Math 230 **Fall 2018**
Homework 3 **Drew Armstrong**

Fun With Axioms. In the following problems you are allowed to use the axioms from the handout and any results that we proved in class. You should document every step of your proofs, but it's okay to skip really boring things like commutativity and associativity.

Problem 1. In this problem you will prove that $(-a)(-b) = ab$ for all integers $a, b \in \mathbb{Z}$.

(a) Recall that $-a$ is the **unique** integer satisfying $a + (-a) = 0$. Prove that $-(-a) = a$.
(b) For all $a, b \in \mathbb{Z}$ prove that $(-a)b = a(-b) = -(ab)$. [Hint: Use the distribution axiom.]
(c) Recall that for all $b, c \in \mathbb{Z}$ we define $b - c := b + (-c)$. For all $a, b, c \in \mathbb{Z}$ prove that $a(b - c) = ab - ac$. [Hint: Use distribution and part (b).]
(d) For all $a, b \in \mathbb{Z}$ prove that $(-a)(-b) = ab$. [Hint: Use parts (a) and (b).]

(a) Let me recall the following fact from class. For all integers $a \in \mathbb{Z}$, the equation

$$a + x = 0$$

has a **unique** integer solution $x \in \mathbb{Z}$. *Proof.* Axiom (A4) says that a solution $x = b$ exists. Suppose that $x = c$ is another solution. Then we have

$$b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c.$$

Since the solution is unique we will give it the special name "$-a$." /// Now I claim that $-(-a) = a$. *Proof.* By definition, $x = -(-a)$ is the unique solution of the equation

$$(-a) + x = 0.$$

But then since $x = a$ is also a solution we must have $a = -(-a)$. □

(b) For all integers $a, b \in \mathbb{Z}$ I claim that $(-a)b = -(ab)$ and $a(-b) = -(ab)$, and hence $(-a)b = a(-b)$. *Proof.* For the first equality note that

$$\begin{aligned} a + (-a) &= 0 && \text{(A4)} \\ (a + (-a))b &= 0b && \text{from class} \\ ab + (-a)b &= 0. && \text{from class and (D)} \end{aligned}$$

But $x = -(ab)$ is the unique solutiion to $ab + x = 0$. Therefore $(-a)b = -(ab)$. For the second equality note that

$$\begin{aligned} b + (-b) &= 0 && \text{(A4)} \\ a(b + (-b)) &= a0 && \text{from class} \\ ab + a(-b) &= 0. && \text{from class and (D)} \end{aligned}$$

Then for the same reason as above, we have $a(-b) = -(ab)$. □

(c) For all $a, b \in \mathbb{Z}$ I claim that $a(b - c) = ab - ac$. *Proof.* Subtraction is defined by $b - c := b + (-c)$. Therefore we have

$$\begin{aligned} a(b - c) &= a(b + (-c)) && \text{by definition} \\ &= ab + a(-c) && \text{(D)} \\ &= ab + -(ac) && \text{from 1(b)} \\ &= ab - ac. && \text{by definition} \end{aligned}$$

□

(d) For all integers $a, b \in \mathbb{Z}$ I claim that $(-a)(-b) = ab$. *Proof.* We have

$$\begin{aligned}(-a)(-b) &= -(a(-b) && \text{from 1(b)}\\ &= -(-(ab)) && \text{from 1(b)}\\ &= ab. && \text{from 1(a)}\end{aligned}$$

□

Problem 2. Given an integer $a \in \mathbb{Z}$ we define its *absolute value* as follows:

$$|a| := \begin{cases} a & \text{if } a > 0,\\ 0 & \text{if } a = 0,\\ -a & \text{if } a < 0.\end{cases}$$

(a) Use this definition to prove that $|ab| = |a|\,|b|$ for all $a, b \in \mathbb{Z}$. [Hint: Problem 1.]
(b) For all $a \in \mathbb{Z}$ prove that $a \neq 0$ if and only if $|a| \geq 1$.

(a) *Proof.* There are at least four cases. (You can do more if you want.)

Case 1. If at least one of a or b is zero then we have $ab = 0$ and hence $|ab| = 0$. But we also know that at least one of $|a|$ or $|b|$ is zero and hence $|a|\,|b| = 0 = |ab|$.

Case 2. If $a > 0$ and $b > 0$ then $ab > 0$ and hence

$$|ab| = ab = |a|\,|b|.$$

Case 3. If $a < 0$ and $b < 0$ then $ab > 0$ and from Problem 1(d) we have

$$|ab| = ab = (-a)(-b) = |a|\,|b|.$$

Case 4. If a and b have opposite signs then without loss of generality we can assume that $a > 0$ and $b < 0$, so that $ab < 0$. Then from Problem 1(b) we have

$$|ab| = -(ab) = a(-b) = |a|\,|b|.$$

□

(b) I proved in class that there are no integers between 0 and 1. It follows that there are no integers between -1 and 0. *Proof.* If $-1 < x < 0$ then multiplying by -1 gives $0 < -x < 1$, contradiction. /// Now for all $a \in \mathbb{Z}$ we will show that $a \neq 0$ if and only if $|a| \geq 1$. *Proof.* For both directions we will prove the contrapositive. In other words, we will prove that

$$a = 0 \quad \Longleftrightarrow \quad |a| < 1.$$

For the first direction let $a = 0$. Then by definition we have $|a| = 0$ and hence $|a| < 1$. For the other direction let $|a| < 1$, i.e., $-1 < a < 1$. But we showed above that 0 is the only integer between -1 and 1. Hence $a = 0$. □

Problem 3. In class we saw that $\mathbb{Z}$ satisfies "additive cancellation." In this problem you will show that $\mathbb{Z}$ also satisfies a form of "multiplicative cancellation." (The proof is quite a bit harder because we are not allowed to divide.) To begin, let $n \in \mathbb{Z}$ and define the statement

$$P(n) := \text{“ for all integers } m \geq 1 \text{ we have } mn \geq 1. \text{ ”}$$

(a) Prove that $P(1)$ is true.

(b) For any positive integer $n \geq 1$ prove that $P(n) \Rightarrow P(n+1)$. Then it follows by induction that $P(n)$ is true for all $n \geq 1$. In other words, you have shown that

$$(m \geq 1 \wedge n \geq 1) \Rightarrow (mn \geq 1) \quad \text{for all } m, n \in \mathbb{Z}.$$

(c) Combine this with Problem 2 to prove for all $a, b \in \mathbb{Z}$ that

$$(a \neq 0 \wedge b \neq 0) \Rightarrow (ab \neq 0).$$

(d) Finally, prove for all integers $a, b, c \in \mathbb{Z}$ that

$$(ab = ac \wedge a \neq 0) \Rightarrow (b = c).$$

[Hint: Use 1(c) and the contrapositive of 3(c).]

(a) The statement $P(1)$ says "for all integers $m \geq 1$ we have $m \geq 1$." This is true.

(b) Now let $n \geq 1$ and assume that $P(n)$ is a true statement. In this case we will prove that $P(n+1)$ is true. *Proof.* For all integers $m \in \mathbb{Z}$ we want to prove that $m \geq 1$ implies $m(n+1) \geq 1$. So let $m \in \mathbb{Z}$ be any integer such that $m \geq 1$. Then since $P(n)$ is true we have $mn \geq 1$. Then the inequality $mn \geq 1$ implies

$$\begin{aligned} mn &\geq 1 \\ mn + m &\geq m + 1 \\ m(n+1) &\geq m + 1 \end{aligned}$$

and the inequalities $m \geq 1$ and $1 \geq 0$ imply

$$m + 1 \geq 1 + 1 \geq 1.$$

Finally, by transitivity we obtain $m(n+1) \geq 1$ as desired. □

(c) For all $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} a \neq 0 \wedge b \neq 0 &\Rightarrow |a| \geq 1 \wedge |b| \geq 1 && \text{from 2(b)} \\ &\Rightarrow |a|\,|b| \geq 1 && \text{from 3(b)} \\ &\Rightarrow |ab| \geq 1 && \text{from 2(a)} \\ &\Rightarrow ab \neq 0. && \text{from 2(b)} \end{aligned}$$

□

(d) Consider $a, b, c \in \mathbb{Z}$ such that $ab = ac$ and $a \neq 0$. We will prove that $b = c$. *Proof.* First note that

$$\begin{aligned} ab &= ac \\ ab - ac &= 0 \\ a(b - c) &= 0. \end{aligned}$$

Now the contrapositive of 3(c) says that $a = 0$ or $b - c = 0$. Since $a \neq 0$ we must have

$$\begin{aligned} b - c &= 0 \\ b &= c, \end{aligned}$$

as desired. □

[Remark: I should have reversed the order of Problems 2 and 3, since 2(a) in some sense requires 3(b). Oh well. Next time I teach the course I'll give axioms for "$<$" instead of "$\leq$."]