Homework 1

Aleck Zhao

September 16, 2016

Section 0.1: Proofs

2. (a) Prove by cases or provide a counterexample: If n is any integer, then $n^2 = 4k + 1$ for some integer k.

   Proof. This is a false statement. Let $n = 2m$ for $m \in \mathbb{Z}$. Then $n^2 = 4m^2 \neq 4k + 1$ for any $k \in \mathbb{Z}$. □

3. (c) Prove by contradiction and prove the converse or provide a counterexample: If a and b are positive numbers and $a \leq b$, then $\sqrt{a} \leq \sqrt{b}$.

   Proof. Assume the opposite, that $\sqrt{a} > \sqrt{b}$. Since square roots are non-negative, we may square both sides to get $a > b$, but we know $a \leq b$, which is a contradiction. Thus $\sqrt{a} \leq \sqrt{b}$, as desired.

   For the converse, we aim to show that if $\sqrt{a} \leq \sqrt{b}$, then $a \leq b$. Since square roots are non-negative, square both sides to get $a \leq b$, as desired. □

6. If p is a statement, let $\sim p$ denote the statement "not p," called the negation of p. Thus, $\sim p$ is true when p is false, and false when p is true. Show that if $\sim q \implies \sim p$, then $p \implies q$.

   Proof. For two statements a and b we have $a \implies b$ is always a true statement except in the case where a is true and b is false. If $\sim q \implies \sim p$ is true then there are three distinct possibilities:

   1. $\sim q$ is true and $\sim p$ is true.
   2. $\sim q$ is false and $\sim p$ is true.
   3. $\sim q$ is false and $\sim p$ is false.

   We tackle these by cases.

   Case 1: If $\sim q$ and $\sim p$ are both true, then q and p are both false, so $p \implies q$ is a true statement.

   Case 2: If $\sim q$ is false and $\sim p$ is true, then q is true and p is false, so $p \implies q$ is a true statement.

   Case 3: If $\sim q$ and $\sim p$ are both false, then q and p are both true, so $p \implies q$ is a true statement.

   Thus $\sim q \implies \sim p$ implies that $p \implies q$, as desired. □

Section 0.3: Mappings

5. (a) For $A \xrightarrow{\alpha} A$, show that $\alpha^2 = \alpha$ if and only if $\alpha(x) = x$ for all $x \in \alpha(A)$.

Proof. If $\alpha(x) = x$ for all $x \in \alpha(A)$, then $(\alpha \circ \alpha)(x) = x = \alpha(x)$, so $\alpha^2 = \alpha$, as desired.

For the other direction, if $\alpha^2 = \alpha$, then $(\alpha \circ \alpha)(x) = \alpha(\alpha(x)) = \alpha(x)$. Let $y = \alpha(x) \in \alpha(A)$, thus $\alpha(y) = y$ for all $y \in \alpha(A)$, as desired. $\square$

(b) If $A \xrightarrow{\alpha} A$ satisfies $\alpha^2 = \alpha$, show that α is surjective if and only if α is injective. Describe α in this case.

Proof. If α is surjective, then for all $a' \in A$, there exists $a \in A$ such that $\alpha(a) = a'$. We know that $\alpha(\alpha(a)) = \alpha(a)$ for all $a \in A$, so we can rewrite this as $\alpha(a') = a'$ for all $a' \in A$. Then if we have $\alpha(a') = \alpha(a^*)$, that means $a' = a^*$, so α is injective, as desired.

If α is injective, then whenever $\alpha(a') = \alpha(a^*)$, it must be true that $a' = a^*$. Assume that $\alpha``(A)$ the image of A under α is not all of A. Since not all elements are mapped to, there must exist some element $a \in A$ that is the image of more than a single element in A. This is a contradiction since we know α is injective, that distinct elements of A map to distinct elements of A. Thus $\alpha``(A)$ is in fact all of $A$. We know that $\alpha(\alpha(a)) = \alpha(a)$ for all $a \in A$. Let $y = \alpha(a) \in \alpha``(A)$, then we $\alpha(y) = y$. Since $\alpha``(A) = A$, it follows that α is surjective since for any $y \in A$, we know $\alpha(y) = y$, as desired.

In this case, we have $\alpha(a) = a$ for all $a \in A$. $\square$

(c) Let $A \xrightarrow{\beta} B \xrightarrow{\gamma} A$ satisfy $\gamma\beta = 1_A$. If $\alpha = \beta\gamma$, show that $\alpha^2 = \alpha$.

Proof. We have

$$\begin{aligned} \alpha^2 &= (\beta\gamma)(\beta\gamma) = \beta(\gamma\beta)\gamma \\ &= \beta \circ 1_A \circ \gamma = \beta\gamma = \alpha, \end{aligned}$$

as desired. $\square$

8. Let $A \xrightarrow{\alpha} B \xrightarrow{\beta} A$ satisfy $\beta\alpha = 1_A$. If either α is surjective or β is injective, show that each of them is invertible and that each of them is the inverse of the other.

Proof. We wish to show that $\alpha\beta = 1_B$, which combined with the fact that $\beta\alpha = 1_A$ will show that α and β are inverses of each other.

If α is surjective, then for any $b \in B$ there exists $a \in A$ such that $\alpha(a) = b$. Since $\beta(\alpha(a)) = a$, that means $\alpha(\beta(\alpha(a))) = \alpha(a), \forall a \in A$ since α is well-defined. Then we let $\alpha(a) = b^* \in B$, so that $\alpha(\beta(b^*)) = b^*$. Because α is surjective, any value of b^* must have at least a single $a \in A$ such that $\alpha(a) = b^*$, thus $\alpha(\beta(b^*)) = b^*$ holds for all $b^* \in B$, so $\alpha\beta = 1_B$, as desired.

We know that $\beta(\alpha(a)) = a$ for all $a \in A$, which means that the image $\beta``(B)$ is actually all of A, so then β is surjective as well, and therefore bijective if β is also injective. It is a theorem that a bijective mapping always has an inverse, so denote β^{-1} to be the inverse of β. Then we have $\beta^{-1}(\beta(\alpha(a))) = (\beta^{-1} \circ \beta)(\alpha(a)) = \alpha(a) = \beta^{-1}(a)$ for all $a \in A$, thus $a = \beta^{-1}$, so $a\beta = 1_B$, as desired. $\square$

Section 0.4: Equivalences

1. In each case, decide whether the relation $\equiv$ is an equivalence on A. If it is, describe the equivalence classes.

   (e) $A = \mathbb{N}; a \equiv b$ means that $b = ka$ for some integer k.

   Solution. $\equiv$ is not an equivalence because it is not symmetric:

   $$a \equiv b \implies b = ka$$

   but then $a = \frac{1}{k}b$, so $b \not\equiv a$, since $\frac{1}{k} \notin \mathbb{N}$.

   □

   (h) $A = \mathbb{R} \times \mathbb{R}; (x, y) \equiv (x_1, y_1)$ means that $x^2 + y^2 = x_1^2 + y_1^2$.

   Solution. $\equiv$ is an equivalence relation because it satisfies:

   1. Reflexivity: $(x, y) \equiv (x, y)$ since $x^2 + y^2 = x^2 + y^2$.
   2. Symmetry: $(x, y) \equiv (x_1, y_1)$ means $x^2+y^2 = x_1^2+y_1^2$, so then $(x_1, y_1) \equiv (x, y)$ since $x_1^2+y_1^2 = x^2+y^2$.
   3. Transitivity: If $(x, y) \equiv (a, b)$, and $(a, b) \equiv (p, q)$, then $x^2 + y^2 = a^2 + b^2$ and $a^2 + b^2 = p^2 + q^2$, so then $x^2 + y^2 = p^2 + p^2$, so $(x, y) \equiv (p, q)$.

   The equivalence classes are concentric circles around the origin.

   □

3. (d) $A = \mathbb{R}^+ \times \mathbb{R}^+; (x, y) \equiv (x_1, y_1)$ means that $y/x = y_1/x_1; B = \{x \in \mathbb{R} \,|\, x > 0\}$. Show that $\equiv$ is an equivalence on A and find a (well-defined) bijection $\sigma : A_\equiv \to B$.

   Proof. $\equiv$ is an equivalence relation because it satisfies:

   1. Reflexivity: $(x, y) \equiv (x, y)$ since $y/x = y/x$.
   2. Symmetry: $(x, y) \equiv (x_1, y_1)$ means $y/x = y_1/x^1$, so then $(x_1, y_1) \equiv (x, y)$ since $y_1/x_1 = y/x$.
   3. Transitivity: If $(x, y) \equiv (a, b)$, and $(a, b) \equiv (p, q)$, then $y/x = b/a$ and $b/a = q/p$, so then $y/x = q/p$ so $(x, y) \equiv (p, q)$.

   The equivalence classes are the lines $y = kx$ for $k \in \mathbb{R}^+$, so σ can map these lines to the value k of their slope. This is well-defined and bijective because each line only gets mapped to a single value corresponding to its slope, and the slope uniquely determines the line. Specifically, $\sigma([x, y]) = y/x$ is the mapping.

   □

6. Let $\equiv$ and $\sim$ be two equivalences on the same set A.

   (a) If $a \equiv a_1$ implies that $a \sim a_1$, show that each $\sim$ equivalence class is partitioned by the $\equiv$ equivalence classes it contains.

   Proof. Since $\equiv$ equivalence classes already partition A, it suffices to prove that any equivalence class $[a]$ under $\equiv$ cannot be part of more than equivalence class under $\sim$. Let $[a]_\equiv$ represent an equivalence class generated by a under $\equiv$, and similarly for $[a]_\sim$.

   If $[a]_\equiv$ only has a single element a, then it can only be part of a single equivalence class under $\sim$. Otherwise, consider two elements $x, y \in [a]_\equiv$. That means $x \equiv a \implies x \sim a$, and $y \equiv a \implies y \sim a$. That means $x \in [a]_\sim$ and $y \in [a]_\sim$, so any two elements in an equivalence class under $\equiv$ are always in the same equivalence class under $\sim$. Thus any $[a]_\equiv$ is fully contained within $[a]_\sim$, so $\equiv$ equivalence classes partition the $\sim$ equivalence classes, as desired.

   □

(b) Define $\cong$ on A by writing $a \cong a_1$ if an only if both $a \equiv a_1$ and $a \sim a_1$. Show that $\cong$ is an equivalence and describe the $\cong$ equivalence classes in terms of the $\equiv$ and $\sim$ equivalence classes.

Proof. We show that $\cong$ is an equivalence relation because it satisfies:

1. Reflexivity: $a \cong a$ because $a \equiv a$ and $a \sim a$ since $\equiv$ and $\sim$ are equivalence relations and therefore reflexive.
2. Symmetry: If $a \cong b$, that means $a \equiv b$ and $a \sim b$, so then since $\equiv$ and $\sim$ are equivalence relations and therefore symmetric, we have $b \equiv a$ and $b \sim a$, thus $b \cong a$.
3. Transitivity: If $a \cong b$ and $b \cong c$, that means $a \equiv b, a \sim b$, and $b \equiv c, b \sim c$, so since $\equiv$ and $\sim$ are equivalence relations and therefore transitive, we have $a \equiv c, a \sim b$, thus $a \cong c$.

A $\cong$ equivalence class is the set of elements such that all elements in the set are equivalent under both $\equiv$ and $\sim$.

□

7. In each case, determine whether $\alpha : \mathbb{Q}^+ \to \mathbb{Q}$ is well defined.

(a) $\alpha\left(\frac{n}{m}\right) = n$

Solution. This is $\boxed{\text{not well defined}}$ since $\alpha(1/2) = 1$ and $\alpha(2/4) = 2$, but $1/2 = 2/4$.

□

(b) $\alpha\left(\frac{n}{m}\right) = \frac{n-m}{n+m}$

Solution. This is $\boxed{\text{well defined.}}$ We wish to show that if $n/m = a/b$ then $\alpha\left(\frac{n}{m}\right) = \frac{n-m}{n+m} = \frac{a-b}{a+b} = \alpha\left(\frac{a}{b}\right)$. Cross multiplying, this is equivalent to

$$\begin{aligned}(n-m)(a+b) &= (n+m)(a-b)\\ an - am + bn - bm &= an + am - bn - bm\\ 2bn &= 2am\\ \frac{n}{m} &= \frac{a}{b},\end{aligned}$$

which is true, as desired.

□

(c) $\alpha\left(\frac{n}{m}\right) = m + n$

Solution. This is $\boxed{\text{not well defined}}$ since $\alpha(1/2) = 1 + 2 = 3$ but $\alpha(2/4) = 2 + 4 = 6$.

□

(d) $\alpha\left(\frac{n}{m}\right) = \frac{5m+7n}{3n+m}$

Solution. This is $\boxed{\text{well defined.}}$ Similarly to part (b), we wish to show that if $n/m = a/b$, then $\alpha\left(\frac{n}{m}\right) = \frac{5m+7n}{3n+m} = \frac{5b+7a}{3a+b} = \alpha\left(\frac{a}{b}\right)$. Cross multiplying, this is equivalent to

$$\begin{aligned}(5m+7n)(3a+b) &= (5b+7a)(3n+m)\\ 15am + 5bm + 21an + 7bn &= 15bn + 5bm + 21an + 7am\\ 8am &= 8bn\\ \frac{a}{b} &= \frac{n}{m}\end{aligned}$$

which is true, as desired. □

9. For a mapping $\alpha : A \to B$, let $\equiv$ denote the kernel equivalence of α and let $\varphi : A \to A_{\equiv}$ denote the natural mapping. Define $\sigma : A_{\equiv} \to B$ by $\sigma([a]) = \alpha(a)$ for all equivalence classes $[a]$ in $A_{\equiv}$.

(a) Show that σ is well defined and injective, surjective if α is surjective.

Proof. σ is well defined if and only if $\sigma([a]) = \sigma([b])$ whenever $[a] = [b]$; this just means an element in the pre-image only gets mapped to a single unique element in the image.

If $[a] = [b]$, then for any $x \in [a]$ we have $x \in [b]$ as well, so $x \equiv a$ and $x \equiv b$, which means $a \equiv b$. Thus, $\alpha(a) = \alpha(b)$ since $\equiv$ is the kernel equivalence. Therefore $\sigma([a]) = \alpha(a) = \alpha(b) = \sigma([b])$, so σ is well defined, as desired.

σ is injective if and only if $[a] = [b]$ whenever $\sigma([a]) = \sigma([b])$. If $\sigma([a]) = \sigma([b])$, that means $\sigma([a]) = \alpha(a) = \alpha(b) = \sigma([b])$. Since $\equiv$ is the kernel equivalence, that means $a \equiv b$. Given some $x \in [a] \implies x \equiv a$, that means $x \equiv b$, so $x \in [b]$, thus $[a] \subset [b]$ and similarly $[b] \subset [a]$, so in fact $[a] = [b]$, thus σ is injective, as desired.

σ is surjective if and only if for all $b \in B$, there exists an equivalence class $[a] \in A_{\equiv}$ such that $\sigma([a]) = b$. We have $\sigma([a]) = \alpha(a)$ for all $[a] \in A_{\equiv}$. If α is surjective, then for all $b \in B$, there exists an $a \in A$ such that $\alpha(a) = b$. Since φ is surjective, for any $[a]$ there exists $a \in A$ such that $\varphi(a) = [a]$, so it follows that for any b, there exists an a and therefore an $[a]$ such that $\sigma([a]) = b$, thus σ is surjective, as desired.

$\square$

(b) Show that $\alpha = \sigma\varphi$, so that α is the composite of a surjective mapping followed by an injective mapping.

Proof. We wish to show that $\alpha(a) = \sigma(\varphi(a))$ for all $a \in A$. We have $\varphi(a) = [a]$ for all $a \in A$ by the natural mapping, then $\sigma([a]) = \alpha(a)$ so $\sigma(\varphi(a)) = \alpha(a)$, thus $\sigma\varphi = \alpha$, as desired.

$\square$

(c) If $\alpha(A)$ is a finite set, show that the set $A_{\equiv}$ of equivalence classes is also finite and that $|A_{\equiv}| = |\alpha(A)|$.

Proof. Suppose the image $\alpha``(A)$ has $k \in \mathbb{N}$ elements $b_1, b_2, \cdots, b_k$ that are all distinct. Assume there are infinitely many equivalence classes, $[a_i]$. Consider the equivalence class $[a_1]$. Then for any $a_1 \in [a_1]$, without loss of generality (WLOG) assume that $\alpha(a_1) = b_1$, where all elements in the equivalence class map to the same image by the definition of the equivalence class. Then without loss of generality assume that $\alpha(a_i) = b_i$ for $a_i \in [a_i]$, with $i = 1, 2, \cdots, k$. All of these equivalence classes are disjoint, and actually equivalence classes since b_i are all distinct.

Next consider $a_{k+1} \in [a_{k+1}]$. We know that $\alpha(a_{k+1})$ must map to one of $b_1, b_2, \cdots, b_k$, WLOG let $\alpha(a_{k+1}) = b_1$. But then $a_{k+1} \in [a_1]$ from earlier, but equivalence classes are disjoint, so this is a contradiction. By induction, any $[a_j]$ where $j > k$ cannot exist disjoint from all $[a_i], i = 1, 2, \cdots, k$, so $A_{\equiv}$ is finite, as desired.

In fact, there are exactly as many equivalence classes as elements of $\alpha``(A)$ by the construction above, so $|A_{\equiv}| = |\alpha``(A)|$, as desired.

$\square$

(d) In each case, find $|A_{\equiv}|$ for the given mapping α.

(i) $A = U \times U$ with $U = \{1, 2, 3, 4, 6, 12\}$, $\quad \alpha : A \to \mathbb{Q}$ defined by $\alpha(n, m) = n/m$.

Solution. The set $A_{\equiv}$ is the set of distinct rational numbers we may form with any two elements in U. These are

$$\left\{1, 2, 3, 4, 6, 12, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}, \frac{1}{12}, \frac{3}{2}, \frac{4}{3}, \frac{2}{3}, \frac{3}{4}\right\}$$

so $|A_{\equiv}| = \boxed{15.}$.

$\square$

(ii) $A = \{n \in \mathbb{Z} \,|\, 1 \leq n \leq 99\}$, $\alpha : A \to \mathbb{N}$ defined by $\alpha(n) =$ the sum of the digits of n.

Solution. The equivalence classes are the distinct values of $\alpha(n)$. The minimum value of $\alpha(n)$ is 1, achieved at $n = 1$ or $n = 10$, and the maximum is 18, achieved when $n = 99$. Since every value in between can be achieved (we won't show this explicitly), $|A_{\equiv}| = \boxed{18.}$

$\square$

10. Let $A = \{\alpha \,|\, \alpha : P \to Q \text{ is a mapping}\}$. Given $p \in P$, define $\equiv$ on A by $\alpha \equiv \beta$ if $\alpha(p) = \beta(p)$.

(a) Show that $\equiv$ is an equivalence on A.

Proof. $\equiv$ is an equivalence relation because it satisfies:

1. Reflexivity: $\alpha \equiv \alpha$ because $\alpha(p) = \alpha(p)$.
2. Symmetry: If $\alpha \equiv \beta$, then $\alpha(p) = \beta(p)$ so $\beta(p) = \alpha(p)$ and thus $\beta \equiv \alpha$.
3. Transitivity: If $\alpha \equiv \beta$ and $\beta \equiv \gamma$, then $\alpha(p) = \beta(p)$ and $\beta(p) = \gamma(p)$, so then $\alpha(p) = \gamma(p)$ and thus $\alpha \equiv \gamma$.

$\square$

(b) Find a mapping $\lambda : A \to Q$ such that $\equiv$ is the kernel equivalence of λ.

Solution. Fix some $p^* \in P$. then let $\lambda(\alpha) = \alpha(p^*) \in Q$ for all $\alpha \in A$. If $\alpha_1 \equiv \alpha_2$, then $\alpha_1(p) = \alpha_2(p)$ for any $p \in P$, so $\lambda(\alpha_1) = \alpha_1(p^*) = \alpha_2(p^*) = \lambda(\alpha_2)$. Thus, $\equiv$ is the kernel equivalence of λ as desired.

$\square$

(c) If $|Q| = n$, how many equivalence classes does $\equiv$ have?

Solution. There are $\boxed{\text{at most } n}$ equivalence classes, one for each distinct element of Q. If α is not surjective, then there are fewer than n.

$\square$