

Notes on Factoring Polynomials in Two Variables

Zachary Miner

November 7, 2006

Let F be a field and consider $Q(x, y) \in F[x, y] \setminus F$. Our task is to factor $Q(x, y)$ into a product of irreducible polynomials.

Remark.

1. $F[x, y]$ is a UFD.
2. $Q(x, y)$ may be irreducible over F but may factor over some extension field L/F .

Factoring a Polynomial in Two Variables

Step 0. Write $Q(x, y) = \sum q_j(x)y^j$, compute the gcd of the $q_j(x)$, and factor it out. WLOG $\gcd(q_j(x))=1$. So, $\text{content}(Q) = 1$ as a polynomial in y with coefficients in $F[x]$.

Step 1. Regard Q as a polynomial in y with coefficients in $F(x)$. Take $\gcd(Q, \frac{\partial Q}{\partial y})$ to remove multiple factors.

Combining the previous two steps we can assume that Q has no factors in $F[x]$, and is square-free.

Step 2. Find $(x_0, y_0) \in \overline{F}^2$ with

$$(*) \quad Q(x_0, y_0) = 0 \text{ and } \frac{\partial Q}{\partial y}(x_0, y_0) \neq 0.$$

The purpose of this is to find a point on the plane curve $Q = 0$ which is non-singular and such that the tangent line at this point is not vertical. This will allow us to write y as a power series in x . Now we justify the existence of such a point before moving on to finding the power series.

Only finitely many points will satisfy the first equation in $(*)$ and not the second. First, compute $\text{Res}_y(Q, \frac{\partial Q}{\partial y}) = r(x) \neq 0$ (by step 1). We want x_0 such that $r(x_0) \neq 0$. (This x_0 may not be in F , but this is why we have

dealt with \overline{F} .) Once we have found x_0 , we can solve for $y_0 \in \overline{F}$. One of them will satisfy (*).

WLOG assume $x_0, y_0 \in F$, by extending F if necessary.

Step 3. Expand y as a power series: $y = y_0 + y_1(x - x_0) + y_2(x - x_0)^2 + \dots$. Now we use a recursive algorithm to compute y_i , $i > 0$. (You may have seen this as Newton's algorithm or Hensel's lemma). Suppose y_0, \dots, y_n are known to satisfy

$$Q(x, y_0 + y_1(x - x_0) + \dots + y_n(x - x_0)^n) \equiv 0 \pmod{(x - x_0)^{n+1}}.$$

When $n = 0$,

$$Q(x, y_0) \equiv Q(x_0, y_0) \equiv 0 \pmod{(x - x_0)}.$$

Now, for ease of notation, let $z = y_0 + y_1(x - x_0) + \dots + y_n(x - x_0)^n$. Then, for some $b \in F$, the induction hypothesis gives

$$Q(x, z) \equiv b(x - x_0)^{n+1} \pmod{(x - x_0)^{n+2}}.$$

To find y_{n+1} , let $h = y_{n+1}(x - x_0)^{n+1}$ and compute

$$\begin{aligned} Q(x, z + h) &= \left(Q(x, z) + \frac{\partial Q}{\partial y}(x, z) \cdot h \right) \pmod{(x - x_0)^{n+2}} \\ &= \left(b(x - x_0)^{n+1} + \frac{\partial Q}{\partial y}(x, z) \cdot h \right) \pmod{(x - x_0)^{n+2}} \\ &= \left(b(x - x_0)^{n+1} + \frac{\partial Q}{\partial y}(x, z) \cdot y_{n+1}(x - x_0)^{n+1} \right) \pmod{(x - x_0)^{n+2}} \\ &= \left(\left(b + \frac{\partial Q}{\partial y}(x_0, y_0) \cdot y_{n+1} \right) (x - x_0)^{n+1} \right) \pmod{(x - x_0)^{n+2}} \end{aligned}$$

So, $y_{n+1} = \frac{-b}{\frac{\partial Q}{\partial y}(x_0, y_0)}$ does the trick. We now have our power series expansion of y in terms of x . Use this method to compute y_n for $n \leq (\deg Q)^2$.

Step 4. For $m = 1, 2, \dots, \deg Q$; try to find $P(x, y) \in F[x, y]$ of degree m , starting with $m = 1$, with

$$P(x, y_0 + y_1(x - x_0) + \dots + y_n(x - x_0)^n) \equiv 0 \pmod{(x - x_0)^{n+1}}.$$

Stop if you find P , else go to next value of m . This is a system of linear equations in the coefficients of P . So find the nullspace. If it is zero, go to the next step.

Claim. The P of minimal degree m found in Step 4 is an irreducible factor of Q .

Assuming the claim, then $P \mid Q$, so if $Q \neq P$, we replace Q with Q/P and repeat steps 2-4.

Why is the claim true? The point (x_0, y_0) about which the power series expansion of y was given is on the plane curve $Q = 0$ and also on $P = 0$. The conditions on P and Q ensure that the intersection multiplicity of $P = 0$ and $Q = 0$ at (x_0, y_0) is at least $(\deg Q)^2 + 1 > \deg P \deg Q$. Bezout's theorem then implies that $P \mid Q$.

Example. Let us illustrate with an easy example. Let $Q(x, y) = x^2 - y^2$. Then $(1, 1) = (x_0, y_0)$ is a point on the curve $Q = 0$. And $\frac{\partial Q}{\partial y}(1, 1) = -2$.

Expanding y in a power series: $y = 1 + y_1(x - 1) + \dots$. We have

$$\begin{aligned} x^2 - (1 + y_1(x - 1) + \dots)^2 &\equiv x^2 - 1 - 2y(x - 1) \pmod{(x - 1)^2} \\ &\equiv (x - 1)(x + 1 + 2y) \pmod{(x - 1)^2}. \end{aligned}$$

So, $1 - 2y_1 = -1$, giving $y_1 = 1$.

Then, $y = 1 + (x - 1) + \dots$. Now, find P of degree 1 satisfying

$$P(x, 1 + (x - 1) + \dots) \equiv 0 \pmod{(x - 1)^2}.$$

Say, $P(x, y) = y - x$, so $P \mid Q$.

A few weeks ago, we talked about how to factor in $\mathbb{Z}[x]$. So, $Q(Y) \in \mathbb{Z}[Y]$. The analogy here is between \mathbb{Z} and $\mathbb{F}[x]$. Find a prime p and a y_0 such that

$$\begin{aligned} Q(y_0) &\equiv 0 \pmod{p} \\ Q'(y_0) &\not\equiv 0 \pmod{p}. \end{aligned}$$

This is the same as finding (x_0, y_0) . Now, use Hensel's lemma: find $y \in \mathbb{Z}/p^n$ with $Q(y) \equiv 0 \pmod{p^n}$, for n large in relation to the coefficients of Q . Step 3 is to find the power series expansion of y :

$$y = y_0 + y_1p + y_2p^2 + \dots + y_np^n$$

Now find $P(Y) \in \mathbb{Z}[Y]$ of small degree and with small coefficients such that $P(y) \equiv 0 \pmod{p^n}$. (This can no longer be done with linear algebra.) This congruence defines a lattice in $\mathbb{Z}^{\deg P + 1}$. To find a short vector in a lattice, there is an algorithm called the LLL-algorithm which we won't explain. Then a height calculation will replace Bezout to prove that $P \mid Q$.