Reading Proofs 2

Below are proofs written by yourself and classmates for the week 12 homework assignment. Many of these proofs contain flaws, while others are correct. You goal is to find errors within proofs and correct them where appropriate. Many of these proofs have been altered slightly from their original version to combine different errors from different individuals.

Scattered throughout are claims and examples that may help you better understand some of the concepts from the assignment. Work through these exercises as you complete this sheet.

1.

Claim 1 (Exercise 6)**.** *Suppose* $x, y \in \mathbb{R}$. *Then* $x^3 + x^2y = y^2 + xy$ *if and only if* $y = x^2$ *or* $y = -x$.

Proof. Suppose $x, y \in \mathbb{R}$ and $x^3+x^2y = y^2+xy$. Rewriting we get $x^2(x+y) = y(y+x)$.

Divide both side by $x+y$ to get $x^2 = y$. Hence, when $x^3+x^2y = y^2+xy$, then $y = x^2$.

Conversely, let $x, y \in \mathbb{R}$ and $y = x^2$ or $y = -x$. If $y = x^2$ then consider

$$x^3 + x^2y = y^2 + xy$$

$$x^3 + x^2(x^2) = (x^2)^2 + x(x^2)$$

$$x^3 + x^4 = x^4 + x^3$$

Since this last equation is true, when $y = x^2$, then $x^3 + x^2y = y^2 + xy$.

Therefore, $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$. □

Proof. Suppose $x, y \in \mathbb{R}$ and $x^3 + x^2y = y^2 + xy$. Consider the following,

$$\begin{aligned} x^3 + x^2y &= y^2 + xy, \\ x^2(x + y) &= y(y + x), \\ x^2(x + y) - y(y + x) &= 0, \\ (x + y)(x^2 - y) &= 0. \end{aligned}$$

We can then solve for $x + y = 0$ and $x^2 - y = 0$ so that $y = -x$ or $y = x^2$. Thus, for $x^3 + x^2y = y^2 + xy$ to be true $y = -x$ or $y = x^2$.

Conversely, let $y = x^2$ or $y = -x$. Then $y - x^2 = 0$ or $y + x = 0$. We see that,

$$\begin{aligned}(y - x^2)(y + x) &= 0,\\ y^2 - x^2y + xy - x^3 &= 0\\ x^3 + x^2y &= y^2 + xy.\end{aligned}$$

Thus, if $y = x^2$ or $y = -x$, then $x^3 + x^2y = y^2 + xy$. Therefore, $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$. □

2.

Claim 2 (Exercise 8)**.** *Suppose* $a, b \in \mathbb{Z}$. *Prove that* $a \equiv b(\text{mod } 10)$ *if and only if* $a \equiv b(\text{mod } 2)$ *and* $a \equiv b(\text{mod } 5)$.

Proof. Suppose $a, b \in \mathbb{Z}$. Prove that if $a \equiv b(\text{mod } 10)$, then $a \equiv b(\text{mod } 2)$ and $a \equiv b(\text{mod } 5)$. By definition, $10|(a - b)$, thus

$$10k = a - b$$

$$5(2k) = a - b$$

$$2(5k) = a - b.$$

Therefore if $a \equiv b(\text{mod } 10)$ then $a \equiv b(\text{mod } 2)$ and $a \equiv b(\text{mod } 5)$.

Now prove that if $a \equiv b(\text{mod } 2)$ and $a \equiv b(\text{mod } 5)$ then $a \equiv b(\text{mod } 10)$. By definition, $2|(a-b)$ and $5|(a-b)$, thus $2k = a-b$ and $5m = a-b$. Let $k = 5p$, $p \in \mathbb{Z}$, then $2(5p) = a-b$, so $10p = a-b$. Let $m = 2n$, $n \in \mathbb{Z}$, then $5(2n) = a-b$, so $10n = a-b$. Therefore, $a \equiv b(\text{mod } 10)$ if and only if $a \equiv b(\text{mod } 2)$ and $a \equiv b(\text{mod } 5)$. □

3. The proof above (and many other submitted proofs) implicitly assumes the following claim. Determine if the following claim is true or false. Prove your answer in either case.

Claim 3. *Let $a, b, c \in \mathbb{Z}$. If $a|c$ and $b|c$ then $(ab)|c$.*

4.

Claim 4 (Exercies 10)**.** *If $a \in \mathbb{Z}$, then $a^3 \equiv a (\text{mod } 3)$.*

Proof. Let $a \in \mathbb{Z}$. Consider then $a^3 \equiv a(\text{ mod } 3)$. By definition of congruent modulo, $3|a^3 - a$. By definition of divides $3k = a^3 - a$. Notice that $3k = a(a^2 - 1)$. we can factor that so $3k = (a-1)a(a+1)$. By way of the division algorithm, $2b + c = n$ for $b, r, b \in \mathbb{Z}$. In this statement $0 \leq r < 3$ so we can have $3b + 0$, $3b + 1$ or $3b + 2$. We can rewrite $3b + 2$ as $3(b + 1) - 1$. Notice that we have a sequence of $b - 1$, b, and $b + 1$ that are all divisible by 3. Notice also we have a sequence of $a - 1$, a, and $a + 1$ that is also divisible by 3. Therefore, if $3k = (a-1)a(a+1)$ then $3|a^3 - a$ so $a^3 \equiv a(\text{mod } 3)$. □

5. Exercise 18 required that you provide a set X such that $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$. This seemed to cause more than a little confusion for much of the class. Complete the

following exercises to hopefully increase your understanding of the situation.

(a) Consider the sets $A = \{0, 1, 2\}$ and $B = \{0, \{1, 2\}\}$. List the elements of each set and the power set of each set. Is $A = B$?

(b) Many of you concluded in your homework that $\{0, \mathbb{N}\} = \{0, 1, 2, 3, \ldots\}$. What is wrong with this statement?

(c) Give a set X such that $\{1, 2\} \in X$ and $\{1, 2\} \subseteq X$.

6.

Claim 5. *Let $a, b, p \in \mathbb{Z}$ where p is prime. If $p|ab$ then $p|a$ or $p|b$.*

Proof. By way of contradiction, suppose $a, b, p \in \mathbb{Z}$, p is prime, $p|ab$, $p \nmid a$, and $p \nmid b$. If $\gcd(a, p) = 1$, notice that by Euclid's Lemma if $p|ab$ and $p \nmid a$, then $p|b$. If $\gcd(b, p) = 1$ and $p|ab$ and $p \nmid b$, then $p|a$. Therefore, if $a, b, p \in \mathbb{Z}$ where p is prime, and $p|ab$, then $p|a$ or $p|b$. □

Proof. Suppose $a, b, p \in \mathbb{Z}$ where p is prime and $p|ab$. We can deduce that p will be odd because it is prime and $p \neq 2$ and also that $pk = ab$ for $k \in \mathbb{Z}$. So $p = 2c + 1$ for $c \in \mathbb{Z}$. Notice that the $\gcd(p, a) = 1$ or p and $\gcd(p, b) = 1$ or p. The greatest common divisor would be p itself in the case that a or b is a multiple of p. Four our first case say that $\gcd(p, a) = 1$. So $1 = np + ma$ for $n, m \in \mathbb{Z}$. We can see that

$$pk = ab$$

$$pmk = amb$$

$$pmk = (1 - np)b$$

$$p(mk + nb) = b.$$

Because $mk + nb \in \mathbb{Z}$, $p|b$. If the $\gcd(p, b) = 1$, the same result would occur, and $p|a$. Now if $\gcd(p, a) = p$, then $p = lp + qa$ for $l, q \in \mathbb{Z}$. We can see that

$$pk = ab$$

$$pqk = aqb$$

$$pqk = (p - lp)b$$

$$p(qk + lb - b) = 1.$$

This would suggest that $p|1$. But the only integer that can divide 1 is 1 and -1. But p cannot be 1 or -1 because they aren't prime numbers. Therefore, we have shown this if $p|ab$ where p is prime, then $p|a$ or $p|b$. □

Proof. Let $a, b, p \in \mathbb{Z}$ where p is prime. Suppose $p|ab$. Because p is prime, $\text{gcp}(a, p) = 1$ or p.

Case 1: Suppose $\gcd(a, b) = 1$. We know that $p|ab$. Recall from claim 1, that if $a|(bc)$ and $\gcd(a, b) = 1$ then $a|c$. Thus if $p|(ab)$ and $\gcd(a, p) = 1$ then $p|b$.

Case 2: Suppose $\gcd(a, p) = p$. By definition of greatest common divisor, if $\gcd(a, p) = p$ the $p|a$.

Therefore, if $p|ab$ then $p|a$ or $p|b$. □