at most d. Thus M is a finite extension of L with $[M : L] \leq d$. $M \cong L[T]/$some monic irreducible polynomial $P(T) \in L[T]$, mapping $T \mapsto t$, where $P(T)$ divides $xG_0(1,t) - G_1(1,t)$.

In the first place, we wanted to find a $Q \in K[x,y]$. We start by finding an expression for y in x. Consider $g(t) \in M$. Because M/L is finite of degree at most d, there exist $a_0, ..., a_d \in L$ not all zero such that $a_0 + a_1 g + ... + a_d g^d = 0$ in M, which follows because M has dimension d as a vector space over L, but $1, g, ..., g^d$ has order $d+1$, yielding a linear relation. Clearing denominators, we may assume $a_0, ..., a_d \in K[x]$. Set $Q = a_0(x) + a_1(x)y + ... + a_d(x)y^d \in K[x,y]$. By construction, $Q(f,g) = 0$. This is not ideal, as the degree in x could be quite large.

Let $I = \{Q \in K[x,y] \mid Q(f,g) = 0\}$. This is an ideal, and we have more-or-less shown that there exists $Q \in I$ with $\deg_y Q \leq d$. By symmetry, there exists $Q' \in I$ with $\deg_x Q' \leq d$.

Exercise. $\gcd(Q, Q') \in I$, i.e. I is principle. Try working in $K(x)[y]$. The Euclidean algorithm and the Gauss lemma probably come up.

The degree bounds hold up to a linear change of coordinates; suppose we have $x^d y^d$, then taking $x \mapsto x + y$ results in a factor of y^{2d}. To finish the argument, choose $Q \in I$ a generator and observe the bounds on the degree. Do a linear change of coordinates such that the degree in the "new y" is equal to the total degree in y.

Exercise 27. This will be a guided discussion rather than a lecture. The goal is to find rational curves on $S : X_0^3 + X_1^3 + X_2^3 + X_3^3 = 0$ over $\mathbb{F}_2$. Mike suggests we pick d, and list all possible 4-tuples $G_0, ..., G_3 \in \mathbb{F}_2[S,T]_d$, and compute $\sum G_i^3$ to see if we get 0. The number of choices is $(2^{d+1})^d$, while the number of possible outcomes is 2^{3d+1}. The estimated number of solutions is $2^{4d+4}2^{-(3d+1)} = 2^{d+3}$.

John observes that the solutions of $\sum X_i^3 = 0$ in $\mathbb{P}^3_{\mathbb{F}_2}$ are $(1:1:1:1)$ and permutations of $(0:0:1:1)$. Johan suggests prescribing a set map $\Phi : \mathbb{P}^1(\mathbb{F}_2) \to S(\mathbb{F}_2)$. and carrying out Mike's method, looking only at those φ with $\varphi|_{\mathbb{P}^1(\mathbb{F}_2)} = \Phi$.

Since we already had the idea of cutting S with a plane (a linear surface) to yield a cubic curve, I suggest that we try cutting S with a higher degree surface S' in a way that yields a curve $S \cap S'$ with an irreducible component which can be parametrized. If S' is a plane, it needs to be tangent at a point of intersection. If S' is a quadric surface, $S \cap S'$ will usually be a genus 4 curve, which means that getting it to be rational requires S and S' having four points of tangency. This is really hard.

Somehow or another, we've ended up talking about the group law on a cubic curve. If we have two points on a cubic over a given field, their composition will also be on the cubic over that field. If we have rational curves through the original pair of points, we can parametrize them with a line, which will cut out a third rational curve as the composition point varies.

6 Sixth Lecture, 6/8

We now discuss graded modules over $R = K[T]$.

Definition. *A **graded ring** is of the form $R = R_0 \oplus R_1 \oplus R_2 \oplus \ldots$. We call R_i the degree i part of R, which takes the form KT^i. We also have the condition $R_d \cdot R_{d'} \subset R_{d+d'}$. A **graded module** is an R-module M together with a direct sum decomposition $M = \bigoplus_{n \in \mathbb{Z}} M_n$ such that $R_d \cdot M_n \subset M_{d+n}$.*

Remark. For reasons of abstract nonsense, all rings are graded from 0 up, while modules are graded over all of $\mathbb{Z}$. Thus viewed as a module over itself, a ring has empty graded pieces for negative indices.

Example. *Let $M = K[T, T^{-1}]$. $M_n = KT^n$ for each $n \in \mathbb{Z}$. Thus each graded piece is nonzero.*

Definition. *An element $x \in M$ is **homogeneous (of degree n)** if and only if $x \in M_n$. Thus zero is homogeneous of every degree.*

Exercise 28. If M is a finitely-generated graded R-module, then it is generated by finitely many homogeneous elements.

Exercise 29. If M is a finitely-generated graded R-module, then (a) $M_n = 0$ for all $n << 0$, and (b) $\dim_K(M_n) < \infty$ for all $n \in \mathbb{Z}$.

Definition. *In the situation of Exercise 29, we define the **Hilbert function** H_M of M to be a map $H_M : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ taking $n \mapsto \dim_K(M_n)$.*

Exercise 30. What are all possible H_M for $R = K[T]$ and M a finitely-generated graded R-module? If $M = (0)$, the function vanishes. If $M = (T)$, the function is 1 for $n \geq 1$, zero otherwise. If $M = R$, the function is 1 for $n \geq 0$, zero otherwise. If $M = R/(T^2)$, the function is 1 for $n = 0, 1$ and zero otherwise. Note that $H_M + H_N = H_{M \oplus N}$.

Definition. *If M is a graded module, then for $e \in \mathbb{Z}$ the **twist** $M(e)$ is the graded module such that the underlying R-module is M, and $M(e)_n = M_{e+n}$.*

Remark. The values of the Hilbert function are determined by the behavior of generators. Since we are looking at finitely generated modules, the function will be constant after a point.

7 Seventh Lecture, 6/11

To do before Friday: Rankeya, Tabes, and John - write a script that works; Mike - flesh out argument posted thus far; Joe - nothing.

Let $R = K[S,T]$, where S,T are homogeneous of degree 1. We continue talking about graded R-modules. If M is a finitely generated R-module, then $M_n = 0$ for $n << 0$, and $\dim_K(M_n) < \infty$. Recall that for each M we have a **Hilbert function** $H_M : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ taking $n \mapsto \dim_K(M_n)$.

Lemma. *In this situation, there exist a, b such that $H_m(n) = an + b$ for all $n >> 0$.*

Proof. Consider multiplication by S, which is a module map $M \xrightarrow{S\cdot} M$ which does not preserve the grading. Let $L = \ker(M \xrightarrow{S\cdot} M)$ and $Q = \operatorname{coker}(M \xrightarrow{S\cdot} M)$. We claim that L and Q are graded R-modules, as $L = \bigoplus_{n\in\mathbb{Z}} \ker(M_n \xrightarrow{S\cdot} M_{n+1})$ and $Q = \bigoplus_{n\in\mathbb{Z}} \operatorname{coker}(M_{n-1} \xrightarrow{S\cdot} M_n)$, and S acts as zero on both L and Q, so we can think of both L and Q as graded $K[T]$-modules via the map $S \mapsto 0$, $T \mapsto T$. Also, Q and L are finitely generated; this fact is obvious for Q since it is a quotient of a finitely generated module. For L, we know that $L \subset M$ is a submodule. It is a fact that over Noetherian rings, submodules of finitely generated modules are finitely generated. $K[S,T]$ is Noetherian, so L is finitely generated. As we observed last time, there exist $\ell, m \geq 0$ such that $H_L(n) = \ell$ for all $n >> 0$ and $H_Q(n) = m$ for all $n >> 0$. For every n, we have an exact sequence of vector spaces

$$0 \to L_n \to M_n \xrightarrow{S\cdot} M_{n+1} \to Q_{n+1} \to 0.$$

This implies that

$$\dim(M_{n+1}) - \dim(M_n) = \dim(Q_{n+1}) - \dim(L_n) = m - \ell$$

for $n >> 0$. Elementary arguments show that $H_M(n) = (m-\ell)n + b$ for all $n >> 0$, for some $b \in \mathbb{Z}$. ■

Definition. *If $H_M(n) = an+b$ for all $n >> 0$, then $an+b$ is called the **Hilbert polynomial** of M.*

Recall that we defined a twisted module $M(e)_n = M_{e+n}$. We can defined $R(e)$ to be the graded R-module with $R(e)_n$ equal to R_{e+n} for $e+n \geq 0$ and 0 for $e+n < 0$. This is, as an R-module, free of rank 1 with a generator 1 in degree $-e$.

Definition. *A finitely generated graded module M is called **graded free** if and only if $M \cong R(e_1) \oplus ... \oplus R(e_r)$ as a graded module.*

Facts about such modules. The dimension of a graded piece is $n+1$ since we have two variables. Thus the dimension of $R(e)_n$ is $n+e+1$, so the Hilbert polynomial is $rn + e_1 + ... + e_r + r$. M has a minimal set of generators $x_i = (0, ..., 1, ..., 0)$ in degree $-e_i$; this set has cardinality r. We claim that if we order $e_1 \leq e_2 \leq ... \leq e_r$, then $e_1, ..., e_r$ is an invariant of the isomorphism class of M.

Definition. *If M is graded free, the sequence $e_1 \leq ... \leq e_r$ such that $M \cong \bigoplus R(e_i)$ is called the* ***splitting type of*** *bfM.*

Exercise 32. Let M be graded free. We want an algorithm to find the splitting type using only the Hilbert function.

Exercise 33 (optional. The kernel of a map of graded free modules is graded free.

Exercise 34. Let $G_0, ..., G_n \in R = K[S, T]$. Let $\varphi = (G_0, ..., G_n) : \mathbb{P}^1 \to \mathbb{P}^n$ be a morphism of degree d. Let

$$\Omega(\varphi) := \ker(R(-d) \oplus ... \oplus R(-d) \xrightarrow{G_0,...,G_n} R)$$

taking

$$(L_0, ..., L_n) \mapsto \sum G_i L_i.$$

We call this module $\Omega(\varphi)$ the **pullback of the cotangent bundle**. Compute the Hilbert polynomial of $\Omega(\varphi)$.

Example. *Let $(G_0, G_1, G_2) = (S^2, ST, T^2) : \mathbb{P}^1 \to \mathbb{P}^2$. $\Omega(\varphi)$ is the kernel of the map $R(-2)^{\oplus 3} \to R$. This map is nontrivial, but it is clearly not surjective, so the rank should be 2 (the module is free by Exercise 33). For $n = 1$, $H_{R(-2)^3} = 0$, $H_R = 2$, $H_{\Omega(\varphi)} = 0$. For $n = 2$, $H_{R(-2)^3} = 3$, $H_R = 3$, $H_{\Omega(\varphi)} = 0$. For $n = 3$, $H_{R(-2)^3} = 6$, $H_R = 4$, and $H_{\Omega(\varphi)} = 2$ if the map is surjective, which is clear. Since the rank is 2, we are done. Thus $\Omega(\varphi) \cong R(-3)^{\oplus 2}$.*

Definition. *We will call the splitting type of $\Omega(\varphi)$ the* ***splitting type of*** *φ.*

Question. Is there a rational curve on the Fermat quintic φ such that the splitting type of φ consists entirely of negative integers.

8 Eighth Lecture, 6/13

Fix a morphism $\varphi = (G_0, ..., G_n) : \mathbb{P}^1 \to \mathbb{P}^n$ of degree d. Recall that we defined

$$\Omega(\varphi) \ker(R(-d)^{\oplus n+1} \to R),$$

where $R = K[S, T]$. The **splitting type of** φ is the splitting type of $\Omega(\varphi)$.

Remark. The pullback of the cotangent bundle will always have rank n.

Example. *If $n = 1$, so $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$, then the splitting type is $-2d$.*

If φ "is" a line, the splitting type is $-2, -1, -1, ..., -1$, where the number of -1 terms is $n - 1$.

Aside. $H_{\Omega(\varphi)}(m) = \dim \ker(R(-d)_m^{oplusn+1} \to R_m)$. It is a fact that if $\gcd(G_0, ..., G_n) = 1$, then the map is surjective for $m >> 0$, so we get $(n+1)\dim(R(-d)_m) - \dim(R_m) = (n+1)\dim(R_{d+m}) - \dim(R_m) = (n+1)(-d+m+1) - (m+1) = nm + (-d(n+1)+n)$; in the definition of Hilbert polynomial, $n = a$, and $(-d(n+1)+n) = b$. It follows that if $e_1, ..., e_n$ is the splitting type of φ, then

$$e_1 + ... + e_n + n = -d(n+1) + n.$$

Last time, we saw that a conic in $\mathbb{P}^3$ has splitting type $-3, -3$, which checks out, as does the case of a line above.

Cubics. In the good case, the splitting type is $-4, -4, -4, -5, -4, -3$, or $-6, -3, -3$. The last of these is the case where φ maps to a a line; the first is the standard case, and the middle case is where we map into a plane (necessarily nodal).

Example. *Let* (T^4, T^3S, TS^3, S^4) *be a morphism of degree* 4. *Then* $\Omega(\varphi) = \ker(R(-4)^4 \to R)$. *The sum* $e_1 + e_2 + e_3$ *must be* $-4(3+1) = -16$. *For* $m = 4$, *the Hilbert function vanishes since there are no relations among the* G_i *with constant coefficients. For* $m = 5$, *the map* $R_1^{\oplus 4} \to R_5$ *is surjective since we can get any degree* 5 *monomial, so the Hilbert function is* $8 - 6 = 2$. *Thus we have* $e_1 = e_2 = -5$, *so we must have* $e_3 = -6$.

If $\varphi : \mathbb{P}^1 \to \mathbb{P}^n$ maps into a nonsingular degree e hypersurface $X : F = 0$, then there is another important module $E_X(\varphi) = \ker(R(d)^{\oplus n+1} \to R(ed))$ given by

$$\frac{\partial F}{\partial X_i}(G_0, ..., G_n)$$

in each coordinate. This roughly measures something to do with infinitesimal perturbations of the curve φ.

Goal. Find φ on the Fermat quintic $X \subset \mathbb{P}^5_{\mathbb{F}_2}$ such that the splitting type of $E_X(\varphi)$ is nonnegative, or prove that it cannot happen. In this case, the first partials all take the form X_i^4.

Exercise 37. Relate the splitting types of $\Omega(\varphi)$ and $E_X(\varphi)$.

Why is the Fermat Hypersurface special? We look for lines on X. A line in $\mathbb{P}^5$ can be parametrized as $(S : T) \mapsto (a_0S + b_0T : ... : a_5S + b_5T)$. This lies on X when

$$(a_0S + b_0T)^5 + ... + (a_5S + b_5T)^5 = 0 \quad = (a_0^5 + ... + a_5^5)S^5 + \binom{5}{1}(a_0^4b_0 + ... + a_5^4b_5)S^4T + ...$$

There seem to be six conditions here, but in fact $\binom{5}{2} = \binom{5}{3} = 10$ automatically vanish in characteristic 2. In characteristic 0 there would be a two-dimensional family of lines on X, but the vanishing of the two equations increases the dimension to four.

Problem. X has *too* many rational curves.

9 Ninth Lecture, 6/15

Lemma. *If* $\psi : M \to N$ *is a (degree preserving) map of graded modules and we have* n *such that* ψ_n *is surjective and* N *can be generated by homogeneous elements in degree at most* n, *then* ψ_m *is surjective for all* $m \leq n$.

We work another example of computing the splitting type. We have a conic on the Fermat quintic given by

$$(S : T) \mapsto (S^2, S^2, ST, ST, T^2, T^2),$$

which is a closed immersion of $\mathbb{P}^1$ in $proj^5_{\mathbb{F}_2}$. $\Omega(\varphi)$ is the kernel of the map $R(-2)^{\oplus 6} \to R$ given by the conic. For $n = 2$, $H_{R(-2)^6} = 6$, while $H_R = H_\Omega = 3$. For $n = 3$, $H_{R(-2)^6} = 12$, while $H_R = 4$ and $H_\Omega = 8$. We have generators $-2, -2, -2, -3, -3$, and we were looking for rank 5, so we are done.

Recall that $E_X(\varphi) = \ker(R(2)^{\oplus 6} \to R(10)$, where the map is given by $(S^8, S^8, S^4T^4, S^4T^4, T^8, T^8)$. For $n = -2$, $H_{R(2)^6} = 6$, $H_{R(10} = 9$, and $H_{E_X} = 3$, which gives the first three generators. For $n = -1$, $H_{R(2)^6} = 12$, $H_{R(10} = 10$, $H_{E_X} = 6$. For $n = 0$, $H_{R(10} = 18$, $H_{R(10} = 11$, and $H_{E_X} = 9$. For $n = 1$, the map is surjective, so $H_{R(2)^6} = 24$, $H_{R(10)} = 12$, and $H_{E_X} = 12$. For $n = 2$, $H_{R(2)^6} = 30$, $H_{R(10} = 13$, and $H_{E_X} = 17$, giving two more generators.

10 Tenth Lecture, 6/18

Lemma. *(Exercise 33) Let $R = K[S,T]$. The kernel of a map of graded free modules is graded free.*

Proof. Say we have a map $\varphi : M \to N$ of graded free modules such that $\varphi(M_n) \subset N_n$. Set $L = \ker\varphi = \bigoplus \ker(M_n \to N_n)$. Consider multiplication by S, so we have a diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & L(1) \arrow[r] \arrow[d, "\cdot S"] & M(1) \arrow[r] \arrow[d, "\cdot S"] & N(1) \arrow[d, "\cdot S"] \\
0 \arrow[r] & L \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & N \arrow[d] \\
 & L/SL \arrow[r] \arrow[d] & M/SM \arrow[r] \arrow[d] & N/SN \arrow[d] \\
 & 0 & 0 & 0.
\end{tikzcd}$$

We claim that $L/SL \to M/SM$ is still injective, which follows from the Snake Lemma. Set $\overline{R} = R/SR \cong K[T]$. Say $M \cong \bigoplus_{i=1}^r R(e_i)$. Then $M/SM = \bigoplus_{i=1}^r \overline{R}(e_i)$ as an $\overline{R}$-module.

We now claim that a submodule of a graded free $\overline{R}$-module is a graded free $\overline{R}$-module. Say U lives in a graded free module, then argue using the following steps:

- U is finitely generated since $\overline{R}$ is Noetherian.
- We can pick a minimal generating set.
- If $\sum a_i u_i = 0$ with a_i homogeneous and all $\deg_T(a_i) > 0$, then $\sum (a_i/T) u_i = 0$ since U has no T-torsion.
- Minimality of u_i means that $\sum a_i u_i = 0$ implies $\deg_t(a_i) > 0$ for all i.

Thus we have that L/SL is a graded free $\overline{R}$-module. Pick $\ell_1, ..., \ell_r$ homogeneous such that the images $\bar{\ell}_1, ..., \bar{\ell}_r \in L/SL$ for a basis (equivalently a minimal generating set). To prove the claim, we need to check that the generate and are linearly independent.

To see generation, note that R is Noetherian, so L is finitely generated, hence $L_n = 0$ for $n << 0$. We show by induction on n that the ℓ_i span L_n. The base case is far to the left. Suppose this is true for L_{n-1}. Pick $x \in L_n$. By the choice of ℓ_i, we can write $x = \sum a_i \ell_i + S \cdot x'$ for some $a_i \in R$ homogeneous and some $x' \in L_{n-1}$. By the induction hypothesis, $x' = \sum a_i \ell_i$, proving the claim.

For linear independence, we argue just as in the proof of the second claim. ■

Computing Splitting Types. Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^n$ be a rational curve of degree d. As it stands, we know that $\Omega(\varphi) = (e_1, ..., e_n)$ is the kernel of $\varphi : R(-d)^{\oplus n=1} \to R$, and the Hilbert polynomial $P_{\Omega(\varphi)}(t) = nt - d(n+1) + n$. We know that $\Omega(\varphi)_t = 0$ for $t < d$, and that $e_i \leq -d$, hence $e_1 + ... + e_n = -d(n+1)$. $e_i = -d$ for some i if and only if there exists a relation $\sum a_i G_i = 0$ with all $a_i \in K$ and not all zero.

If $n = 2$, we can plot the possible values (e_1, e_2). They lie on a line with negative slope through $(-3d, -3d)$, with neither coordinate greater than $-d$, which reveals that neither coordinate can be less than $-2d$.

Computing the Hilbert Function. The straightforward way is to compute the matrix of φ in degree t. Choose a basis for R_t, the monomials in S, T of degree t. Call $S^i T^j = \alpha_{ij}$. Choose a basis for $(R(-d)^{\oplus n})_t = R^{\oplus n+1}_{-d+t}$, the monomials of degree $t - d$ for each copy. Call $S^i T^j$ in the k-th summand β_{ijk}. β_{ijk} maps to $G_k S^i T^j$.

Things We Want.

- A function that computes $H_{\Omega(\varphi)}(t)$ using the matrix method.
- A function that uses $H_{\Omega}(t)$, d, n, and spits out $e_1, ..., e_n$.
- Find some curves on X.
- Relate the splitting types of Ω and E_X.

11 Eleventh Lecture, 6/20

We are looking for either free or very free rational curves. A **free** curve is one for which the splitting type of $E_X(\varphi)$ is nonnegative. A **very free** curve is one for which the splitting type is strictly positive.

Proposition. *(Mingmen Shen) If the Fermat hypersurface X has a rational normal curve C, then C is very free on X.*

Definition. *A **rational normal curve** of degree m in $\mathbb{P}^n$ is a rational curve such that the $G_0, ..., G_n$ are linearly independent over K; equivalently, they are a basis of $K\left[S, T\right]_m$.*

Fact. Given $n+3$ points in $\mathbb{P}^n_K$, there exists a unique rational normal curve passing through them. This sounds difficult.

Difficulties. Curves for which multiple G_i are equal will almost surely not be free.

Relating Bundles. An element of $\Omega(\varphi)$ is a sextuple $(A_0, ..., A_5)$ such that $A_0G_0 + ... + A_5G_5 = 0$. An element of $E_X(\varphi)$ is a sextuple $(B_0, ..., B_5)$ such that $B_0G_0^4 + ... + B_5G_5^4 = 0$. These are related since taking the fourth power is a ring map in characteristic 2. Thus for $\xi \in \Omega(\varphi)$, $\deg(\xi^4) = 4 \deg \xi$.

Example. *Take $\varphi : R^2 \to R(1)$ given by (S, T). (T, S) is a generator of $\Omega(\varphi)$, so $e_1 = -1$. Similarly, (T^4, S^4) generates $E_X(\varphi)$, so $f_4 = -4$. This suggests that we have just multiplied the splitting type by 4.*

Background. We have looked mainly at $\mathbb{P}^1, \mathbb{P}^n$, and hypersurfaces in $proj^n$. One could also consider intersections of a bunch of hypersurfaces to obtain a general variety. There is a notion of dimension which is roughly n minus the number of equations, counted properly. Nonsingular curves of genus 0 are isomorphic to $\mathbb{P}^1$: conics, lines. Nonsingular curves of genus 1 are elliptic curves, i.e. nonsingular cubics. Curves of genus ≥ 2 are all the rest.

Suppose $K = \mathbb{Q}$ or a number field, X a nonsingular curve over K. If $g = 0$, it can happen that $X(K) = \emptyset$. After at worst a quadratic extension, $X_K \cong \mathbb{P}^1_K$, so $X(K)$ is huge. If $g = 1$, it can happen that $X(K)$ is empty, but after some finite extension of K, we get that $X(K)$ is infinite (no bound on the degree of the necessary extension). For $g \geq 2$, Gerd Faltings proved Mordell's conjecture: $X(K)$ is always finite.

Varieties of dimension n split into $n+2$ classes similarly to the case of curves; the classification is done according to $\kappa \in \{-\infty, 0, 1, ..., n\}$, the Kodaira dimension. The Kodaira dimension of $\mathbb{P}^n$ is always $-\infty$. A very nice subclass of varieties of Kodaira dimension $-\infty$ are the rationally connected (RC) varieties.

Definition. *A variety X over $\mathbb{C}$ is* ***rationally connected*** *if and only if for almost all pairs $(x, y) \in X(\mathbb{C})$, there exists a morphism $\varphi : \mathbb{P}^1 \to X$ with $\varphi(0) = x$ and $\varphi(\infty) = y$. This analogous to the notion of a path-connected space in topology, but in many ways quite different.*

In some ways, this definition is really bad, since it gives no clear way to check this.

Theorem. *Let $K = \mathbb{C}$. X is RC if and only if there exists a very free rational curve on X.*

A line in $\mathbb{P}^2$ is very free. A line on a quadric (in one of the pencils) is free, but not very free. In characteristic p, we still have that the existence of a very free curve implies X is RC, but the converse is false.

Definition. *A morphism $\varphi : \mathbb{P}^1 \to X$ is called* ***very free*** *(resp. free) if and only if $\varphi^* T_X$ is an ample vector bundle (resp. $\varphi^* T_X$ is globally generated).*

Hypersurfaces. Let $X_e \subset \mathbb{P}^n$ be a smooth hypersurface over any algebraically closed field. Then $\kappa(X_e) = -\infty$ if and only if $e \leq n$. If $char(K) = 0$, then these are always rationally connected. If $char(K) = p$, then these are always rationally chain connected (there is a chain of rational curves connecting any pair of points).

"And maybe we get nothing, and that's okay too, because that's your *typical* research experience!" -Johan