MATH 287 HOMEWORK 6

ANDREW MOORE

Date: October 8, 2021.

Exercise 1. The derivative of x^2 is $2x$.

Proof. Let $f(x) = x^2$. Using the limit definition of derivative, we have

$$
\begin{aligned}
\lim_{h\to 0} \frac{f(x+h)-f(x)}{h} &= \lim_{h\to 0} \frac{(x+h)^2 - x^2}{h} \\
&= \lim_{h\to 0} \frac{x^2 - x^2 + 2xh + h^2}{h} \\
&= \lim_{h\to 0} \frac{2xh + h^2}{h} \\
&= \lim_{h\to 0} \frac{2xh}{h} + \frac{h^2}{h} \qquad (1) \\
&= \lim_{h\to 0} 2x + h \\
&= 2x + 0 \\
&= 2x.
\end{aligned}
$$

□

Exercise 2. Project 6.9. On $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ we define the relation $(m_1, n_1) \sim (m_2, n_2)$ if $m_1 n_2 = n_1 m_2$. Prove that the relation defined in the book is transitive.

Proof. Let $a, b, c \in \mathbf{Z} \times (\mathbf{Z} - \{0\})$, and let $a = (a_1, a_2)$, $b = (b_1, b_2)$, and $c = (c_1, c_2)$. We intend to show that if $a \sim b$ and $b \sim c$, then $a \sim c$. In this case, the relation $\sim$, is defined as $m_1 n_2 = n_1 m_2$. Let us assume that $a \sim b$ and $b \sim c$. That is,

$$\begin{aligned} a &\sim b & & & b &\sim c \\ (a_1, a_2) &\sim (b_1, b_2) & &\text{and} & (b_1, b_2) &\sim (c_1, c_2) \\ a_1 b_2 &= b_1 a_2 & & & b_1 c_2 &= c_1 b_2. \end{aligned} \tag{2}$$

We intend to show

$$\begin{aligned} a &\sim c \\ (a_1, a_2) &\sim (c_1, c_2) \\ a_1 c_2 &= c_1 a_2. \end{aligned} \tag{3}$$

Notice that we can we can redefine b_1 as

$$\begin{aligned} b_1 c_2 &= c_1 b_2 \\ b_1 &= \frac{c_1 b_2}{c_2}. \end{aligned} \tag{4}$$

This is permissible because the set that our relation is defined upon explicitly ensures that $a_2, b_2, c_2 \neq 0$, (i.e., our set is $\{(m, n) \in \mathbf{Z} \times (\mathbf{Z} - \{0\})\}$). Then, substituting the new definition of b_1 into $a \sim b$, we have:

$$\begin{aligned} a &\sim b \\ a_1 b_2 &= b_1 a_2 \\ a_1 b_2 &= (\frac{c_1 b_2}{c_2}) a_2 \text{ (replacing } b_1) \\ a_1 b_2 c_2 &= c_1 b_2 a_2 \text{ (multiplying by } c_2 \text{ allowed } \because c_2 \neq 0) \\ a_1 c_2 &= c_1 a_2 \text{ (we can cancel } b_2 \text{ here } \because b_2 \neq 0) \\ a &\sim c. \end{aligned} \tag{5}$$

Thus, we have shown that $a_1 b_2 = (\frac{c_1 b_2}{c_2}) a_2 = b_1 a_2$. We know this is possible because of our assumptions ($a_1 b_2 = b_1 a_2$ and $b_1 c_2 = c_1 b_2$), i.e. $a \sim b$ and $b \sim c$. Thus, we can conclude that $a \sim c$, which means the relation is transitive. $\square$

Exercise 3. Prop. 6.17. Let $m \in \mathbf{Z}$. This number m is even, iff m^2 is even.

Proof. Assume that m is even, i.e. $2 \mid m$. This means that $m = 2n$ for some $n \in \mathbf{Z}$. So, by the definition of powers we can write

$$m^2 = m \cdot m = (2n) \cdot (2n) = (2n)^2 = 4n^2 = 2 \cdot (2n^2).$$

Because n is an integer, the term $2n^2$ is also an integer, and since it is being multiplied by 2, we know the product is even.

Conversely, assume that m is not even. This means that m is odd, and we can write $m = 2q + 1$ for some $q \in \mathbf{Z}$. Again, by the definition of powers we have

$$m^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1.$$

Let $z = (2q^2 + 2q)$. We know that the integers are closed under multiplication, and thus the product of $2z$ is also an integer. Therefore, we have

$$m^2 = 2z + 1,$$

which we know must be odd (Proposition 6.15).

We have shown that if m is even, m^2 must also be even. Additionally, we have shown that if m is odd, m^2 must also be odd. This means that m is even if and only if m^2 is even. $\square$

Exercise 4. Explain the proof of Proposition 6.29(i): $gcd(m, n)$ divides both m and n. Let $m, n \in \mathbf{Z}$.

Answer. This proposition formally defines the **greatest common divisor** of two arbitrary integers (referred to as m and n) as a concept. Its first item, (i) establishes that the greatest common divisor ("gcd") divides both m and n. This is a necessary precondition for being the *largest* divisor of both m and n.

Proof. Let $g = gcd(m, n)$, i.e., g is the smallest element of

$$S = \{k \in \mathbf{N} : k = mx + ny \text{ for some } x, y \in \mathbf{Z}\}.$$

If $m = n = 0$, then $g = 0$ (because $0 = (0)x + (0)y$) and the statement holds. If $m = 0$ and $n \neq 0$ then

$$S = \{|n|y : y \in \mathbf{N}\}$$

and $g = |n|$, which satisfies (i). Rephrased, this means that if $m = 0$ and $n \neq 0$ the absolute value of n must be larger than m. The case of $m \neq 0$, and $n = 0$ is analogous.

Now, we'll examine cases where $m, n \neq 0$. S will be unchanged if m or n are negative, (because we didn't require x and y to be positive or negative), so to simplify, we'll assume m and n are positive.

For the sake of contradiction, suppose that g does not divide m. By the Division Algorithm, there exist $q, r \in \mathbf{Z}$ such that

$$m = qg + r \text{ and } 0 < r < g.$$

That is, r is bigger than 0, and is smaller than g. By our definition of g, $g = mx + ny$ for some $x, y \in \mathbf{Z}$. So, rearranging terms we have

$$
\begin{aligned}
r &= m - qg \\
&= m - q(mx + ny) \\
&= m - qmx - qny \text{ (distributing)} \qquad (6)\\
&= (m - qmx) - qny \\
&= m(1 - qx) + n(-qy).
\end{aligned}
$$

This implies that $r \in S$. However, we posited that g does not divide m, therefore $0 < r < g$, but this contradicts the fact that g is the smallest element of S. Therefore g must divide m. The same argument can be applied with n to show that g divides n. $\square$

$\diamond$