1. Use the definitions of $\forall$ and $\exists$ to prove that, if U is the universal set in question and $P(x)$ is an indefinite assertion (depending on $x \in U$), then

a) $(\forall x, P(x)$ is true$) \Leftrightarrow \sim(\exists x, P(x)$ is false$)$;
b) $(\exists x, P(x)$ is true$) \Leftrightarrow \sim(\forall x, P(x)$ is false$)$.

The definition of the universal quantifier is that the truth set of the proposition is the entire universe, i.e. $(\forall x, P(x)$ is true$)$ means by definition, $\{x\text{: } P(x) \text{ is true}\} = U$. And the definition of the existential quantifier yields that $(\exists x, P(x)$ is false$)$ means $\{x\text{: } P(x) \text{ is false}\} \neq \emptyset$. So $\sim(\exists x, P(x)$ is false$)$ means $\{x\text{: } P(x) \text{ is false}\} = \emptyset$, which is equivalent to $\{x\text{: } P(x) \text{ is true}\} = U$. Thus a) is established. And b) is handled similarly.

2. Let A, B and C be nonempty sets. If R is a relation between A and B, and S is a relation between B and C, recall that we have defined the relation $S\circ R$ between A and C by pairs$(S\circ R) = \{(a, c)\text{: } \exists\, b \in B,\ aRb \wedge bSc\}$.

Let B and C be nonempty sets and let S_1 and S_2 be a relations between B and C. For each of the following assertions, prove if true, or give a counterexample if false.

a) If A is a nonempty set and R is a relation between A and B, and $S_1\circ R = S_2\circ R$, then $S_1 = S_2$.

This assertion is false. For example, if R is the empty relation, then $S_1\circ R = S_2\circ R$, regardless of S_1 and S_2 so any appropriate choice of relations will give an example. (Or if you don't like the empty relation, construct any example in which R is not onto all of B.)

b) If A is a nonempty set and $\forall$ relations R between A and B, and $S_1\circ R = S_2\circ R$, then $S_1 = S_2$.

This assertion is true, because A is nonempty. Let a be in A, and for any b in B let R_b be the relation whose only pair is (a, b). If $S_1\circ R_b = S_2\circ R_b$, then it is easy to deduce that these two relations agree on b, and since this statement is true for every b, the two relations agree.

c) If $\forall$ nonempty sets A and relations R between A and B, and $S_1 \circ R = S_2 \circ R$, then $S_1 = S_2$.

We already saw in b) that it is enough to have this condition hold for any nonempty A (and all relations R) in order to draw the conclusion, so if it holds for ALL such A the conclusion most certainly holds.

3. For each of the following assertions, prove if true, or give a counterexample if false.

a) Let A be a partially ordered set, with partial order denoted by $\preccurlyeq$. If $m, M \in A$ and m is a minimal element for A and M is a maximal element for A, then $m \preccurlyeq M$.

This assertion is false. For example, let $A = \{a, b, m, M\}$ have four distinct elements, and let the pairs of $\preccurlyeq$ be $\{(a, a), (b, b), (m, m), (M, M), (m, a), (b, M)\}$; then m and M are minimal and maximal respectively, but it is not true that $m \preccurlyeq M$.

b) Let A be a partially ordered set, with partial order denoted by $\preccurlyeq$, such that A has both a minimum element m and a maximum element M. Then A is totally ordered by $\preccurlyeq$.

This assertion is also false. For example, let $A = \{a, b, m, M\}$ have four distinct elements, and let the pairs of $\preccurlyeq$ be $\{(a, a), (b, b), (m, m), (M, M), (m, a), (m, b), (m, M), (a, M)\}, (b, M)\}$. Then m and M are minimum and maximum, respectively, but A is not totally ordered because a is not related to b.

4. Let $\mathbf{R}$ denote the usual real numbers, with order relation $\leq$. Let "∞" denote an object not in $\mathbf{R}$, and let $A = \mathbf{R} \cup \{\infty\}$. Define a relation R on A by

1) for all $a, b \in \mathbf{R}$, aRb means $a \leq b$;
2) for all $a \in A$, $aR\infty$.

a) Prove that R is a total order on A.

This assertion is pretty straightforward. You have to consider cases because of the ∞.

b) Prove the following assertion if true, or give a counterexample if false:

"Every nonempty subset X of A which is bounded above has a least upper bound."

The assertion is true. If X does not contain ∞ then the result holds from the axioms on **R**. And if X contains ∞ then it is easy to show that ∞ is the least upper bound of X.

c) Prove the following assertion if true, or give a counterexample if false.

"Every nonempty subset X of A which is bounded below has a greatest lower bound."

The assertion is true. If X contains any point other than ∞ then the result holds from the axioms on **R**. And otherwise X contains only ∞ and then it is easy to show that ∞ is the greatest lower bound.

5. Let $P(\mathbf{R})$ denote the set of real polynomials (in other words, the set of functions p: $\mathbf{R} \to \mathbf{R}$ of the form $p(x) = \sum_{j=0}^{n} a_j x^j$. Define a relation $\approx$ on $P(\mathbf{R})$ as follows: $p \approx q$ means p and q have the same number of real roots counting multiplicities.
(So, for example, $(x - 1)(x - 1) \approx (x - 1)(x - 2)$; $(x - 1)(x - 1) \not\approx (x - 1)$;
$(x - 1) \approx (x - 1)(x^2 + 1)$.) *You can use what we know about real polynomials below.*

a) Prove that $\approx$ is an equivalence relation.

This assertion is pretty straightforward.

b) For $n \geq 0$, let P_n denote the equivalence class of all polynomials with n real roots. Set $P_n P_m = \{pq: p \in P_n, q \in P_m\}$. Give a simple description of $P_n P_m$.

Show that $P_n P_m = P_{n+m}$.

c) Define a relation R on $P(\mathbf{R})$ by pRs means $p|s$ (p divides s in the sense of division of polynomials, i.e. there is a real polynomial q such that $s = pq$). Prove that R is a partial order on $P(\mathbf{R})$, or disprove it by finding exactly which of the requirements for a partial order is violated.

It is straightforward to show that this relation is reflexive and transitive, but it is not anti-symmetric since, for example, the constant polynomials 2 and 8 divide each other but are not equal to each other.

6. Let A be a partially ordered set, with partial order denoted by $\preccurlyeq$. Let M denote a fixed object not in A. Set $B = A \cup \{M\}$. Define a relation R on B as follows:

1) for all $a, b \in \boldsymbol{A}$, aRb means $a \preccurlyeq b$;
2) for all $a \in B$, aRM.

Prove that R is a partial order on B, and prove that B has a maximum element.

It is straightforward to show that this relation is a partial order. And condition 2) means that M is a maximum.

7. Let A be a nonempty finite set which is totally ordered. Prove that A has a minimum.

Since A is nonempty and finite there is a natural number n and there is a bijection from $\{1, . . . , n\}$ to A. Such a bijection can be written in sequence notation, i.e. $A = \{a_1, . . . , a_n\}$. (Note: this listing does NOT mean that the elements are in increasing order relative to the order on A.) Use induction on n to show that A is has a minimum: if $n = 1$, then clearly a_1 is the minimum (and only element) of A. Now suppose that any finite nonempty set with fewer than n elements has a minimum, and $n > 1$. Then $\{a_1, . . . , a_{n-1}\}$ has a minimum, call it m. If $m \leq a_n$, then easily we can show that m is the minimum for $\{a_1, . . . , a_n\}$. And if $a_n \leq m$, then (by the transitivity of the total order), clearly we can show that a_n is the minimum for $\{a_1, . . . , a_n\}$.

8. Let **F** be a field. Let $L(\mathbf{F})$ = {finite lists $(c_j)_{j=0}{}^{n}$ with entries in **F**}. Define a relation ≈ on $L(\mathbf{F})$ as follows: $(a_j) \approx (b_j)$ means $\sum_{j=0}{}^{n} a_j x^j = \sum_{j=0}{}^{n} b_j x^j$ for all $x \in \mathbf{F}$. (Clearly ≈ is an equivalence relation on $L(\mathbf{F})$.) *In the following, you can use all of the algebra you know to be true in a field.*

a) Show that there is a field **F** such that every equivalence class under ≈ in $L(\mathbf{F})$ has exactly one element.

For example, you can pick the rationals or the reals or the complexes. From algebra we know that two polynomials are equal at every value of *x* if and only if their difference is a polynomial which is zero at every point, and the only way that happens in the rationals or reals or complexes is if it is the zero polynomial. Now, I realize that the way I phrased this in terms of lists, that means that all of the coefficients are zero, but I did not specify that lists of zeros of different lengths are treated as the same. So I am guilty of poor phrasing here.

b) Show that there is a field **F** such that every equivalence class under ≈ in $L(\mathbf{F})$ has more than one element.

THIS is the part that I really care about your seeing. Remember that we have the integers mod a prime as an important other family of examples of fields. In the integers mod a prime, there are LOTS of different polynomials, but only FINITELY MANY ELEMENTS. SO you would expect that there are lots of DIFFERENT polynomials that give the same values on those elements. SO, here is a quick sketch: let *p* be your favorite prime. Then the 0 polynomial and the polynomial $x(x – 1) \cdot \cdot \cdot (x – p – 1)$ (or just $x(x – 1)$ if $p = 2$) are both zero at every point of the field $\mathbf{Z}_p$, but they are not the same polynomial, i.e. they don't have the same coefficients. And more generally, if *f* is any polynomial on that field, *f* and

$f + x(x – 1) \cdot \cdot \cdot (x – p – 1)$ are polynomials with different coefficients which give the same value at every point of the field.

9. Let (h_n) be the sequence defined recursively by $h_1 = 1$, $h_2 = 1$, and for $n \geq 3$, $h_n = h_{n-1} + (h_{n-2})^3$. What are the first seven terms in this sequence?

a) Prove or disprove the following assertion: For $n \geq 1$, $h_n \leq 2^{(3^n)}$.

This result is true. You show that it is true for $n = 1$ and $n = 2$. Then you will use the inductive hypothesis for k and you will use BOTH $k = n - 1$ and $k = n - 2$ in establishing the inductive step. It involves carefully using the algebra of exponents: the definition and the inductive hypothesis yield that for $n \geq 3$,

$h_n \leq 2^{(3^{n-1})} + [2^{(3^{n-2})}]^3 = 2^{(3^{n-1})} + 2^{3(3^{n-2})} = 2^{(3^{n-1})} + 2^{(3^{n-1})} = 2 \cdot 2^{(3^{n-1})}$

$\leq 8 \cdot 2^{(3^{n-1})} = 2^{(3^n)}$.

b) Prove or disprove the following assertion: For $n \geq 3$, $h_n \geq 2^{(3^{(n-3)/2})}$.

This result is also true. Here you show that it is true for $n = 3$ and $n = 4$. Of course, in working this out in office hours, we decided it is FALSE for $n = 4$, but that is neither here nor there; I just should have had you prove it for $n \geq 5$. Then again you will use the inductive hypothesis for k and you will use BOTH $k = n - 1$ and $k = n - 2$ in establishing the inductive step.

10. Define $n!$ recursively as follows: $0! = 1$, and, for $n \geq 1$, $n! = n[(n-1)!]$. Prove that, for all $n \in \mathbf{N}$, $(1 + x)^n = \sum_{j=0}^{n}[n!/j!(n-j)!]x^j$.

This is a straightforward example of a PMI proof. You will need to use the $n - 1$ case, multiply both sides by $(1 + x)$, collect terms with like powers in the resulting sum, and show that the corresponding sums of pairs of coefficients give you the right expression. You have to be REALLY careful with the indices.

11. Recall, sets are called equinumerous is there is a bijection between them, and in that case they are said to have the same cardinality.

a) Prove that $[0,1] \times [0,1]$ has the same cardinality as $[0,1]$. (*Hint: represent real numbers in the interval (0,1] by their unique non-terminating decimal expansions, i.e. any such number is* *uniquely specified as* $0.d_1d_2d_2\ldots$ *for a sequence of digits* d_j *between 0 an 9. Construct a bijection from* $[0,1] \times [0,1]$ *to* $[0,1]$.)

This is a classic. Remember, if you want to define $f(x, y)$ from $[0,1] \times [0,1]$ to $[0,1]$, you can assume that you know the digits of x and of y, i.e. $x = 0.a_1a_2a_2\ldots$ *and* $y = 0.b_1b_2b_2\ldots$ *and you want to produce the digits of* $f(x, y)$. Try interspersing the digits from x and y: set *of* $f(x, y) = 0.a_1b_1a_2b_2a_2b_2\ldots$. Show that this map is one-to-one and onto $[0, 1]$.

b) Prove that $[0,1]$ and **R** have the same cardinality.

Strategy: first do a bijection f from **(**0,1) to **R** (we did a bijection between a bounded open interval and **R** explicitly in class; you could translate and rescale the that one). Then do a bijection g from $[0,1]$ to **R** by throwing in the two endpoints and here is a cool way to do it:
Let $g(0) = 1$, $g(1) = 2$, $g(x) = f(x)$ for every x EXCEPT for the values of x that mapped into the natural numbers, and for THOSE values of x, let $g(x) = f(x) + 2$. Check to see that g is a bijection!

c) Prove that **R** and **R** $\times$ **R** (also know as $\mathbf{R}^2$) have the same cardinality.

Put together bijections (and their inverses) from parts a) and b).

12. a) Let **N** denote the natural numbers, and let p be an object. Prove that **N** and $\mathbf{N} \cup \{p\}$ have the same cardinality.

OK, so I should have given you this one BEFORE part b) of #11 to see what I was thinking. Let $f(p) = 1$, and $f(n) = n + 1$ for n in **N**. Show that f is a bijection from $\mathbf{N} \cup \{p\}$ to **N**. (This is Hilbert's hotel problem: you have countably infinitely many rooms in a hotel, each of which is booked by one person. One more person arrives: how does everyone get a room and no-one have to share a room.)

b) Let **R** denote the real numbers, and let p be an object. Prove that **R** and $\mathbf{R} \cup \{p\}$ have the same cardinality.

Use the same map defined above, on the subset $\mathbf{N} \cup \{p\}$, and let $f(x) = x$ for every other element of $\mathbf{R}$. Show that the resulting map is a bijection!