Math 230 **Fall 2018**
Homework 2 **Drew Armstrong**

Problem 1. De Morgan's Laws say that for all statements P, Q we have

$$\neg(P \vee Q) = \neg P \wedge \neg Q \qquad \text{and} \qquad \neg(P \wedge Q) = \neg P \vee \neg Q.$$

(a) Use truth tables to prove these laws.
(b) Use a truth table to prove that $(P \Rightarrow Q) = (\neg P) \vee Q$ for all statements P, Q.
(c) Combine parts (a) and (b) to prove that for all statements P, Q we have

$$(P \Rightarrow Q) = (\neg Q \Rightarrow \neg P).$$

Do **not** use a truth table.

(a) Here is a truth table proving $\neg(P \vee Q) = \neg P \wedge \neg Q$:

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$
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

And here is a truth table proving $\neg(P \wedge Q) = \neg P \vee \neg Q$:

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

(b) And here is a truth table proving that $(P \Rightarrow Q) = (\neg P) \vee Q$:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

(c) *Proof.* From part (b) we know that $(A \Rightarrow B) = \neg A \vee B$ for all statements A and B. Substituting $A = P$ and $B = Q$ gives

$$(P \Rightarrow Q) = \neg P \vee Q,$$

and substituting $A = \neg Q$ and $B = \neg P$ gives

$$(\neg Q \Rightarrow \neg P) = \neg(\neg Q) \vee (\neg P) = Q \vee \neg P.$$

Since $\neg P \vee Q = Q \vee \neg P$ we conclude that $(P \Rightarrow Q) = (\neg Q \Rightarrow \neg P)$. $\square$

Problem 2. Practice with logical analysis.

(a) Use the results of Problem 1 to prove that for all statements P, Q, R we have

$$P \Rightarrow (Q \vee R) = (\neg Q \wedge \neg R) \Rightarrow \neg P.$$

Do **not** use a truth table.

(b) Use the result of (a) to prove that for all $a, b, c, d \in \mathbb{Z}$ we have

$$a + b \leq c + d \quad \Longrightarrow \quad a \leq c \quad \text{or} \quad b \leq d.$$

(c) Prove that the converse of the statement in part (b) is **false**. [Hint: To prove that a universal statement is false it is enough to provide a single counterexample.]

(a) *Proof.* For all statements P, Q, R we have

$$\begin{aligned} P \Rightarrow (Q \vee R) &= \neg(Q \vee R) \Rightarrow \neg P && \text{by 1(c)} \\ &= (\neg Q \wedge \neg R) \Rightarrow \neg P. && \text{by 1(a)} \end{aligned}$$

$\square$

(b) Let $a, b, c, d \in \mathbb{Z}$ and define the statements

$$\begin{aligned} P &= \text{“} a + b \leq c + d, \text{”} \\ Q &= \text{“} a \leq c, \text{”} \\ R &= \text{“} b \leq d. \text{”} \end{aligned}$$

I claim that $P \Rightarrow (Q \vee R)$. *Proof.* By part (a) it is enough to prove that $(\neg Q \wedge \neg R) \Rightarrow \neg P$. In other words, we will prove that

$$(a > c \text{ and } b > d) \quad \Longrightarrow \quad (a + b > c + d).$$

So let us assume that $a > c$ and $b > d$. By adding b to both sides of $a > c$ we obtain

$$\begin{aligned} a &> c \\ a + b &> b + c, \end{aligned}$$

and by adding c to both sides of $b > d$ we obtain

$$\begin{aligned} b &> d \\ b + c &> c + d. \end{aligned}$$

Then by the “transitivity” of the relation “$>$” we conclude that $a + b > c + d$. $\square$

(c) The statement from (b) says that

$$\forall a, b, c, d \in \mathbb{Z}, (a + b \leq c + d) \Longrightarrow (a \leq c \vee b \leq d).$$

and the **converse** of this statement says that

$$\forall a, b, c, d \in \mathbb{Z}, (a \leq c \vee b \leq d) \Longrightarrow (a + b \leq c + d).$$

To prove that the converse is **false** we will prove that the **opposite** of the converse is true. By applying de Morgan's law and the property $(P \not\Rightarrow Q) = \neg(P \Rightarrow Q) = P \wedge \neg Q$, the statement we want to prove is

$$\begin{aligned} &\neg\Big[\forall a, b, c, d \in \mathbb{Z}, (a \leq c \vee b \leq d) \Longrightarrow (a + b \leq c + d)\Big] \\ &= \exists a, b, c, d \in \mathbb{Z}, (a \leq c \vee b \leq d) \not\Longrightarrow (a + b \leq c + d) \\ &= \exists a, b, c, d \in \mathbb{Z}, (a \leq c \vee b \leq d) \wedge \neg(a + b \leq c + d) \\ &= \exists a, b, c, d \in \mathbb{Z}, (a \leq c \vee b \leq d) \wedge (a + b > c + d). \end{aligned}$$

In order to prove that such integers exist, it is enough to give one example. So let us choose $(a, b, c, d) = (1, 2, 1, 1)$. Then $(1 \leq 1 \vee 2 \leq 1)$ is a true statement because at least one of the statements $1 \leq 1$ and $2 \leq 1$ is true, and the statement $(1 + 2 > 1 + 1)$ is also true. $\square$

[Remark: It is okay for you to skip some of the logical analysis and jump right to the counterexample, but I wanted to show all the gory details for pedagogical reasons.]

Problem 3. I will guide you through an induction proof that

$$(a-1)\Big|(a^n-1) \quad \text{for all integers } a, n \in \mathbb{Z} \text{ such that } n \geq 1.$$

For the purpose of the proof, let $a \in \mathbb{Z}$ be a fixed integer. We will use induction on n.

(a) Prove that $(a-1)\big|(a^n-1)$ when $n=1$.
(b) Now assume that $(a-1)\big|(a^n-1)$ is true for some fixed $n \geq 1$. In this case, prove that

$$(a-1)\Big|(a^{n+1}-1).$$

(a) *Proof.* Since $(a-1) = (a-1)\cdot 1$ and $1 \in \mathbb{Z}$ we conclude that $(a-1)\big|(a-1)$. $\square$

(b) Fix a positive integer $n \geq 1$ and **assume** that $(a-1)\big|(a^n-1)$. By definition this means that there exists some $k \in \mathbb{Z}$ such that $(a^n-1) = (a-1)k$. Now multiply both sides of this equation by a to get

$$\begin{aligned} (a^n-1) &= (a-1)k \\ (a^{n+1}-a) &= (a-1)ak, \end{aligned}$$

and then add $(a-1)$ to both sides to get

$$\begin{aligned} (a^{n+1}-a) &= (a-1)ak \\ (a^{n+1}-a)+(a-1) &= (a-1)ak+(a-1) \\ (a^{n+1}-1) &= (a-1)(ak+1). \end{aligned}$$

Since $(ak+1) \in \mathbb{Z}$ we conclude that $(a-1)\big|(a^{n+1}-1)$ as desired. $\square$

[Remark: It follows, for example, that $58^{100}-1$ is a multiple of 57.]

Problem 4. For all integers $d \in \mathbb{Z}$ let us define the statement

$$P(d) := \text{“ } \forall n \in \mathbb{Z}, d|n^2 \Rightarrow d|n. \text{ ”}$$

(a) Now fix an integer $d \geq 2$ and prove that

$$P(d) \Longrightarrow \sqrt{d} \notin \mathbb{Q}$$

[Hint: Mimic the proofs from class when $d=2$ and $d=3$.]
(b) Prove that $P(5)$ is a true statement, and hence that $\sqrt{5}$ is irrational.
(c) Prove that $P(12)$ is a false statement. [Remark: It is still true that $\sqrt{12}$ is irrational, but the method of proof from part (a) will not work. Maybe you can see how to fix it.]

(a) *Proof that $P(d) \Rightarrow \sqrt{d} \notin \mathbb{Q}$.* Fix an integer $d \geq 2$ and let us assume that $P(d)$ is a true statement. In other words, let us assume that

$$(*) \qquad d|n^2 \Rightarrow d|n \quad \text{for all } n \in \mathbb{Z}.$$

In this case we will prove that $\sqrt{d} \notin \mathbb{Q}$. So let us **assume for contradiction** that $\sqrt{d} \in \mathbb{Q}$. Then we can write $\sqrt{d} = a/b$ where a and b are integers with no common factors other than ± 1. Now square both sides to get

$$\begin{aligned} d &= a^2/b^2 \\ db^2 &= a^2. \end{aligned}$$

Since $b^2 \in \mathbb{Z}$ this last equation implies that $d|b^2$ and then from $(*)$ we get $d|n$. In other words, we have $n = dk$ for some $k \in \mathbb{Z}$. Substituting into the previous equation gives

$$\begin{aligned} db^2 &= a^2 \\ db^2 &= (dk)^2 \\ db^2 &= d^2k^2 \\ b^2 &= da^2. \end{aligned}$$

Since $a^2 \in \mathbb{Z}$ this last equation tells us that $d|b^2$ and then from $(*)$ we get $d|b$. In summary, we have shown that $d|a$ and $d|b$, which contradicts the fact that a and b have no common factor. We conclude that $\sqrt{d} \in \mathbb{Q}$ is false, and hence $\sqrt{d} \notin \mathbb{Q}$. $\square$

But is the statement $P(d)$ true or false?

(b) $P(5)$ is true, hence it follows from part (a) that $\sqrt{5} \notin \mathbb{Q}$. *Proof.* For all $n \in \mathbb{Z}$ we want to show that $5|n^2$ implies $5|n$ and we will do this by showing the contrapositive statement:

$$5 \nmid n \Rightarrow 5 \nmid n^2.$$

So consider any $n \in \mathbb{Z}$ and assume that $5 \nmid n$. There are four cases:

- If $n = 5k + 1$ for some $k \in \mathbb{Z}$ then we have
$$n^2 = (5k+1)^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1.$$
- If $n = 5k + 2$ for some $k \in \mathbb{Z}$ then we have
$$n^2 = (5k+2)^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4.$$
- If $n = 5k + 3$ for some $k \in \mathbb{Z}$ then we have
$$n^2 = (5k+3)^2 = 25k^2 + 30k + 9 = 5(5k^2 + 6k + 1) + 4.$$
- If $n = 5k + 4$ for some $k \in \mathbb{Z}$ then we have
$$n^2 = (5k+4)^2 = 25k^2 + 40k + 16 = 5(5k^2 + 8k + 3) + 1.$$

In any case, we conclude that $5 \nmid n^2$. $\square$

(c) $P(12)$ is false. *Proof.* The opposite of the statement $P(12)$ is

$$\begin{aligned} \neg(\forall n \in \mathbb{Z}, 12|n^2 \Rightarrow 12|n) &= (\exists n \in \mathbb{Z}, 12|n^2 \not\Rightarrow 12|n) \\ &= (\exists n \in \mathbb{Z}, 12|n^2 \text{ but } 12 \nmid n). \end{aligned}$$

To prove the existence of such an integer $n \in \mathbb{Z}$ it is enough to take $n = 6$ and observe that

$$12 \,|\, 36 \qquad \text{but} \qquad 12 \nmid 6.$$

$\square$

Bonus Material. $\sqrt{12} \notin \mathbb{Q}$.

Proof. We already proved in class that $\sqrt{3} \notin \mathbb{Q}$ is irrational. Now assume for contradiction that $\sqrt{12} \in \mathbb{Q}$. This means we can write $\sqrt{12} = a/b$ for some integers $a, b \in \mathbb{Z}$. But then we have

$$\begin{aligned} \sqrt{12} &= a/b \\ 2\sqrt{3} &= a/b \\ \sqrt{3} &= a/(2b). \end{aligned}$$

Since a and $2b$ are integers this implies that $\sqrt{3} \in \mathbb{Q}$. Contradiction. $\square$

[Remark: Much later in the course we will see that $P(d)$ is a true statement for all integers d that have **no repeated prime factors**. Then by mimicking the proof of the case $d = 12$ it will follow that

$$\sqrt{d} \notin \mathbb{Z} \Rightarrow \sqrt{d} \notin \mathbb{Q} \qquad \text{for all integers } d \in \mathbb{Z}.$$

But you won't have to wait that long because there are easier ways to prove this.]