1.3 06/14/24 - Parametric Curves

Today we'll discuss parametrization of curves, and what you can do with them.

Example 1.3.1. Given a field k and $u, v, w, z \in k$ with not both u, w zero, you can look at the subset given parametrically by

$$C := \{(ut + v, wt + z) : t \in k\} \subset \mathbb{A}^2_k.$$

This is the line C_ℓ defined by the polynomial

$$\ell(x, y) := wx - uy - wv + uz \in k[x, y].$$

Conversely, any line ℓ can be similarly parametrized (this uses that ℓ is not constant!).

Example 1.3.2. For any field k, the parametrization (t, t^2) traces the parabola $y - x^2 = 0$.

Example 1.3.3. Take $k = \mathbb{R}$ and the subset

$$C := \{(t^2, t^2 + 1) : t \in \mathbb{R}\} \subset \mathbb{A}^2_{\mathbb{R}}.$$

This is the ray defined by $y - x - 1 = 0$ and $x \geq 0$. This example shows that a "quadratic" parametrization can give rise to a linear curve, and the image of a parametrization of this sort need not be an entire algebraic curve, even if it is part of one.

One might argue that the above phenomenon occurs only because t^2 cannot be negative in $\mathbb{R}$, i.e. that $\mathbb{R}$ is not algebraically closed. However, as the following example shows, the same thing can happen also over any field.

Example 1.3.4. For any field k, the subset

$$C := \left\{ \left(\frac{t+1}{t+3}, \frac{t-2}{t+5} \right) : t \in k \smallsetminus \{-3, -5\} \right\} \subset \mathbb{A}^2_k$$

traces out the hyperbola defined by

$$f(x, y) = 2xy + 5x - 4y - 3 \in k[x, y],$$

except for the point $(1, 1)$, i.e.

$$C = C_f \smallsetminus \{(1, 1)\}.$$

As we shall see, this is the typical situation–that over an algebraically closed fied k, a rational parametrization of an algebraic curve C can miss at most one point–more on that next time.

Here's one example of a thing we can *do* with parametrizations.

Theorem 1.3.5 (Primitive Pythagorean Triples)**.** If $X, Y, Z \in \mathbb{Z}$ are pairwise coprime positive integers such that $X^2 + Y^2 = Z^2$, then there are coprime integers m, n of different parity such that $m > n > 0$ and either (X, Y, Z) or (Y, X, Z) is $(m^2 - n^2, 2mn, m^2 + n^2)$.

Of course, this result can be used to produce or characterize *all* Pythagorean triples, not just primitive ones (how?).

Proof. Over any field k (of characteristic other than 2 for simplicity), we can parametrize the circle C defined by $x^2+y^2-1 \in k[x,y]$ by projection from the point $(-1,0)$. In other words, for each $t \in k$, we may look at the line through $(-1,0)$ with slope t, which is given by the vanishing of $y-t(x+1)$, and consider its intersection with the circle C. We can now solve the system of equations

$$\begin{aligned} x^2+y^2-1&=0 \\ y-t(x+1)&=0 \end{aligned}$$

by substituting the expression for y from the second line in the first to get

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

One of the roots of this quadratic equation is the expected $x=-1$, and, as long as $1+t^2 \neq 0$, the other root is

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

which yields the point

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

This recipe tells us that, in fact, this is a parametrization of all of C–except the point $(-1,0)$ itself, i.e.

$$\left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) : t \in k, 1+t^2 \neq 0\right\} = C \setminus \{(-1,0)\}.$$

Make sure you understand this! Of course, this is the familiar "half-angle" parametrization of the circle, i.e. we have the trigonometric identities

$$\cos\theta = \frac{1-\tan^2\theta/2}{1+\tan^2\theta/2} \text{ and } \sin\theta = \frac{2\tan\theta/2}{1+\tan^2\theta/2}.$$

See Figure 1.6.

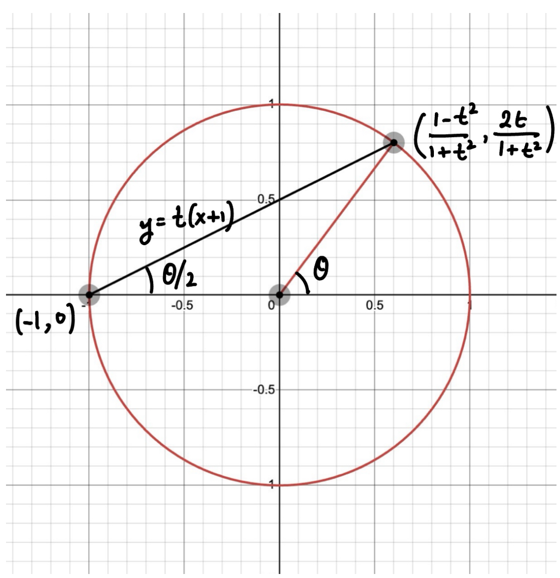

Figure 1.6: Parametrizing the circle $x^2+y^2=1$.

Now, let's specialize to the case $k = \mathbb{Q}$. If X, Y, Z are as in the statement, then the point

$$(x, y) := \left(\frac{X}{Z}, \frac{Y}{Z}\right) \in C(\mathbb{Q}) \smallsetminus \{(-1, 0)\},$$

so there is a $t \in \mathbb{Q}$ such that

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

Then $0 < t < 1$ because $X, Y > 0$. Write $t = m/n$ for some positive coprime integers m, n with $m > n > 0$ to get

$$\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right).$$

If m and n are of opposite parity, then the expression on the right is in lowest terms (check!) and hence we conclude that

$$(X, Y, Z) = (m^2 - n^2, 2mn, m^2 + n^2)$$

as needed. If m and n are both odd, then

$$\gcd(m^2 - n^2, m^2 + n^2) = \gcd(2mn, m^2 + n^2) = 2,$$

from which we conclude that

$$\begin{aligned} 2X &= m^2 - n^2, \\ 2Y &= 2mn, \\ 2Z &= m^2 + n^2. \end{aligned}$$

In this case, we can take

$$m' := \frac{m+n}{2} \text{ and } n' := \frac{m-n}{2},$$

which are again coprime, of different parity (check!), such that $m' > n' > 0$ and

$$(Y, X, Z) = \left((m')^2 - (n')^2, 2m'n', (m')^2 + (n')^2\right).$$

■

Let's now do some parametrizations of higher degree curves.

Example 1.3.6 (Cuspidal Cubic)**.** For any field k, consider the set

$$C := \{(t^2, t^3) : t \in k\} \subset \mathbb{A}_k^2.$$

If we let

$$f(x, y) := y^2 - x^3 \in k[x, y],$$

then it is clear that

$$C \subset C_f.$$

To go the other direction, suppose we have a point $(p, q) \in C_f$. If $p = 0$, then $q = 0$ as well, and then $(p, q) = (t^2, t^3)$ for $t = 0$. Else, if $p \neq 0$, then it is easy to see (check!) that $(p, q) = (t^2, t^3)$ for $t := q/p$. This tells us that

$$C = C_f.$$

Again, what we are doing geometrically is that we are parametrizing points of the cuspidal cubic by the slope of the line joining the point to the cusp.

Example 1.3.7 (Nodal Cubic)**.** For any field k, consider the curve C_f defined by the vanishing of

$$f(x,y) = y^2 - x^3 - x^2 \in k[x,y].$$

This is a nodal cubic with a node at $(0,0)$. For any $t \in k$, consider the line of slope t through the node, which has the equation $y - tx = 0$. We may now solve the system of equations

$$\begin{aligned} y^2 - x^3 - x^2 &= 0 \\ y - tx &= 0 \end{aligned}$$

as before by subsituting the second line into the first to get

$$0 = t^2x^2 - x^3 - x^2 = x^2(-x + t^2 - 1).$$

This is a cubic equation with a "double root" at $x = 0$; this captures the fact that the point $(0,0)$ is a node (how?). The third root is then the unique point of intersection of this line with the curve C_f other than the origin, and has x-coordinate $x = t^2 - 1$ and hence coordinates

$$(x,y) = (t^2 - 1, t^3 - t^2).$$

This is easily seen to be (check!) a parametrization of C_f, i.e.

$$C_f = \{(t^2 - 1, t^3 - t^2) : t \in k\}.$$

The above examples lead us to ask the following natural questions:

Question 1.3.8. Does every curve $C \subset \mathbb{A}^2_k$ admit a rational parametrization? In other words, given any curve $C \subset \mathbb{A}^2_k$, are there rational functions $u(t), v(t) \in k(t)$ such that

$$C = \{(u(t), v(t)) : t \in k \smallsetminus S\},$$

where $S \subset k$ is the finite set of poles of $u(t)$ and $v(t)$?

Question 1.3.9. Is every subset of $\mathbb{A}^2_k$ given parametrically by rational functions an algebraic curve? In other words, given any $u(t), v(t) \in k(t)$ and S as before, can we always find an $f(x,y) \in k[x,y]$ such that

$$\{(u(t), v(t)) : t \in k \smallsetminus S\} = C_f?$$

The answer to Question 1.3.8 is "yes" if C is a line (Example 1.3.1), "almost yes" if C is a conic, and "no, in general" if C has higher degree. Here's what the "almost yes" means: it means that if C is a conic and $C(k) \neq \emptyset$, then given any point $P \in C(k)$, there is a parametrization of $C(k) \smallsetminus P$ (by projection from the point P to any line not containing P, as in the proof of Theorem 1.3.5), and in some cases we may have a complete parametrization of $C(k)$ as well[6], as in Example 1.3.2. For curves of higher degree, the situation is drastically different: *most* curves of higher degree (in some sense of the word) do not admit rational parametrizations. However, proving this is beyond our tools at the moment. The simplest example of a curve that does *not* admit a rational parametrization is probably given by taking

$$f(x,y) := y^2 - x^3 + x \in k[x,y]$$

[6]This happens precisely when $\overline{C} \smallsetminus C$ contains a k-rational point, where $\overline{C} \subset \mathbb{P}^2_k$ is the projective closure of C. If you don't know what this means, you can ignore it now.

when $\operatorname{ch} k \neq 2$. In Exercise 2.2.1, you will be guided through a proof of this result, at least when $\operatorname{ch} k = 0$.

The answer to Question 1.3.9 is also "no", at least the way it is currently stated, as Examples 1.3.3 and 1.3.4 illustrate. However, the claim actually admits a very nice salvage; as it turns out, we can always find an f such that $C \subset C_f$, and at least when k is algebraically closed (a notion to be discussed soon), either C is all of C_f or all of C_f except perhaps one point. We will not prove this general statement here, although see Remark 1.3.11.

Given u and v, finding such an f as in Question 1.3.9 amounts to "eliminating" t from the system of equations

$$\begin{aligned} u(t) - x &= 0 \\ v(t) - y &= 0. \end{aligned}$$

This is the beginning of a vast subject called elimination theory; we won't get into the general theory here, and only discuss specific examples. Let's start with one.

Example 1.3.10 (Student Example)**.** For any field k, consider the curve given parametrically as

$$C = \{(t^3 - 2t^2 + 7, t^2 + 1) : t \in k\} \subset \mathbb{A}^2_k.$$

To produce such an f, perform Euclid's algorithm on the polynomials

$$\begin{aligned} A &= t^3 - 2t^2 + 7 - x \\ B &= t^2 + 1 - y \end{aligned}$$

in the polynomial ring $K[t]$ where $K = k(x, y)$ is the field of rational functions in two variables x and y. The algorithm runs to give us

$$\begin{aligned} A &= Bq_1 + r_1, \\ B &= r_1 q_2 + r_2, \text{ and} \\ r_1 &= r_2 q_3, \end{aligned}$$

where

$$\begin{aligned} q_1 &= t - 2, & r_1 &= (y-1)t - (x + 2y - 9), \\ q_2 &= \frac{1}{y-1}t + \frac{x + 2y - 9}{(y-1)^2}, & r_2 &= \frac{(x + 2y - 9)^2 - (y-1)^3}{(y-1)^2}, \end{aligned}$$

and $q_3 = r_1 r_2^{-1}$. We claim that taking

$$f(x, y) = (x + 2y - 9)^2 - (y - 1)^3 \in k[x, y]$$

suffices in the sense that at least $C \subset C_f$. To see this, use backward substitution in Euclid's algorithm to obtain the polynomial identity

$$f = P \cdot A + Q \cdot B \in k[x, y, t]$$

where

$$\begin{aligned} P &= -(y-1)t - (x + 2y - 9), t \text{ and} \\ Q &= (y-1)t^2 + (x-7)t + y^2 - 2x - 6y + 19. \end{aligned}$$

This identity tells us that if for some $x, y, t \in k$ we have $(x, y) = (t^3 - 2t^2 + 7, t^2 + 1)$, then $A = B = 0$ and hence $f(x, y) = 0$, proving that $C \subset C_f$. Note that

$$f(x,y) = \det \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ -2 & 1 & 0 & 1 & 0 \\ 0 & -2 & 1-y & 0 & 1 \\ 7-x & 0 & 0 & 1-y & 0 \\ 0 & 7-x & 0 & 0 & 1-y \end{bmatrix}.$$

(Where on earth did this matrix come from?) In this case, we have in fact that $C = C_f$ when k is algebraically closed; you are invited to solve the mystery of this matrix and show this last result in Exercise 2.2.4. Get Desmos to plot the curve C of Example 1.3.10 over $k = \mathbb{R}$. Geometrically, we are taking the intersection of the surfaces in (x, y, t) space defined by the vanishing of A and B and projecting the resulting curve to the (x, y)-plane–can you get Desmos 3D to illustrate this?

Here's a slightly more advanced explanation that I do not expect you to fully understand right now; I include it for the sake of completeness and for when you revisit this topic later.

Remark 1.3.11. Suppose we are given a parametrization of the form

$$C = \{(u(t), v(t)) : t \in k \smallsetminus S\}$$

for some rational functions $u(t), v(t) \in k(t)$ and finite set S of all poles of $u(t)$ and $v(t)$; for the sake of nontriviality, we'll assume that $S \subsetneq k$. Write

$$u(t) = \frac{p(t)}{q(t)} \text{ and } v(t) = \frac{r(t)}{s(t)}$$

for some $p, q, r, s \in k[t]$ with $qs \neq 0$ and $(p, q) = (r, s) = (1)$. Consider the elements

$$A := p - xq \text{ and } B := r - ys$$

of $k[x, y, t] \subset K[t]$ where $K = k(x, y)$. Now consider the ideal $(A, B) \subset K[t]$. Since $K[t]$ is a Euclidean domain and hence a PID, either $(A, B) = (q)$ for some $q \in K[t]$ of positive degree, or $(A, B) = (1)$. In fact, the former case cannot happen, although we don't quite yet have the tools to prove this.[7] It follows that the Euclidean algorithm can be used as above to produce $P, Q \in k[x, y, t]$ and nonzero[8] $f \in k[x, y]$ such that

$$f = P \cdot A + Q \cdot B \in k[x, y, t]. \tag{1.1}$$

The polynomial f then cannot be constant: if it were a nonzero constant c, then we could take any value of $t \in k \smallsetminus S$ and substitute $x = u(t), y = v(t)$ in (1.1) to produce the contradiction $c = 0$. It follows as before that

$$C \subset C_f.$$

[7]Here's a proof: if A and B had a common factor $q \in K[t]$ of positive degree, then there would be an $\alpha \in \overline{K} = \overline{k(x,y)}$ such that $p(\alpha) - xq(\alpha) = r(\alpha) - ys(\alpha) = 0$. Now, we claim that $q(\alpha) \neq 0$. Indeed, if $q(\alpha) = 0$, then $p(\alpha) = 0$ as well, but already there are $m, n \in k[t]$ such that $mp + nq = 1$, so plugging in $t = \alpha$ would give $0 = 1$, which is false. Similarly, $s(\alpha) \neq 0$. Therefore, in $K(\alpha)$, we have

$$x = \frac{p(\alpha)}{q(\alpha)} \text{ and } y = \frac{r(\alpha)}{s(\alpha)}.$$

Therefore, $k(\alpha) \supset k(x, y)$ is a finite algebraic extension, but that cannot happen because the transcendence degree of $k(x, y)$ over k is 2. Alternatively, more "elementary" proofs can be given using the theory of Gröbner bases.

[8]This uses that $(A, B) = (1)$ in $K[t]$.

In fact, if f is chosen to be of minimal degree such that an equation like (1.1) holds (e.g. such as when f is coprime to P and Q–which we always do by cancelling common factors), then this f is none other than the resultant of A and B with respect to t, i.e. $f = \mathrm{Res}_t(A, B)$.

Finally, it is not always true that $C_f \subset C$, although if k is algebraically closed then C is either all of C_f or C_f minus at most one point; we certainly don't have the tools to prove this (at least at this level of generality) either.[9]

[9] Here's a proof: the rational parametrization amounts to a morphism

$$\varphi : \mathbb{A}^1_k \smallsetminus S \to C_f$$

which extends by smoothness of $\mathbb{P}^1_k$ to a morphism

$$\varphi : \mathbb{P}^1_k \to \overline{C}_f \subset \mathbb{P}^2_k,$$

where $\overline{C}_f$ is the projective closure of $\mathbb{P}^2_k$. Since, by assumption, φ is not constant, it follows from the general theory of curves that this morphism is surjective on k-points. Note that any point in S must map to $\overline{C}_f \smallsetminus C_f$ by the hypothesis that S is the set of poles of $u(t)$ and $v(t)$. If we let ∞ denote the unique k-point of $\mathbb{P}^1_k \smallsetminus \mathbb{A}^1_k$, then we have two cases: either $\varphi(\infty) \in \overline{C}_f \smallsetminus C_f$, in which case it follows that $\varphi : \mathbb{A}^1_k \smallsetminus S \to C_f$ is surjective on k-points, or $\varphi(\infty) \in C_f$, in which case $\varphi : \mathbb{A}^1_k \smallsetminus S \to C_f$ is surjective onto $C_f(k) \smallsetminus \{\varphi(\infty)\}$.