Given an algebraic plane curve $f(x, y) = 0$, we’ve been looking at the problem of finding a rational parametrization $(x(t), y(t))$ for it, where $x(t)$ and $y(t)$ are rational functions of $t$. In several examples (and in a couple of general cases) we’ve been able to show that curves are rational and exhibit rational parametrizations.

It’s natural to ask the reverse question as well: given a parametric rational curve $(x(t), y(t))$, can we find a polynomial $f(x, y) \in \mathbb{R}[x, y]$ so that $f(x(t), y(t)) = 0$? (One of the homework problems asks you to do this for a non-rational parametrization of the cardioid.)

**Proposition.** Given rational functions $x(t)$ and $y(t)$, there exists a polynomial $f(x, y) \in \mathbb{R}[x, y]$ such that $f(x(t), y(t)) \equiv 0$.

**Proof.** We can write the given rational functions as $x(t) = \frac{a(t)}{q(t)}$ and $y(t) = \frac{b(t)}{q(t)}$ for some polynomials $a(t), b(t), q(t) \in \mathbb{R}[t]$. For some large degree $N$, we’ll try to find a polynomial $f(x, y) \in \mathbb{R}[x, y]$ of degree $N$ so that $f(x(t), y(t)) \equiv 0$, or equivalently so that

$$q(t)^N(f(x(t), y(t))) \equiv 0.$$

Let $n = \deg q(t)$ and $m = \max\{\deg a(t), \deg b(t)\}$. Then $q(t)^N f(x(t), y(t))$ is a polynomial in $t$ of degree at most $Nn + Nm$, whose coefficients are homogeneous linear functions of the coefficients of $f$. Thus setting all of its coefficients equal to zero give at most $Nn + Nm + 1$ homogeneous linear equations for the coefficients of $f$, and if we can pick $N$ so that there are at least as many variables as there are equations (i.e. $f$ has at least $Nn + Nm + 1$ coefficients), then we can solve the system and find an $f$ with $q(t)^N f(x(t), y(t)) \equiv 0$, and we’ll be done.

The degree $k$ part of $f$ is

$$f_k(x, y) = c_{k,0}x^k + c_{k-1,1}x^{k-1}y + \cdots + c_{0,k}y^k,$$

which has $k + 1$ coefficients. Overall then, $f$ has $1 + 2 + \cdots + (N + 1) = \frac{N(N+1)}{2}$ coefficients, and since this is quadratic in $N$ and $Nn + Nm + 1$ is linear, for sufficiently large $N$ we have $\frac{N(N+1)}{2} \geq Nn + Nm + 1$ as desired. □

While this proves that it is always possible to find a polynomial vanishing on a rationally parametrized curve, there are a few things that we might not like so much about it. For one thing, $N$ may be bigger than it has to be; for example, in the parametrization $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ for the circle, the proof would use the value $N = 8$ to find a degree $\leq 8$ polynomial $f(x, y)$ vanishing on the circle, i.e. the solutions to the system would be the $f(x, y) = (x^2 + y^2 - 1)g(x, y)$ for arbitrary polynomials $g(x, y)$ of degree $\leq 6$. This isn’t really a big problem though, since we could always try to solve the systems for lower degrees first.

The bigger complaint we might have is that even for small degree examples, this involves solving a big system of linear equations in a big number of variables. Of course, computers are pretty good at solving systems of linear equations, but this certainly isn’t something we’d want to do by
hand, and even computer algebra systems might have some trouble dealing with huge numbers of
variables.
In fact, there is a nicer way to do the computation, and it involves thinking about the problem
more geometrically. We can think of the graph of the rational function \((x(t), y(t)) = \left( \frac{a(t)}{p(t)}, \frac{b(t)}{q(t)} \right)\) in
\(\mathbb{R}^3 = \mathbb{R}^2 \times \mathbb{R}\) as being the common zeros of the two polynomials
\[ g(x, y, t) = a(t) - xp(t) \quad \text{and} \quad h(x, y, t) = b(t) - yq(t) \]
in \(\mathbb{R}[x, y, t]\). Our goal then is to find a polynomial \(f(x, y)\) in only the variables \(x\) and \(y\) so that
whenever \(g(x_0, y_0, t) = h(x_0, y_0, t) = 0\) for some value of \(t\), we have \(f(x_0, y_0) = 0\). If we could write
some polynomial \(f(x, y) \in \mathbb{R}[x, y]\) in the form
\[ f(x, y) = a(x, y, t)f(x, y, t) + b(x, y, t)g(x, y, t), \]
for polynomials \(a(x, y, t), b(x, y, t) \in \mathbb{R}[x, y, t]\), then \(f(x, y)\) would certainly have this property, and
thus be a polynomial vanishing on the parametrized curve. For example,
\[ x^2 + y^2 - 1 = \left( \frac{1}{2}txy + \frac{1}{2}ty - x + \frac{1}{2}y^2 - 1 \right) \left( 1 - t^2 - (1 + t^2)x \right) \]
\[ - \left( \frac{1}{2}tx^2 + tx + \frac{1}{2}t + \frac{1}{2}xy + \frac{1}{2}y \right) \left( 2t - (1 + t^2)y \right). \]

Over the next few weeks, we’ll start learning about a computational tool called Gröbner bases
that will tell us how to find such an \(f\), and will more generally allow us to study the question of,
given polynomials \(h_1, \ldots, h_k \in \mathbb{R}[x_1, \ldots, x_n]\), which polynomials \(f \in \mathbb{R}[x_1, \ldots, x_n]\) can be written
in the form
\[ f = q_1h_1 + \cdots q_kh_k \]
for some \(q_1, \ldots, q_k \in \mathbb{R}[x, \ldots, x_n]\)?

We’ll begin with some terminology. If \(f_1, \ldots, f_k \in \mathbb{R}[x_1, \ldots, x_n]\) are polynomials then the ideal
generated by \(f_1, \ldots, f_k\) is the set
\[ \langle f_1, \ldots, f_k \rangle = \{ q_1f_1 + \cdots + q_kf_k : q_1, \ldots, q_k \in \mathbb{R}[x_1, \ldots, x_n] \}. \]
More generally, a subset \(I \subseteq \mathbb{R}[x_1, \ldots, x_n]\) is defined to be an ideal if \(g(x_1, \ldots, x_n)f(x_1, \ldots, x_n) \in I\)
for every \(f(x_1, \ldots, x_n) \in I\) and \(g(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]\).

**Theorem** (Hilbert Basis Theorem). Every ideal \(I \subseteq \mathbb{R}[x_1, \ldots, x_n]\) is generated by finitely many
polynomials, so that
\[ I = \langle f_1, \ldots, f_k \rangle \]
for some \(f_1, \ldots, f_k \in I\).

We probably won’t prove this. We should note that this theorem doesn’t say anything about
the size of the smallest generating set of \(I\), so \(k\) here could be much bigger than \(n\).

When dealing with polynomials in one variable, a polynomial always has a clear leading term,
namely the term of highest degree. For polynomials in several variables, there are many different
ways we might want to order the monomials. For convenience, if \(\alpha = (a_1, \ldots, a_n)\) is an \(n\)-tuple of
non-negative integers, then we will write
\[ x^\alpha = x_1^{a_1}x_2^{a_2} \cdots x_n^{a_n} \]
as an abbreviated notation for the corresponding monomial. Although there are many orderings on the monomials to choose from, we want them to respect the algebraic structure. For example if \( x^\alpha \) divides \( x^\beta \), then we would like \( x^\alpha \) to be smaller than \( x^\beta \).

A monomial order for \( R[x_1, \ldots, x_n] \) is a total order\(^1\) on the monomials such that if \( x^\alpha < x^\beta \) then \( x^\gamma x^\alpha < x^\gamma x^\beta \) for all monomials \( x^\gamma \) which is a well-ordering\(^2\).

**Example: Lexicographic order**

Probably the simplest monomial ordering is the lexicographic (or “dictionary”) ordering. In this ordering, the power of the first variable is used to determine the order, with powers of the second variable only looked at when the first variable appears to the same power in two monomials. Similarly, we only look at the third variable when the first two are tied, and so on. For example, in the lex order for \( R[x, y, z] \) with \( x > y > z \), we have

\[
x^4 > x^3y^2z > x^3yz^2 > x^2y^3z > xy^2z^2 > xy > xz^2 > x > y^6 > y^5z^3 > yz^6 > y > z^3 > 1.
\]

More formally, given two monomials \( x^\alpha \) and \( x^\beta \) in \( R[x_1, \ldots, x_n] \), we say that \( x^\alpha >_{\text{lex}} x^\beta \) if in the difference of vectors \( \alpha - \beta \), the leftmost non-zero entry is positive. One can check that this does in fact define a monomial order.\(^3\)

**Example: Graded lexicographic order**

One thing we might not like about lex order is that it doesn’t respect degrees (e.g. \( xy > y^3z^4 \)). We can define a new order, called graded lexicographic order by saying that higher degree monomials are bigger and using lex order to break ties. For example,

\[
x^7 > z^7 > x^2y^2z^2 > x^2yz^3 > xy^5 > y^3z^3 > yz^5 > x^5 > x^4y > x^3y^2 > x^3yz > x^3z^2.
\]

More formally, we say that \( x^\alpha >_{\text{grlex}} x^\beta \) if \( \deg x^\alpha > \deg x^\beta \) or if \( \deg x^\alpha = \deg x^\beta \) and \( x^\alpha >_{\text{lex}} x^\beta \). Since the partial ordering by degree and the lexicographic ordering both have the property that

\[
x^\alpha < x^\beta \implies x^\gamma x^\alpha < x^\gamma x^\beta \quad \text{for all monomials } x^\gamma,
\]

the graded lexicographic order has this property as well. Since any graded order (an order in which degree is used first and then something else is used as a tie-breaker) satisfies well-ordering automatically (because there are only finitely many monomials of each degree), we see that grlex is a term order.

---

\(^1\)This means that: (1) it is never the case that both \( x^\alpha < x^\beta \) and \( x^\beta < x^\alpha \), and (2) if \( x^\alpha < x^\beta \) and \( x^\beta < x^\gamma \), then \( x^\alpha < x^\gamma \).

\(^2\)Well-ordering means that if \( S \) is any subset of monomials, then \( S \) has a least element according to the ordering. This implies that 1 is the least monomial, since if \( x^\alpha < 1 \) were the least monomial, then \( x^{2\alpha} < x^\alpha \) would be even smaller, a contradiction.

\(^3\)See section 2.2 of Cox, Little, and O’Shea for more details about term orderings, including proofs that the well-ordering property holds, etc.
Example: Graded reverse lexicographic order

Perhaps one of the most frequently used term orders in practice (because it tends to result in faster computations) is graded reverse lexicographic or grevlex order. This one is perhaps a little more confusing. As the name suggests, graded reverse lexicographic order uses degree first, and uses “reverse lexicographic order” to break ties.

If we reverse the lexicographic order however, so that \( x^\alpha >_{\text{revlex}} x^\beta \) if \( x^\alpha <_{\text{lex}} x^\beta \), the result isn’t a monomial ordering. It fails well-ordering, because there are infinite descending sequences, e.g. in revlex order we have

\[ 1 >_{\text{revlex}} z >_{\text{revlex}} z^2 >_{\text{revlex}} z^3 >_{\text{revlex}} \cdots >_{\text{revlex}} yz >_{\text{revlex}} y^2 >_{\text{revlex}} y^3 >_{\text{revlex}} \cdots. \]

However, the reverse of an order preserved under multiplication by \( x^\gamma \) is at least still preserved under multiplication by \( x^\gamma \), so while reverse lexicographic order isn’t a monomial order by itself, we can still use it to break ties in a graded order (for which well-ordering is automatic).

There’s one final issue to defining grevlex: when we reverse the lex order, it reverses the order of the variables, but we still want to get an order with \( x_1 > x_2 > \cdots > x_n \) in the end. Thus we start with a lex order with \( x_n > \cdots > x_1 \), so that when we reverse it we get a reverse lexicographic order with \( x_1 >_{\text{revlex}} x_2 >_{\text{revlex}} \cdots >_{\text{revlex}} x_n \). We then say that \( x^\alpha >_{\text{grevlex}} x^\beta \) if \( \deg x^\alpha > \deg x^\beta \) or if \( \deg x^\alpha = \deg x^\beta \) and \( x^\alpha >_{\text{revlex}} x^\beta \).

For example, in the graded reverse lexicographic order on \( \mathbb{R}[x, y, z] \) with \( x > y > z \), we have

\[ y^2 z^2 > x^3 > xy^2 > xyz > y^2 z > xz^2 > x^2 > xy > y^2 > xz > yz > z^2 > x. \]

Basically, we order by degree first, and break ties by saying a monomial is bigger if it has a smaller power of the least significant variable. More formally, we say that \( x^\alpha > x^\beta \) if \( \deg x^\alpha > \deg x^\beta \) or if \( \deg x^\alpha = \deg x^\beta \) and in the vector difference \( \alpha - \beta \), the rightmost non-zero entry is negative.