

Learn You Some Algebras for Glorious Good!

Peter Harpending jpharpend2@gmail.com

December 31, 2014

Copyright 2014 Peter Harpending {pharpend2@gmail.com}.

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 § A.

Editors & Noted Contributors

Randy Brown	randy@beingbrown.net
Nick Chambers	DTSCode@gmail.com
Anton Golov	jesyspa@gmail.com
Ng Wei En	wei2912.sup0rt@gmail.com
Ben Z RF	benzrf@benzrf.com

Contents

1	Introduction	9
1.1	Introduction (for real this time)	10
1.2	The community	11
1.3	Licensing	11
1.4	Conventions used in this book	12
2	Sets	15
2.1	Numeric sets	21
2.2	Functions	22
2.3	Injective Functions	26
2.4	Subsets	27
2.5	Cardinalities	30
2.6	The Power Set	30
2.7	The Category of Sets	30
2.8	Special kinds of sets	30
2.8.1	Magnas	30

2.8.2	Semigroups	30
2.8.3	Monoids	30
3	Proofs	33
3.1	Peano Axioms	33
	Appendices	41
A	GNU Free Documentation License	45
1.	APPLICABILITY AND DEFINITIONS	45
2.	VERBATIM COPYING	46
3.	COPYING IN QUANTITY	46
4.	MODIFICATIONS	47
5.	COMBINING DOCUMENTS	48
6.	COLLECTIONS OF DOCUMENTS	49
7.	AGGREGATION WITH INDEPENDENT WORKS	49
8.	TRANSLATION	49
9.	TERMINATION	49
10.	FUTURE REVISIONS OF THIS LICENSE	50
11.	RELICENSING	50
	ADDENDUM: How to use this License for your documents	50
B	How to learn math	53

Chapter 1

Introduction

Before I bore you with a bunch of crap you don't care about, let's do some math, shall we?

There are basically three notions with which you need to be familiar in order to do anything interesting in math. Those three things are *sets*, *functions*, and *proofs*. Unfortunately, to be familiar with one, you have to be familiar with the other two.¹

So, what are each of those things?

- A *set* is an unordered collection of things. There is also no repetition. For instance, $\{2, 5\}$ is the same as $\{5, 2\}$ (because order doesn't matter). $\{2, 5, 5\}$ would be the same set, because there's no notion of multiplicity.
- A *function* is a mathematical construct (well, obviously, else I wouldn't be talking about it). Basically, it takes some input, does something to it, and spits out some output. If you give the function the same input a bunch of times, you should get the same result each time. This concept is called "referential transparency." If the function is not referentially transparent, then it's not a function. It's something else.

¹You'll learn as we go along, when math people use a common term like *set*, *function*, *proof*, *group*, *continuous* or *closed*, they usually mean something similar in concept to the colloquial term, but there are some strings attached. This is usually the case in the sciences too (e.g. *theory*, *hypothesis*, *experiment*).

- A *proof* is basically where you take a bunch of simple facts, called *axioms*, and chain them together to make *theorems*. It's sort of like sticking puzzle pieces together to form a picture.

The puzzle pieces (in this case, the axioms) aren't usually very interesting on their own. However, the picture they form (in this case, the theorem) can be really cool and enlightening. The proof would be analogous to an explicit set of instructions explaining how to put the pieces together.

Once you are familiar with each of those concepts, we can do all sorts of cool stuff. Throughout the book, we will prove all of the following:

- If you tap your finger against a bridge at exactly the right frequency, the bridge will collapse. (Resonance)
- The formula used to calculate the interest rate on your mortgage is actually just a fancy form of the ratios of angles in a triangle. (Euler's formula)
- Logic can't be used to prove everything we know to be true. (Gdel's incompleteness theorem)

1.1 Introduction (for real this time)

This is a math book. Well, duh. Why did I write it?

Most math (and science) books nowadays seem to value keeping an academic tone over ensuring that the reader understands the material, and — more importantly — enjoys reading the book.

I take the opposite approach. I want to create a book that is fun to read and easy to understand, while eschewing the practice of making myself look good.

The inspiration for this book is *Learn You a Haskell for Great Good!*, by Miran Lipovaa. Haskell is a programming language, and LYAH is a great

book for learning Haskell. If you are interested in a print copy of LYAH, see [2].

1.2 The community

Despite the fact that I used “I” in the first part of the book, LYSA is actually a community project, and many people participate in the writing of this book.

If you want to talk to us, or to other math people, come see us in `#lysa` on Freenode. If you don’t know what IRC is, or you don’t have a client set up, you can connect through Freenode’s webchat (<http://webchat.freenode.net/?channels=lysa>).

If you have any questions about LYSA (or math), feel free to ask in the IRC channel (`#lysa` on FreeNode in case you forgot).

If you want to submit a correction, or have some issue, or want to add some content, really anything having to do with the content of the book, you can visit <https://gitlab.com/lysa/lysa> (ourGitLabpage). We also have a community on Reddit (<https://lysa.reddit.com/>).

1.3 Licensing

This book is free, in the sense of freedom. You can copy this book and give it to your friend. You can even print it out and sell it to your friends.²

If, for instance, you are a schoolteacher and want to use this for your class, you are free to edit it to your liking and give the modified copy to your students.

LYSA is licensed under the GNU Free Documentation License. § A contains the license. Please read the license; it’s actually pretty comprehensible.

The source for this book can be downloaded at <https://gitlab.com/>

²There are some restrictions though, see § A.

lysa/lysa/repository/archive.tar.gz. If you are looking to contribute, it's probably best to clone the git repository. You can clone the git repository by running `git clone https://gitlab.com/lysa/lysa.git` in a terminal.

1.4 Conventions used in this book

The

Chapter 2

Sets

Anyway, now that that boring introduction is out of the way, we can get to some math! The first thing we are going to cover are *sets*.

Sets were first studied by Georg Cantor, a German mathematician, in the second half of the nineteenth century. Back in his own day, the patterns Cantor found by studying set theory were considered so thoroughly bizarre that many of his colleagues simply refused to believe that Cantor could be right. In the end, Cantor turned out to be right all along. His ideas can be found in any introductory text on mathematics—including this one.

Sets are basically like lists, except there's no duplication, and there's no order. Examples:

1. $\{0, 1, 2, 3\}$ is a set.
2. $\{1, 2, 0, 3\}$ is the same set.
3. $\{1, 1, 2, 0, 3\}$ is the same set, because there's duplication.

To give you some more notation:

1. $0, 1, 2, 3$ **is not** a set, it is instead the numbers 0 through 3, which are to be considered separately.

2. $\{0, 1, 2, 3\}$ **is** indeed a set (notice the braces).
3. If some object is in a set, the notation is ‘ $\text{OBJECT} \in \text{SET}$ ’, which should be read “OBJECT is an element of SET”.
4. If the object is not in the set, the notation is ‘ $\text{OBJECT} \notin \text{SET}$ ’, which should be read “OBJECT is not an element of SET”.
5. $0 \in \{0, 1, 2, 3\}$ should be read “0 is an element of $\{0, 1, 2, 3\}$ ”, and indeed it is.
6. $0, 1 \in \{0, 1, 2, 3\}$ should be read “0 and 1 **are both** elements of $\{0, 1, 2, 3\}$ ”. They are.
7. $\{0, 1\} \notin \{0, 1, 2, 3\}$ should be read “ $\{0, 1\}$ **is not** an element of $\{0, 1, 2, 3\}$ ”. $\{0, 1\}$ is indeed not an element of $\{0, 1, 2, 3\}$.

Now, here, we’re faced with an interesting problem. $\{0, 1, 2, 3\}$ encapsulates $\{0, 1\}$, but $\{0, 1\}$ is not an element of $\{0, 1, 2, 3\}$. So, how do we express this notion of ‘encapsulation’? The answer is by using “subset” notation.

1. $\{0, 1\} \subseteq \{0, 1, 2, 3\}$ is **true**. $\{0, 1\} \subseteq \{0, 1, 2, 3\}$ should be read as “ $\{0, 1\}$ is an **improper** subset of $\{0, 1, 2, 3\}$.”
2. $\{0, 1\} \subset \{0, 1, 2, 3\}$ is **true**. $\{0, 1\} \subset \{0, 1, 2, 3\}$ should be read as “ $\{0, 1\}$ is a **proper** subset of $\{0, 1, 2, 3\}$.”
3. $\{0, 1, 2, 3\} \subseteq \{0, 1, 2, 3\}$ is **true**. Intuitively, you should think “ $\{0, 1, 2, 3\}$ is entirely encapsulated inside of $\{0, 1, 2, 3\}$.”
4. $\{0, 1, 2, 3\} \subset \{0, 1, 2, 3\}$ is **false**. This highlights the difference between \subset and \subseteq .
 $\{0, 1\} \subset \{0, 1, 2, 3\}$ implies that $\{0, 1, 2, 3\}$ contains some stuff that is not contained in $\{0, 1\}$. $\{0, 1\} \subseteq \{0, 1, 2, 3\}$ does not have this implication. That is, $\{0, 1\} \subseteq \{0, 1, 2, 3\}$ does not say for sure that $\{0, 1, 2, 3\}$ has more stuff than $\{0, 1\}$, it just acknowledges it as a possibility.

Alright, my apologies, that was a lot of crap to throw at you at once, and you probably remember absolutely none of it. However, you’ll get used to

that particular *set* of crap¹ as time goes along. Anyway, the next page has some exercises.

I would recommend that you do all of the exercises. Many books berate you with dozens of exercises all exercising the same problem. I'm too lazy to do that; instead, I'm going to give you a small number of exercises. The reason I do that is, I have to solve the exercises, too. The solutions are on the page after the exercises.

¹I, for one, would never condone such terrible puns.

Exercises

Ex. 1 — Say you are given a set. It can be any set, it doesn't matter which set. However, for the sake of brevity, I'm going to call that set S . Next, you are given a number, I'm going to call the number n . Does it make sense to ask "how many times does S contain n ?" Why or why not?

Ex. 2 — Say you are given the same set, S . However, you are also given another set, T . If you know $S \subset T$, is it also true that $S \subseteq T$? Why or why not?

Ex. 3 — What about, if you know $S = T$, is it also true that $S \subseteq T$? Why or why not?

Ex. 4 — If it is known that $S \subseteq T$, is it also true that $S \subset T$? Why or why not?

Ex. 5 — Let's look back at S , T , and n . Let's say that you know $n \in S$ (that is, n is in S). You also know that $S \subseteq T$. Does this also mean $n \in T$? Why or why not? To put this in mathematical notation:

$$\{n \in S, S \subseteq T\} \stackrel{?}{\implies} n \in T$$

Ex. 6 — Since I'm lazy, and the math notation is probably much easier for you to understand,

$$\{n \in T, S \subseteq T\} \stackrel{?}{\implies} n \in S$$

Ex. 7 — What about the opposite? That is,

$$S \subseteq T \stackrel{?}{\Longleftarrow} \{n \in S, n \in T\}$$

Answers

Answer (Ex. 1) — No, because repetition doesn't matter.

Answer (Ex. 2) — Yes. $S \subseteq T$ means that one of $\{S \subset T, S = T\}$ is true. If $S \subset T$ is true, then the condition of $S \subseteq T$ is satisfied. Thus, $S \subset T \implies S \subseteq T$.

Answer (Ex. 3) — Yes, by the same logic above. If $S = T$, then the conditions for $S \subseteq T$ are satisfied.

Answer (Ex. 4) — No.

- $S \subset T$ can be stated as “all of $\{S \subseteq T, S \neq T\}$ are true.”
- By the previous problem, if $S \neq T$ is false (i.e. $S = T$ is true), then $S \subseteq T$ is true.
- In this case, the set above could be written as $\{S \subseteq T, S \neq T\} = \{True, False\}$. $S \subset T$ means that both of those have to be true. That is, $S \subset T$ is true if (and only if) $\{S \subseteq T, S \neq T\} = \{True, True\}$.
- In this case, we have $\{S \subseteq T, S \neq T\} = \{True, False\}$, which means $S \not\subset T$.
- Thus, we have just found a case in which $S \subseteq T$ is true, but $S \subset T$ is false. Therefore, it cannot be the case that $S \subseteq T \implies S \subset T$. Or, to put it another way, $S \subseteq T \not\implies S \subset T$.

Answer (Ex. 5) — Yes. $S \subseteq T$ means that all of the elements in S are also in T , but not necessarily the other way around.. Thus, if $n \in S$, it must be true that $n \in T$.

Answer (Ex. 6) — No. $S \subseteq T$ means that it is possible that $S \subset T$ is true. $S \subset T$ means that T has all of the elements in S , but there are also

more elements. It's entirely plausible that n is one of the additional elements. Thus,

$$\{n \in T, S \subseteq T\} \not\Rightarrow n \in S$$

Answer (Ex. 7) — No. $n \in S$ can be stated as $\{n\} \subseteq S$. Likewise, $n \in T \iff \{n\} \subseteq T$. This means there are 3 possible cases for the relation between S and T :

$$1. S = T$$

$$2. S \subset T$$

$$3. S \supset T$$

$S \subseteq T$ means that either 1 or 2 is true, but the third one is false. The third one can be true when $\{n \in S, n \in T\}$ is true. Thus, we have found a case in which $\{n \in S, n \in T\}$ is true, but $S \subseteq T$ is false. Thus, it must be that.

$$S \subseteq T \not\Leftarrow \{n \in S, n \in T\}$$

2.1 Numeric sets

Now, I'm going to throw more crap at you. I'm sorry for all the notation, but it is important that you get used to it. There are a bunch of common sets you'll encounter in the real world.

1. First of all, there are the integers: these are just the whole numbers, like $-3, -2, -1, 0, 1, 2$. Traditionally, this set is denoted \mathbb{Z} .
2. The natural numbers, denoted \mathbb{N} , are all non-negative integers².
3. The set of “rational” numbers, denoted \mathbb{Q} is the set of all numbers that can be written as a quotient (or fraction) $\frac{p}{q}$, where p and q are integers.

In mathematical notation, you would write this as $\left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \right\}$. You should read that as “the set of all numbers p over q , such that p and q are elements of \mathbb{Z} .”

4. Finally, the real numbers, denoted \mathbb{R} , contain everything on the number line. Equivalently, a real number is just any number you can write down by writing down an integer, a decimal point, and then writing any sequence of digits after the decimal point (even an infinite sequence).

Let us show you an example. Let's write down an integer. 2. There we go. Now, let's just write down a bunch of digits all in a row. 215455211. By the definition in the previous paragraph, 2.215455211 is a real number. You should get in the habit of writing “2.215455211 is a real number” as $2.215455211 \in \mathbb{R}$.

Sets certainly look simple enough to understand intuitively, but are they also interesting enough to be worth studying? The answer to that is a resounding ‘yes.’ Exciting, right?

To give you a taste of the results, let's take a look at some of them.

²Conventions differ as to what the natural numbers are. Everyone agrees that positive whole numbers (1, 2, 3...) are natural. Some people say 0 is also a natural number, while others disagree. In this book, 0 is a natural number, so the natural numbers are 0, 1, 2, and so on. This might seem like a stupid fight, why can't we just choose a side? However, it actually turns out to be really important.

Intuitively, sets can be of different sizes: it's clear that the empty set is the smallest possible set, and that $\{2, 4\}$ is smaller than $\{1, 2, 3\}$. When we get to infinite sets, however, the intuition fails.

Cantor formalised this intuition, and the formal version also worked for infinite sets. The results he got were very surprising: for example, he found that there are as many natural numbers as rational numbers, but that there are strictly more real numbers. Even worse, he proved that given any set, there is always a set larger than it. If you've ever heard of people talking about "different kinds of infinity", this is probably what they meant.

Exercises

1. Suppose x is some object and S is a set. Does it make sense to ask "How many times does S contain x ?"
2. Earlier, we constructed the set $\{3, 5\}$. We can also construct the set $\{5, 3\}$. Are these the same set?
3. Are the following true or false?
 - $\emptyset \in \emptyset$
 - $\emptyset \in \{\emptyset\}$
 - $\emptyset = \{\emptyset\}$
 - $\{\emptyset\} \in \{\emptyset\}$

2.2 Functions

A function from a set X to a set Y specifies for every element of X a corresponding element of Y . In other words, if f is a function from X to Y (denoted $f : X \rightarrow Y$) and $x \in X$, then $f(x) \in Y$. A lot of high school mathematics is about functions from \mathbb{R} to \mathbb{R} , even if they are never presented that way. For example, solving linear equations is actually a question about functions: "given a function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by

$$f(x) = 5x - 10$$

find all $r \in \mathbb{R}$ such that $f(r) = 0$.”

It turns out that by taking sets X and Y and asking what kind of functions exist between them, we can find out a lot about X and Y themselves. We'll continue this line of thought after some exercises.

Exercises

1. We can construct the set $\{0, 1\}$. What functions can you find from $\{0, 1\}$ to $\{0, 1\}$? How many such functions are there?
2. Can you find a function from \emptyset to $\{0, 1\}$? What about in the other direction?
3. Suppose X is a set. Prove that there exists at least one function from X to X . How can this function be defined? Why does this work if X is the empty set?
4. Suppose X , Y , and Z are sets, and you are given functions $f : X \rightarrow Y$ and $g : Y \rightarrow Z$. Can you make a function from X to Z ? How?
5. Suppose X and Y are sets, $f : X \rightarrow Y$, and $x, y \in X$. Do you think $x = y$ implies $f(x) = f(y)$? Why, or why not?

Solutions

2.3 Injective Functions

In the exercises, you saw that if $f : X \rightarrow Y$ and you had $x, y \in X$ such that $x = y$, then necessarily $f(x) = f(y)$. A function f is said to be injective if the converse is also true: if $x, y \in X$ and $x \neq y$, then $f(x) \neq f(y)$.

Let's consider some examples. Let $f : \mathbb{N} \rightarrow \mathbb{Z}$ be defined by $f(x) = x$. Is this definition correct? Well, we need to check that for any $n \in \mathbb{N}$, we have $f(n) \in \mathbb{Z}$. But by definition, $f(n) = n$, so we need to check that if $n \in \mathbb{N}$, then also $n \in \mathbb{Z}$. Every non-negative integer is certainly an integer, so yes, the definition is correct.

Now, is this function injective? For that, let $n, k \in \mathbb{N}$ so that $f(n) = f(k)$. We need to prove that $n = k$. Again, this is easy: $f(n) = n$ and $f(k) = k$, so by putting the three equalities together, we have $n = k$.

We can construct the set $\{f(0), f(1), f(2) \dots\}$. If we want to be precise, we can use the *set comprehension* notation:

$$\{f(x) \mid x \in \mathbb{N}\}$$

You should read this as “the set that contains $f(x)$ for each $x \in \mathbb{N}$.” That's rather a mouthful, so we'll abbreviate this by $f(\mathbb{N})$. Just imagine that instead of applying f to one value in \mathbb{N} , you're applying it to all the values and looking at the results as a set.

We can now ask ourselves: how big is $f(\mathbb{N})$? In this case, we can see that $\mathbb{N} = f(\mathbb{N})$, so of course they're exactly the same size. However, what if instead of the f we chose, we had chosen $f(x) = -x$, or $g : \mathbb{N} \rightarrow \mathbb{Q}$ defined by $g(x) = \frac{1}{1+x}$? Prove that both of these are injective functions, and imagine $f(\mathbb{N})$ and $g(\mathbb{N})$. How big are these sets?

It should be clear that given any sets X and Y and any function $f : X \rightarrow Y$, $f(X)$ cannot possibly be bigger than X . For every element $y \in f(X)$, there is some element $x \in X$ so that $f(x) = y$; that's how we defined $f(X)$ in the first place.

On the other hand, if f is injective, $f(X)$ also shouldn't be any smaller

than X . Why? Well, we can just define a function the other way. Let $g : f(X) \rightarrow X$, and define $g(f(x)) = x$. Now we know that $g(f(X))$ is no larger than $f(X)$. But $g(f(X)) = \{g(f(x)) \mid x \in X\} = \{x \mid x \in X\} = X$! That means, by the argument above, that $f(X)$ is no larger than X , just as we wanted.

The careful reader might notice that the definition of g is fishy. Does a function defined this way really work? The answer is that it does, but only because we were careful about f . We know that if we have an element $y \in f(X)$, then there is an element $x \in X$ so that $y = f(x)$. This means that g really is defined for all $y \in f(X)$. That's not all, though. Additionally, suppose there was also a $z \in X$ so that $y = f(z)$. Then $g(y) = g(f(x)) = x$, but also $g(y) = g(f(z)) = z$. For g to be a function, we need to prove that $x = z$. Here is where we need the injectivity of f : we know that since $f(x) = y = f(z)$, that $f(x) = f(z)$, and thus $x = z$. Therefore, g really is a function, and so our argument holds.

Our intuition thus tells us that however we define size, we should make sure that for any set X and any injective function $f : X \rightarrow Y$, we should have X and $f(X)$ be of equal size. As $f(X)$ is just a part of Y , this means that X should also be no bigger than Y . By themselves, all these loose bits of intuition might not seem very useful, but in the next section we'll use them to show that a certain approach to define size *doesn't* work. First, however, some exercises.

Exercises

1. In an older exercise, you saw there were four functions from $\{0, 1\}$ to itself. How many injective functions are there? What about between $\{0, 1, 2\}$ and itself? What if you have even more elements?

2.4 Subsets

When people first hear that there are as many integers as natural numbers, their reaction is often "Surely that can't be right? Every natural number is

an integer, and there are some others, too!”

To make this argument formal we should introduce the notion of a subset. We say that X is a subset of Y if every element of X is also an element of Y . We denote this by $X \subseteq Y$. We have, then $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. We will use $X \subset Y$ when X is a subset of Y , but X and Y are not equal.

Now let's denote the size of X by $|X|$. Can we define this size in such a way that for finite sets, $|X|$ is the number of elements in X , that for any sets X and Y such that $X \subset Y$ we have $|X| < |Y|$, and that if there exists an injective function $f : X \rightarrow Y$ then $|X| = |f(X)|$?

We've already given away that this isn't possible. The question becomes, how do we prove it? It isn't enough to just try a few definitions of 'size' and see that they don't work, as there'll always be a few that we haven't yet attempted. We need a way of showing that whatever definition we come up with, we'll be able to show it doesn't work.

To do that, we'll assume that we were given some definition of 'size' that satisfies the above requirements, but with no other assumptions. You can imagine it as being given the definition by a friend, and now you have to show why it's wrong. If the definition allows us to derive something that isn't true then there's certainly something wrong with it, so that's what we'll try to do.

Assume that for every set X , we defined $|X|$. Define $f : \mathbb{Z} \rightarrow \mathbb{Z}$ by $f(x) = 2x$. We required that $|\mathbb{Z}| = |f(\mathbb{Z})|$. But because $1 \notin f(\mathbb{Z})$, $f(\mathbb{Z}) \subset \mathbb{Z}$. This implies $|f(\mathbb{Z})| < |\mathbb{Z}|$, and so we conclude $|\mathbb{Z}| = |f(\mathbb{Z})| < |\mathbb{Z}|$. Surely, though, a set can't be smaller than itself, so we've just derived a falsehood, and the definition of 'size' that we started with can't work.

If this proof doesn't feel quite right to you, don't worry: we'll look at arguments like this in-depth in the next chapter. For now, the main result is that we are too strict in how we want to define size. We need to relax one of the requirements, and in the next section we'll see that if we remove the requirement that $X \subset Y$ implies $|X| < |Y|$, we can find a good definition.

Exercises

In these exercises we'll explore some more operations for constructing sets. The three most important ones are *union*, *intersection*, and *difference*.

The union of X and Y is written as $X \cup Y$ and contains every element of X and every element of Y . We can write this using set comprehension notation:

$$X \cup Y = \{x \mid x \in X \text{ or } x \in Y\}$$

1. Write out the following sets:
 - (a) $\{0, 1\} \cup \{2, 3\}$
 - (b) $\{0, 1\} \cup \{1, 2\}$
 - (c) $\{0, 1\} \cup \{0, 1\}$
 - (d) $\{0, 1\} \cup \emptyset$
2. We say that a set A is the identity of \cup if for every set X we have $X \cup A = X = A \cup X$. Does \cup have an identity?
3. Suppose X and Y are sets. Convince yourself that $X \cup Y = Y \cup X$. This property of \cup is called *commutativity*.
4. Suppose X , Y , and Z are sets. Convince yourself that $(X \cup Y) \cup Z = X \cup (Y \cup Z)$. This property is called *associativity*.

The intersection of X and Y is written as $X \cap Y$ and contains all elements that are both in X and Y .

1. Do the first exercise on unions again, but replace \cup with \cap .
2. Let X and Y be sets. Write $X \cap Y$ as a set comprehension.
3. Does \cap have an identity?
4. Is \cap commutative and associative, just like \cup is?

The difference between X and Y is written as $X - Y$ (or, sometimes, $X \setminus Y$) and contains all elements that are in X but are not in Y .

1. Do the first exercise on unions a third time, but now taking the difference.
2. Does set difference have an identity?
3. Is set difference commutative? What about associative?

2.5 Cardinalities

2.6 The Power Set

2.7 The Category of Sets

2.8 Special kinds of sets

2.8.1 Magmas

2.8.2 Semigroups

2.8.3 Monoids

Chapter 3

Proofs

3.1 Peano Axioms

This section covers the Peano axioms. As I said in ??, these are a way for mathematicians to understand arithmetic.

Arithmetic (hopefully) seems simple enough, and easy to understand. Maybe an expression like

$$(2048282 \times 33221) + (3254 \times 11)$$

seems difficult to calculate, but you hopefully understand what each of the operators mean in concept. If you don't, well. In theory, reading this chapter alone will teach you arithmetic. However, I wrote this chapter assuming you already know arithmetic.

So, why is it important that you read this chapter?

Arithmetic is pretty simple and easy to understand. However, later on in this book, we're going to approach concepts that aren't so simple and easy to understand. Mathematicians have a systemic approach to these problems. This approach is called "mathematical proof." We prove things mathematically. Instead of approaching new concepts with proofs, I'm instead going to use proofs to illustrate some (hopefully) familiar concepts.

Alright, with all that out of the way, let's get started.

The basic idea of proofs is, you take a small set of obvious facts, called *axioms*, chain them together to make *theorems*. The following obvious facts, or axioms, are called the “Peano Axioms.” They describe what we call “natural numbers.” Natural numbers are the numbers $\{0, 1, 2, 3, 4, 5, 6, \dots\}$.

Axiom 1 0 is a natural number. Again, obvious.

I'm going to use letters in the place of numbers right here. So, if I say “ x is a natural number,” that means that x is a placeholder for one of the numbers in $\{0, 1, 2, 3, 4, 5, 6, \dots\}$. I could use any letter, such as a , b , q , r , θ , Γ , or \aleph . If I use a letter instead of a number, it usually means either

1. it doesn't matter which number I choose, or
2. it does matter which number I choose, but I don't know which number it is yet.

Axiom 2 If x is a natural number, it is true that $x \equiv x$.

You can read that \equiv sign as $=$, for the time being. There are some subtle differences between the two, which I will get to in ???. You are supposed to read $a \equiv b$ as one of these:

1. “ a is equivalent to b ,”
2. “ a is identically equivalent to b ,”
3. “ a is congruent to b .”

$=$ should be read as “ a is equal to b ,” or “ a equals b .” Again the difference between \equiv and $=$ isn't really important until ???.

If you don't know what either of those signs are, $a \equiv b$ or $a = b$ means “ a is the same thing as b .” The difference can be summarized as $==\equiv\neq=$.

So, in essence, this axiom says that each number is the same thing as itself. This is hopefully very obvious.

A math person would state this axiom as “congruence is reflexive.”

Axiom 3 If x and y are both natural numbers, and $x \equiv y$, then it's true that $y \equiv x$. You can phrase this axiom as “if two numbers are the same number, then they are the same number.” A math person would state this axiom as “congruence is symmetric.”

Axiom 4 If x , y , and z are all natural numbers, and $x \equiv y$, and $y \equiv z$ then it's true that $x \equiv z$. You can phrase this axiom as “if three numbers are all the same number, then they are the same number.” A math person would state this axiom as “congruence is transitive.”

These last three axioms mean that we can be lazy, and write things like $a \equiv b \equiv c \equiv a$.

Axiom 5 If x is a natural number, and we know $x \equiv y$, then it's also true that y is a natural number. A math person would say “congruence forms a closure.”

Axiom 6 If x is a natural number, then there is another number, $\text{suc}(x)$, which is also a natural number. suc is short for “successor.” You should read $\text{suc}(x)$ as “the successor of x .” You can think of the successor as “the next number.” So, $\text{suc}(0) \equiv 1$, $\text{suc}(1) \equiv 2$, and so on.

Axiom 7 There isn't a number whose successor is 0. Basically this means “0 is the lowest natural number.”

Axiom 8 If x and y are both natural numbers, and we know $\text{suc}(x) \equiv \text{suc}(y)$, then it's true that $x \equiv y$. This is what we would call the “converse” of Axiom 6. That is, Axiom 6 tells us that we can always go “up” a number. This axiom (almost) tells us that we can go “down” a number. Axiom 7 defines the limit of this, meaning that 0 is the only number where you can't go down any further.

Now, the previous 8 axioms have basically said “these numbers are all natural numbers.” This next, and final axiom states “these numbers are all *of* the natural numbers.”

Axiom 9 Let's say K is a set of numbers (a bunch of numbers). If we know that

1. if 0 is in K , and
2. if some number x is in K , then $\text{suc}(x)$ is in K ,
3. then K contains every single natural number.

Continue with...

1. \mathbb{N} is a Monoid
2. Quasigroups
3. Loops
4. Groups
5. Abelian Groups
 - (a) \mathbb{Z}
 - i. \mathbb{Z} is an Abelian Group
 - ii. \mathbb{Z} is a ring
6. Fields
 - (a) \mathbb{R}
 - i. \mathbb{R} is a field
7. Categories
8. Groupoids

Appendices

Appendix A

GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.

`<http://fsf.org/>`

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “**Document**”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “**you**”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “**Modified Version**” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “**Secondary Section**” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “**Invariant Sections**” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “**Cover Texts**” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “**Transparent**” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “**Opaque**”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “**Title Page**” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “**publisher**” means any person or entity that distributes copies of the Document to the public.

A section “**Entitled XYZ**” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “**Acknowledgements**”, “**Dedications**”, “**Endorsements**”, or “**History**”.) To “**Preserve the Title**” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.

- I. Preserve the section Entitled “History”, Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy’s public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

“Massive Multiauthor Collaboration Site” (or “MMC Site”) means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A “Massive Multiauthor Collaboration” (or “MMC”) contained in the site means any set of copyrightable works thus published on the MMC site.

“CC-BY-SA” means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

“Incorporate” means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is “eligible for relicensing” if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME. 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”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with . . . Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Appendix B

How to learn math

Now that that's all out of the way, let's talk a little about math. When this chapter is over, we're going to dive right in to proving a bunch of things you already know to be true. We feel that without a little explanation, these proofs may leave you a little lost or confused. We'll save the explanation of the proofs for later, but right now, we're going to talk about how to actually learn math, and the proofs are a great example.

Most people's experience with math is through their primary and possibly secondary education, which is or was a dreary affair in general, and math probably even moreso, unless you're one of the lucky few. By lucky few, we don't mean those wizards with a sort of inherent ability to do math—the first thing you need to know about learning math is that math is for everyone with a brain—that's you, right? You see, your brain is a pattern recognition engine, and that's all math is: the study of patterns. Unlike reading or history, your body comes with a biological imperative to know math. There's some really great brain studies on the topic, but that's boring, and I said we're already done with the boring part, so let's move on.

In that last paragraph, we presented what we hold to be the proper answer to 'what is math': the study of patterns. This is completely different from most people's interaction with math: in primary school, we are taught how to apply four operations to solve math problems. You're given something about two trains leaving a station and going different speeds and different directions and yadda yadda yadda and before you know it your teacher turned

everything into a math problem and it all seemed so forced—a layer on top of what was intuitive, and made everything complicated. We agree—this is a counterintuitive approach to math, and it makes math very confusing and disconnected. Math is just the study of patterns. That is, math is not so much a way to solve a set of problems that exist in a sphere apart from what is natural, but a way to understand what’s going on in the world around us. When you learn math, you should think of it as a science—another level of detail in the amazing world we live in.

That’s how this book is written. It’s written to reflect that math is a single unified study. While you’re reading it, try to think of how what you’re learning clarifies or refines early material. This is a big deal to us, because one thing we dislike most about the standard way of learning math is that at some point in everyone’s math career, they learn they were taught something that wasn’t actually true. We want to avoid that.

Bibliography

- [1] Edmund Landau. *Foundations of Analysis*. Providence, RI: AMS Chelsea Publishing, 1966.
- [2] Miran Lipovača. *Learn You a Haskell for Great Good!* 245 8th Street, San Francisco, CA, 94103: No Starch Press, 2011.