5 Derivatives

The other main difference between $k[x]$ and $\mathbb{Z}$ is the operation called the derivative. We develop the derivative using only algebraic techniques, no limits.

We require the following properties of the derivative (with respect to x) on $k[x]$.

(1) The derivative d maps $k[x]$ to $k[x]$.

(2) $d(x) = 1$.

(3) Linearity: $d(f + g) = d(f) + d(g)$.

(4) The Product Rule: $d(fg) = fd(g) + gd(f)$.

Exercises 5.1. Using just the rules above, show the following for $\mathbb{Q}[x]$:

(a) $d(0) = 0$ [use linearity].

(b) $d(1) = 0$ [use the product rule].

(c) $d(m) = 0$ for $m \in \mathbb{Z}$ [use linearity].

(d) (HW) $d(a) = 0$ for $a \in \mathbb{Q}$ [use the product rule].

(e) (HW) $d(ax^m) = amx^{m-1}$ (induction, product rule).

(f) (HW) $d(\sum_m a_m x^m) = \sum_{m>0} a_m m x^{m-1}$.

For arbitrary fields we add one more assumption:

(5) The derivative of a constant is 0.

This was proven from the properties of a derivative in $\mathbb{Q}[x]$ in the exercise above, but more generally it has to be assumed. In fact, the derivative can be defined much more generally (of a ring R relative to a subring (call it k) and derivatives of elements of k are 0).

We will use $f'(x)$ for the derivative of $f(x)$.

Exercises 5.2. (HW)

(a) Show that the derivative can be extended to to $k(x)$ and that the quotient rule must hold (first use the product rule to establish the reciprocal rule $d(1/a(x)) = a'(x)/(a(x))^2$).

Exercises 5.3. (HW) Let $f(x) \in k[x]$ with k a field of characteristic 0.

(a) Suppose a is a root of multiplicity m of f. Show that a is a root of multiplicity $m - 1$ of $f'(x)$.

(b) Suppose the unique factorization of $f(x)$ is $u(x-a_1)^{r_1}(x-a)_2^{r_2}\cdots(x-a_k)^{r_k}$. Show that $f'(x) = (x-a_1)^{r_1-1}(x-a)_2^{r_2-1}\cdots(x-a_k)^{r_k-1}h(x)$. For some $h(x)$ that does not have any of the a_i as roots.

(c) More generally, suppose the unique factorization of $f(x)$ is $u\big(p_1(x)\big)^{e_1}\big(p_2(x)\big)^{e_2}\cdots\big(p_t(x)\big)^{e_t}$. Show that $f'(x) = \big(p_1(x)\big)^{e_1-1}\big(p_2(x)\big)^{e_2-1}\cdots\big(p_t(x)\big)^{e_t-1}h(x)$ for some $h(x)$ that is not divisible by any of the $p_i(x)$.

(d) For $f \in k[x]$ and f monic, show that $\operatorname{rad}(f) = f/\gcd(f, f')$.

Strange things happen in finite characteristic.

Exercises 5.4. Let p be prime and q a power of p. We will consider derivatives in $\mathbb{F}_{p^r}[x]$.

(a) Over any field, check that the derivative map is a homomorphism of vector spaces.

(b) (HW) Over a field of characteristic 0, the kernel is just the constant polynomials. What is the kernel for $\mathbb{F}_q[x]$?

6 Mason-Stothers Theorem and Fermat's Last Theorem for Polynomial rings

We can now prove the analogues of the *abc*-conjecture and Fermat's Last Theorem for $k[x]$. We assume the characteristic of k is 0.

Mason-Stothers

In the previous exercises we showed $\text{rad}(f) = f/\gcd(f, f')$. Let's introduce the unique factorization of f, $f = u\prod_{i=1}^{t} p_i^{e_i}$ with the p_i irreducible, $e_i \geq 1$ and u a constant. Now introduce some notation for the radical f_r, the "excess", f_e, and another term derived from the derivative that I will call f_k.

$$\begin{aligned} f &= u\prod_{i=1}^{t} p_i^{e_i} \\ f_r &= \prod_{i=1}^{t} p_i \\ f_e &= u\prod_{i=1}^{t} p_i^{e_i-1} = \frac{f}{f_r} \end{aligned}$$

Taking the derivative,

$$\begin{aligned} f' &= u\Big(\sum_{i=1}^{t} e_i p_i' p_i^{e_i-1}\big(\prod_{j\neq i} p_j^{e_j}\big)\Big) \\ &= u\Big(\prod_{i=1}^{t} p_i^{e_i-1}\Big)\Big(\sum_{i=1}^{t} e_i p_i' \prod_{j\neq i} p_j\Big) \\ &= f_e f_k \end{aligned}$$

where,

$$f_k = \sum_{i=1}^{t} e_i p_i' \prod_{j\neq i} p_j = \sum_i e_i p_i' \frac{f_r}{p_i}$$

Note that f_k is comprime to f since for each irreducible factor p_i of f, p_i divides all summands of f_k, except for the ith term, which it does not divide.

Now we can prove the Mason-Strothers theorem.

Theorem 6.1. *Let k be a field of characteristic 0. Let f, g, h be nonconstant coprime polynomials in $k[x]$ satisfying $f + g = h$. Then*

$$\max\Big(\deg(f), \deg(g), \deg(h)\Big) < \deg\big(\operatorname{rad}(fgh)\big)$$

Proof. Note that if any two of f, g, h have a common factor of positive degree then all do, so it is enough to assume that any two are coprime.

Taking the derivative of both sides of the equation, we have these two equalities:

$$f + g = h$$
$$f' + g' = h'$$

Multiplying the first by g' and the second by g we have

$$fg' + gg' = hg'$$
$$f'g + g'g = h'g$$

Substracting,

$$fg' - f'g = hg' - h'g$$

Now we introduce the notation defined above,

$$f_r f_e g_e g_k - f_e f_k g_r g_e = h_r h_e g_e g_k - h_e h_k g_r g_e$$
$$f_e g_e\big(f_r g_k - f_k g_r\big) = h_e g_e\big(h_r g_k - h_k g_r\big)$$

Observe that f_e, g_e, h_e are coprime and each divides $fg' - f'g$, which equals $hg' - h'g$. Thus

$$\deg(f_e) + \deg(g_e) + \deg(h_e) \leq \deg(fg' - f'g)$$

Observe also that

$$\deg(f'g - fg') \leq \max(\deg(f'g), \deg(fg')) = \deg(f) + \deg(g) - 1$$

Now we substitute $\deg(f_e) = \deg(f) - \deg(f_r)$ and similarly for the others.

$$\deg(f) - \deg(f_r) + \deg(g) - \deg(g_r) + \deg(h) - \deg(h_r) \leq \deg(f) + \deg(g) - 1$$

Rearranging,

$$\deg(h) \leq \deg(f_r) + \deg(g_r) + \deg(h_r) - 1$$

Using comprimality of f, g, h,

$$\deg(f_r) + \deg(g_r) + \deg(h_r) = \deg(f_r g_r h_r) = \deg\big(\operatorname{rad}(fgh)\big)$$

So

$$\deg(h) \leq \deg(\operatorname{rad}(fgh)) - 1$$

The argument is easily reworked to show the same bounds for $\deg(f)$ and $\deg(g)$. □

Exercises 6.2. Extend the Mason-Stother theorem to fields of finite characteristic.

(a) Let f, g, h be nonconstant coprime polynomials in $k[x]$ satisfying $f + g = h$. Then either

$$\max \deg(f), \deg(g), \deg(h) < \deg(\operatorname{rad}(fgh))$$

or each of f, g, and h has derivative 0. [hint: the key step is either $fg' - f'g = 0$ or it does not equal 0.

The analogue of Fermat's last theorem

Theorem 6.3. *Let k be a field of characteristic 0 and let $n \geq 3$ be an integer. Suppose that $a(t)$, $b(t)$, and $c(t)$ are three coprime polynomials in $k(t)$ satisfying $a(t)^n + b(t)^n = c(t)^n$. Then all three polynomials are constants.*

Exercises 6.4.

(a) Prove FLT for polynomials using the Mason-Stother's theorem.

(b) (HW) Show that the FLT holds for polynomials that aren't coprime provided $a(t)$ and $b(t)$ aren't associates.

(c))HW) Show that there do exist polynomials $a(t), b(t), c(t)$ of positive degree such that $a(t)^2 + b(t)^2 = c(t)^2$.