

Name: ANSWER KEY

Be sure to show your work!

1. (20 points) Memorization

(a) Let T be a (non-empty) set with relation $<$. What properties must $(T, <)$ possess so that it is *totally ordered* (i.e. simply ordered)? Don't just state these properties. Define the properties themselves – give details!

- **Irreflexive:** For all $a \in T$ we have $a \not< a$.
- **Transitive:** For all $a, b, c \in T$ such that $a < b$ and $b < c$ we have $a < c$.
- **Comparability:** For all $a, b \in T$ exactly one of the following holds: $a < b$, $b < a$, or $a = b$.

There are many other equivalent ways to characterize a total order. This is just one possible set of axioms.

If we use a partial ordering \leq (related to the above characterization by $x \leq y$ iff $x < y$ or $x = y$), then we can define a totally order set as a set with a relation which is (1) **Reflexive:** $x \leq x$ for all $x \in X$, (2) **Anti-symmetric:** $x \leq y$ and $y \leq x$ implies $x = y$, (3) **Transitive:** $x \leq y$ and $y \leq z$ implies $x \leq z$, and (3) **Comparable:** either $x \leq y$ or $y \leq x$ for all $x, y \in X$.

(b) State *Zorn's Lemma*.

Zorn's lemma states: Let X be a set partially ordered by \leq . Suppose that every chain in X (i.e. every totally ordered subset) has an upper bound (i.e. if $C \subseteq X$ is a chain, then there exists some $b \in X$ such that $c \leq b$ for all $c \in C$). Then X has a maximal element (i.e. there is some $m \in X$ such that if $x \in X$ and $m \leq x$, then $m = x$).

Or we can restate this in terms of strict partial orders: Let X be set strictly partially ordered by $<$. Suppose that every chain in X (i.e. every totally ordered subset) has an upper bound (i.e. if $C \subseteq X$ is a chain, then there is some $b \in X$ such that $c < b$ or $c = b$ for every $c \in C$). Then X has a maximal element (i.e. there is some $m \in X$ such that for all $x \in X$, we never have $m < x$).

2. (20 points) A few proofs

(a) Let $f : X \rightarrow Y$ and suppose that $A, B \subseteq Y$. Show that $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

$$x \in f^{-1}(A \cap B) \iff f(x) \in A \cap B \iff f(x) \in A \text{ and } f(x) \in B \iff x \in f^{-1}(A) \text{ and } x \in f^{-1}(B) \iff x \in f^{-1}(A) \cap f^{-1}(B)$$

(b) Let $f : X \rightarrow Y$ and suppose that $A, B \subseteq X$. Show that $f(A \cap B) \subseteq f(A) \cap f(B)$.

Suppose $y \in f(A \cap B)$ then there exists some $x \in A \cap B$ such that $f(x) = y$. But then $x \in A$ and $x \in B$ so that $y = f(x) \in f(A)$ and $y = f(x) \in f(B)$. Therefore, $y \in f(A) \cap f(B)$.

(c) Let $A_i \subseteq X$ for all $i \in I$ and $B \subseteq X$. Show that $\left(\bigcup_{i \in I} A_i\right) \cap B = \bigcup_{i \in I} (A_i \cap B)$.

Note: I is an arbitrary non-empty index set. Do not assume it is finite or countable.

$$\begin{aligned} x \in \left(\bigcup_{i \in I} A_i\right) \cap B &\iff x \in \bigcup_{i \in I} A_i \text{ and } x \in B \iff x \in A_j \text{ for some } j \in I \text{ and } x \in B \iff x \in A_j \cap B \text{ for} \\ \text{some } j \in J &\iff x \in \bigcup_{i \in I} (A_i \cap B) \end{aligned}$$

3. (20 points) A proofs about functions.

(a) Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$ are injections. Show that $g \circ f : A \rightarrow C$ is an injection as well.

Suppose $(g \circ f)(x) = (g \circ f)(y)$. So $g(f(x)) = g(f(y))$. Thus $f(x) = f(y)$ since g is injective. Thus $x = y$ since f is injective. Therefore, $g \circ f$ is injective.

(b) Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$ are surjections. Show that $g \circ f : A \rightarrow C$ is a surjection as well.

Suppose $c \in C$. Then there exists some $b \in B$ such that $g(b) = c$ since g is surjective. Consider $b \in B$. There exists some $a \in A$ such that $f(a) = b$ since f is surjective. Therefore, $(g \circ f)(a) = g(f(a)) = g(b) = c$. Thus $g \circ f$ is surjective.

(c) Prove that $|\mathcal{P}(X)| = |2^X|$ where $\mathcal{P}(X)$ is the power set of X and 2^X is the set of all functions from X to $\{0, 1\}$. Do not assume anything about the set X (it could be finite, infinite, or even empty).

Given $A \subseteq X$, we can define its **characteristic function** $\chi_A : X \rightarrow \{0, 1\}$ as follows: $\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$

Consider $\psi : \mathcal{P}(X) \rightarrow 2^X$ where $\psi(A) = \chi_A$. If we can show that ψ is a bijection, we'll have that $|\mathcal{P}(X)| = |2^X|$.

Suppose $\psi(A) = \psi(B)$. This means that $\chi_A = \chi_B$. By definition: $x \in A \iff \chi_B(x) = \chi_A(x) = 1 \iff x \in B$. Thus $A = B$ so that ψ is injective.

Suppose that $f \in 2^X$. Consider $A = f^{-1}\{1\}$ (which is a subset of the domain of $f = X$). Consider $x \in A$ (i.e. $\chi_A(x) = 1$), then $x \in f^{-1}\{1\}$ so that $f(x) = 1$. Thus $\chi_A(x) = 1 = f(x)$. Now suppose $x \notin A$ (i.e. $\chi_A(x) = 0$). Then $x \notin f^{-1}\{1\}$ so that $f(x) \neq 1$. Since $f(x)$ must be either 1 or 0, we have $f(x) = 0$. Thus $\chi_A(x) = 0 = f(x)$. Therefore, $\chi_A(x) = f(x)$ for all $x \in X$. Thus $\chi_A = f$. We have shown that $\psi(A) = \chi_A = f$. Therefore, ψ is surjective.

4. (20 points) Put the following sets in order from smallest to largest. Use $<$ and $=$ to indicate relationships.

For example: $|A| = |B| < |C| < |D| = |E| = |F| = |G|$. [By the way, this is not the correct answer.] Justify your answer!

- $A = \{n \in \mathbb{Z} \mid n \text{ is even and } n < -999\}$
- $B = \{x \in \mathbb{C} \mid x \text{ is a solution of } x^{15} - \sqrt{6}x^9 + 4x^8 - x^5 + 17x + \pi = 0\}$
- $C = \mathcal{P}(B)$
- $D = \mathbb{R}^{\mathbb{Z}}$ (functions from \mathbb{Z} to \mathbb{R})
- $E = \mathbb{R}^{\mathbb{R}}$ (functions from \mathbb{R} to \mathbb{R})
- $F = \{X \subseteq \mathbb{Z} \mid X \text{ is not finite}\}$
- $G = \mathbb{Q} \times \mathbb{Q}$

Let's analyze each of these sets. [I have included a lot more detail than I required anyone to show on their test.]

- $A = \{-1000, -1002, -1004, \dots\}$ is clearly countable (i.e. $|A| = |\mathbb{Z}|$).
- Non-zero polynomials with coefficients in \mathbb{C} (or any field or more generally any integral domain) have no more roots than their degrees. So the equation " $x^{15} - \sqrt{6}x^9 + 4x^8 - x^5 + 17x + \pi = 0$ " has no more than 15 solutions. [In fact, it can be shown that this equation has *exactly* 15 solutions, but this isn't important here.] Therefore, $|B| \leq 15$ (i.e. B is finite).
- One of Cantor's famous theorems (which we proved in class) shows that $|X| < |\mathcal{P}(X)|$ for any set (finite or infinite). Therefore, $|B| < |\mathcal{P}(B)| = 2^{|B|} \leq 2^{15}$ (i.e. C is finite, yet strictly bigger than B and again (un-importantly) it can be shown $|C| = 2^{15}$ precisely).
- The real numbers have the same cardinality as the power set of the integers (this is known as the cardinality of the *continuum*), so $|\mathbb{R}| = |\mathcal{P}(\mathbb{Z})| = 2^{|\mathbb{Z}|}$. Thus $|\mathbb{R}^{\mathbb{Z}}| = (2^{|\mathbb{Z}|})^{|\mathbb{Z}|} = 2^{|\mathbb{Z}| \times |\mathbb{Z}|} = 2^{|\mathbb{Z}|} = |\mathbb{R}|$ by a cardinal exponent law and the fact that $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$ (finite cartesian products of infinite sets take on the maximum cardinality of the sets being producted). In summary, $|D| = |\mathbb{R}|$ (continuum sized). Also, $|D| = |\mathcal{P}(\mathbb{Z})| > |\mathbb{Z}| = |A|$
- $|\mathbb{R}^{\mathbb{R}}| = (2^{|\mathbb{Z}|})^{|\mathbb{R}|} = 2^{|\mathbb{Z}| \times |\mathbb{R}|} = 2^{|\mathbb{R}|} = |\mathcal{P}(\mathbb{R})|$. So $|E| = |\mathcal{P}(\mathbb{R})| > |\mathbb{R}| = |D|$.
- One of our homework problems showed that $Y = \{X \subseteq \mathbb{Z} \mid X \text{ is finite}\}$ is a countable set (i.e. $|Y| = |\mathbb{Z}|$). Notice that F is its complement: $F = \mathcal{P}(\mathbb{Z}) - Y$. Therefore, $F \cup Y = \mathcal{P}(\mathbb{Z})$. So $|F| + |Y| = |\mathbb{R}|$. But Y is countable and addition of infinite cardinals is the same as taking the maximum of the two cardinals, so $|\mathbb{R}| = \max\{|F|, |Y|\} = \max\{|F|, |\mathbb{Z}|\} = |F|$.
- Recall that \mathbb{Q} (the set of rational numbers) is countable. Therefore, $|G| = |\mathbb{Q} \times \mathbb{Q}| = |\mathbb{Q}| = |\mathbb{Z}| = |A|$.

$$\begin{array}{ccccccc}
 |B| < |C| & < & |A| = |G| & < & |D| = |F| & < & |E| \\
 \text{finite} & & \text{countably infinite} & & \text{continuum} & & \text{powerset of continuum}
 \end{array}$$

5. (20 points) Everyone's favorite...True, Possible, or False?! If a statement is always true, prove that it is always true. If a statement is always false, show that it cannot be true. If a statement is true in some cases and false in others, give an example of it holding and an example of it failing to hold.

(a) Let $X \subseteq \{n \in \mathbb{N} \mid n \text{ is prime}\}$.

Is it True / Possible / False that $\emptyset \in \mathcal{P}(X)$ and $\emptyset \subseteq \mathcal{P}(X)$?

This is true of **any** powerset! The empty set is a subset of every set: $\emptyset \subseteq Y$ (no matter what set Y is). Why? For $A \subseteq B$ to hold, every element of A must also belong to B . The empty set has no elements, so (quite vacuously - pun intended) every element of \emptyset (all none of them) belong to Y thus $\emptyset \subseteq Y$.

Thus $\emptyset \subseteq \mathcal{P}(X)$ and $\emptyset \subseteq X$. Next, because $\emptyset \subseteq X$, we have $\emptyset \in \mathcal{P}(X)$ (the empty set is one of the subsets of X).

(b) Let $X \subseteq \mathbb{R}$ and $f : X \rightarrow X$ be defined by $f(x) = 2x$.

Is it True / Possible / False that f is onto?

If $X = \mathbb{R}$, then f is onto. Since given $y \in \mathbb{R}$, then $x = y/2 \in \mathbb{R}$ and $f(x) = 2x = 2(y/2) = y$.

On the other hand, if $X = \mathbb{Z}$, then f is not onto. Since, for example, 1 is not in the range of f . Why? Suppose $f(x) = 1$. Then $2x = 1$ and so $x = 1/2 \notin \mathbb{Z}$. Therefore, nothing in $X = \mathbb{Z}$ maps to $1 \in X = \mathbb{Z}$. Therefore, f is not onto. [More briefly: If $X = \mathbb{Z}$, then the range of f is (by the definition of even) the set of even integers. So clearly f is not onto.]

(c) Let X be a set.

Is it True / Possible / False that $\mathcal{P}(X)$ is countably infinite?

Recall that Cantor's theorem says that $|X| < |\mathcal{P}(X)|$ for any set X . If X is finite, say $|X| = n$, then $|\mathcal{P}(X)| = 2^{|X|} = 2^n$. Thus $\mathcal{P}(X)$ is also finite. If X is countable, then $\mathcal{P}(X)$ must be uncountable since $|\mathcal{P}(X)| > |X| = |\mathbb{Z}|$. Furthermore, if X is uncountable (i.e. $|X| > |\mathbb{Z}|$), then $|\mathcal{P}(X)| > |X| > |\mathbb{Z}|$ and so $\mathcal{P}(X)$ is also uncountable.

This shows that $\mathcal{P}(X)$ is either finite or uncountable, but it can *never* be countably infinite.

(d) Let $\prod_{i \in I} B_i \subseteq \prod_{i \in I} A_i$ (Recall that $\Pi =$ cartesian product)

Is it True / Possible / False that $B_i \subseteq A_i$ for all $i \in I$?

This is kind of tricky. With a (small) additional assumption it is true. But first the (technically accurate) answer.

This can be true. For example: If $I = \{1, 2\}$ and $A_1 = A_2 = B_1 = B_2 = \mathbb{Z}$, then clearly $B_1 \times B_2 = \mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z} = A_1 \times A_2$. Also, $B_i = \mathbb{Z} \subseteq \mathbb{Z} = A_i$ for $i = 1, 2$. [A very silly example. We could, of course, get much more creative.]

This can also fail to be true. For example: Let $I = \{1, 2\}$. Let $B_1 = \emptyset$, $B_2 = \mathbb{R}$, $A_1 = \mathbb{Z}$, and $A_2 = \emptyset$. Then $B_1 \times B_2 = \emptyset \times \mathbb{R} = \emptyset \subseteq \emptyset = \mathbb{Z} \times \emptyset = A_1 \times A_2$. Notice that even though $B_1 \times B_2 \subseteq A_1 \times A_2$, we have $B_2 = \mathbb{R} \not\subseteq \emptyset = A_2$.

Note: Why is $\emptyset \times X = \emptyset$? Recall that $\emptyset \times X = \{(a, b) \mid a \in \emptyset \text{ and } b \in X\}$ since " $a \in \emptyset$ " is never true (the empty set is *empty*), the condition required of (a, b) cannot hold. Thus there is nothing in this cartesian product. More generally,

$\prod_{i \in I} B_i$ is empty if any of the B_i 's is empty. [The converse: " B_i non-empty for all i implies $\prod_{i \in I} B_i$ is non-empty" is essentially the statement of the axiom of choice.]

Now what if we rule out the (kind of odd) case where some B_i is empty? Then this is true.

Suppose $\prod_{i \in I} B_i \subseteq \prod_{i \in I} A_i$ and $B_i \neq \emptyset$ for all $i \in I$.

Select some $k \in I$ and let $x \in B_k$. Since $B_i \neq \emptyset$ for all $i \in I$, we may select $y_i \in B_i$ for each $i \in I$ (here we used the axiom of choice). Define $\mathbf{x} \in \prod_{i \in I} B_i$ by letting $\mathbf{x}_j = y_j (\in B_j)$ for all $j \in I$ such that $j \neq k$ and letting $\mathbf{x}_k = x (\in B_k)$.

By assumption, $\prod_{i \in I} B_i \subseteq \prod_{i \in I} A_i$ so that $\mathbf{x} \in \prod_{i \in I} A_i$. This means that $\mathbf{x}_j \in A_j$ for all $j \in I$. In particular, $x = \mathbf{x}_k \in A_k$. Therefore, $B_k \subseteq A_k$ for all $k \in I$.

6. (30 points) Rework the test. [See above. ☺]

7. (10 points) [5710 – Grad Problem] Let \mathcal{A} be a well-ordered set. Let $\mathcal{A}_0 \subseteq \mathcal{A}$. We say \mathcal{A}_0 is *inductive* if for every $\alpha \in \mathcal{A}$ we have that $S_\alpha = \{\beta \in \mathcal{A} \mid \beta < \alpha\} \subseteq \mathcal{A}_0$ implies that $\alpha \in \mathcal{A}_0$. Prove the *principle of transfinite induction*: If \mathcal{A} is well-ordered and \mathcal{A}_0 is an inductive subset of \mathcal{A} , then $\mathcal{A}_0 = \mathcal{A}$. Also, discuss how this is related to our familiar “mathematical induction”.

Let \mathcal{A}_0 be an inductive subset of a well ordered set \mathcal{A} . Suppose $\mathcal{A}_0 \neq \mathcal{A}$.

Consider $\mathcal{B} = \mathcal{A} - \mathcal{A}_0$. Our above supposition implies that $\mathcal{B} \neq \emptyset$. Since \mathcal{B} is a non-empty subset of a well ordered set, it has a least element, say $\beta = \min(\mathcal{B}) \in \mathcal{B}$.

Consider $\alpha \in \mathcal{A}$ such that $\alpha < \beta$. Since β is the least element of \mathcal{B} , we have $\alpha \notin \mathcal{B}$ so $\alpha \in \mathcal{A}_0$. This shows that $S_\beta = \{\alpha \in \mathcal{A} \mid \alpha < \beta\} \subseteq \mathcal{A}_0$. But \mathcal{A}_0 is inductive, so $\beta \in \mathcal{A}_0$ (contradiction).

Therefore, no such β exists. This means that $\mathcal{B} = \emptyset$ so that $\mathcal{A}_0 = \mathcal{A}$.

How is this related to our usual principle of induction? Well, usually we induct on $\mathbb{Z}_{>0} = \{1, 2, 3, \dots\}$. Notice that $\mathbb{Z}_{>0}$ is a well ordered set (using the usual $<$ ordering).

Consider $X = \{k \in \mathbb{Z}_{>0} \mid \text{some statement depending on } k\}$. Notice that this statement holding for $k = 1, 2, \dots, n - 1$ implying that the statement holds for $k = n$ is the same as saying $\{1, 2, \dots, n - 1\} \subseteq X$ implies $n \in X$. If this is true (by induction on $\mathbb{Z}_{>0}$), we must have $X = \mathbb{Z}_{>0}$ and so our statement holds for all $n \in \mathbb{Z}_{>0}$. This is often called *strong induction*.

An observant student might notice that we seem to be lacking a “base case” in our discussion! Recall that when we do inductive proofs, we always need to establish some base case. It is interesting to note that this is actually built into the above definition. If we consider the case of $n = 1$, notice that $S_1 = \emptyset$. Since $S_1 = \emptyset \subseteq X$, we must have $1 \in X$. So we must have that our statement holds for $n = 1$.

Therefore, we must be careful when interpreting “this statement holds for $k = 1, 2, \dots, n - 1$ implies that this statement holds for $k = n$ ”. We need to include the case $n = 1$ which is equivalent to just assuming the statement holds for $n = 1$!

In general if we want to prove some statement using transfinite induction (on some well ordered set \mathcal{A}), we will need to start by establishing that statement for the minimum of our index set (i.e. $\min(\mathcal{A})$).

8. (10 points) [5710 – Grad Problem] Explain why $X = \{1, 2\} \times \mathbb{Z}_{>0}$ and $Y = \mathbb{Z}_{>0} \times \{1, 2\}$ are well-ordered when we give $\{1, 2\}$ and $\mathbb{Z}_{>0}$ their usual orders and X, Y dictionary orders. Do these sets have the same order type? That is – is there a bijection between X and Y which preserves orders (i.e. a bijection $\varphi : X \rightarrow Y$ such that $\mathbf{v} < \mathbf{w}$ iff $f(\mathbf{v}) < f(\mathbf{w})$)?

Suppose that $S \subseteq X$ is non-empty. Then consider $S_1 = \{n \mid (n, k) \in S\}$. Since $S \neq \emptyset$, we also have $S_1 \neq \emptyset$. This means that S_1 is a non-empty subset of the well ordered set $\{1, 2\}$. Thus $s_1 = \min(S_1)$ exists. Let $S_2 = \{n \in \mathbb{Z}_{>0} \mid (s_1, n) \in S\}$. Then since $s_1 \in S_1$ there is $(s_1, k) \in S$ for some $k \in \mathbb{Z}_{>0}$ thus $k \in S_2$ and so $S_2 \neq \emptyset$. Therefore, since S_2 is a non-empty subset of a well ordered set $\mathbb{Z}_{>0}$, $s_2 = \min(S_2)$ exists.

Consider $(x, y) \in S$. Then we have that $s_1 \leq x$ since s_1 was minimal among first coordinates. If $s_1 = x$ (i.e. $(x, y) = (s_1, y)$), then $y \in S_2$ and so $s_2 \leq y$ since s_2 was minimal among second coordinates following s_1 . Therefore, $(s_1, s_2) \leq (x, y)$. This shows that (s_1, s_2) is the least element of S . Therefore, every non-empty subset of X has a least element and so X is well ordered.

There wasn’t anything special about $\{1, 2\}$ or $\mathbb{Z}_{>0}$ in the argument above (except that they are well ordered). So essentially the same argument shows that if A and B are well ordered, then $A \times B$ is well ordered when given the dictionary order. In particular, Y is well ordered as well.

Next, X and Y are both countably infinite, so there is a bijection from X to Y . However, there isn’t one that preserves order types. This is more or less obvious when we list off the elements of these sets from lowest to highest.

$$\begin{aligned} X : & (1, 1) < (1, 2) < (1, 3) < \dots < (2, 1) < (2, 2) < (2, 3) < \dots \\ Y : & (1, 1) < (1, 2) < (2, 1) < (2, 2) < (3, 1) < (3, 2) < \dots \end{aligned}$$

It seems that Y has the same order type as $\mathbb{Z}_{>0}$ while X is like 2 copies of $\mathbb{Z}_{>0}$ one slapped onto the end of the other.

Let’s prove that no order isomorphism exists. Suppose that $f : X \rightarrow Y$ is an order preserving bijection. Clearly $S_{(2,1)} = \{(x, y) \mid (x, y) < (2, 1)\} = \{(1, 1), (1, 2), (1, 3), \dots\}$ is infinite. Therefore, $f(S_{(2,1)})$ must be infinite as well.

Notice that $f(S_\alpha) = S_{f(\alpha)}$. Why? Suppose $y \in f(S_\alpha)$. Then $y = f(\beta)$ for some $\beta \in S_\alpha$. Therefore, $\beta < \alpha$. Thus $y = f(\beta) < f(\alpha)$ (f is order preserving). Therefore, $y \in S_{f(\alpha)}$. Likewise, suppose that $y \in S_{f(\alpha)}$. Then $y < f(\alpha)$. The function f is onto, so there must exist some $\beta \in X$ such that $f(\beta) = y$. We cannot have $\beta \geq \alpha$, since then $y = f(\beta) \geq f(\alpha)$ (f is order preserving). Thus $\beta < \alpha$ and so $\beta \in S_\alpha$. Thus $y = f(\beta) \in f(S_\alpha)$. Therefore, $f(S_\alpha) = S_{f(\alpha)}$.

Now we have a problem. $S_{f((2,1))} = f(S_{(2,1)})$ is infinite. But S_β is finite for any $\beta \in Y$. [Why? Suppose $\beta = (x, 2)$. Then $S_\beta = \{(1, 1), (1, 2), \dots, (x - 1, 1), (x - 1, 2), (x, 1), (x, 2)\}$ (clearly finite). Likewise for $\beta = (x, 1)$.] Thus we have a contradiction. Therefore, no order preserving bijection can exist (i.e. X and Y have different order types).