Course Notes for Math 737 (Algebraic Geometry)

4. Introduction. Getting Familiar with our Field(s) The fields of rational functions on varieties (affine or projective) are a central focus of much of algebraic geometry. Some basic properties of these fields are investigated and related to the problem of parametrizing a variety. Conics and cubics yield some first examples.

First, a definition. Let k be a fixed field.

Definition: A field extension $k \subset K$ is of **finite type over** k if there are elements $\alpha_1, ..., \alpha_n \in K$ such that every $\alpha \in K$ can be expressed as a rational function in the α_i (with coefficients in k).

Examples: (a) An algebraic extension $k \subset E$ is of finite type if and only if it is a finite extension.

(b) The fields $k(t_1, ..., t_n)$ are of finite type over k by definition.

(c) Any field of rational functions on an affine variety $V \subset \mathbf{A}_k^n$ is of finite type over k. The α_i can be taken to be the images of the x_i in $k(V)$.

Assume that k is an infinite field. Then:

Claim: $k(V)$ is of finite type over k if $V \subset \mathbf{P}_k^n$ is a projective variety.

To prove this, I need to talk about homogenizing and dehomogenizing:

Dehomogenizing: Suppose that $f_0 : \mathbf{A}_k^n \hookrightarrow \mathbf{P}_k^n$ is the map from §1:

$$f_0(a_1, ..., a_n) = (1 : a_1 : ...a_n)$$

and let

$$f_0^* : k[x_0, ..., x_n] \to k[x_1, ..., x_n]$$

be the (non-graded!) homomorphism evaluating $x_0 = 1$. It is immediate that if $I \subset k[x_0, ..., x_n]$ is a homogeneous ideal, then: $f_0^{-1}(V(I)) = V(f_0^*(I))$ so that in particular, if $V(I) = V(J)$, then $V(f_0^*(I)) = V(f_0^*(J))$.

Let's identify $\mathbf{A}_k^n$ with its image, and rewrite the compatibility as:

$$V(I) \cap \mathbf{A}_k^n = V(f_0^*(I))$$

Homogenizing: Suppose that $f \in k[x_1, ..., x_n]$ is a polynomial (usually not homogeneous!) of degree d. Then we homogenize f to get:

$$F(x_0, ..., x_n) := x_0^d \cdot f(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}).$$

We homogenize an **ideal** as follows. Given $I \subset k[x_1, ..., x_n]$, we let:

$$I^h := \langle F \in k[x_0, ..., x_n] \mid F = x_0^d \cdot f(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}) \text{ for some } f \in I \rangle.$$

It is often the case that I^h is not generated by the homogenized generators for I (see the HW). In fact, without the Basis Theorem, it is hard to see why a finitely generated ideal should homogenize to a finitely generated ideal!

Remarks: The two operations are almost inverses. Namely,

(a) If $I \subset k[x_1, ..., x_n]$, then $f_0^*(I^h) = I$ and

(b) If $I \subset k[x_0, ..., x_n]$ is homogeneous, then $(f_0^*(I))^h$ is the ideal generated by all polynomials $F(x_0, ..., x_n)$ with the property that $x_0^e \cdot F \in I$ for some e.

Given an algebraic subset $W = V(I) \subset \mathbf{A}_k^n$, recall from (§3 HW) that $W = V(I(W))$. We get a well-defined enlargement of W to:

$$\overline{W} := V(I(W)^h) \subset \mathbf{P}_k^n$$

which by remark (a) has the property that $\overline{W} \cap \mathbf{A}_k^n = W$. Similarly, by remark (b) and Lemma 3.1, if we are given $V = V(I) \subset \mathbf{P}_k^n$, we have:

$$\overline{(V \cap \mathbf{A}_k^n)} \subseteq V$$

with equality if $F(x_0, ..., x_n) \in I$ whenever $x_0^e \cdot F \in I$ for some power x_0^e.

Now we are ready to prove the claim. Suppose $V \subset \mathbf{P}_k^n$ is a projective variety.

Step 1: There is a basis for k^{n+1} such that $V = \overline{V \cap \mathbf{A}_k^n}$.

Proof: Since V is irreducible, $I(V)$ is prime by Lemma 1.1 and §1 HW. If $V \neq \overline{V \cap \mathbf{A}_k^n}$, then $I(V) \neq I(f_0^* V)^h$, which implies by remark (b) that there is an element $x_0^e F \in I(V)$ such that $F \notin I(V)$. Since $I(V)$ is prime, it follows that $x_0 \in I(V)$. Clearly $x_i \notin I(V)$ for some i, otherwise $V = \emptyset$, so we can reorder the basis for k^{n+1} to get the desired result.

Note: From the proof of Step 1, we see that if V is a projective variety, then either $\overline{V \cap \mathbf{A}_k^n} = V$ or else $x_0 \in I(V)$, in which case $V \cap \mathbf{A}_k^n = \emptyset$!

Step 2: With a choice of basis satisfying Step 1, let $W = V \cap \mathbf{A}_k^n$. Then W is an affine variety and $k(V) \cong k(W)$.

Proof: Suppose that $W = W_1 \cup W_2$. Then for each $i = 1, 2$ we have $I(W) \subseteq I(W_i)$ and it follows that the homogenized ideals must also satisfy $I(W)^h \subseteq I(W_i)^h$ so by Lemma 3.1, we have $\overline{W_i} \subseteq \overline{W} = V$. Thus we get:

$$V = \overline{W}_1 \cup \overline{W}_2 \cup (V \cap V(x_0))$$

and if $W_i \neq W$, then $\overline{W}_i \neq \overline{W}$ so that the irreducibility of W follows from the irreducibility of V.

Next, you check that the map:

$$f : k(V) \to k(W) \text{ defined by } \frac{f}{g} \mapsto \frac{f_0^*(f)}{f_0^*(g)}$$

is well-defined and an isomorphism. (Recall the similar exercise in §1.)

This completes the proof of the claim, because Steps 1 and 2 show that $k(V)$ is isomorphic to $k(W)$, where W is an affine variety. To complete the picture, I would like to argue that **every** field of finite type over k arises as $k(V)$ for some affine or projective variety V. In fact, this is true when k is algebraically closed, by the Hilbert Nullstellensatz, as we will see later.

Here are some specific examples of homogenizing and dehomogenizing:

Examples: (i) If $\Lambda \subset \mathbf{P}_k^n$ is a projective subspace of codimension r, then we saw that Λ is irreducible and $\Lambda = V(L_1, ..., L_r)$. Thus:

$$\Lambda \cap \mathbf{A}_k^n = V(L_1(1, x_1, ..., x_n)) \cap ... \cap V(L_r(1, x_1, ..., x_n))$$

is either empty or is an ordinary linear subpace (not necessarily passing though the origin) in k^n. One fact you should remember from linear algebra is that such a linear subspace is the translation of a vector subpace of k^n of dimension at least $n - r$. Do notice that $x_0 \in \langle L_1, ..., L_r \rangle$ if and only if x_0 is in the linear span of $L_1, ..., L_r$

(ii) $Q = V(xy - zw) \subset \mathbf{P}^3_k$ dehomogenizes to: $V(xy - z) \subset \mathbf{A}^3_k$, the saddle surface. Keeping in mind the previous example, it follows that each projective line on Q is either contained in $V(w)$ or else dehomogenizes to an ordinary line on $V(xy - z)$. Since Q is irreducible, we have $\overline{V(xy - z)} = Q$.

(iii) Plane conics all become projectively equivalent when homogenized:

Circles: $\overline{V(x^2 + y^2 - 1)} = V(x^2 + y^2 - z^2) \subset \mathbf{P}^2_{\mathbf{R}}$.

More generally than circles, we have **ellipses:**

$$\overline{V(a^2(x - r)^2 + b^2(y - s)^2 - c^2)} = V(a^2(x - zr)^2 + b^2(y - zs)^2 - c^2z^2).$$

Parabolas: $\overline{V(y - x^2)} = V(yz - x^2)$.

Hyperbolas: $\overline{V(xy - 1)} = V(xy - z^2)$ or

$$\overline{V(x^2 - y^2 - a)} = V(x^2 - y^2 - az^2).$$

(I leave the most general form for hyperbolas and parabolas to you.)

Given $W \subset \mathbf{A}^n_k$, we know that $\overline{W} - W = V(I(W)^h) \cap V(x_0) \subset \mathbf{P}^n_k$ is a projective algebraic subset, which we can also think of as an algebraic subset of $\mathbf{P}^{n-1}_k = \mathbf{P}^n_k - \mathbf{A}^n_k$. In our examples:

(i) $\Lambda - (\Lambda \cap \mathbf{A}^n_k) = \Lambda'$, a projective subspace of $\mathbf{P}^n_k$ (or $\mathbf{P}^{n-1}_k$) of dimension one less than Λ. (That is, as long as $\Lambda \cap \mathbf{A}^n_k \neq \emptyset$).

(ii) $Q - (Q \cap \mathbf{A}^3_k) = V(xy) \subset \mathbf{P}^2_k$. This is a pair of intersecting lines.

(iii) Circles and ellipses: $\overline{W} - W = V(a^2x^2 + b^2y^2) = \emptyset$.

Parabolas: $\overline{W} - W = V(x^2) \subset \mathbf{P}^1_{\mathbf{R}}$. One point!

Hyperbolas: $\overline{W} - W = V(xy)$ or $V((ax - by)(ax + by))$. Two points!!

Recall from the homework in §2 that there is no qualitative difference among the $\overline{W}$ when W is an ellipse, parabola or hyperbola in $\mathbf{R}^2$. All of them are (projectively) equivalent to the:

$$\textbf{basic projective conic} \quad C := V(xz - y^2) \subset \mathbf{P}^2_k$$

(here $k = \mathbf{R}$). There obviously IS a qualitative difference among the W's, however (for example, the number of connected components is different), which is accounted for by the number of points of $\overline{W} - W$.

Definition: (a) An algebraic subset $C \subset \mathbf{A}_k^2$ is called an **affine plane curve of degree** d if $I(C) = \langle f \rangle$ and $\deg(f(x,y)) = d > 0$.

(b) An algebraic subset $C \subset \mathbf{P}_k^2$ is called a **projective plane curve of degree** d if $I(C) = \langle F \rangle$ and $F \in k[x,y,z]_d$.

Proposition 4.1: (a) If $W \subset \mathbf{A}_k^n$ has the property that $I(W)$ is a principal ideal, then $\overline{W}$ has the same property. In particular, the enlargement of an affine plane curve is a projective plane curve.

(b) If $C \subset \mathbf{A}_k^2$ is an affine plane curve of degree d, then $\overline{C} - C$ consists of at most d points. If k is algebraically closed, then $\overline{C} - C \neq \emptyset$. (Contrast this with the circles and ellipses over $\mathbf{R}$, which is not algebraically closed(!))

Proof: Exercise.

Let's return to the fields, and ask a **very** difficult question:

Question: What are all the fields of finite type over a fixed field k?

In fact, notice that thus far, our only examples are all isomorphic to $k(t_1, ..., t_n)$ for some n. One could obviously take finite algebraic extensions of these, but how do we know that such an extension is not itself isomorphic to some $k(s_1, ..., s_n)$? (And many extensions do have this property!)

Definition: (a) A variety V is **rational** if $k(V) \cong k(t_1, ..., t_n)$.

(b) V is **unirational** if $k(V)$ is isomorphic to a subfield of $k(t_1, ..., t_n)$ for some n (which may or may not be larger than the dimension of V).

Next, we will investigate the fields of rational functions of plane curves of degrees 2 and 3. Ultimately, we will discover a field of finite type which is not unirational! (The problem of finding a field which is unirational but not rational is **much** harder.) First, a related definition:

Definition: A collection $\phi_1, ..., \phi_m \in k(t_1, ..., t_n)$ **parametrizes** a variety $W \subset \mathbf{A}_k^m$ if they determine a "rational" map:

$$\Phi = (\phi_1, ..., \phi_m) : \mathbf{A}_k^n - - > W \subset \mathbf{A}_k^m$$

whose image is dense in W, in the sense that the image of Φ (where it is defined) does not lie in any algebraic subset of $\mathbf{A}_k^m$ properly contained in W.

Assume k is an infinite field and $W \subset \mathbf{A}_k^m$ is an affine variety. Then:

Proposition 4.2: W is unirational iff W can be parametrized.

Proof: Suppose $f : k(W) \hookrightarrow k(t_1, ..., t_n)$ is an injective map of fields. Let $\phi_i = f(\frac{x_i}{1})$ where $\frac{x_i}{1}$ are the images in $k(W)$ of the coordinate functions $x_i \in k[x_1, ..., x_n]$. Then I claim that:

$$\Phi = (\phi_1, ..., \phi_m) : \mathbf{A}_k^n - - > \mathbf{A}_k^m$$

is a parametrization of W. First of all, the image of Φ lies in W because if $f \in I(W)$, then from the identity $f(x_1, ..., x_m) = 0$ in $k[W]$, it follows that $f(\phi_1, ..., \phi_m) = 0$ which means that $f(p) = 0$ for every p in the image of Φ. On the other hand, if $f \notin I(W)$, then $f(\phi_1, ..., \phi_m) \neq 0$, so that (because k is infinite!) there is a $q \in \mathbf{A}_k^n$ such that $f(\phi_1(q), ..., \phi_m(q)) \neq 0$, and it follows that the image of Φ does not land in a smaller algebraic subset.

Conversely, if $\Phi = (\phi_1, ..., \phi_m)$ parametrizes $W \subset \mathbf{A}_k^m$, then consider the map $k[W] \to k(t_1, ..., t_n)$ given by sending $x_i \mapsto \phi_i(t_1, ..., t_n)$. This is well-defined since every $f \in I(W)$ satisfies $f(\phi_1(q), ..., \phi_m(q)) = 0$ for all $q \in \mathbf{A}_k^n$, hence $f(\phi_1, .., \phi_m) = 0$. It determines a well-defined map of **fields** $k(W) \to k(t_1, ..., t_n)$ since **no further** equations are satisfied by the ϕ_i, as the image of Φ does not lie in a proper algebraic subset. But a nonzero map of fields is an injection.

Remark: We'll see later that W is **rational** if and only if W can be parametrized by a map Φ which is "generically injective" in a suitable sense.

Definitions: (a) A plane curve of degree 2 is called a **conic**.
(b) A plane curve of degree 3 is called a **cubic**.

Warning: Not every quadratic equation $f(x, y) = 0$ (or its homogenized $F(x, y, z) = 0$) determines a plane conic, and similarly for degree three equations. Several things can go "wrong" to prevent this.

(i) $V(f)$ may be empty, which often occurs when $k = \mathbf{Q}$. For example:

$$\emptyset = V(2x^2 + y^2 - 5z^2) \subset \mathbf{P}_{\mathbf{Q}}^2 \text{ (why?)}$$

(ii) $V(f)$ may be a single point, for example $V(x^2 + y^2) \subset \mathbf{A}_{\mathbf{R}}^2$.

(iii) $V(f)$ may be a line, for example if $f(x, y) = 3l(x, y)^2$.

However, assume that k is infinite. Then:

Proposition 4.3: If $f(x, y)$ has degree two, is not divisible by the square of a linear polynomial, and if $C = V(f) \subset \mathbf{A}^2_k$ consists of two or more points, then C is an affine conic.

Proof: We can assume, after translating, that C contains the origin $(0, 0) \in \mathbf{A}^2_k$, so that $f(x, y) = ax^2 + bxy + cy^2 + dx + ey$ for some $a, b, c, d, e \in k$. I want to construct a parametrization $\Phi : \mathbf{A}^1_k - - > C$ as follows. For each $t \in \mathbf{A}^1_k$, consider the line through $(0, 0)$ and $(1, t)$. This line ought to meet C in one point other than $(0, 0)$, which we denote by $\Phi(t)$ when it exists.

To see that Φ is given by rational functions in t, we write the **line** through $(0, 0)$ and $(1, t)$ as $\{(s, st) \mid s \in k\}$. Plugging this into $f(x, y)$, we get:

$$s(d + et + s(a + bt + ct^2)) = 0.$$

Suppose first that $d = e = 0$ so that $f(x, y) = ax^2 + bxy + cy^2$. Such an equation always factors as a product of linear forms over $\overline{k}$. If it doesn't factor over k, then $(0, 0)$ is the **unique** point of C. Otherwise, either $f(x, y)$ is divisible by some $l(x, y)^2$ or $f(x, y) = l(x, y)l'(x, y)$ is a product of linearly independent linear polynomials, and it is easy to check that in this case $V(ll') = \langle ll' \rangle$, so that by our definition, this is an affine conic.

Otherwise, we can solve for s, and we get our map Φ as:

$$\Phi(t) = (\phi_1(t), \phi_2(t)) = \left(\frac{-d - et}{a + bt + ct^2}, t\frac{-d - et}{a + bt + ct^2} \right)$$

and the denominators do not vanish identically because $f(x, y)$ is quadratic. Now I want to homogenize this map!

$$\overline{\Phi}(r : t) = (ar^2 + brt + ct^2 : -dr^2 - ert : -drt - et^2)$$

is a map from $\mathbf{P}^1_k$ to $\overline{C}$ which restricts to $\Phi : \mathbf{A}^1_k - - > C \subset \mathbf{A}^2_k$. Exercise: If $f(x, y)$ is not a product of linear polynomials, then $\overline{\Phi}$ is bijective and the "pull-back" map:

$$\overline{\Phi}^* : k[w, x, y]_d \to k[r, t]_{2d};\ w \mapsto ar^2 + brt + ct^2, \text{ etc}$$

is surjective for all d. In this case, it follows from a Hilbert polynomial computation that $I(\overline{C}) = \langle ax^2 + bxy + cy^2 + dwx + ewy \rangle$, hence that the ideal $I(C) = \langle f(x, y) \rangle$ is indeed generated by a quadratic polynomial, as desired!

Two particular parametrizations are of some historical significance:

Example 1: Generating Pythagorean triples.

We define a parametrization $\Phi : \mathbf{A}^1_{\mathbf{Q}} \to C = V(x^2 + y^2 - 1) \subset \mathbf{A}^2_{\mathbf{Q}}$ by:

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

Note that every (Pythagorean) triple of integers x, y, z satisfying $x^2+y^2 = z^2$ comes from a point of C (not uniquely, though) by dividing through by z^2. Thus our map $\Phi(t)$ made up out of rational functions of t generates all the Pythagorean triples!

Example 2: Computing indefinite integrals in closed form.

Let $C = V(y^2-(x^2+ax+b)) \subset \mathbf{A}^2_{\mathbf{R}}$. The existence of the parametrization in Proposition 4.3 has the following consequence. Any integral of the form:

$$\int_0^s f\left(x, \sqrt{x^2+ax+b}\right) dx, \quad f \in \mathbf{R}(x,y)$$

has a "closed-form" solution, in terms of elementary functions of s. The idea is to use Φ to change variables, in which case the integral converts to an integral of a **rational** function of t, which we can do(!) This is significant because if the power x^2 is replaced by x^3 (the infamous elliptic integrals) or higher, then there is, in general, no such closed-form solution!

Onward to cubics!

Observation: Proposition 4.3 just doesn't work for cubics! For example, the Fermat cubic:

$$V(x^3 + y^3 - 1) \subset \mathbf{A}^2_{\mathbf{Q}}$$

has exactly two points, namely $(0,1)$ and $(1,0)$. And there are cubics with more points, for instance:

$$V(y^2 - x(x+81)(x+256)) \subset \mathbf{A}^2_{\mathbf{Q}}$$

consists of 16 points. It turns out that this is the most possible without being infinite, but that is very hard to prove!

So things are less obvious (but more interesting). Let's be more modest:

Proposition 4.4: Suppose $f(x,y) = y^2 - (x+a)(x+b)(x+c)$ for some $a,b,c \in k$ and $C = V(f) \subset \mathbf{A}^2_k$ is infinite. Then $I(C) = \langle f \rangle$ so C is a cubic.

Proof: Suppose $g \in I(C)$. Then we can substitute $(x+a)(x+b)(x+c)$ for each y^2 term in g to get:

$$h(x,y) = h_1(x)y + h_0(x) \in \langle f, g \rangle \subset I(C).$$

If $h = 0$, then $g \in \langle f \rangle$.

If $h_1 = 0$ but $h_0 \neq 0$, then there are only finitely many "x-coordinates" satisfying $h_0(x) = 0$, and plugging into $f(x,y)$, we find only finitely many points in C.

Similarly, if $h_1 \neq 0$, we can solve $y = -\frac{h_0(x)}{h_1(x)}$ and plug this into $f(x,y) = 0$, yielding only finitely many x-coordinates and therefore only finitely many points of C. This finishes the proof.

Here are some cubics which can be parametrized:

Example 1: Cuspidal cubic $C = V(y^2 - x^3)$.

Consider the lines through $(0,0) \in C$ and the point $(1,t)$. You will discover that we get the following parametrization:

$$\phi = (t^2, t^3) : \mathbf{A}^1_k \to C$$

and of course the parametrization shows that there are infinitely many points in C as long as k is infinite, so that C is indeed a cubic.

Example 2: Nodal cubic $C = V(y^2 - x^2(x+1))$.

Again, the lines through $(0,0)$ and $(1,t)$ yield:

$$\phi = (t^2 - 1, t(t^2 - 1)) : \mathbf{A}^1_k \to C$$

and again, the parametrization proves that C is a cubic if k is infinite.

Remark: Both of these examples share a common trait. Namely,

All lines through $(0,0)$ "intersect C at the origin with multiplicity 2"

Later, this will be what we mean when we say C is **singular** at $(0,0)$.

Proposition 4.5: $C = V(y^2 - (x+a)(x+b)(x+c))$ cannot be parametrized provided that a, b, c are distinct.

This depends upon Fermat's method of "infinite descent":

Lemma 4.6: Suppose K is a field and $p(t), q(t) \in K[t]$ are relatively prime polynomials with the property that four distinct linear combinations of them are perfect squares. Then $p(t), q(t) \in K$.

Remark: We consider $ap(t) + bq(t)$ and $a'p(t) + b'q(t)$ to be distinct when $(a : b) \neq (a' : b') \in \mathbf{P}^1_K$.

Proof of the Lemma: First of all, we may as well assume that K is algebraically closed (if $p(t), q(t)$ are relatively prime in $K[t]$, they are also relatively prime in $\overline{K}[t]$... by Euclid's algorithm!).

Once that is done, we can assume (replacing $p(t)$ and $q(t)$ by suitable linear combinations) that the perfect squares are of the form:

$$p(t), q(t), p(t) - q(t), p(t) - \lambda q(t)$$

Thus there are $u(t), v(t) \in K[t]$ such that $u^2(t) = p(t), v^2(t) = q(t)$, and $u^2(t) - v^2(t) = a^2(t)$ and $u^2(t) - \lambda v^2(t) = b^2(t)$. The first two equations force $u(t)$ and $v(t)$ to be relatively prime and the last two tell us that the linear combinations

$$u(t) - v(t), u(t) + v(t), u(t) - \sqrt{\lambda}v(t), u(t) + \sqrt{\lambda}v(t),$$

which are relatively prime, are also all perfect squares. If $p(t), q(t)$ are not constants, then $u(t), v(t)$ would satisfy:

$$0 < \max\{\deg(u(t)), \deg(v(t))\} < \max\{\deg(p(t)), \deg(q(t))\}$$

which eventually (repeating the process with p, q replaced by u, v) produces a contradiction.

Proof of the Proposition: Suppose that we are given polynomials $p, q, r, s \in k[t_1, ..., t_n]$ such that C contains the image of the rational map:

$$\Phi(t) = \left(\frac{p(t_1, ..., t_n)}{q(t_1, ..., t_n)}, \frac{r(t_1, ..., t_n)}{s(t_1, ..., t_n)} \right) : \mathbf{A}^n_k - - > \mathbf{A}^2_k$$

We show that Φ cannot be a parametrization of C.

Let $K = k(t_1, ..., t_{n-1})$ and think of p, q, r, s as elements of the polynomial ring $K[t_n]$. We can assume that p/q and r/s are in lowest terms (by Gauss' lemma) and clear denominators to find that these polyomials must satisfy:

$$r^2q^3 = s^2(p + aq)(p + bq)(p + cq)$$

Since r and s are relatively prime, it follows that $s^2|q^3$ and similarly, $q^3|s^2$ because q shares no factors with $(p + aq), (p + bq)$ or $(p + cq)$. Thus

$$s^2 = \delta q^3 \text{ for some } \delta \in K$$

so that $\delta q = (\frac{s}{q})^2$ is a square in $K[t]$. But then $r^2 = \delta(p+aq)(p+bq)(p+cq)$, which implies that $\alpha(p + aq)$, $\beta(p + bq)$ and $\gamma(p + cq)$ are all squares for some $\alpha, \beta, \gamma \in K$. Thus we can apply Lemma 4.6 to conclude that $p, q \in K$, from which it follows that $r, s \in K$, so the variable t_n is eliminated! We can similarly eliminate all the other variables, leaving us with $p, q, r, s \in k$, i.e. Φ is the constant map, hence in particular, not a parametrization of C.

Corollary 4.7: If $k = \mathbf{R}$ or $\mathbf{C}$, then the field of fractions of:

$$k[x, y]/\langle y^2 - (x + a)(x + b)(x + c)\rangle$$

is not unirational if a, b, c are distinct.

Proof: Observe first that $f(x, y) = y^2 - (x+a)(x+b)(x+c)$ is irreducible by Eisenstein's criterion, so that $\langle f\rangle$ is a prime ideal. Thus $k[x, y]/\langle f\rangle$ is indeed an integral domain, and by (§3 HW), $C = V(f)$ is an affine variety.

Next, observe that it is easy to find infinitely many solutions to $f(x, y) = 0$ (for the indicated fields), hence $I(C) = \langle f\rangle$ by Proposition 4.4.

Finally, Proposition 4.5 tells us that C cannot be parametrized, so that Proposition 4.2 tells us that $k(C)$ is not unirational, as desired.

Remark: If $k = \mathbf{Q}$, or more generally, a number field, then it is a much more interesting problem to try to determine whether or not C has infinitely many points for given a, b, c. (Sometimes it does and sometimes it doesn't!)

Fourth Homework Assignment

1. Let $f(x,y,z) = y - x^2, g(x,y,z) = z - xy$ and $I = \langle f, g\rangle$. Then of course, $C = V(I) = \{(t, t^2, t^3) \in \mathbf{A}_k^3\}$. This is called the **affine** twisted cubic curve.

(a) Let F, G be the homogenizations of f, g and prove that $\langle F, G\rangle \neq I^h$.

(b) Prove that $\overline{C}$ is the twisted cubic curve from §3 HW.

(c) What is $V(F, G) \subset \mathbf{P}_k^3$?

2. (a) Prove Proposition 4.1.

(b) If $W \subset \mathbf{A}_k^n$ is a finite set of points, prove that $W = \overline{W}$. Conclude that $V(f) \subset \mathbf{A}_k^n$ is infinite if k is algebraically closed, $f \notin k$ and $n \geq 2$.

3. Suppose (as in 4.3) that $f(x,y) = ax^2 + bxy + cy^2 + dx + ey$ is not a product of linear polynomials. Let $C = V(f)$. Prove that:

$$\overline{\Phi}(r:t) = (ar^2 + brt + ct^2 : -dr^2 - ert : -drt - et^2)$$

is a bijection from $\mathbf{P}_k^1$ to $\overline{C}$ and that $\overline{\Phi}^* : k[w,x,y]_d \to k[r,t]_{2d}$ is surjective for all d. (Hint: Change basis for $\mathbf{P}_k^1$.) Conclude that $I(C) = \langle f\rangle$.

4. Suppose $F, G \in k[x,y,z]$ are homogeneous of degrees 2 and d respectively over an infinite field k. Prove that if $V(F) \cap F(G)$ is finite, then it consists of at most $2d$ points. (Hint: three cases (i) $V(F)$ finite, (ii) $V(F)$ a union of projective lines, and (iii) $V(F)$ parametrizable as in Proposition 4.3.)

5. Generate all the integral solutions to the following equations:

(a) $x^2 + y^2 = 3$, (b) $x^2 + y^2 - 5$.

6. Calculate the following integral as a function of s (for $s < 1$):

$$\int_0^s \frac{1}{\sqrt{1-x^2}+1}dx$$

7. Find as many points as you can on the "Ramanujan taxicab cubic":

$$V(x^3 + y^3 - 1729) \subseteq \mathbf{A}_{\mathbf{Q}}^2$$

To get started: Ramanujan observed that the number "1729" on the license plate of a taxicab was the first integer that could be expressed as a sum of cubes of integers in two different ways: $1729 = (10)^3 + 9^3$ and $1729 = (12)^3 + 1^3$. That accounts for four points. But there are more!