Math 75 notes, Lecture 22

P. Pollack and C. Pomerance

The formal derivative of a polynomial

While the derivative is a familiar concept from calculus, what might the derivative of a polynomial $f \in F[x]$ mean when F is a field not contained in the complex numbers? In particular, if $f(x) = \sum_{i=0}^{d} a_i x^i$, we can try to write down the "derivative" $\sum_{i=1}^{d} i a_i x^{i-1}$, but does this expression even make sense? That is, if $a \in F$ and $i \in \mathbb{N}$ (here $\mathbb{N}$ is the set of positive integers), does it make sense to form the product ia? Actually it does, and we have discussed this. It makes sense if we think of it not as a product but as repeated addition, where we have i copies of the field element a added together.

For $f(x) = \sum_{i=0}^{d} a_i x^i \in F[x]$, let us define

$$D(f(x)) = \sum_{i=1}^{d} i a_i x^{i-1}.$$

Thus, $D(f)$ is another polynomial in $F[x]$. Good, we have a definition, but why bother? In calculus, we actually did not define the derivative this way, but in terms of a limit, and we proved the above identity for the derivative of a polynomial as a consequence. Now, when dealing with an arbitrary field F, the idea of a limit may make no sense, so we cannot take that route. In calculus, we used the derivative to find where a function is increasing or decreasing, where it is maximal or minimal, etc. But when dealing with an arbitrary field F, these ideas may make no sense. So, what good is $D(f)$? We shall see shortly, but let us postpone this until we prove a few properties.

As you know from calculus, a function defined on an interval has derivative 0 if and only if it is a constant function on that interval. That is why when you learned to integrate you had to perpetually write "$+C$" at the end of any indefinite integral. Do we have this property when we leave the familiar confines of calculus? Well almost.

Lemma 1. *Suppose F is a field and $f \in F[x]$. If $D(f) = 0$, then f is a constant polynomial, or the field F has characteristic p (a prime number) and $f(x) = u(x^p)$ for some $u \in F[x]$. The converse holds as well.*

So, this is perhaps a surprise that other things than constants can have derivative 0. We shall leave the proof of this result as a homework problem.

We all know the addition rule for derivatives and the constant multiple rule. It is easy to see that this continues to hold for the formal derivative.

Lemma 2. *If F is a field, $f, g \in F[x]$ and $a \in F$, then $D(f + g) = D(f) + D(g)$ and $D(af) = aD(f)$.*

This too shall be left as a homework assignment. An easy generalization of this result is that if $f_1, \ldots, f_k \in F[x]$ and $a_1, \ldots, a_k \in F$, then

$$D(a_1 f_1 + \cdots + a_k f_k) = a_1 D(f_1) + \cdots + a_k D(f_k).$$

The technical term for D is that it is a linear operator.

The next familiar property of derivatives we shall investigate is the product rule. There is no surprise: it works.

Lemma 3. *Suppose F is a field and $f, g \in F[x]$. Then $D(fg) = D(f)g + fD(g)$.*

Proof. First we note that the result will hold if we prove it in the case of the special polynomials $g(x) = x^k$. Indeed, if the lemma holds for these polynomials, and now we have a general $g(x) = \sum_{i=0}^{d} a_i x^i$, then by Lemma 2, we have

$$D(fg) = D\left(f(x)\sum_{i=0}^{d} a_i x^i\right) = \sum_{i=0}^{d} a_i D(f(x)x^i).$$

But if we assume the product rule for products of the form $f(x)x^i$, then we have

$$\begin{aligned} D(fg) &= \sum_{i=0}^{d} a_i (D(f(x))x^i + f(x)D(x^i)) = \sum_{i=0}^{d} a_i D(f(x))x^i + \sum_{i=0}^{d} a_i f(x) D(x^i) \\ &= D(f(x))\sum_{i=0}^{d} a_i x^i + f(x) D\left(\sum_{i=0}^{d} a_i x^i\right), \end{aligned}$$

where for the last step, we again used linearity (or, if you like, just the definition of the derivative). Now this last expression is seen to be exactly $D(f)g + fD(g)$.

Thus, we've reduced the general product rule to the case when $g(x) = x^k$ for some k. Now we play the same game with $f(x)$, so we will have the general product rule for $f(x)x^k$ if we can prove it in the special case when $f(x) = x^l$ for some l. But this we can easily handle! First, if either k or l is 0, there is no problem, since the product rule works when one of the factors is 1. (Can you prove that?) So assume both $k, l > 0$. We have

$$D(x^l x^k) = D(x^{l+k}) = (l+k)x^{l+k-1}$$

on the one hand, and

$$D(x^l)x^k + x^l D(x^k) = lx^{l-1} \cdot x^k + x^l \cdot kx^{k-1} = lx^{l+k-1} + kx^{l+k-1} = (l+k)x^{l+k-1}.$$

The two expressions are one and the same, and we have proved the lemma. □

As a consequence of the product rule and induction, we have the power rule.

Lemma 4. *If F is a field and $f \in F[x]$, $k \in \mathbb{N}$, then $D(f^k) = kf^{k-1}D(f)$.*

When the deriviative is 0

Let us return to the mysterious case of zero derivative; that is, when $f(x) = u(x^p)$, where $f, u \in F[x]$ and the field F has characteristic p. Can such a polynomial $f(x)$ actually be irreducible? The answer depends on which field of characteristic p you have. Here's an example where $u(x^p)$ can in fact be irreducible. Let p be a prime number and let $F = \mathbb{F}_p(t)$ be the field of rational functions (quotients of polynomials) in the indeterminate t with coefficients in $\mathbb{F}_p$. That's a mouthful, but the upshot is that the polynomial $f(x) = x^p - t \in F[x]$ is indeed of the form $u(x^p)$, and it is irreducible. (We will not develop the proof but the idea is to use the analogue of Gauss's Lemma for polynomials in $\mathbb{Q}[x]$.)

On the other hand, if F is a finite field of characteristic p, then any polynomial $f \in F[x]$ of the form $u(x^p)$ for $u \in F[x]$ is the pth power of some polynomial $v \in F[x]$. Indeed, if $F = \mathbb{F}_p$, then the bad student's binomial theorem plus the fact that for every $a \in F$ we have $a^p = a$, gives us that

$$\sum_{i=0}^{d} a_i x^{pi} = \sum_{i=0}^{d} a_i^p x^{pi} = \left(\sum_{i=0}^{d} a_i x^i \right)^p,$$

that is $u(x^p) = u(x)^p$. In general for $F = \mathbb{F}_{p^k}$ we have seen that every element of F is a pth power of an element from F. We've seen this because we know that raising to the pth power is an *automorphism* of F, and so is onto. And we've also seen this more directly: since $\alpha^{p^k} = \alpha$ for all $\alpha \in F$, if we let $\beta = \alpha^{p^{k-1}}$, we see that $\beta^p = \alpha$. The consequence of this is that if $u(x) = \sum_{i=0}^{d} \alpha_i x^i$ and we let $\beta_i \in F$ with $\beta_i^p = \alpha_i$, then if $v(x) = \sum_{i=0}^{d} \beta_i x^i$, we have

$$u(x^p) = v(x)^p.$$

Thus, if our field F is $\mathbb{F}_{p^k}$, then $D(f) = 0$ implies that $f = v^p$ for some $v \in F[x]$.

The greatest common divisor of a polynomial f and it's derivative $D(f)$

We now come to a very important property of the formal derivative $D(f)$. Recall that if f, g are polynomials that are not both 0, then $\gcd(f, g)$ is the monic common divisor of f and g of greatest degree.

Proposition 1. *If $f \in \mathbb{F}_{p^k}[x]$ is monic and of positive degree, then exactly one of the following is true:*

1. $\gcd(f, D(f)) = 1$,
2. $0 < \deg \gcd(f, D(f)) < \deg f$,
3. $\gcd(f, D(f)) = f$.

Moreover, item 1 occurs if and only if f is squarefree.

Proof. Note that either $D(f) = 0$ or $\deg D(f) < \deg f$. The first possibility gives us item 3. The second possibility implies that $\gcd(f, D(f))$ has degree $\leq \deg D(f) < \deg f$, so if this gcd is 1, we're in case 1, and if not, we're in case 2. This proves the first assertion.

For the second assertion, assume that g is irreducible and $g^2 \mid f$, say $f = g^2 h$ for some h. Then by the product rule and power rule,

$$D(f) = D(g^2 h) = 2gD(g)h + g^2 D(h),$$

which is clearly a multiple of g. Thus $g \mid \gcd(f, D(f))$ so that item 1 does not occur. Conversely, suppose f is squarefree and let g be an irreducible factor of f, say $f = gh$, where $g \nmid h$. Note that

$$D(f) = D(gh) = D(g)h + gD(h),$$

so that $g \mid \gcd(f, D(f))$ if and only if $g \mid D(g)h$ if and only if $g \mid D(g)$. But $D(g)$ has degree smaller than the degree of g, and in particular $D(g)$ is not 0. (Here is where we use that F is a finite field and not say the function field $\mathbb{F}_p(t)$.) Thus, we cannot have $g \mid D(g)$, and so we cannot have $g \mid D(f)$. Since this is true for every irreducible divisor of f it follows that $\gcd(f, D(f))$ does not have any irreducible divisors; i.e., it must be 1. Thus, item 1 occurs. $\square$

Recall that earlier in the course we proved that the polynomial $x^{p^k} - x$ is squarefree in $\mathbb{F}_p[x]$. This can be seen instantly as a consequence of Proposition 1: If $f(x) = x^{p^k} - x$, then $D(f) = -1$, so item 1 of the proposition occurs, and so f is squarefree. You can see that the derivative has it's uses!