Rule of inference	Name
p $p \to q$ $\therefore q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	Modus tollens
p $\therefore p \vee q$	Addition
$p \wedge q$ $\therefore p$	Simplification
p q $\therefore p \wedge q$	Conjunction
$p \to q$ $q \to r$ $\therefore p \to r$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	Resolution

- Modus Ponens
  - $p, p \to q \vdash q$

Theorem 6 $\alpha \to \beta, \neg\beta \vdash \neg\alpha$

Rule 7 $\alpha \vdash \alpha \vee \beta$

Rule 8 $\beta \vdash \alpha \vee \beta$

Rule 4 $\alpha \wedge \beta \vdash \alpha$

Rule 5 $\alpha \wedge \beta \vdash \beta$

Theorem 10 $\alpha, \beta \vdash \alpha \wedge \beta$

Theorem 2 $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$

Theorem 11 $\alpha \vee \beta, \neg\alpha \vdash \beta$

Not in cheat sheet, but easily provable

VALID ARGUMENTS

- With these hypotheses:

  "It is not sunny this afternoon and it is colder than yesterday."

  "We will go swimming only if it is sunny."

  "If we do not go swimming, then we will take a canoe trip."

  "If we take a canoe trip, then we will be home by sunset."

- Using the inference rules, construct a valid argument for the conclusion:

  "We will be home by sunset."

Solution:

1. Choose propositional variables:

   p : "It is sunny this afternoon." r : "We will go swimming."

   t : "We will be home by sunset."

   q : "It is colder than yesterday." s : "We will take a canoe trip."

2. Translation into propositional logic:

$$\text{Hypotheses: } \neg p \wedge q,\ r \rightarrow p,\ \neg r \rightarrow s,\ s \rightarrow t$$
$$\text{Conclusion: } t$$

Continued on next slide →

VALID ARGUMENTS

3. Construct the Valid Argument

Step	**Reason**
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

RULES OF INFERENCE FOR QUANTIFIED STATEMENTS

Table 2.13.1: Rules of inference for quantified statements.

Rule of Inference	Name	Example
c is an element (arbitrary or particular) $\underline{\forall x\, P(x)}$ $\therefore P(c)$	Universal instantiation	Sam is a student in the class. Every student in the class completed the assignment. Therefore, Sam completed his assignment.
c is an arbitrary element $\underline{P(c)\quad}$ $\therefore \forall x\, P(x)$	Universal generalization	Let c be an arbitrary integer. $c \leq c^2$ Therefore, every integer is less than or equal to its square.
$\underline{\exists x\, P(x)}$ $\therefore$ (c is a particular element) $\land P(c)$	Existential instantiation*	There is an integer that is equal to its square. Therefore, $c^2 = c$, for some integer c.
c is an element (arbitrary or particular) $\underline{P(c)\quad}$ $\therefore \exists x\, P(x)$	Existential generalization	Sam is a particular student in the class. Sam completed the assignment. Therefore, there is a student in the class who completed the assignment.

*Note: each use of Existential instantiation must define a new element with its own name (e.g., "c" or "d").

ZyBook 2.13.2

USING RULES OF INFERENCE

Example 1: Using the rules of inference, construct a valid argument to show that

"John Smith has two legs"

is a consequence of the premises:

"Every man has two legs." "John Smith is a man."

Solution: Let $M(x)$ denote "x is a man" and $L(x)$ " x has two legs" and let John Smith be a member of the domain.

Valid Argument:

Step	**Reason**
1. $\forall x(M(x) \rightarrow L(x))$	Premise
2. $M(J) \rightarrow L(J)$	UI from (1)
3. $M(J)$	Premise
4. $L(J)$	Modus Ponens using (2) and (3)

DEFINITIONS

- A *theorem* is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - *axioms* (statements which are given as true)
  - rules of inference
- A *lemma* is a 'helping theorem' or a result which is needed to prove a theorem.
- A *corollary* is a result which follows directly from a theorem.
- Less important theorems are sometimes called *propositions*.
- A *conjecture* is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

IN "LESS FORMAL" PROOFS

$P \rightarrow Q$ EQUIVALENTLY $P \vdash Q$

- *While* $p \rightarrow q$ *or* $p \vdash q$ are different in our formal proofs:
  - $p \rightarrow q$ *is a proposition*
  - $p \vdash q$. *says that q can be "proved" assuming p is a premise*
- In the proofs starting on Chapter 4 of ZyBooks the above are technically the same and in questions in and after chapter 4 we can use them interchangeably.

DEFINITIONS

Definition 4.1.1: Even and odd integers.

An integer x is ***even*** if there is an integer k such that $x = 2k$.
An integer x is ***odd*** if there is an integer k such that $x = 2k+1$.

Definition 4.1.2: The real number r is *rational* if there exist integers p and q where $q \neq 0$ such that $r = p/q$

Definition 4.1.3: Divides.

An integer x ***divides*** an integer y if and only if $y = kx$, for some integer k.

The fact that x divides y is denoted $x|y$. If x does not divide y, then that fact is denoted $x \nmid y$.

If x divides y, then y is said to be a ***multiple*** of x, and x is a ***factor*** or ***divisor*** of y.

Definition 4.1.4: Prime and composite numbers.

An integer n is ***prime*** if and only if $n > 1$, and for every positive integer m, if m divides n, then $m = 1$ or $m = n$.

An integer n is ***composite*** if and only if $n > 1$, and there is an integer m such that $1 < m < n$ and m divides n.

ZyBook 4.1 exercises

ALLOWED ASSUMPTIONS IN PROOFS

The rules of algebra.

For example if x, y, and z are real numbers and $x = y$, then $x+z = y+z$.

The set of integers is closed under addition, multiplication, and subtraction.

In other words, sums, products, and differences of integers are also integers.

Every integer is either even or odd.

This fact is proven elsewhere in the material.

If x is an integer, there is no integer between x and $x+1$.

In particular, there is no integer between 0 and 1.

The relative order of any two real numbers.

For example $1/2 < 1$ or $4.2 \geq 3.7$.

The square of any real number is greater than or equal to 0.

This fact is proven in a later exercise.

DIRECT PROOFS

$P \rightarrow Q$ OR $P \vdash Q$

- Step 1:
  - Write down premises (hypothesis) i.e., p
- Step 2:
  - Use definitions to express premises/hypothesis P in mathematical terms
- Step 3:
  - Use definitions to express the conclusion Q in mathematical terms (what we want to prove)
- Step 4
  - Use algebra/previous results/etc. to arrive at the mathematical expression for Q.

PROVING CONDITIONAL STATEMENTS: $p \to q$

- *Direct Proof*: Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

Theorem: If n is an odd integer, then n^2 is odd.

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k. Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

(integers are closed under multiplication)

We have proved that if n is an odd integer, then n^2 is an odd integer.

◀

(◀ marks the end of the proof. Sometimes **QED** is used instead.)

INDIRECT PROOFS

- Proof by contraposition
- Proof by contradiction

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.

CONTRAPOSITIVE PROOF OF $P \rightarrow Q$ *I.E., DIRECT PROOF OF* $\neg Q \rightarrow \neg P$

- Step 1:
  - Write down premises (hypothesis) i.e., $\neg Q$
- Step 2:
  - Use definitions to express premises/hypothesis $\neg Q$ in mathematical terms
- Step 3:
  - Use definitions to express the conclusion $\neg P$ in mathematical terms (what we want to prove)
- Step 4
  - Use algebra/previous results/etc. to arrive at the mathematical expression for $\neg P$.

PROOF BY CONTRAPOSITION: $P \rightarrow Q$ I.E. PROVING $\neg Q \rightarrow \neg P$

- *Proof by Contraposition*: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow$ q.

Example: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: Assume n is even. So, $n = 2k$ for some integer k. Thus

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even) , then n is odd (not even).

◀

INDIRECT PROOFS

- Proof by contraposition
- Proof by contradiction

- If direct methods of proof do not work:
  - We may need a clever use of a proof by contraposition.
  - Or a proof by contradiction.

PROOF BY CONTRADICTION

Meta – Theorem Let Γ be a set of premises

$$\Gamma, \neg\alpha \vdash \beta, \neg\beta \implies \Gamma \vdash \alpha$$

Meta – Corollary

$$(a)\Gamma, \alpha \vdash \beta, \neg\beta \implies \Gamma \vdash \neg\alpha$$

$$(b)\Gamma, \neg\alpha \vdash \alpha \implies \Gamma \vdash \alpha$$

PROOF BY CONTRADICTION THEOREM 4.6.1 (ZYBOOKS)

Example: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors. Then

$$2 = \frac{a^2}{b^2} \qquad\qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (previously proven). Since a is even, $a = 2c$ for some integer c. Thus,

$$2b^2 = 4c^2 \qquad\qquad b^2 = 2c^2$$

Therefore b^2 is even. Again then b must be even as well.

But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational

THEOREMS THAT ARE BICONDITIONAL STATEMENTS $P \leftrightarrow Q$

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Example: Prove the theorem: "given n is an integer, n is even if and only if n^2 is even."

Sometimes *iff* is used as an abbreviation for "if an only if," as in

"n is even iif n^2 is even."

PROVE ONE DIRECTION $P \rightarrow Q$

→. We show that if x is even then x^2 *is* even using a direct proof (the *only if*).

If x is even then $x = 2k$ for some integer k.

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 on next slide →

PROVE THE OTHER DIRECTION $Q \rightarrow P$

We show that if x^2 is even then x must be even (the *if* part). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even.

If x is not even then it must be odd. So, $x = 2k + 1$ for some k. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2\mathrm{k}) + 1$

which is odd and hence not even. This completes the proof of case 2.

Since x was arbitrary, the result follows by UG.

Therefore we have shown that x is even if and only if x^2 is even.

PROOF BY CASES: SOMETIMES P CAN BE DIVIDED IN DIFFERENT PARTS

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

- Use the tautology

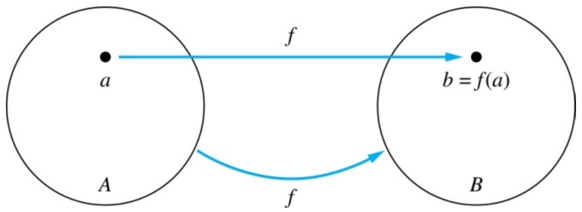
$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow \\ [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

- Each of the implications $p_i \rightarrow q$ is a *case*.

ZyBook 4.7

DEFINITIONS

Given a function f: $A \rightarrow B$:



- We say *f maps A* to *B or*

  f is a *mapping* from *A* to *B*.
- *A* is called the *domain* of *f*.
- *B* is called the *codomain, target* of *f*.
- If $f(a) = b$,
  - then *b* is called the *image* of *a* under *f*.
  - *a* is called the *preimage* of *b.*
- The range of f is the set of all images of points in **A** under *f*. We denote it by $f(\boldsymbol{A})$.
- Two functions are *equal* when they have the same domain, the same codomain and map each element of the domain to the same element of the codomain.

FUNCTION DEFINITIONS

- **Function**: a subset of *A*x*B* such that $\forall x \exists ! y (x, y) \in f$
- **One-to-one**: $\forall a \forall b \left[f(a) = f(b) \rightarrow a = b \right]$
- **Onto**: $\forall b \; \exists a \quad f(a) = b$
- **Bijection**: both one-to-one and onto
- Using the above definitions we can find the cardinality of sets
  - Especially, infinite sets

SHOWING THAT f IS (OR IS NOT) ONE-TO-ONE (INJECTIVE) OR ONTO (SURJECTIVE)

One-to-one aka Injective iff $\forall a \forall b\,[f(a) = f(b) \rightarrow a = b]$

Onto aka Surjective iff $\forall b\ \exists a \quad f(a) = b$

Suppose that $f : A \rightarrow B$.

To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$ then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

RECALL THAT CARDINALITY IS DEFINED WITH BIJECTIONS

Definition: The *cardinality* of a set A is equal to the cardinality of a set B, denoted

$$|A| = |B|,$$

if and only if there is a bijection from A to B.

- If there is a one-to-one function (*i.e.*, an injection) from A to B, the cardinality of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$.
- When $|A| \leq |B|$ and A and B have different cardinality, we say that the cardinality of A is less than the cardinality of B and write $|A| < |B|$.

SHOWING THAT A SET IS COUNTABLE

Show that the set of integers **Z** is countable (i.e., it has the same cardinality as the natural numbers).

Define a bijection from **N** to **Z**:

- When n is even: $f(n) = n/2$
- When n is odd: $f(\mathrm{n}) = -(n-1)/2$

THE RATIONAL NUMBERS ARE COUNTABLE: IT HAS CARDINALITY $\aleph_0$

1, ½, 2, 3, 1/3,1/4, 2/3, ….

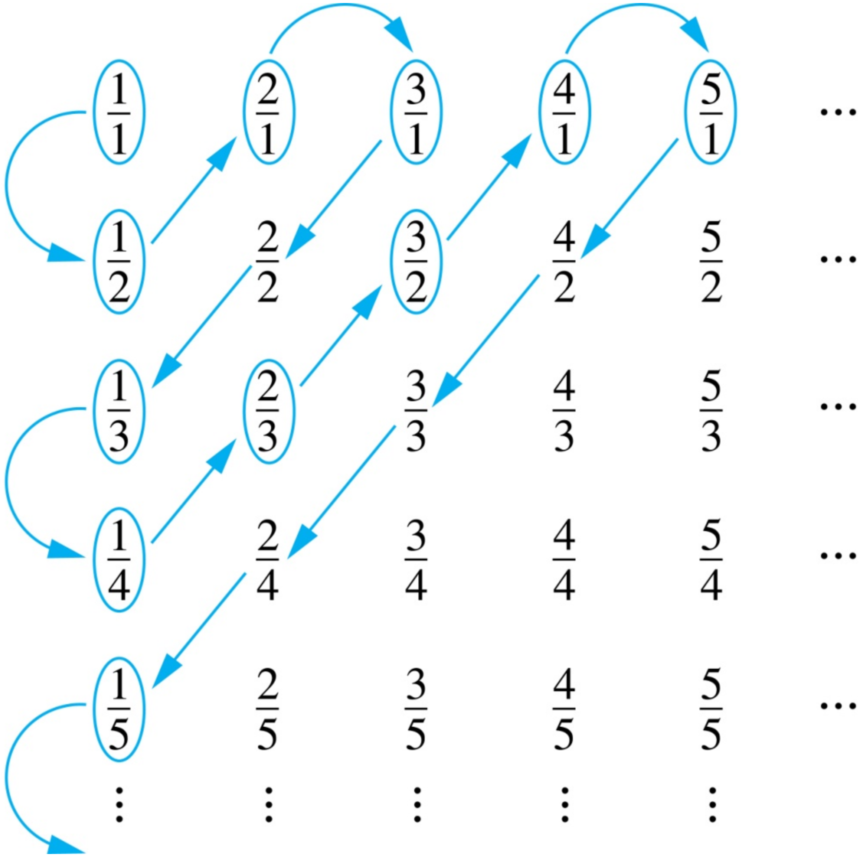
Constructing the List

First list p/q with $p + q = 2$.
Next list p/q with $p + q = 3$

And so on.

First row $q = 1$.
Second row $q = 2$.
etc.

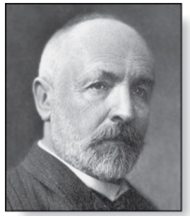
Terms not circled are not listed because they repeat previously listed terms



You can find the proof for all the rational numbers in "Book of Proof" Third Edition, Theorem 14.4

The set of real numbers is uncountable.

Georg Cantor
(1845-1918)



$$|\mathbb{R}| \neq \aleph_0 = |\mathbb{Z}| = |\mathbb{N}|$$

Solution: The method is called the Cantor diagonalization argument and is a proof by contradiction.

1. Suppose **R** is countable. Then the real numbers between 0 and 1 are also countable (any subset of a countable set is countable).
2. The real numbers between 0 and 1 can be listed in order $r_1, r_2, r_3, \ldots$.
3. Let the decimal representation of this listing be

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}\ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}\ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}\ldots \\ &\vdots \end{aligned}$$

4. Form a new real number with the decimal expansion

$$r = .r_1r_2r_3r_4\ldots$$

where

$$r_i = 3 \text{ if } d_{ii} \neq 3 \text{ and } r_i = 4 \text{ if } d_{ii} = 3$$

5. r is not equal to any of the $r_1, r_2, r_3, \ldots$ Because it differs from r_i in its ith position after the decimal point. Therefore there is a real number between 0 and 1 that is not on the list since every real number has a unique decimal expansion. Hence, all the real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable.
6. Since a set with an uncountable subset is uncountable (an exercise), the set of real numbers is uncountable.

Pages 271-272 of "Book of Proof"

THE CONTINUUM HYPOTHESIS (P 289 BOOK OF PROOF, 3RD EDITION)

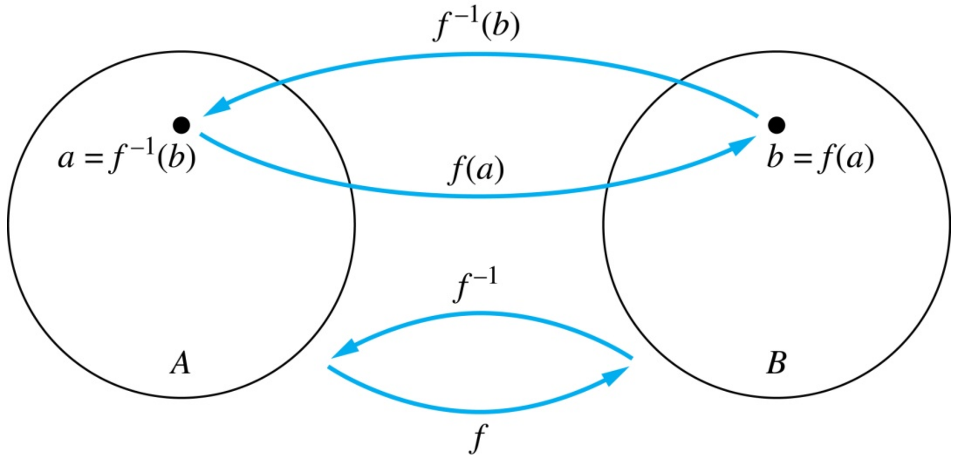
- Cantor proved that $|\mathbb{R}| \neq \aleph_0$
- In fact, the following two facts are also true:
  - $|\mathbb{R}| = \mathcal{P}(\mathbb{N})$
  - $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \ldots.$
- Continuun hypothesis:
  - Is there a cardinality in between $|\mathbb{N}|$ and $|\mathcal{P}(\mathbb{N})|$?
  - Continuun hypothesis: $\aleph_1 = |\mathbb{R}|$
- Logicomix
  - One of Hilbert's Problems of his speech in Chapter 3
  - Gödel proved that there are statements that cannot be proven or disproven (Chapter 6: Incompleteness)
- Gödel and later Cohen proved that the continuum hypothesis cannot be proved

INVERSE FUNCTIONS

Definition: Let f be a bijection from A to B. Then the *inverse* of f, denoted f^{-1}, is the function from B to A defined as

$$f^{-1}(y) = x \text{ iff } f(x) = y$$

No inverse exists unless f is a bijection. Why?

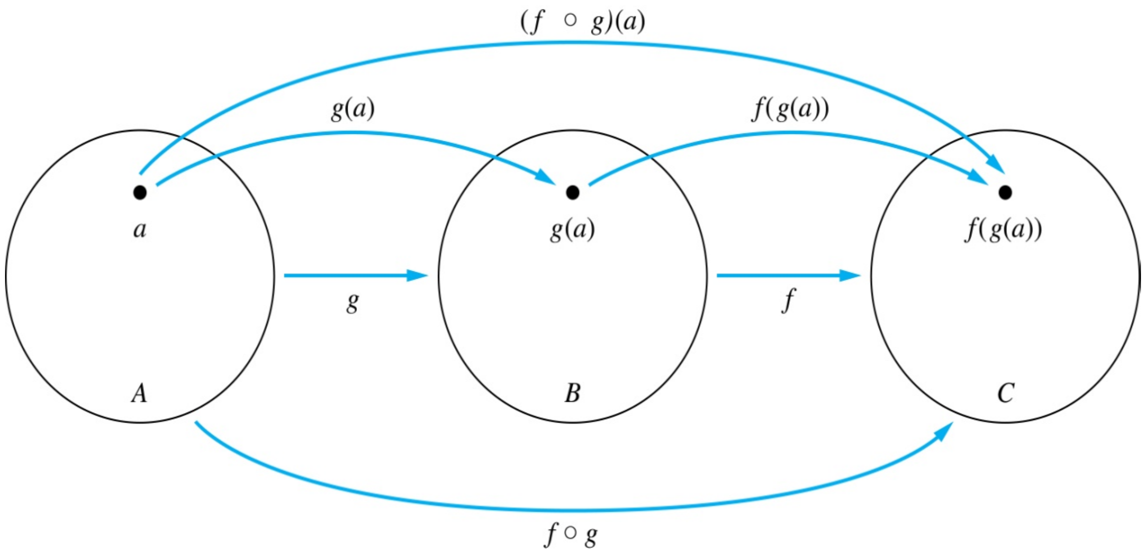


ZyBooks 5.4

COMPOSITION

- **Definition**: Let $f: B \to C$, $g: A \to B$. The *composition of f with g*, denoted $f \circ g$ is the function from A to C defined by

$$f \circ g(x) = f(g(x))$$



BINARY RELATIONS

Examples: “>“,“=”, “≤”, “⊆”

Definition: A *binary relation* R from a set A to a set B is a subset

$R \subseteq A \times B$.

Example:

- Let $A = \{0,1,2\}$ and $B = \{a,b\}$
- $\{(0, a), (0, b), (1,a) , (2, b)\}$ is a relation from A to B.

- Recall that a function is a subset of AxB defined by

$$\forall x \exists! y (x, y) \in f$$

Relations are more general than functions. A function is a relation where exactly one element of B is related to each element of A.

RELATION DEFINITIONS

Definition: R is *reflexive* iff $(a,a) \in R$ for every element $a \in A$. Written symbolically, R is reflexive if and only if

$$\forall x[x \in U \longrightarrow (x,x) \in R]$$

Definition: R is *symmetric* iff $(b,a) \in R$ whenever $(a,b) \in R$ for all $a,b \in A$. Written symbolically, R is symmetric if and only if

$$\forall x \forall y\, [(x,y) \in R \longrightarrow (y,x) \in R]$$

Definition: A relation R on a set A such that for all $a,b \in A$ if $(a,b) \in R$ and $(b,a) \in R$, then $a = b$ is called *antisymmetric*. Written symbolically, R is antisymmetric if and only if

$$\forall x \forall y\, [(x,y) \in R \wedge (y,x) \in R \longrightarrow x = y]$$

Definition: A relation R on a set A is called transitive if whenever $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$, for all $a,b,c \in A$. Written symbolically, R is transitive if and only if

$$\forall x \forall y\, \forall z[(x,y) \in R \wedge (y,z) \in \mathrm{R} \longrightarrow (x,z) \in R\,]$$

ZyBooks 6.1 & 6.2