proof forms

cs201.1 **8 april 1999**

name	definition	to prove...	once known
general			
direct	If p then q.	Assume p is true. ... so q is true. Therefore if p then q.	If you also know that p is true, then you can say q is true.
indirect	If p then q.	Assume q is not true. ... so p is not true. Therefore if p then q.	If you also know that p is true, then you can say q is true.
contradiction	p is true.	Assume p is not true. ... so we get a contradiction. Therefore p is true.	p is true.
equivalence	p if and only if q.	... so if p then q. ... so if q then p. Therefore p if and only if q.	If p then q and if q then p.
integers			
even	A number n is even if and only if there exists some integer k such that $n = 2k$.	... so $n = 2k$. ... so k is an integer. Therefore n is even.	There is some integer k such that $n = 2k$.
odd	A number n is odd if and only if there exists some integer k such that $n = 2k + 1$	... so $n = 2k + 1$. ... so k is an integer. Therefore n is odd.	There is some integer k such that $n = 2k + 1$.
divides	For two numbers a and b, $a\|b$ if and only if there exists some integer k such that $ak = b$.	... so $ak = b$. ... so k is an integer. Therefore $a\|b$.	There is some integer k such that $ak = b$.
sets			
subset	For any sets A and B, $A \subseteq B$ if and only if for any element x, $x \in A \rightarrow x \in B$	Assume that for some x, $x \in A$. ... so $x \in B$. Therefore $A \subseteq B$.	If you also know $x \in A$, then you can say $x \in B$.

name	definition	to prove...	once known
equality	For any sets A and B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.	... so $A \subseteq B$. ... so $B \subseteq A$. Therefore $A = B$.	$A \subseteq B$ and $B \subseteq A$.
union	$x \in A \cup B$ if and only if $x \in A$ or $x \in B$.	... so $x \in A$ or $x \in B$. Therefore $x \in A \cup B$.	$x \in A$ or $x \in B$.
intersection	$x \in A \cap B$ if and only if $x \in A$ and $x \in B$.	... so $x \in A$. ... so $x \in B$. Therefore $x \in A \cap B$.	$x \in A$ and $x \in B$.
complement	$x \in \bar{A}$ if and only if $x \notin A$.	... so $x \notin A$. Therefore $x \in \bar{A}$.	$x \notin A$.
powerset	$x \in P(A)$ if and only if $x \subseteq A$.	... so $x \subseteq A$. Therefore $x \in P(A)$	$x \subseteq A$.
set-builder	$x \in \{a \mid P(a)\}$ if and only if $P(x)$ is true.	... so $P(x)$ is true. Therefore $x \in \{a \mid P(a)\}$.	$P(x)$ is true.
functions			
one-to-one	A function f is one-to-one if and only if for any x and y in the domain of f, whenever $f(x) = f(y)$ then $x = y$.	Assume we have an x and y such that $f(x) = f(y)$. ... so $x = y$. Therefore f is one-to-one.	If you also know $f(x) = f(y)$, then you can say $x = y$.
onto	A function f is onto if and only if for any y in the co-domain of f, there is an x in the domain such that $f(x) = y$.	Assume y is in the co-domain of f. ... so $f(x) = y$. Therefore f is onto.	If you also know that y is in the co-domain of f, then you can say there is an x such that $f(x) = y$.
one-to-one correspondence	A function f is a one-to-one correspondence if and only if f is one-to-one and f is onto.	... so f is one-to-one. ... so f is onto. Therefore f is a one-to-one correspondence.	f is one-to-one and f is onto.
inverse	A function g from domain C to co-domain D is an inverse of a function f from domain D to co-domain C, if and only for every element x in D, $g \circ f(x) = x$ and for every element y in C, $f \circ g(y) = y$.	Assume $x \in D$. ... so $g \circ f(x) = x$. Assume $y \in C$. ... so $f \circ g(y) = y$. Therefore g is an inverse of f.	If you also know $x \in D$, then you can say $g \circ f(x) = x$. If you also know $y \in C$, then you can say $f \circ g(y) = y$.

name	definition	to prove...	once known
relations			
composition	$aR \circ Sb$ if and only if there is some c such that aRc and cSb.	... so aRc. ... so cSb. Therefore $aR \circ Sb$.	There is some c such that aRc and cSb.
power	$aR^n b$ if and only if $aR^{n-1} \circ Rb$.	... so $aR^{n-1} \circ Rb$. Therefore $aR^n b$.	$aR^{n-1} \circ Rb$.
reflexivity	A relation R is reflexive if and only if for any element a in the domain of R, aRa.	Assume a is some element of the domain of R. ... so aRa. Therefore R is reflexive.	If a is an element of the domain of R, then aRa.
symmetry	A relation R is symmetric if and only if whenever aRb, then bRa.	Assume we have an a and b such that aRb. ... so bRa. Therefore R is symmetric.	If you also know aRb then you can say bRa.
antisymmetry	A relation R is anti symmetric if and only if whenever aRb and bRa, then $a = b$.	Assume we have an a and b such that aRb and bRa. ... so $a = b$. Therefore R is antisymmetric.	If you also know aRb and bRa then you can say $a = b$.
transitivity	A relation R is transitive if and only if whenever aRb and bRc, then aRc.	Assume we have an a, b, and c such that aRb and bRc. ... so aRc. Therefore R is transitive.	If you also know aRb and bRc then you can say aRc.
equivalence	A relation R is an equivalence relation if and only if R is reflexive, symmetric, and transitive.	... so R is reflexive. ... so R is symmetric. ... so R is transitive. Therefore R is an equivalence relation.	R is reflexive. R is symmetric. R is transitive.
inverse	$(a, b) \in R^{-1}$ if and only if $(b, a) \in R$.	... so $(b, a) \in R$. Therefore $(a, b) \in R^{-1}$.	If you also know $(b, a) \in R$, then you can say $(a, b) \in R^{-1}$.
identity	A relation I is an identity relation of the domain A if and only if, for any other relation R over A, $R \circ I = R$ and $I \circ R = R$.	Assume R is a relation over the domain A. ... so $R \circ I = R$. ... so $I \circ R = R$. Therefore I is an identity relation of the domain A	If you also know that R is a relation over the domain A, then you can say $R \circ I = R$ and $I \circ R = R$.

name	definition	to prove...	once known
cardinality			
equinumerous	Two sets A and B are equinumerous if and only if there exists a function f from A to B which is a one-to-one correspondence.	... so f is from A to B. ... so f is a one-to-one correspondence. Therefore A and B are equinumerous.	There exists a function f from A to B which is a one-to-one correspondence.
less numerous	A set A is less numerous than a set B if and only if there exists a function f from A to B which is one-to-one.	... so f is from A to B. ... so f is one-to-one Therefore A is less numerous than B.	There exists a function f from A to B which is one-to-one.