1. (20 pts) Match each proposition or predicate in the first column with the one that is logically equivalent to it in the second column. (For expressions involving quantifiers, the logical equivalence should hold no matter what domain of discourse is chosen.)

i.	$(1 \neq 2) \to P(x,y)$	a.	$\forall x\, \forall y\, P(x,y)$
ii.	$(1 = 2) \to P(x,y)$	b.	$\forall x\, \forall y\, \neg P(x,y)$
iii.	$\forall x\, \neg \exists y\, P(x,y)$	c.	$1 \neq 2$
iv.	$\exists x\, \exists y\, (P(x,y) \wedge (1=2))$	d.	$1 = 2$
v.	$\neg \exists x\, \exists y\, \neg P(x,y)$	e.	$P(x,y)$

(i) $\leftrightarrow$ (e) Since $1 \neq 2$ is true, $(1 \neq 2) \to P(x,y)$ is equivalent to $P(x,y)$

(ii) $\leftrightarrow$ (c) Since $1=2$ is false, $(1=2) \to P(x,y)$ is true

(iii) $\leftrightarrow$ (b) by negation of quantifiers

(iv) $\leftrightarrow$ (d) $P(x,y) \wedge (1=2)$ is always false, so its existential quantification is also false (on any domain of discourse)

(v) $\leftrightarrow$ (a) by negation of quantifiers

2. (20 pts) Explain what is wrong with the following reasoning. *Perfect square* means the square of an integer.

Theorem: Every positive integer is the difference of two distinct perfect squares.

Proof. Let n be a positive integer. Factor n as $n = pq$, where p and q are positive integers and we may assume without loss of generality that $p \geq q$. Clearly this is always possible, for example with $p = n$ and $q = 1$.

Let $a = (p+q)/2$ and $b = (p-q)/2$. Then $p = a + b$ and $q = a - b$, so $n = pq = (a+b)(a-b) = a^2 - b^2$. Since $n \neq 0$, a^2 and b^2 must be distinct.

The error is that a and b are not necessarily integers.

3. (20 pts) Prove that if $f: A \to B$ is an injective function, and the set A is not empty, then f has a left inverse, that is, there exists a function $g: B \to A$ such that $g \circ f$ is the identity function on A.

Since $A \neq \phi$, we can choose one element $a_0 \in A$ and define $g: B \to A$ as follows:

- If $b \in f(A)$, let $g(b)$ be the unique (since f is injective) $a \in A$ such that $f(a) = b$.
- If $b \notin f(A)$, let $g(b) = a_0$.

For any $a \in A$, we then have $g(f(a)) = a$ by the first case of the definition of g. This shows $g \circ f = id_A$.

4. For each of the following sets X, say whether it is finite, countably infinite, or uncountable, and do one of the following:

- If X is finite, find its number of elements $|X|$.
- If X is countably infinite, find a bijective function $f\colon \mathbb{N} \to X$.
- If $|X| = |\mathbb{R}|$, find a bijective function $f\colon \mathbb{R} \to X$.

(a) (6 pts) $X = \{x \in \mathbb{R} \mid x > 0\}$. uncountable with $|X| = |\mathbb{R}|$.
A bijection $f : \mathbb{R} \to X$ is $f(x) = e^x$; its inverse is $\ln x : X \to \mathbb{R}$.

(b) (7 pts) $X = \{x \in \mathbb{R} \mid x^3 \in \mathbb{N}\}$. Countably infinite. A bijection $f : \mathbb{N} \to X$ is $f(x) = \sqrt[3]{x}$. It is injective since the cube root of a real number is unique. It is surjective since by definition X is the set of cube roots of non-negative integers.

(c) (7 pts) $X = P(P(\{\emptyset, \{1\}\}))$, where P denotes power set.
Finite with $2^{2^2} = 2^4 = 16$ elements.

5. (20 pts) Suppose S is an algorithm that takes as input a list of n distinct integers, and returns as output the same integers sorted into increasing order. Find a lower bound on the worst case number of comparisons that S must do for $n = 4$, that is, a number k such that S must perform at least k comparisons for some input (a_1, a_2, a_3, a_4). Your answer should be as large as possible, not a trivial lower bound such as $k = 0$.

Justify the fact that your answer is a lower bound. You are not required to prove that it is the largest possible lower bound.

The input list could be in any of 24 possible orders relative to the desired sorted output. To distinguish among these possibilities, the number of comparisons k must satisfy $2^k \geq 24$. Since $2^4 < 24$, this implies $k \geq 5$, i.e. 5 is a lower bound.

It is, in fact, possible to sort every list of 4 numbers using at most 5 comparisons, so 5 is the largest possible lower bound, but it was not required to prove this.