Math 4030-001/Foundations of Algebra/Fall 2017
Numbers at the Foundations: Real Numbers

In calculus, the derivative of a function $f(x)$ is defined using limits. As a particular case, the derivative of

$$f(x) = a_dx^d + \cdots + a_0$$

is

$$f'(x) = da_{d-1}x^{d-1} + \cdots + a_1$$

We will take this as the definition of the derivative of a polynomial. Notice that:

- The derivative of $f(x) \in \mathbb{Q}[x]$ is another polynomial $f'(x) \in \mathbb{Q}[x]$.
- The derivative of $x^n$ is $nx^{n-1}$
- The derivative of $cf(x)$ is $cf'(x)$ for any constant $c$.
- The derivative of $f(x) + g(x)$ is $f'(x) + g'(x)$.

These are easy to check. It is a bit more involved to check:

**Leibniz’s Rule:** The derivative of $f(x)g(x)$ is $f'(x)g(x) + f(x)g'(x)$.

**Proof.** The rule holds for $x^m$ and $x^n$ since $x^m x^n = x^{m+n}$ and:

1. The derivative of $x^{m+n}$ is $(m+n)x^{m+n-1}$ and
2. $(mx^{m-1})x^n + x^m(nx^{n-1}) = mx^m + nx^{m+n-1} = (m+n)x^{m+n-1}$

Next, Leibniz’s rule satisfies the following distributive properties:

(a) If the Leibniz rule holds for $f(x)g(x)$ and $c$ is a constant, then the derivative of $(cf(x))g(x) = c(f(x)g(x))$ is:

$$c(f'(x)g(x) + f(x)g'(x)) = (c f'(x))g(x) + (cf(x))g'(x)$$

so the Leibniz rule holds for $(cf(x))g(x)$.

(b) If the Leibniz rule holds for $f(x)g(x)$ and $h(x)g(x)$, then the derivative of $(f(x) + h(x))g(x) = f(x)g(x) + h(x)g(x)$ is:

$$f'(x)g(x) + f(x)g'(x) + h'(x)g(x) + h(x)g'(x)$$

$$= (f'(x) + h'(x))g(x) + (f(x) + h(x))g'(x)$$

so Leibniz’s rule holds for $(f(x) + h(x))g(x)$.

Putting (a) and (b) together with (i) and (ii), we may deduce first that the Leibniz rule holds for all products of polynomials of the form:

$$(a_mx^m + \cdots + a_0) \cdot x^n$$

and then that it holds for all products:

$$(a_mx^m + \cdots + a_0)(b_nx^n + \cdots + b_0)$$

i.e. that it holds for all products of polynomials. □
Example. Suppose \( f(x) = (x - r)^2g(x) \). Then by Leibniz’s rule,
\[
  f'(x) = 2(x - r)g(x) + (x - r)^2g'(x) = (x - r)(2g(x) + g'(x))
\]
so \( f'(x) \) and \( f(x) \) share \( (x - r) \) as a common factor!

Conversely, suppose \( x - r \) divides \( f(x) \) and \( f'(x) \). Then:
\[
  f(x) = (x - r)h(x) \quad \text{and} \quad f'(x) = h(x) + (x - r)h'(x)
\]
and it follows that \( (x - r) \) divides \( h(x) \), so \( (x - r)^2 \) divides \( f(x) \).

When \( (x - r)^2 \) divides \( f(x) \) we say that \( r \) is a **multiple** root of \( f(x) \).

One of many applications of the derivative is its use in an algorithm to **approximate** the roots of polynomials with rational numbers.

**Newton’s Method.** Let \( r \in \mathbb{Q} \) be an approximate rational solution to \( f(x) = 0 \) for \( f(x) \in \mathbb{Q}[x] \). If \( f'(r) \neq 0 \), Newton’s method offers:
\[
  s = r - \frac{f(r)}{f'(r)}
\]
as a new (and often much better) approximate rational solution.

Example. (a) Start with \( r = 1 \) as an approximate square root of 2, that is, an approximate solution to \( f(x) = x^2 - 2 \). Using \( f'(x) = 2x \), the first few iterated results of Newton’s method are:

<table>
<thead>
<tr>
<th>( r )</th>
<th>( r^2 - 2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>3/2 = 1 - ((-1)/2)</td>
<td>1/4</td>
</tr>
<tr>
<td>17/12 = 3/2 - (1/4)/3</td>
<td>1/144</td>
</tr>
<tr>
<td>577/408 = 17/2 - (1/144)/(17/6)</td>
<td>1/166,464</td>
</tr>
</tbody>
</table>

yielding a sequence of rational numbers 1, 3/2, 17/12, 577/408, ... with rapidly decreasing value of \( r^2 - 2 \).

(b) Let \( r = 1 \) and \( f(x) = x^3 - 5x + 1 \) with \( f'(x) = 3x^2 - 5 \). Then:

<table>
<thead>
<tr>
<th>( r )</th>
<th>( r^3 - 5r + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1/5 = 0 - 1/(-5)</td>
<td>1/125</td>
</tr>
<tr>
<td>123/610 = 1/5 - (1/125)/(-122/25)</td>
<td>367/226,981,000</td>
</tr>
</tbody>
</table>

rapidly approaches a root of \( x^3 - 5x + 1 \).

This is the “hare” method for approximating roots with a sequence of rational numbers. When it works, the results are impressive, but this method is not guaranteed to work (for example, it may produce a rational number with \( f'(r) = 0 \), ending the sequence in failure).
There is a more reliable “tortoise” method.

**Decimal Expansions.** If \( f(x) \in \mathbb{Q}[x] \) has no rational roots and:

\[
f(a) < 0 \text{ and } f(a + 1) > 0
\]

for some integer \( a \), then we find a real root of \( f(x) \) by:

**START.** Let \( r = a \) and set \( m = 1 \).

**LOOP.** There is first digit \( d_m \in \{0,...,9\} \) so that:

\[
f(r + d_m/10^m) < 0 \text{ and } f(r + (d_m + 1)/10^m) > 0
\]

Add \( d_m/10^m \) to \( r \). Increase \( m \) by one and REPEAT.

This produces a non-decreasing sequence of rational numbers:

\[
\begin{align*}
  r_0 &= a \\
  r_1 &= a + d_1/10 \\
  r_2 &= a + d_1/10 + d_2/100 \\
  &\vdots
\end{align*}
\]

with the property that \( f(r_i) < 0 \) for all \( i \).

It also produces a non-increasing sequence of rational numbers:

\[
\begin{align*}
  s_0 &= r_0 + 1 \\
  s_1 &= r_1 + 1/10 \\
  s_2 &= r_2 + 1/100 \\
  &\vdots
\end{align*}
\]

with the property that \( f(s_i) > 0 \) for all \( i \). The real numbers are designed so that this situation **defines** a real number:

\[
\alpha = \lim_{i \to \infty} r_i = \lim_{i \to \infty} s_i
\]

with the property that \( f(\alpha) = 0 \).

**Remarks.** (i) If instead there is an integer \( a \) such that \( f(a) > 0 \) and \( f(a + 1) < 0 \), then the algorithm above may be run with the inequalities reversed to also find a real root of \( f(x) \).

(ii) If \( f(x) \) has odd degree \( d \) and positive leading coefficient \( a_d \), then there is guaranteed to be an \( a \in \mathbb{Z} \) with \( f(a) < 0 \) and \( f(a + 1) > 0 \) to start the algorithm. Similarly, if the leading coefficient is negative then the algorithm of (i) with reversed signs is guaranteed to produce a root. For polynomials of even degree, however, there is no such guarantee (though it still happens in many cases). The polynomials \( x^{2k} + 1 \), for example, have no real roots!
Example. The polynomial \( f(x) = x^3 - 5x + 1 \) satisfies:
\[
f(2) = -1 \text{ and } f(3) = 13
\]
so there is a root between 2 and 3. This is a different root than the one that Newton’s method is finding in the example above.

As another use of the derivative, consider the cubic polynomial:
\[
f(x) = x^3 - px + q
\]
in the derivation of the cubic formula (with the sign of \( p \) changed).

Proposition 9.1. Let \( \Delta = \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3 \). Then \( f(x) \) has:

(i) Three different real roots when \( \Delta < 0 \)

(ii) A multiple (rational) root \( (r = 3q/2p) \) when \( \Delta = 0 \)

(iii) Only one real root when \( \Delta > 0 \)

Remark. This is the analogue of the discriminant:
\[
\Delta = b^2 - 4ac
\]
for the quadratic polynomial \( ax^2 + bx + c \), which has:

(i) No real roots when \( \Delta < 0 \)

(ii) One multiple rational root \( (r = -b/2a) \) when \( \Delta = 0 \)

(iii) Two real roots when \( \Delta > 0 \).

as we know from the quadratic formula.

Proof of the Proposition. Consider the derivative:
\[
f'(x) = 3x^2 - p
\]
If \( p < 0 \), then \( f'(x) > 0 \) for all \( x \) so \( f(x) \) is strictly increasing, and then \( f(x) \) has exactly one real root (and \( \Delta > 0 \)). If \( p = 0 \), then \( f(x) \) is strictly increasing except at \( x = 0 \). If \( q = 0 \), then \( f(x) \) has a multiple root at \( 0 \) (and \( \Delta = 0 \)). Otherwise, \( f(x) \) has one real root (and \( \Delta > 0 \)).

This leaves \( p > 0 \). The roots of \( f(x) \) are real numbers \( r = \pm \sqrt[3]{\frac{p}{3}} \).

Plugging these in to \( f(x) \), there is a multiple root if and only if:
\[
f \left( \sqrt[3]{\frac{p}{3}} \right) = \left(\frac{p}{3}\right)^{\frac{2}{3}} - p\sqrt[3]{\frac{p}{3}} + q = q - 2 \left(\frac{p}{3}\right)^{\frac{2}{3}} = 0 \text{ or}
\]
\[
f \left( -\sqrt[3]{\frac{p}{3}} \right) = -\left(\frac{p}{3}\right)^{\frac{2}{3}} + p\sqrt[3]{\frac{p}{3}} + q = q + 2 \left(\frac{p}{3}\right)^{\frac{2}{3}} = 0
\]
In other words, there is a multiple root if and only if: \( \frac{q}{2} = \pm \left(\frac{p}{3}\right)^{\frac{2}{3}} \), which is the case if and only if \( \left(\frac{q}{2}\right)^2 = \left(\frac{p}{3}\right)^3 \). This gives (ii).
For the rest of the cases, notice from the graph of \( y = f(x) \) that \( f(x) \) has three real roots if and only if:

\[
f\left(-\sqrt{\frac{p}{3}}\right) > 0 \quad \text{and} \quad f\left(\sqrt{\frac{p}{3}}\right) > 0
\]

and then there is one root in each of the intervals:

\[
\left(-\infty, -\sqrt{\frac{p}{3}}\right), \left(-\sqrt{\frac{p}{3}}, \sqrt{\frac{p}{3}}\right) \quad \text{and} \quad \left(\sqrt{\frac{p}{3}}, +\infty\right)
\]

Thus, there are three roots if and only if:

\[
\frac{q}{2} > -\left(\frac{p}{3}\right)^{\frac{3}{2}} \quad \text{and} \quad \frac{q}{2} < \left(\frac{p}{3}\right)^{\frac{3}{2}}
\]

which is the case if and only if \( \Delta < 0 \). \( \square \)

The real numbers \( \mathbb{Q} \subset \mathbb{R} \) are least upper bounds of bounded sequences of rational numbers. They complete the rational numbers with points of the number line, and conversely, every point of the number line is the least upper bound of a sequence of rational numbers. Notice that the ordering of the rational numbers extends to an ordering of the reals.

The positive real numbers are presented as infinite decimals:

\[
n.d_1d_2d_3\ldots \text{ for an integer } n \geq 0 \text{ and digits } d_i \in \{0, ..., 9\}
\]

and negative real numbers are usually presented as the negatives of positive real numbers, i.e. in the form: \(-n.d_1d_2d_3\ldots\).

The operations of addition, multiplication, subtraction and division extend from the rational numbers to the real numbers by continuity. That is, if \( \alpha, \beta \in \mathbb{R} \) are limits of sequences of rational numbers:

\[
\alpha = \lim_{n \to \infty} r_n \quad \text{and} \quad \beta = \lim_{n \to \infty} s_n
\]

then:

\[
\alpha + \beta = \lim_{n \to \infty} (r_n + s_n), \quad \alpha \cdot \beta = \lim_{n \to \infty} (r_n \cdot s_n) \text{ etc}
\]

The associative, commutative and distributive rules hold by continuity, and \( \mathbb{R} \) is a field.

**Exercises.** 9.1. Prove that if \( f(x) \in \mathbb{Q}[x] \) and \( g(x) \in \mathbb{Q}[x] \), then:

\[
f(g(x)) \in \mathbb{Q}[x]
\]

9.2. Prove the chain rule for compositions of polynomials.

\[
f(g(x))' = f'(g(x)) \cdot g'(x)
\]
9.3. Prove that the only polynomials that have a polynomial inverse function are the linear polynomials \( f(x) = ax + b \) (with \( a \neq 0 \)).

9.4. Work out several iterations of Newton’s method and then describe what you see for the polynomial \( x^2 + 1 \) with the approximations:

(i) \( r = 1 \)

(ii) \( r = \frac{1}{2} \).

9.5. Prove that if \( f(x) = x^3 + px + q \) has no rational roots, then there is an integer \( a \) so that:

\[
f(a) < 0 \quad \text{and} \quad f(a + 1) > 0
\]

What can go wrong with this if \( f(x) \) has a rational root?

9.6. Show that if \( f(x), f'(x) \) and \( f''(x) \) share a common root, then:

\[
f(x) = (x - r)^3 g(x)
\]

i.e. \( r \) is a triple root of \( f(x) \).

9.7. Sketch the graph of a polynomial function:

\[
y = x^3 - px + q
\]

with \( p > 0 \) and \( \Delta > 0 \).