

# Mathematical and Logical Basis of Computing: a Workbook

Howard A. Blair

Copyright © 2012 Howard A. Blair

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

## 1 A quick reference: some definitions and notation

This section is intended to serve only as a quick reference when you need to look up a definition or what some symbol or notation means. We will add to this section from time to time.

The next section contains a few questions that illustrate the kinds of questions that will be on the first exam. This exam is a tests the mathematical reasoning skills you should have when you **finish** the course. It does not count in any way towards your grade in this course.

The course properly begins with section 3 where will begin again and construct much of what is in this first section.

**Definition 1.1:** For any sets  $A$  and  $B$ , the set  $A \times B$ , called the *Cartesian Product* of  $A$  and  $B$ , is the set of all ordered pairs  $(a, b)$  such that  $a \in A$  and  $b \in B$ . In other words,

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

△

**Example 1.1:** Let  $A = \{0, 1, 2\}$  and let  $B = \{0, 1\}$ . Then

$$A \times B = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}.$$

△

**Example 1.2:** Let  $\mathbf{N}$  be the set of non-negative integers. That is,  $\mathbf{N} = \{0, 1, 2, 3, \dots\}$ . Then

$$\mathbf{N} \times \mathbf{N} = \{(m, n) \mid m \in \mathbf{N} \text{ and } n \in \mathbf{N}\}.$$

△

**Definition 1.2:** For any sets  $A$  and  $S$ ,  $A$  is a *subset* of  $S$  if, and only if, every member of  $A$  is a member of  $S$ . We denote that  $A$  is a subset of  $S$  by  $A \subseteq S$ . △

**Definition 1.3:** For any set  $S$ , the *power set* of  $S$ , denoted by  $\mathbf{P}(S)$ , is the set of all subsets of  $S$ . That is,

$$\mathbf{P}(S) = \{B \mid B \subseteq S\}.$$

△

**Note 1.1:** The definition of power set implies that for anything  $x$ ,  $x \in \mathbf{P}(S)$  if, and only if,  $x \subseteq S$ . △

**Definition 1.4:** A *dyadic relation*  $R$  from set  $A$  to set  $B$  is a subset of  $A \times B$ . △

**Definition 1.5:** A dyadic relation  $f$  from  $A$  to  $B$  is called a *function* from  $A$  to  $B$  if, and only if, for each  $a \in A$  there is exactly one  $b \in B$  such that  $(a, b) \in f$ . Suppose  $f$  is a function from  $A$  to  $B$ . Given  $a \in A$ , the  $b \in B$  for which  $(a, b) \in f$  is denoted by  $f(a)$ . The expression  $f : A \rightarrow B$  means that  $f$  is a function from  $A$  to  $B$ . △

**Definition 1.6:** The *composition* of dyadic relation  $R$  from set  $A$  to set  $B$  with dyadic relation  $S$  from  $B$  to set  $C$  is denoted by  $S \circ R$  and is a dyadic relation from  $A$  to  $C$  defined by

$$(x, z) \in S \circ R \quad \text{iff} \quad \text{there is an element } y \text{ of } B \text{ such that } (x, y) \in R \text{ and } (y, z) \in S.$$

With  $S \circ R$  we apply  $R$  first, then  $S$ . Another convenient notation is to write  $R; S$ . By definition,  $R; S = S \circ R$ . △

**Remark 1.1** The definition of the composition of dyadic relations also applies, in particular, to the composition of functions. △

**Definition 1.7:** A function  $f : A \rightarrow B$  is called an *injection*, if and only if the following condition for  $f$  is true: for all elements  $x$  and  $y$  of  $A$  such that  $x \neq y$ :  $f(x) \neq f(y)$ . When a function is an injection, we also say that the function is *injective*, and we also say that the function is *one-to-one*. These phrases are equivalent ways of expressing the same thing. △

**Note 1.2:** The definition says that  $f : A \rightarrow B$  is injective if, and only if, for every two different inputs to  $f$  we must get two different outputs. Equivalently, we cannot get the same output from  $f$  from two different inputs. The condition for  $f$  to be injective can be restated in the following equivalent form: for all elements  $x$  and  $y$  of  $A$ , if  $f(x) = f(y)$ , then  $x = y$ . △

**Definition 1.8:** A function  $f : A \rightarrow B$  is called a *surjection*, if and only if, the following condition for  $f$  is true: for each element  $b$  of  $B$ , there exists at least one  $a \in A$  such that  $f(a) = b$ . A surjection is also said to be *onto*. △

**Example 1.3:** Let  $\mathbf{R}$  be the set of real numbers. The function  $g : \mathbf{R} \rightarrow \mathbf{R}$  that is specified by  $g(x) = x^2$  is not surjective and is not injective. The function  $h : \mathbf{R} \rightarrow \mathbf{R}$  that is specified by  $h(x) = x^3 - x$  is surjective but not injective. The function  $\exp : \mathbf{R} \rightarrow \mathbf{R}$  specified by  $\exp(x) = e^x$  is injective, but not surjective, and the function  $f : \mathbf{R} \rightarrow \mathbf{R}$  specified by  $f(x) = x^3$  is both injective and surjective. △

**Definition 1.9:** Let  $f : X \rightarrow Y$ . There are two functions associated with  $f$  that we will now define. The function  $\hat{f} : \mathbf{P}(X) \rightarrow \mathbf{P}(Y)$  is specified by

$$\hat{f}(A) = \{y \in Y \mid \text{for some } a \in A, y = f(a)\}.$$

The function  $\hat{f}^{-1} : \mathbf{P}(Y) \rightarrow \mathbf{P}(X)$  is specified by

$$\hat{f}^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

△

**Note 1.3:** Do not jump to conclusions. The function  $\hat{f}^{-1}$  is not the *inverse* of  $f$  or even the inverse of  $\hat{f}$ .

With the following definition we begin to pick out certain special restricted kinds of mathematical entities that were defined above. It is important that you realize that, although the idea introduced next is new relative to the above definitions, the new idea *restricts* the preceding definitions. Restriction buys special properties useful in important contexts, but not necessarily in all contexts. You should organize your knowledge and understanding in such a way that you automatically see these kinds of logical relationships among the ideas you know about.  $\triangle$

**Definition 1.10** A partial ordering on set  $A$  is a dyadic relation from  $A$  to  $A$  which is reflexive, anti-symmetric and transitive. (We typically use some such as symbol as  $\sqsubseteq$  to denote an ordering relation, and write it in infix position. e.g.  $x \sqsubseteq y$ .) Specifically,

- (reflexive property) For every  $a \in A$ ,  $a \sqsubseteq a$ .
- (anti-symmetric property) For every  $a \in A$  and  $b \in A$  if  $a \sqsubseteq b$  and  $b \sqsubseteq a$  then  $a = b$ .
- (transitive property) For every  $a \in A$ ,  $b \in A$  and  $c \in A$ , if  $a \sqsubseteq b$  and  $b \sqsubseteq c$  then  $a \sqsubseteq c$ .

A partial order is a pair  $(A, \sqsubseteq)$  where  $A$  is a set and  $\sqsubseteq$  is a partial ordering on  $A$ . A partial order is also called a *poset*. When the partial ordering relation is clear from the context we refer to a poset  $(A, \sqsubseteq)$  by just mentioning  $A$  as in for example, “Let  $A$  be a poset such that ...”. Often, we read expressions such as  $x \sqsubseteq y$  as, “ $x$  is below  $y$ ”.  $\triangle$

## 2 Some previous preliminary assessment exam questions with answers

**Question 2.1:** Let  $f : X \rightarrow Y$ .

**Part 1:** Let  $B \subseteq Y$  and suppose  $B$  is a subset of the  $f$ -image of  $A$ , where  $A \subseteq X$ . Must it be the case that there is a set  $E \subseteq A$  such that  $B$  is the  $f$ -image of  $E$ ? If it must be the case, prove it; otherwise give a counterexample.

There is a set  $E \subseteq A$  such that  $B$  is the  $f$ -image of  $E$ . Consider  $\hat{f}^{-1}(B) \cap A$  and let  $x$  be an arbitrary element of  $\hat{f}^{-1}(B) \cap A$ . Then  $x \in \hat{f}^{-1}(B)$ . Therefore,  $f(x) \in B$ . Since  $x$  is arbitrary in  $\hat{f}^{-1}(B) \cap A$ , the  $f$ -image of  $\hat{f}^{-1}(B) \cap A$  is contained in  $B$ . Let  $y$  be an arbitrary element of  $B$ . Then  $y \in \hat{f}(A)$ , since  $B \subseteq \hat{f}(A)$ . Then, there is an element  $x$  in  $A$  such that  $f(x) = y \in B$ . Thus, we also have  $x \in \hat{f}^{-1}(B)$ . Therefore,  $x \in \hat{f}^{-1}(B) \cap A$ . It follows that  $f(x)$ , which is  $y$ , is in the  $f$ -image of  $\hat{f}^{-1}(B) \cap A$ . Since  $y$  is arbitrary in  $B$ ,  $B \subseteq \hat{f}^{-1}(B) \cap A$ . Therefore, the  $f$ -image of  $\hat{f}^{-1}(B) \cap A$  is  $B$ .

**Part 2:** Let  $B \subseteq Y$ . Suppose  $A \subseteq \hat{f}^{-1}(B)$ . Must it be the case that there is a subset  $D$  of  $Y$  such that  $A$  is the  $f$ -preimage of  $D$ ? If it must be the case, prove it; otherwise give a counterexample.

It does not have to be that there is a subset  $D$  of  $Y$  such that  $A$  is the  $f$ -preimage of  $D$ ,  $f$  is not injective. Here is a counterexample: Let  $X = \{0, 1, 2\}$  and  $Y = \{0, 1\}$ . Let  $f : X \rightarrow Y$  be the following function:  $f(0) = 0$ , and  $f(1) = f(2) = 1$ . Note that  $f$  is not injective, but  $f$  is surjective. Let  $B = \{1\}$ . Then  $\hat{f}^{-1}(B) = \{1, 2\}$ . Let  $A = \{1\} \subseteq \hat{f}^{-1}(B)$ . There are four subsets of  $Y$ :  $\emptyset$ ,  $\{0\}$ ,  $\{1\}$  and  $\{0, 1\}$ .  $A$  is not the  $f$ -preimage of any of them, since  $\hat{f}^{-1}(\emptyset) = \emptyset$ ,  $\hat{f}^{-1}(\{0\}) = \{0\}$ ,  $\hat{f}^{-1}(\{1\}) = \{1, 2\}$  and  $\hat{f}^{-1}(\{0, 1\}) = \{0, 1, 2\}$ .  $\triangle$

**Question 2.2:** Let  $f : X \rightarrow Y$ .

**Part 1:** If the following statement is true, prove it; if false, give a counterexample: If  $A_1$  and  $A_2$  are any subsets of  $X$ , then

$$\hat{f}(A_1 \cap A_2) = \hat{f}(A_1) \cap \hat{f}(A_2)$$

It need not be true that  $\hat{f}(A_1 \cap A_2) = \hat{f}(A_1) \cap \hat{f}(A_2)$ . Let  $X = \{0, 1\}$  and  $Y = \{0\}$ . Let  $A_1 = \{0\}$  and  $A_2 = \{1\}$ . Let  $f(0) = f(1) = 0$ . Then,  $\hat{f}(A_1) = \hat{f}(A_2) = \{0\}$ .

Thus,  $\hat{f}(A_1) \cap \hat{f}(A_2) = \{0\}$ , but  $\hat{f}(A_1 \cap A_2) = \hat{f}(\emptyset) = \emptyset$ . (Homework: Under what conditions on  $f$  can you guarantee that  $\hat{f}(A_1 \cap A_2) = \hat{f}(A_1) \cap \hat{f}(A_2)$ ? Prove it.)

**Part 2:** If the following statement is true, prove it; if false, give a counterexample:  
If  $A_1$  and  $A_2$  are any subsets of  $X$ , then

$$\hat{f}(A_1 \cup A_2) = \hat{f}(A_1) \cup \hat{f}(A_2)$$

The equation must hold:

$$\begin{aligned}\hat{f}(A_1 \cup A_2) &= \{f(x) \mid x \in A_1 \cup A_2\} \\ &= \{f(x) \mid x \in A_1 \text{ or } x \in A_2\} \\ &= \{f(x) \mid x \in A_1\} \cup \{f(x) \mid x \in A_2\} \\ &= \hat{f}(A_1) \cup \hat{f}(A_2)\end{aligned}$$

△

**Question 2.3:** Let  $f : X \rightarrow Y$ .

**Part 1:** If the following statement is true, prove it; if false, give a counterexample:  
If  $B_1$  and  $B_2$  are any subsets of  $Y$ , then

$$\hat{f}^{-1}(B_1 \cap B_2) = \hat{f}^{-1}(B_1) \cap \hat{f}^{-1}(B_2)$$

It must be that  $\hat{f}^{-1}(B_1 \cap B_2) = \hat{f}^{-1}(B_1) \cap \hat{f}^{-1}(B_2)$ .

$$\begin{aligned}\hat{f}^{-1}(B_1 \cap B_2) &= \{x \in X \mid f(x) \in B_1 \cap B_2\} \\ &= \{x \in X \mid f(x) \in B_1 \text{ and } f(x) \in B_2\} \\ &= \{x \in X \mid f(x) \in B_1\} \cap \{x \in X \mid f(x) \in B_2\} \\ &= \hat{f}^{-1}(B_1) \cap \hat{f}^{-1}(B_2)\end{aligned}$$

**Part 2:** If the following statement is true, prove it; if false, give a counterexample:  
If  $A_1$  and  $A_2$  are any subsets of  $X$ , then

$$\hat{f}^{-1}(B_1 \cup B_2) = \hat{f}^{-1}(B_1) \cup \hat{f}^{-1}(B_2)$$

It must be that  $\hat{f}^{-1}(B_1 \cup B_2) = \hat{f}^{-1}(B_1) \cup \hat{f}^{-1}(B_2)$ .

$$\begin{aligned}\hat{f}^{-1}(B_1 \cup B_2) &= \{x \in X \mid f(x) \in B_1 \cup B_2\} \\ &= \{x \in X \mid f(x) \in B_1 \text{ or } f(x) \in B_2\} \\ &= \{x \in X \mid f(x) \in B_1\} \cup \{x \in X \mid f(x) \in B_2\} \\ &= \hat{f}^{-1}(B_1) \cup \hat{f}^{-1}(B_2)\end{aligned}$$

△

**Question 2.4:** Let  $X$  be a set with exactly 5 elements and let  $Y$  be a set with exactly 2 elements.

**Part 1:** How many functions are there from  $X$  to  $Y$ ?

If  $S$  is a finite set, let  $\|S\|$  denote the number of elements in  $S$ . A notation for the set of *all* functions from a set  $X$  to a set  $Y$  is  $Y^X$ . Then

$$\|Y^X\| = \|Y\|^{\|X\|}$$

In this question,  $\|Y\|^{\|X\|} = 2^5 = 32$ .

**Part 2:** How many functions are there from  $X$  to  $Y$  that are surjective?

If a function  $f$  from  $X$  to a set  $Y$ , where  $Y$  has just two elements, is not surjective, it must be constant; i.e.  $f$  must return the same output for every input. There are just two constant functions from  $X$  to a set  $Y$  with two elements. Therefore there are  $2^{\|X\|} - 2$  surjective functions from  $X$  to  $Y$ ; i.e. in this question, 30 such functions.

**Part 3:** How many functions are there from  $X$  to  $Z$  that are surjective, where  $Z$  is a set with exactly 3 elements?

If a function from  $X$  to  $Z$  is not surjective, it is either constant (if  $Z$  has exactly 3 elements, then there are 3 constant functions from  $X$  to  $Z$ ) or its range has exactly 2 elements. There are three 2-element subsets of  $Z$ , and for each 2-element subset  $W$  of  $Z$ , there are, as we saw in Part (2), 30 functions whose range is  $W$ . Therefore there are  $3 \cdot 30 + 3 = 93$  functions from  $X$  to  $Z$  that are not surjective. There are a total of  $3^5 = 243$  functions from  $X$  to  $Z$ . So, there are  $243 - 93 = 150$  surjective functions from  $X$  to  $Z$ .  $\triangle$

**Question 2.5:** Let  $\mathbb{N}$  be the set of non-negative integers. For each non-negative integer  $n$ , let  $f_n : \mathbb{N} \rightarrow \{0, 1\}$ . Let  $g : \mathbb{N} \rightarrow \{0, 1\}$  be defined by

$$g(k) = \begin{cases} 0 & \text{if } f_k(k) = 1 \\ 1 & \text{if } f_k(k) = 0 \end{cases}$$

Prove that for every  $n \in \mathbb{N}$ ,  $g \neq f_n$ .

[**Note:** By definition, two functions  $f$  and  $g$  with the same domain and codomain are equal if, and only if, for every input  $x$ ,  $f(x) = g(x)$ .]

Suppose the conclusion is false; i.e. for some  $k$ ,  $g = f_k$ . Then, for every non-negative integer  $m$ ,

$$g(m) = f_k(m)$$

But, by definition of  $g$ , if  $f_k(k) = 0$ , then  $g(k) = 1$ . And if  $f_k(k) = 1$ , then  $g(k) = 0$ . So,

$$g(k) \neq f_k(k)$$

Contradiction. Therefore, there is no  $k$  such that  $g = f_k$ .  $\triangle$

### 3 We shall begin with nothing *and* our ability to reason logically

**Directive 3.1:** Read the Wikipedia article on *Set Theory* at

[http://en.wikipedia.org/wiki/Set\\_theory](http://en.wikipedia.org/wiki/Set_theory)

Then work through the material in the Wikibook *Discrete Mathematics/Set Theory* found at

[http://en.wikibooks.org/wiki/Discrete\\_Mathematics/Set\\_theory#Set\\_Theory\\_Exercise\\_1](http://en.wikibooks.org/wiki/Discrete_Mathematics/Set_theory#Set_Theory_Exercise_1)

Work through the first three exercise sections whose links are found on the Wikibook page. △

**Directive 3.2:** Consider the empty set, which is something but has no elements in it. We will denote the empty set with the symbol:

$$\emptyset$$

Now contemplate what it is in it. We will take as a starting point an assumption, i.e. an *axiom*:

$\emptyset$  is a set.

This kind of assumption is called a *comprehension axiom*. Intuitively, the idea is that we can comprehend the idea of a set with no elements in it in a way that is logically consistent with lots of other ideas we have about sets. It is an assumption. We cannot prove there is such a set. We will make that assumption one of our starting points. The other starting points are the basic operations that can be applied to sets that are discussed in the wiki article and wiki book in the previous directive. In this section, we will build the low levels of the *Von Neumann Universe* that are of interest to us in computer science and engineering. △

**Note 3.1:** When you read technical material in this course, such as textbooks, wikibooks, technical articles, etc., verify what you read and read critically. △

**Note 3.2:** According to the wikibook on sets a set can be defined as *a collection of things that are brought together because they obey a certain rule*. What's a *collection*? What's a *rule*? What does it mean, *mathematically*, to bring things together? You will never succeed in making a mathematical model of these things without presupposing mathematics that amounts to presupposing that we already have sets available. And around and around we go – which makes the wikibook definition of a set a piece of crap. But - this is extremely important - a piece of crap like this so-called definition can still embody powerful and highly useful intuitions.

As we proceed we will state various comprehension axioms that conveniently allow us to express specific rules for forming sets without the need to have a general theory of rules, collections, and “bringings together”.

In this note I have criticized using a term like *rule* in a mathematical definition, and then I used the very word I criticized in the previous paragraph. This seems inconsistent. What needs to be reflected upon here is that the use of the word *rule* in the previous paragraph is in *commentary* on mathematical description and not in mathematical description itself.

In section (1) we used sets to define relations. We now introduce a few specific relation-like ideas that are not relations according to what was given in section (1). We make the assumption that for anything  $x$ , it is true that  $x$  is a set, or it is true that  $x$  is not a set, but not both. Secondly, we make the assumption that for anything  $x$  and any set  $S$ , that it is either true that  $x$  is a *member* of  $S$  or it is not true that  $x$  is a *member* of  $S$  but not both. (If everything is a set, then we can dispense with the first of these two assumptions - and that is what is done in formal set theory. We need not worry about that for now.  $\triangle$

## 4 Some set-theoretic constructions

**Definition 4.1:** For any sets  $A$  and  $B$ , the set  $A \times B$ , called the *Cartesian Product* of  $A$  and  $B$ , is the set of all ordered pairs  $(a, b)$  such that  $a \in A$  and  $b \in B$ . In other words,

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

$\triangle$

**Remark 4.1:** The preceding definition begs a question: What is an ordered pair? The issue is that whatever an ordered pair is, it should be something independent of how it is denoted. One way to rigorously define ordered pairs, and while we’re at it, ordered  $n$ -tuples in terms of previously understood notions is the following: Let  $\mathbb{N}$  be the set of non-negative integers. Let  $n \in \mathbb{N}$ . An sequence of elements of a set  $A$  of length  $n$  is a function from  $\{0, \dots, n - 1\}$  to  $A$ . Let  $\mathbf{a}$  be a sequence of length  $n$ , where  $n > 0$ . Then we also denote  $\mathbf{a}$  by  $(\mathbf{a}_0, \dots, \mathbf{a}_{n-1})$ . Thus, the ordered pair

$(x, y)$  of elements of a set  $S$ , is a function from  $\{0, 1\}$  to  $S$  where the application of the function to 0 is  $x$  and the application of the function to 1 is  $y$ . An  $n$ -tuple is a sequence of length  $n$ .  $\triangle$

**Remark 4.2:** There's a problem with the previous remark: An ordered pair is a function and a function is a certain kind of set of ordered pairs - which seems circular. What's the way out of the circularity? One way out is to construct *basic* ordered pairs out of sets. Given two things  $x, y$ , which may or may not be the same, we obtain *basic* ordered pairs  $\{\{x\}, \{x, y\}\}$  and  $\{\{y\}, \{y, x\}\}$ . We denote these two *basic* ordered pairs by  $(x, y)$  and  $(y, x)$ , respectively. We can then take functions to be a certain kinds of sets of *basic* ordered pairs.  $\triangle$

**Directive 4.1:** Prove that  $(x, y) = (x', y')$  iff  $x = x'$  and  $y = y'$ , where  $(x, y)$  and  $(x', y')$  are *basic* ordered pairs.  $\triangle$

**Notation 4.1:** Let  $A_0, \dots, A_{n-1}$  be a sequence of length  $n$  of sets. Then

$$A_0 \times \dots \times A_{n-1}$$

is the set of sequences  $\mathbf{a}$  of length  $n$  to the set  $A_0 \cup \dots \cup A_{n-1}$  such that  $\mathbf{a}_k \in A_k$ , for each  $k \in \{0, \dots, n-1\}$ .  $\triangle$

**Example 4.1:** Let  $A = \{0, 1, 2\}$  and let  $B = \{0, 1\}$ . Then

$$A \times B = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}.$$

$\triangle$

**Example 4.2:** Let  $\mathbb{N}$  be the set of non-negative integers. That is,  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ . Then

$$\mathbb{N} \times \mathbb{N} = \{(m, n) \mid m \in \mathbb{N} \text{ and } n \in \mathbb{N}\}.$$

$\triangle$

**Definition 4.2:** A *relation*  $R$  from set  $A$  to set  $B$  is a triple  $(P, A, B)$  where  $P$  is a subset of  $A \times B$ . (We usually just write  $R$  instead of writing the whole triple  $(R, A, B)$  when we refer to a relation  $R$  from a set  $A$  to a set  $B$ ; i.e. we abuse notation and let the subset of  $A \times B$  stand in for  $R$ .)  $\triangle$

**Remark 4.3:** We informally identify a *relation*  $R$  from  $A_0 \times \dots \times A_{n-1}$  to  $B$  with a subset of  $A_0 \times \dots \times A_{n-1} \times B$ . We call such a relation an  $n$ -ary relation. This begs a question: what is  $A_0 \times \dots \times A_{n-1}$ , if  $n = 0$ ? This cartesian product is a set of sequences from the empty set, to some set. There is only one such such function (remember: a sequence is a function), the empty function. The empty function takes no inputs and returns nothing. So, the *empty cartesian product* is a set containing the empty function and no other elements.  $\triangle$

**Definition 4.3:** (*Cartesian powers of a set*). Let  $A$  be a set. For each  $n \in \mathbb{N}$ ,  $A^n$  is the set  $A_0 \times \dots \times A_{n-1}$ , where each  $A_k$  is  $A$ .  $A^n$  is called the  $n^{\text{th}}$  *cartesian power* of  $A$ .  $A^0$  is the empty cartesian product.  $\triangle$

**Definition 4.4:** ( *$n$ -ary relation on a set*). Let  $n \in \mathbb{N}$ . An  $n$ -ary relation on a set  $A$ , where  $n > 0$  is a relation from  $A^{n-1}$  to  $A$ . A 0-ary relation on a set  $A$  is a subset of  $A^0$ . A *unary* relation is a 1-ary relation. A *binary* relation is a 2-ary relation.  $\triangle$

**Problem 4.1:** How many 0-ary relations are there on a nonempty set  $A$ ? Describe them. How many 0-ary relations are there on the empty set? Describe them. Explain why no 0-ary relation on the set  $\{0\}$  can be same relation as any 0-ary relation on the set  $\{1\}$ .  $\triangle$

**Problem 4.2:** Show that  $A^1$  is in one-to-one correspondence with  $A$ .  $\triangle$

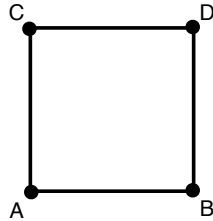
**Definition 4.5:** (*Directed graph*). A *directed graph* is a pair  $(V, E)$ , consisting of a set  $V$  and a binary relation  $E$  on  $V$ . A member of  $V$  is called a *vertex* (*vertices* [pl.]). A member of  $E$  is called an *edge*.  $\triangle$

**Notation 4.2:** Let  $D = (V_D, E_D)$  be a directed graph. Let  $u$  be a vertex in  $V_D$ . Let  $E_D \upharpoonright u = \{(u, v) \mid (u, v) \in E_D\}$ . (These are the edges in  $D$  from  $u$  to some vertex.)  $\triangle$

**Problem 4.3:** How many directed graphs are there with vertex set  $\{0, 1, 2\}$ ? Explain your reasoning.  $\triangle$

## 5 An excursion through symmetry

**Note 5.1:** Consider a graph  $\mathcal{S}$  (a graph is a set of vertices together with a symmetric relation on the set of vertices called the edge relation).



The relation depicted by this graph is a relation from  $\{A, B, C, D\}$  to  $\{A, B, C, D\}$  and is determined by one of the subsets of

$$\{A, B, C, D\} \times \{A, B, C, D\}$$

In other words, the relation depicted by this graph is a triple

$$(\{A, B, C, D\}, \{A, B, C, D\}, R)$$

where

$$R \subseteq \{A, B, C, D\} \times \{A, B, C, D\}$$

Thus,  $R$  is a set of pairs. △

**Problem 5.1:** List the pairs in  $R$ . [**Hint:** There are eight pairs (8 because the edges point both ways).] △

**Problem 5.2:** Look up definitions as necessary. In class, you can ask me questions. There are four particularly important properties of 2-place relations on a set: *reflexivity*, *symmetry*, *transitivity* and *antisymmetry*. Give an example of a nonempty 2-place relation on a set that is reflexive and symmetric, but not transitive; reflexive and transitive, but not symmetric, and symmetric and transitive but not reflexive. △

**Definition 5.1:** (*field of a relation*) Let  $R$  be a 2-place relation on set  $A$ . Then

$$\text{field}(R) = \{x \in A \mid \exists y [(x, y) \in R \vee (y, x) \in R]\}$$

△

**Problem 5.3:** Argue that a symmetric and transitive relation is symmetric on its field.  $\triangle$

**Definition 5.2:** (*neighborhood*) Let  $D$  be the directed graph  $(V, E)$  ( $V$  is a set and  $E$  is a relation on  $V$ ). Let  $x \in V$ ; i.e. let  $x$  be a vertex of  $D$ . Any set of vertices of  $D$  that contains the set

$$\{y \in V \mid (x, y) \in D\}$$

is a *neighborhood* of  $x$ . In particular,  $\{y \in V \mid (x, y) \in D\}$  is the least neighborhood of  $x$ .  $\triangle$

**Definition 5.3:** (*subset*) Let  $A$  and  $B$  be sets. (They may, or may not, be the same set.)  $A$  is a *subset* of  $B$  (denoted by  $A \subseteq B$ ) iff for every element  $y$  of  $A$ ,  $y$  is a member of  $B$ . The subset relation is also called *set-inclusion*.  $\triangle$

**Note 5.2:** Notice that the preceding definition gives a test to see whether one set is a subset of another. If you are given two sets  $P$  and  $Q$ , to see whether  $P \subseteq Q$ , you test each element of  $P$  to see whether it is a member of  $Q$ . This of course depends on already having a way to range over the elements of  $P$ , and a test to see whether or not something is an element of  $Q$ . The test for  $P \subseteq Q$  also depends on being able to test, if  $P$  is infinite and the test can be finished, all of the infinitely many elements of  $P$  in some finite amount of time. This is not as absurd as it seems. Although we cannot *do* infinitely many tests in a finite amount of time, we can *reason* about infinitely many things in a finite amount of time, at least sometimes. For example, we can reason that every one of the infinitely many prime numbers is not a perfect square.  $\triangle$

**Note 5.3:** In reading, understanding, and using mathematical discourse, it is important to understand such words/phrases as “every”, “each” and “for all”. Suppose it is given that there are no square circles. (There are no square circles in Euclidean geometry, unless we consider single points as so-called *degenerate cases*. It follows that every square circle is a triangle. This seemingly absurd statement follows from the given assertion that there are no square circles because, if it were false, then there would be a square circle that is not a triangle. In other words, “Every square circle is a triangle.” would have a *counterexample*. But since, there are no square circles, there cannot be a counterexample. This “no counterexample” interpretation is simply built into the use of such words as “every” in mathematical discourse.  $\triangle$

**Note 5.4:** Incidentally, in ancient Greek philosophy and mathematics, their concept of “every” did not quite have this no-counter example idea built in. When Aristotle, for example, used what we in our time translate as “every”, his notion had what we call “existential import”. When he said, “Every person is mortal”, he meant what we mean by “Every person is mortal and there is at least one person.” “Existential import” and “no-counterexample” are not fully compatible. So Aristotle’s reasoning does not always *appear* valid to us, and our reasoning would not always *appear* valid to him. But this does not make either notion of what counts as valid reasoning into something subjective, because we and he could discuss in an exact way (after he and we worked at learning enough in common about our languages) enough of our background assumptions to resolve the apparent incompatibility.  $\triangle$

**Problem 5.4:** This task applies the no-counterexample interpretation. Let  $A$  be a set, and let  $\emptyset$  be the empty set (also called the null set). The empty set does not have any members. Give a careful, accurately expressed argument that proves  $\emptyset \subseteq A$ .  $\triangle$

**Definition 5.4:** (symmetry) A binary relation  $R$  on a set  $A$  is *symmetric* iff for every  $x \in A$  and  $y \in A$ , if  $x R y$ , then  $y R x$ .  $\triangle$

**Problem 5.5:** The least neighborhood of the vertex  $A$  in  $\mathcal{S}$  is  $\{B, C\}$ . What are the least neighborhoods of  $B$ ,  $C$  and  $D$ ? Verify the answer given below.

**Answer:** Let  $\text{LNbhd}(x)$  be the least neighborhood of  $x$ . Then

$$\begin{aligned} \text{LNbhd}(A) &= \{B, C\} \\ \text{LNbhd}(B) &= \{A, D\} \\ \text{LNbhd}(D) &= \{B, C\} \\ \text{LNbhd}(C) &= \{A, D\} \end{aligned}$$

$\triangle$

**Note 5.5:** What does *least* mean? To answer this question we will sort out the concepts of *minimal*, *minimum*, *maximal* and *maximum*. *least* and *smallest* are synonyms for *minimum*. *greatest* and *largest* are synonyms for *maximum*. We will also consider *lower bound* and *upper bound*.  $\triangle$

**Definition 5.5:** (*minimum*, *maximum*) Let  $(D, \sqsubseteq)$  be a poset and let  $A \subseteq D$ .  $a$  is a *minimum element* of  $A$  iff  $a \in A$  and for every  $b \in A$ ,  $a \sqsubseteq b$ .  $a$  is a *maximum element* of  $A$  iff  $a \in A$  and for every  $b \in A$ ,  $b \sqsubseteq a$ .  $\triangle$

**Definition 5.6:** (*minimal*) Let  $(D, \sqsubseteq)$  be a poset and let  $A \subseteq D$ .  $a$  is a *minimal element* of  $A$  iff  $a \in A$  and for every  $b \in A$ , if  $b \sqsubseteq a$ , then  $b = a$ . **Comment:** Less formally, a minimal element of  $A$  is an element  $a$  of  $A$  such that there is no element of  $A$  below  $a$ .  $\triangle$

**Definition 5.7:** (*maximal*) Let  $(D, \sqsubseteq)$  be a poset and let  $A \subseteq D$ .  $a$  is a *maximal element* of  $A$  iff  $a \in A$  and for every  $b \in A$ , if  $a \sqsubseteq b$ , then  $a = b$ .  $\triangle$

**Definition 5.8:** (*lower bound, upper bound*) Let  $(D, \sqsubseteq)$  be a poset and let  $A \subseteq D$ . An element  $x$  in  $D$  is a *lower bound* of  $A$  iff for every  $a$  in  $A$ ,  $x \sqsubseteq a$ . An element  $x$  in  $D$  is an *upper bound* of  $A$  iff for every  $a$  in  $A$ ,  $a \sqsubseteq x$ . We use the notation  $x \sqsubseteq A$  to say that  $x$  is a lower bound of  $A$ . Similarly, we write  $A \sqsubseteq x$  to say that  $x$  is an upper bound of  $A$ . **Comment:** An upper bound of  $A$  may or may not be an element of  $A$ .  $\triangle$

**Proposition 5.1:** Let  $(D, \sqsubseteq)$  be a poset and let  $A \subseteq D$ . Then,  
 (i)  $a$  is a *least* element of  $A$  iff  $a$  is a greatest lower bound of  $A$ , and  $a \in A$ .  
 (ii)  $a$  is a *greatest* element of  $A$  iff  $a$  is a least upper bound of  $A$ , and  $a \in A$ .  $\triangle$

**Problem 5.6:** Find an example of an infinite poset  $D$  and subset  $A$  of  $D$  that has a *unique* minimal element that is not the least element of  $A$ . You may find it helpful to sketch posets by using Hasse diagrams - check out the wiki article at

[http://en.wikipedia.org/wiki/Hasse\\_diagram](http://en.wikipedia.org/wiki/Hasse_diagram)

$\triangle$

**Problem 5.7:** Let  $(D, \sqsubseteq)$  be a poset and let  $A \subseteq D$ . Show that there is at most one greatest lower bound of  $A$ . (Therefore, if  $A$  has a greatest lower bound, then it is unique.) Show that there is at most one least upper bound of  $A$ .  $\triangle$

**Note 5.6:** Recall that we were considering least neighborhoods of the vertices of directed graph  $\mathcal{S}$ . Thus when we mention the least neighborhood of vertex  $A$ , the underlying partial order is set-inclusion  $\subseteq$ , the poset is  $(2^{\{A,B,C,D\}}, \subseteq)$ , and the subset of  $2^{\{A,B,C,D\}}$  to be considered is the set of all neighborhoods of vertex  $A$ .  $\triangle$

**Definition 5.9:** (*homomorphism*) Suppose we have two directed graphs (which might or might not actually be different)  $D_1 = (V_1, E_1)$  and  $D_2 = (V_2, E_2)$ . Suppose

$$\varphi : V_1 \longrightarrow V_2$$

$\varphi$  is a *homomorphism* of  $D_1$  and  $D_2$  iff for all vertices  $x$  and  $y$  of  $D_1$ , if  $(x, y) \in E_1$ , then  $(\varphi(x), \varphi(y)) \in E_2$ .  $\triangle$

**Definition 5.10:** (*permutation*) A permutation of a set  $S$  is a 1-to-1 and onto function from  $S$  to  $S$ . △

**Remark 5.1:** We think of permutations of a set as reordering of an ordered set. It is true that all permutations of a finite set (except the identity function which can be thought of as the trivial permutation that does nothing) reorder the set. But a permutation of an infinite set need not reorder it. For example, the function that adds 1 to each integer is a permutation of the integers but does not reorder them. In the next few items we will concentrate on permutations of finite sets. △

**Definition 5.11:** (*cycle*) Let  $\sigma$  be a permutation of set  $S = a_1, \dots, a_n$  such that for distinct  $a_{j_1}, \dots, a_{j_k}$

$$\begin{aligned}\sigma(a_{j_1}) &= a_{j_2} \\ \sigma(a_{j_2}) &= a_{j_3} \\ &\vdots \\ \sigma(a_{j_k}) &= a_{j_1}\end{aligned}$$

and for all  $a \in S$  other than  $a_{j_1}, \dots, a_{j_k}$ ,  $\sigma(a) = a$ . Then  $\sigma$  is a *cycle*. The cycle  $\sigma$  can be denoted by  $(a_{j_1} a_{j_2} \dots a_{j_k})$  [no commas]. △

**Example 5.1:** (*some cycles of a 5-element set*) Consider the cycle

$$(1\ 3\ 4)$$

on the set  $\{1, 2, 3, 4, 5\}$ . This cycle maps 1 to 3, 3 to 4 and 4 to 1. The cycle leaves 2 and 5 fixed.

Now consider the permutation whose I/O table is

Input	Output
1	3
2	5
3	4
4	1
5	2

This permutation maps 1 to 3, 3 to 4, and 4 to 1. It also maps 2 to 5 and 5 to 2. It is the composition of two cycles:  $(1\ 3\ 4); (2\ 5)$ : The notation says that to calculate the results of this noncyclic permutation we apply  $(1\ 3\ 4)$  first, then apply  $(2\ 5)$ . It turns out that the composition of these two cycles in the opposite order yields the

same result the two cycles are disjoint. Consider the composition of two cycles that are not disjoint:  $(1\ 3\ 5); (2\ 5)$ . What does this permutation map 1 to? It maps 1 to 3 and the second 2-cycle maps 3 to 3, so the composition maps 1 to 3. The first 3-cycle maps 2 to 2 and the 2-cycle maps 2 to 5. Therefore, 2 is mapped to 5. Hence 2 is mapped to 5 by the composition. The 3-cycle maps 3 to 5 and the 2-cycle maps 5 to 2. Hence 3 is mapped to 2 by the composition. 4 is left fixed by the composition and 5 is mapped to 1 by it.  $\triangle$

**Problem 5.8:** Verify that permutation  $(2\ 5); (1\ 3\ 5)$  on the set  $\{1, 2, 3, 4, 5\}$  maps 1 to 3, 2 to 1, 3 to 5, 4 to 4, and 5 to 2. Thus

$$(1\ 3\ 5); (2\ 5) \neq (2\ 5); (1\ 3\ 5)$$

$\triangle$

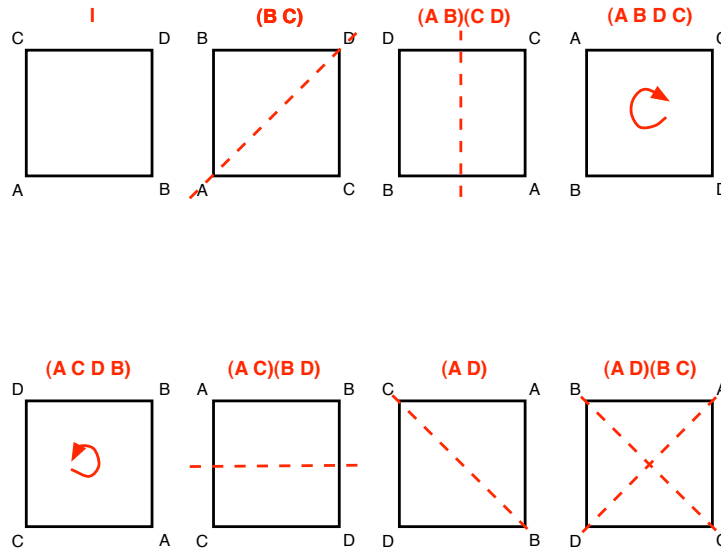
**Example 5.2:** Consider the permutation  $(C\ D)$  of the vertices of  $\mathcal{S}$ . (We are using cycle notation.) Let  $\rho = (C\ D)$ . Then (recall the definition of the image of a set with respect to a function that was given in class)

$$\rho(\{A, C\}) = \{A, D\}$$

Notice that there is an edge  $(A, C)$  in  $\mathcal{S}$ , but there is no edge  $(A, D)$  in  $\mathcal{S}$ . Therefore,  $\pi$  is **not** a homomorphism from  $\mathcal{S}$  to  $\mathcal{S}$ .  $\triangle$

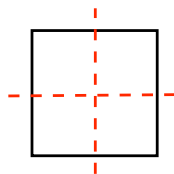
**Problem 5.9** Verify the answer give below to the problem of finding all of the permutations of the set of vertices of  $\mathcal{S}$  that are homomorphisms from  $\mathcal{S}$  to  $\mathcal{S}$ . (There are eight such homomorphisms.)

**Answer:**



$\triangle$

**Problem 5.10** What homomorphism is suggested by:



△

**Definition 5.12** (*Group*). A *group*  $G$  is a set  $|G|$  together with an operation

$$\cdot : (|G| \times |G|) \longrightarrow |G|$$

such that there is an element  $i$  in  $|G|$  such that for any  $x, y, z$  in  $G$ ,

1.  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2.  $x \cdot i = x$
3. there is an element (denoted by  $x^{-1}$  such that  $x \cdot x^{-1} = i$ )

The function  $\cdot : (|G| \times |G|) \longrightarrow |G|$  is called the *operation* of  $G$ . The element  $i$  is the *identity* of the group and  $x^{-1}$  is the *inverse* of  $x$ . When the group operation is sufficiently clear from the context we often suppress the notation for the operation and write e.g.  $xy$  for  $x \cdot y$ . △

**Example 5.3** (*Symmetric Group  $S_3$* ) The elements of the symmetric group  $S_3$  are the permutations on a set of three elements such as  $\{P, Q, R\}$ : namely  $()$ ,  $(P Q)$ ,  $(P R)$ ,  $(Q R)$ ,  $(P Q R)$ ,  $(P R Q)$ . This collection of permutations forms a group where the operation is function composition  $\circ$ . Recall that if we have two functions  $f : A \longrightarrow B$  and  $g : B \longrightarrow C$ , then  $(f; g) : A \longrightarrow C$ , where  $(f; g)(a) = g(f(a))$ , for all  $a \in A$ . The operation of a group is often called *multiplication*. Sometimes, when it seems appropriate, the group operation is called addition. The result of multiplying group elements is called a *product* of the elements. △

**Problem 5.11** Fill in the group operation table depicted below:

$\circ$	$()$	$(P Q)$	$(P R)$	$(Q R)$	$(P Q R)$	$(P R Q)$
$()$	$()$	$(P Q)$	$(P R)$	$(Q R)$	$(P Q R)$	$(P R Q)$
$(P Q)$			$(P Q R)$			
$(P R)$				$(P Q R)$		
$(Q R)$		$(P Q R)$				
$(P Q R)$	$(P Q R)$					
$(P R Q)$						

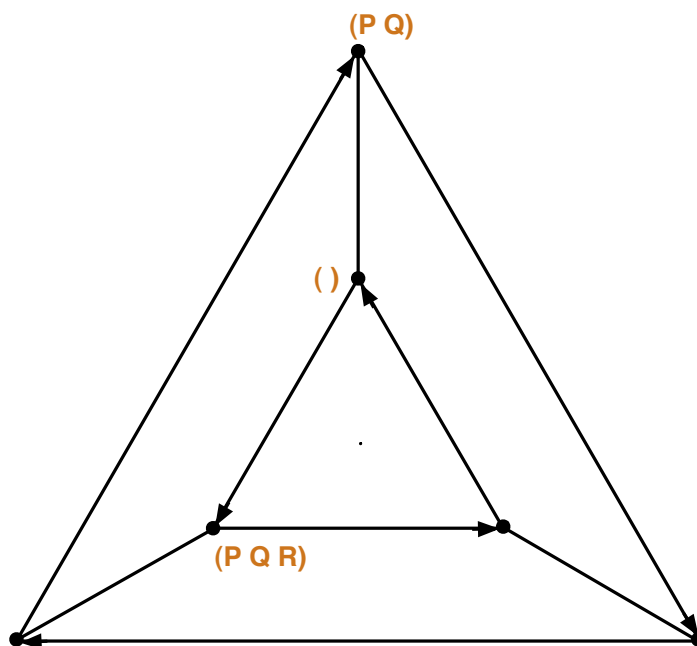
One hint that we will use below:  $(P R Q)^{-1} = (P Q R)$ . △

**Definition 5.13** (*Generators*). A set of *generators* for a group is a set of elements of the group such that every element of a group is a product of generators and inverses of generators. There is no assumption about the independence of generators. A generator might or might not be the product of other generators, and the inverse of a generator might or might not be a generator. △

**Problem 5.12** Verify that  $\{(P Q), (PQR)\}$  is a set of generators for  $S_3$ . △

**Definition 5.14** (*Cayley graph*) The *right Cayley graph* of a group  $G$  with respect to a set of generators  $S \subseteq |G|$  is the directed graph  $(V, E)$ , where  $V = |G|$  and  $(x, y) \in E$  iff there is a generator  $g \in S$  such that  $x \cdot g = y$ . (Guess the definition of left Cayley graphs.) △

**Example 5.4** The right Cayley graph of  $S_3$  with respect to the set of generators  $\{(P Q), (PQR)\}$ :



△

**Problem 5.13** Part 1: Correctly label the remaining three unlabeled vertices of the Cayley graph, above. Part 2: Include an extra generator ( $P R$ ) and add the appropriate edges to the Cayley graph that correspond the new generator.  $\triangle$

**Problem 5.14** Explain why addition mod 3 on the set of integers  $\{0, 1, 2\}$  forms a group. This group is denoted  $\mathbb{Z}_3$  (or sometimes for emphasis:  $(\mathbb{Z}_3, +)$ ).  $\triangle$

**Definition 5.15** (*Group homomorphism*) Let  $G$  and  $H$  be groups and let  $\varphi : G \rightarrow H$  be a function such that  $\varphi(xy) = \varphi(x)\varphi(y)$ , for all  $x, y \in |G|$ . Then  $\varphi$  is said to be a *homomorphism*. If  $G = H$ , then  $\varphi$  is said to be an *endomorphism*. If  $\varphi$  is injective, then  $\varphi$  is a *monomorphism* (and sometimes called an *injection*). If  $\varphi$  is a bijection, then  $\varphi$  is an *isomorphism*.

$\triangle$