Math 230 D **Fall 2015**
Homework 2 **Drew Armstrong**

Problem 1. Logical Analysis.

(a) Let Q and R be logical statements. Use a truth table to prove that $\neg(Q \vee R)$ is logically equivalent to $\neg Q \wedge \neg R$. [This is called de Morgan's law.]

(b) Let P, Q, and R be logical statements. Use a truth table to prove that $(Q \vee R) \Rightarrow P$ is logically equivalent to $(Q \Rightarrow P) \wedge (R \Rightarrow P)$.

(c) Apply the principles from (a) and (b) to prove that for all integers m and n we have

$$\text{“}mn \text{ is even”} \Longleftrightarrow \text{“}m \text{ is even or } n \text{ is even”}.$$

[Hint: Let $P =$“mn is even”, $Q =$“m is even”, and $R =$“n is even”. Use part (a) for the “$\Rightarrow$” direction and use part (b) for the “$\Leftarrow$” direction.]

Here is the truth table for part (a):

Q	R	$Q \vee R$	$\neg(Q \vee R)$	$\neg Q$	$\neg R$	$(\neg Q \wedge \neg R)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Note that the third and sixth columns are equal. And here is the truth table for part (b):

P	Q	R	$Q \vee R$	$(Q \vee R) \Rightarrow P$	$Q \Rightarrow P$	$R \Rightarrow P$	$(Q \Rightarrow P) \wedge (R \Rightarrow P)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	T	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	F	F	F	F
F	T	F	T	F	F	T	F
F	F	T	T	F	T	F	F
F	F	F	F	T	T	T	T

Note that the fifth and eighth columns are equal. Finally, here is the proof of part (c):

Proof. Let $m, n \in \mathbb{Z}$ and consider the statements $P =$“mn is even”, $Q =$“m is even”, and $R =$“n is even”. We will prove that $P \Leftrightarrow (Q \vee R)$, in two separate steps.

First we will prove that $P \Rightarrow (Q \vee R)$. To do this we will rewrite the statement using the contrapositive and de Morgan's law to get

$$\begin{aligned} P &\Rightarrow (Q \vee R), \\ \neg(Q \vee R) &\Rightarrow \neg P, \\ (\neg Q \wedge \neg R) &\Rightarrow \neg P. \end{aligned}$$

This last statement says that “m and n are both odd” $\Rightarrow$ “mn is odd”. To prove this, assume that m and n are both odd, i.e., assume that there exist integers $k, \ell \in \mathbb{Z}$ such that $m = 2k+1$ and $n = 2\ell + 1$. In this case we have

$$\begin{aligned} mn &= (2k+1)(2\ell+1) \\ &= 4k\ell + 2k + 2\ell + 1 \\ &= 2(2k\ell + k + \ell) + 1, \end{aligned}$$

which is odd as desired.

Next we will prove that $(Q \vee R) \Rightarrow P$. By part (b) it is enough to prove the equivalent statment $(Q \Rightarrow P) \wedge (R \Rightarrow P)$. In other words, we have to show that "m is even" $\Rightarrow$ "mn is even" and "n is even" $\Rightarrow$ "mn is even". So assume that m is even, i.e., assume that there exists an integer $k \in \mathbb{Z}$ such that $m = 2k$. Then we have $mn = (2k)n = 2(kn)$, hence mn is even. Similarly, assume that n is even so there exists $\ell \in \mathbb{Z}$ with $n = 2\ell$. Then we have $mn = m(2\ell) = 2(m\ell)$, hence mn is even. This proves the result.

Since we have separately shown that $P \Rightarrow (Q \vee R)$ and $(Q \vee R) \Rightarrow P$, we conclude that $P \Leftrightarrow (Q \vee R)$, as desired. $\square$

Problem 2. Absolute Value. Given an integer a we define its absolute value as follows:

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

Prove that for all integers a and b we have $|ab| = |a||b|$. [Hint: Your proof will break into at least five separate cases. You may assume without proof the properties $(-a)(-b) = ab$ and $(-a)b = a(-b) = -(ab)$; we'll prove them later.]

Proof. Consider any integers $a, b \in \mathbb{Z}$. We want to show that $|ab| = |a||b|$. We will break the proof into five cases.

Case 1: If at least one of a or b is zero then we have $ab = 0$, and hence $|ab| = 0$. On the other hand we also know that at least one of $|a|$ or $|b|$ is zero, hence $|a||b| = 0$. We conclude that $|ab| = |a||b|$.

Case 2: If $a > 0$ and $b > 0$ then $ab > 0$, so we have $|ab| = ab$. On the other hand we have $|a| = a$ and $|b| = b$, hence $|a||b| = ab$. We conclude that $|ab| = |a||b|$.

Case 3: If $a > 0$ and $b < 0$ then $ab < 0$, so we have $|ab| = -(ab)$. On the other hand, we have $|a| = a$ and $|b| = -b$, hence $|a||b| = a(-b)$. Since we have assumed that $a(-b) = -(ab)$, this implies that $|ab| = |a||b|$.

Case 4: If $a < 0$ and $b > 0$ then $ab < 0$, so that $|ab| = -(ab)$. On the other hand, we have $|a| = -a$ and $|b| = b$, so that $|a||b| = (-a)b$. Since we have assumed that $(-a)b = -(ab)$ this implies that $|ab| = |a||b|$.

Case 5: If $a < 0$ and $b < 0$ then $ab > 0$, so that $|ab| = ab$. On the other hand, we have $|a| = -a$ and $|b| = -b$, hence $|a||b| = (-a)(-b)$. Since we have assumed that $(-a)(-b) = ab$, this implies that $|ab| = |a||b|$.

$\square$

[Remark: You've probably used the identity $|ab| = |a||b|$ many times, but maybe you've never thought about **why** it's true. On HW3 you will finish the job by proving that $(-a)b = a(-b) = -(ab)$ and $(-a)(-b) = ab$ directly from the definition of the integers.]

Problem 3. Divisibility. Given integers m and n we will write "$m|n$" to mean that "there exists an integer k such that $n = mk$" and when this is the case we will say that "m divides n" or "n is divisible by m". Now let a, b, and c be integers. Prove the following properties.

(a) If $a|b$ and $b|c$ then $a|c$.
(b) If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.

(c) If $a|b$ and $b|a$ then $a = \pm b$. [Hint: Use the fact that $uv = 0$ implies $u = 0$ or $v = 0$.]
(d) If $a|b$ and b is nonzero then $|a| \leq |b|$. [Hint: Use the result of Problem 2.]

Proof. For part (a), assume that $a|b$ and $b|c$, i.e., assume that there exist integers $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = b\ell$. Then we have

$$c = b\ell = (ak)\ell = a(k\ell),$$

hence $a|c$, as desired.

For part (b), assume that $a|b$ and $a|c$, i.e., assume that there exist integers $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = a\ell$. Then for any integers $x, y \in \mathbb{Z}$ we have

$$bx + cy = (ak)x + (a\ell)y = a(kx) + a(\ell y) = a(kx + \ell y),$$

hence $a|(bx + cy)$ as desired.

For part (c) assume that $a|b$ and $b|a$, i.e., assume that there exist integers $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $a = b\ell$. Then we have

$$\begin{aligned} a &= b\ell \\ a &= (ak)\ell \\ a &= a(k\ell) \\ 0 &= a(k\ell) - a \\ 0 &= a(k\ell - 1). \end{aligned}$$

If $a = 0$ then we must have $b = 0$ and hence $a = \pm b$ as desired. If $a \neq 0$ then the equation $0 = a(k\ell - 1)$ implies that $k\ell - 1 = 0$, hence $k\ell = 1$. Since k and ℓ are integers, this can only happen when $k = \ell = \pm 1$. We conclude that $a = bk = \pm b$ as desired.

For part (d), let $b \neq 0$ and assume that $a|b$, i.e., assume that there exists $k \in \mathbb{Z}$ such that $b = ak$. Note that $k \neq 0$ since otherwise we would have $b = 0$, which is a contradiction. Since k is a nonzero integer we must have $1 \leq |k|$. Then multiplying both sides by $|a|$ and using the result of Problem 2 gives

$$\begin{aligned} 1 &\leq |k| \\ |a| &\leq |a||k| \\ |a| &\leq |ak| \\ |a| &\leq |b|, \end{aligned}$$

as desired. □

[Remark: Some of the steps here, such as the fact that $1 \leq |k|$ and the implication "$1 \leq |k|$" $\Rightarrow$ "$|a| \leq |a||k|$", were not fully explained. We'll fill in the gaps later when we see the formal definition of $\mathbb{Z}$.]

Problem 4. The Square Root of 5. Prove that $\sqrt{5}$ is not a ratio of integers, in two steps.

(a) First prove the following **lemma**: Let n be an integer. If n^2 is divisible by 5, then so is n. [Hint: Use the contrapositive and note that there are four separate ways for an integer to be **not** divisible by 5. Sorry it's a bit tedious; we will find a better way to do this later.]
(b) Use the method of contradiction to prove that $\sqrt{5}$ is not a ratio of integers. Explicitly quote your lemma in the proof. [Hint: Your proof should begin as follows: "Assume for contradiction that $\sqrt{5}$ **is** a ratio of integers. In this case, ..."]

Lemma: Let n be an integer. Then we have "$5|n^2 \Rightarrow 5|n^2$".

Proof. We prove the contrapositive statement "$5 \nmid n \Rightarrow 5 \nmid n^2$". So assume that 5 does **not** divide n. In this case we want to show that 5 does **not** divide n^2. There are four cases.

Case 1: If $n = 5k + 1$ for some $k \in \mathbb{Z}$ then we have

$$n^2 = (5k+1)^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1,$$

hence n^2 is not divisible by 5.

Case 2: If $n = 5k + 2$ for some $k \in \mathbb{Z}$ then we have

$$n^2 = (5k+2)^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4,$$

hence n^2 is not divisible by 5.

Case 3: If $n = 5k + 3$ for some $k \in \mathbb{Z}$ then we have

$$n^2 = (5k+3)^2 = 25k^2 + 30k + 9 = 5(5k^2 + 6k + 1) + 4,$$

hence n^2 is not divisible by 5.

Case 4: If $n = 5k + 4$ for some $k \in \mathbb{Z}$ then we have

$$n^2 = (5k+4)^2 = 25k^2 + 40k + 16 = 5(5k^2 + 8k + 3) + 1,$$

hence n^2 is not divisible by 5. □

[Remark: Here we used the fact that remainders are unique. For example, if $n^2 = 5(\text{something})+4$, this means that the remainder of n^2 mod 5 is 4. In particular, the remainder is not zero. We haven't proved uniqueness of remainders but we will do soon.]

Theorem: $\sqrt{5} \notin \mathbb{Q}$.

Proof. Assume for contradiction that $\sqrt{5} \in \mathbb{Q}$. In this case we can write $\sqrt{5} = a/b$ where a and b are integers with no common factor except ± 1. Square both sides to get

$$\begin{aligned} \sqrt{5} &= a/b \\ 5 &= a^2/b^2 \\ 5b^2 &= a^2. \end{aligned}$$

Since a^2 is a multiple of 5 the lemma implies that $a = 5k$ for some $k \in \mathbb{Z}$. Now substitution gives

$$\begin{aligned} 5b^2 &= a^2 \\ 5b^2 &= (5k)^2 \\ 5b^2 &= 25k^2 \\ b^2 &= 5k^2. \end{aligned}$$

Since b^2 is a multiple of 5 the lemma implies that $b = 5\ell$ for some $\ell \in \mathbb{Z}$. But now we see that 5 is a common factor of a and b, which contradicts the fact that they have no common factor except ± 1. This contradiction implies that our original assumption (i.e., that $\sqrt{5} \in \mathbb{Q}$) was false. □

[Remark: In this proof we assumed that every element of $\mathbb{Q}$ can be written in "lowest terms", which we haven't proved yet. We will.]