I CONSIDER IT AN IMPORTANT FEATURE OF MY APPROACH TO MATHEMATICS, WHICH FEELS RELATED TO THE INSIDE VIEW SKILL, THAT I CONSISTENTLY GET FRUSTRATED AT DEFINITIONS THAT I DON’T UNDERSTAND HOW TO REINVENT INSTEAD OF TAKING THEM AS GIVEN. A LARGE PART OF MY MATH BLOGGING IS ABOUT MOTIVATING DEFINITIONS. SOMETIMES IT WOULD TAKE ME YEARS BETWEEN MY FIRST EXPOSURE TO AND FRUSTRATION AT A DEFINITION AND THE TIME THAT I FINALLY HAD A SATISFYING MOTIVATION FOR IT; FOR CHAIN COMPLEXES IT TOOK SOMETHING LIKE 4 YEARS, AND THE SATISFYING MOTIVATION IS MUCH MORE COMPLICATED TO EXPLAIN THAN THE DEFINITION. (FOR AN EXAMPLE THAT HASN’T FINISHED YET, I AM STILL FRUSTRATED ABOUT ENTROPY, EVEN AFTER WRITING THIS POST, WHICH CLARIFIED A LOT OF THINGS FOR ME.)

QIAOCHU YUAN

I CAN ILLUSTRATE THE SECOND APPROACH WITH THE SAME IMAGE OF A NUT TO BE OPENED.

THE FIRST ANALOGY THAT CAME TO MY MIND IS OF IMMERSING THE NUT IN SOME SOFTENING LIQUID, AND WHY NOT SIMPLY WATER? FROM TIME TO TIME YOU RUB SO THE LIQUID PENETRATES BETTER, AND OTHERWISE YOU LET TIME PASS. THE SHELL BECOMES MORE FLEXIBLE THROUGH WEEKS AND MONTHS – WHEN THE TIME IS RIPE, HAND PRESSURE IS ENOUGH, THE SHELL OPENS LIKE A PERFECTLY RIPENED AVOCADO!

A DIFFERENT IMAGE CAME TO ME A FEW WEEKS AGO.

THE UNKNOWN THING TO BE KNOWN APPEARED TO ME AS SOME STRETCH OF EARTH OR HARD MARL, RESISTING PENETRATION... THE SEA ADVANCES INSENSIBLY IN SILENCE, NOTHING SEEMS TO HAPPEN, NOTHING MOVES, THE WATER IS SO FAR OFF YOU HARDLY HEAR IT.. YET IT FINALLY SURROUNDS THE RESISTANT SUBSTANCE.

ALEXANDER GROTHENDIECK

IN OUR ACQUISITION OF KNOWLEDGE OF THE UNIVERSE (WHETHER MATHEMATICAL OR OTHERWISE) THAT WHICH RENOVATES THE QUEST IS NOTHING MORE NOR LESS THAN COMPLETE INNOCENCE. IT IS IN THIS STATE OF COMPLETE INNOCENCE THAT WE RECEIVE EVERYTHING FROM THE MOMENT OF OUR BIRTH. ALTHOUGH SO OFTEN THE OBJECT OF OUR CONTEMPT AND OF OUR PRIVATE FEARS, IT IS ALWAYS IN US. IT ALONE CAN UNITE HUMILITY WITH BOLDNESS SO AS TO ALLOW US TO PENETRATE TO THE HEART OF THINGS, OR ALLOW THINGS TO ENTER US AND TAKEN POSSESSION OF US.

THIS UNIQUE POWER IS IN NO WAY A PRIVILEGE GIVEN TO “EXCEPTIONAL TALENTS” – PERSONS OF INCREDIBLE BRAIN POWER (FOR EXAMPLE), WHO ARE BETTER ABLE TO MANIPULATE, WITH DEXTERITY AND EASE, AN ENORMOUS MASS OF DATA, IDEAS AND SPECIALIZED SKILLS. SUCH GIFTS ARE UNDENIABLY VALUABLE, AND CERTAINLY WORTHY OF ENVY FROM THOSE WHO (LIKE MYSELF) WERE NOT SO “ENDOWED AT BIRTH, FAR BEYOND THE ORDINARY”.

YET IT IS NOT THESE GIFTS, NOR THE MOST DETERMINED AMBITION COMBINED WITH IRRESISTIBLE WILL-POWER, THAT ENABLES ONE TO SURMOUNT THE “INVISIBLE YET FORMIDABLE BOUNDARIES” THAT ENCIRCLE OUR UNIVERSE. ONLY INNOCENCE CAN SURMOUNT THEM, WHICH MERE KNOWLEDGE DOESN’T EVEN TAKE INTO ACCOUNT, IN THOSE MOMENTS WHEN WE FIND OURSELVES ABLE TO LISTEN TO THINGS, TOTALLY AND INTENSELY ABSORBED IN CHILD’S PLAY.

ALEXANDER GROTHENDIECK

YU JIE TEO

# A MATH BEDTIME STORYBOOK

template and format made by

tufte-latex.github.io/tufte-latex/

*First printing, May 2025*

# Contents

# *List of Figures*

# *List of Tables*

*To my parents.*

# Introduction

As a hobbyist in mathematics, I have found that my needs in understanding mathematics come from my struggle to make sense of the world. It also comes from a personal struggle of an unhealthy suppression of a lot of pain in reality and find comfort in a less real world.

This book is meant to be a sense of personal fulfilment, that I have understood some small part of the world in some formal sense. Previously, I was working with a plain text file with everything I have learnt conveyed in it.

This was not enough with regards to my ambition. I want to be able to really prove to myself my understanding and do things properly.

As such, I have chosen to write a book about what I have read, in a style that is most suitable to my ambitions.

This is not a replacement for dedicated books and courses. The goal of this book is rather selfish, the values are that of personal idiosyncratic perspective on mathematics. It is one limited perspective in a vast ocean of personal realities and objective truth.

Since this book is as a result of pure curiosity (due to my finanicial and personal circumstance and fears, I am not able to pursue a career in pure mathematics), this books is written such that narrative and natural or historical explanations supersede rigour due to the nature of this work.

However, rigour is one of the main reasons why I started writing this book. I want a formal presentation and to prove to myself that I can make these arguments rigorous. I was not proving lemmas and was only writing and thinking in terms of natural explanations when I was learning mathematics. I have learnt so much to the point that my foundations was lacking due to a lack of rigour. [1]

Evan Chen have some nice remarks on this. [2]

> Understanding "why" something is true can have many forms. This is sometimes accomplished with a complete rigorous proof; in other cases, it is given by the idea of the proof; in still other cases, it is just a few key examples with extensive

[1] I basically have a plain text file with everything I want in one place. That has gotten fragmented because I have exercises with my solutions, questions I have yet to ask, and lemmas that I have proved off the top of my memory because I understood it but really it was copied in some sense scattered in several places. I really want everything I know in one place now, and properly written up so I can trust its solidity.

[2] Evan Chen. *Napkin Project*. Self-Published, May 2025

cheerleading. Obviously this is nowhere near enough if you want to e.g. do research in a field; but if you are just a curious outsider, I hope that it’s more satisfying than the elevator pitch or Wikipedia articles.

I have realised that one of my mathematical weaknesses is not being able to ground stuff concretely in examples. This book will therefore be biased (but because of the author, not that I want to) towards generalities.

I will try to put exercises as sidenotes. Solutions to all exercises are provided at the end of each section.

# *Considerations*

## *Remarks*

Here are some remarks on topics:

1. Number theory is the most important topic in mathematics. However, there is a contradiction between how I feel and what I think. I feel very disinterested in number theory, but I think it is basically the source of all of our good ideas in mathematics. In general, my feelings are more aligned with abstraction and generality, but my thoughts of what is important are the concrete and what historically happened. Therefore, every chapter will present the most general and powerful versions of the ideas with as much generality as I can handle, but the focus and precedence will always be what happened in history and what came first, with number theory being the central motivation for most of the topics.

2. Linear algebra would start with Grassmann's abstraction of the exterior algebra first. Historically, this came first but was hard to understand. Therefore, my view of linear algebra is a geometric one first, followed by linear maps between spaces.

3. The metric topology came first, then problems without distances in the bridge problems, then abstract general and algebraic topology. I will try to follow this order in presentation.

4. For group theory, I intend to start by motivating Galois theory first. Galois theory for me is the least interesting topic when I started learning mathematics, but I have appreciated it better with history and more advanced applications. My goal is to present group theory more concretely with the classification of groups of small order and lots of examples, but my real inclinations tend to be very categorical and groupoid like in nature from the axioms. The goal is to somehow do the more concrete approach in this book.

5. Commutative algebra is very important to me, however I tend to

take a very abstract approach so I am not very good at commutative algebra. Likewise, I will focus on examples and history (or fake history) in commutative algebra similar to Eisenbud [3].

6. Measure theory is used as a build up to the Lebesgue integral as a key example. Majority of my motivations in measure theory is for probability theory, so likely my intuitions will be slanted towards that.

7. Probability theory will always be very special to me because it was my first taste of real mathematics when Nassim Taleb motivated me to think more about pure mathematics. Therefore, the pedagogical slant in probability theory is probably more concrete, with a greater focus on information theory.

8. Functional analysis is also one of my favourite topics in analysis. However, my approach will probably lean towards the abstract rather than the concrete since many of the inklings of abstraction started here.

9. Partial differential equations is the most difficult topic for me, since I still lack the functional analysis and measure theory background to manage it.

10. Representation theory is important precisely because it is closest to linear algebra and generalises it. It was the first topic that made me think that I can do a lot better with concrete examples.

11. Sets are seen as the fundamental examples in mathematics that is closest to the integers. However, I am not very interested in set theory though I should.

12. Algebraic topology is the topic that makes me feel more connected to people in mathematics, since most of the online inspirational figures.

13. Algebraic geometry is a topic I was very interested in at the start and the interest starts to wane over time as I got more interested in the basics and having a better grasp on ideas in linear algebra.

14. Algebraic number theory is very important since it is number theory. I have zero clue what it is about other than a good source of historical motivation.

## *Conventions*

The set of natural numbers is the set of positive integers. I will try my best to stick to positive integers or nonnegative integers.

[3]

All rings are commutative with identity.

The axiom of choice is accepted.

## *Ontology and learning*

I think there is a lower level of description that is not emphasised enough in mathematics. There are glimpses of it when one studies history or problems like the Bongard problem, but really definitions evolve and are fluid. Definitions put into focus the important features of an idea, and a lot of time is spent trying to find the right definitions or the right ontology.

As part of my learning, I quickly realised that one must expand the set of all ideas in your head on a conscious or unconscious level to learn something. This means reading to identify what all the main objects are, how they relate to each other and make it actionable.

Another big thing about ontology is that a lot of mathematical history grew out of not sidestepping issues and making distinctions between various ontology. One must therefore remodel the relationships and properties of ideas with some understanding of conceptual or historical prerequisites and background.

I still believe there really is no correct definition to certain things and that there are several definitions each serving various purposes.

# *Number Theory*

**Lemma 0.1.** *Suppose $a$ and $b$ are integers. Then there exists unique integers, defined as the quotient $q$ and the remainder $r$, such that $a = qb + r$ with the condition that the remainder $r$ is more than or equal to zero, but less than $b$.*

*Proof.* Assume $b$ is larger than $a$ without loss of generality, if they are equal then the quotient is 1 and the remainder is 0 which is unique. Otherwise, one can swap between $a$ and $b$. Since the integers are closed under subtraction by assumption (one will have to use the successor function and define subtraction, or use the fact that the integers are a ring), therefore $a - nb$ is an integer, for $n$ an integer. These integers are all unique, one can apply mathematical induction on $n = 1$ to show that all these integers are unique to each other. We now show that there exists a case where $r$ is less than $b$. This must exist without loss of generality, since if $r = a - nb$ is greater than $b$, then redefine the remainder $r$ to be $a - (n + 1)b$ which must be less than $b$ but still greater than 0, with the quotient being $n + 1$ and all these case follow from the closure of the integers as a ring under subtraction. Therefore, the remainder $r$ exists, and the corresponding coefficient of integer $b$ must be the quotient $n$. □

**Lemma 0.2.** *Let $a$ and $b$ be nonzero integers, then there exists a linear combination with coefficients $u$ and $v$ in the integers such that $au + bv$ is equal to the greatest common divisor $gcd(a, b)$.*

*Proof.* A divisor of $a$ is an integer $u$ such that $au$ is an integer. A divisor of $b$ is an integer $v$ such that $bv$ is an integer. The greatest common divisor exist, since $au + bv$ is an integer, so it is equal to $gcd(a, b)w$, where $gcd(a, b)w$ is a product of an integer $w$ that is not equal to 1 and 1 without loss of generality, if it is 1 we are done and it is nonzero without loss of generality since once can choose divisors of $u$ and $v$ to make it nonzero. We have $gcd(a, b)m_a u + gcd(a, b)m_b v = gcd(a, b)w$ so $m_a u + m_b v = w$. We can iterate this process, and since $w$ is nonzero and with each step, the integers $w$ decreases, by the well ordering of the integers, $w$ will terminate at 1 after correcting up to sign by taking $-1$ when necessary onto integers $u$ and $v$, and the product of $gcd(a,b)m_{a_1}m_{a_2}...$ and $gcd(a,b)m_{b_1}m_{b_2}...$ terminates the the integers $u$ and $v$ of interest. $\square$

# *Sets and Foundations*

**Lemma 0.3** (Well ordering principle of the natural numbers)**.** *A nonempty partition of the natural numbers have a least element.*

*Proof.* Consider the successor function construction of the natural numbers. One can construct any partition of the natural numbers by removing natural numbers from the set of natural numbers. This set has a least element of 1 by the principle of mathematical induction. Suppose we remove the least element in any step of the construction leaving behind a nonempty partition fo the natural number. The successor of the least element becomes the new least element. If it does not exist in the set, then consider the successor of that element by the principle of mathematical induction. This terminates since we assumed the remaining partition is nonempty, and the least element would be designated. Since any nonempty partition of the natural numbers can be constructed this way, therefore a nonempty partition of the natural numbers have a least element. □

**Lemma 0.4.** *Mathematical induction is a valid way to show that statements $P_n$ are true for all natural numbers $n$.*

*Proof.* Define the set of all statements where $P_n$ is false as the set $S$. If the set is empty, then the lemma is true. Suppose the set is nonempty, for contradiction. Consider the case of $n > 1$ without loss of generality, since there is a contradiction from the initial step of $P_0$ being true by mathematical induction. Since we assume the well ordering principle, therefore this set has a minimal element. We will want to show that this is not the minimal element. The contrapositive of mathematical induction is that if $P_{n+1}$ is false, then $P_n$ is false. If we consider the minimal element to be $P_{n+1}$, and statements up to $P_n$ are not in the set, then $P_n$ is also in this set. This is contrary to the minimality of $P_{n+1}$ by hypothesis. Since the set must be empty if mathematical induction is valid, therefore mathematical induction is a valid way to show that statements $P_n$ are true for all natural numbers $n$. □

**Lemma 0.5** (Fermat's Little Theorem)**.** *Let $a$ be a non-negative integer, and $p$ be a prime. Then $a^p - a$ is divisible by the prime $p$.*

*Proof.* Pick the set $X$ as the partition from $0$ to $a$, and apply the p-group fixed point theorem with the cyclic group $P$ of prime order $p$. □

# Groups

## Groups from Galois theory

It is strange that Galois is typically not mentioned right at the start as to why groups are invented. They wanted to make sure to some extent when you do permutations, the remaining result is still a permutations.

**Definition 0.6** (Prototype psuedodefinition by Galois and Cauchy). *A group is a set of permutations that preserves "the structure" such that if you compose any two permutations, it is still a permutation that preserves "the structure".*

Cauchy's first definition was that of substitutions, and you can derive substitutions.

## Some unmotivated lemmas

I am trying to motivate these, but these seem to be very crucial to group theory.

**Lemma 0.7.** *Let $S$ be a set, and let $\equiv$ be an equivalence relation on the set $S$. Let $a$ and $b$ be elements of the set $S$, then either the equivalence classes containing $a$ called $S_a$ is equal to the equivalence class containing $b$ called $S_b$, or these equivalence classes are disjoint. Further, the set $S$ is the disjoint union of distinct equivalence classes. The number of elements in each equivalence class adds to become the number of elements in the set $S$.*

*Proof.* Suppose without loss of generality that $a$ is distinct from $b$, and the non-empty equivalence classes with more than two elements are not disjoint since if they are disjoint that is one case and we are done. Likewise if there is only one element in the set $S$. We want to show that if $a$ and $b$ are in the intersection of $S_a$ and $S_b$, then this intersection is equal to both $S_a$ and $S_b$. Indeed, $b$ is equivalent to $a$ since it is contained in $S_a$, so they must be the same equivalence class. Therefore, the intersection of $S_a$ and $S_b$ is equal to $S_a$ and $S_b$, and if a set has same elements, they are equal. By case analysis, there can only be two cases the equivalence classes $S_a$ is equal to $S_b$, or they are disjoint. The set $S$ must contain the disjoint union of equivalence classes, since if two equivalence classes intersect they are the same set. Since a set must have distinct elements, the number of elements in each equivalence class under disjoint union add up to the number of elements in the set $S$. □

**Lemma 0.8** (p-group fixed point theorem)**.** *Suppose $P$ is a finite p-group. Suppose $X$ is a set in which the finite p-group $P$ acts, then the subset $X^p$ of fixed points satisfy $|X^P|$ is congruent to $|X|$ modulo $P$. Particularly, if $|X|$ is not congruent to $0$ modulo $p$, then this action has a fixed point.*

*Proof.* A set $X$ can be decomposed into a finite disjoint union of subsets.

These are acted on by the finite $p$-group $P$ by hypothesis. Suppose this action does not have a fixed point, then all subsets of this disjoint union are acted on by the finite $p$-group $P$, and all have cardinality that is divisible by $p$. This means the cardinality of the disjoint union is divisible by $p$, and therefore if this action does not have a fixed point, then $|X|$ is congruent to $0$ modulo $p$. By contrapositive, $|X|$ is not congruent to $0$ modulo $p$, then this action has a fixed point. If we consider the exclusion of subsets acted on by the finite $p$-group $P$, then this is equivalent to considering the cardinality of $X$ modulo positive integer $p$. □

**Lemma 0.9.** *Orbits of cyclic group of prime order p have orbit sizes of $1$ and $p$.*

*Proof.* By the $p$-group fixed point theorem, using case analysis, there are either fixed points or elements in the orbit of the cyclic group of size $p$, with no larger orbits since these are of prime order. □

**Lemma 0.10.** *Suppose $G$ is a finite p-group. It has nontrivial centre $Z(G)$, and every such group is nilpotent.*

*Proof.* Consider the self action of the finite $p$-group $G$ on its conjugate $G$ $1$ to rule out the determination of a product of the remaining elements and its inverse.

If $G$ is of prime power order, then this set has the cardinality of $p^n - 1$, which is not divisible by $p$. By the $p$-group fixed point theorem, the finite $p$-group $G$ has a fixed point. This fixed point commutes with every element of the finite $p$-group $G$, and hence is a nontrivial central element since it commutes with every other element of $g$ as a fixed point with orbits being disjoint unions. It terminates in the trivial subgroup or a fixed point of finite length since the group $G$ is finite, and hence it is nilpotent. □

**Lemma 0.11** (Fermat's Little Theorem). *Let $a$ be a non-negative integer, and $p$ be a prime. Then $a^p - a$ is divisible by the prime $p$.*

*Proof.* Pick the set $X$ as the partition from $0$ to $a$, and apply the p-group fixed point theorem with the cyclic group $P$ of prime order $p$. □

## *Hints or Solutions*

# *Galois Theory*

**Lemma 0.12.** *Elements of finite extensions are algebraic. Algebraic elements are always contained in finite extensions.*

*Proof.* The idea is to suppose an algebraic integer $a$ is in a finite extension of $L$, then we have $[L : K]$ is n less than infinity, then take $1, a, a^2, ..., a^n$, this is $n + 1$ elements of a n-dimensional vector space. Since this is of higher dimension, there must be a nontrivial linear relation $k_0 + k_1 a + ... k_n a^n$, so $a$ is algebraic. For the converse, suppose $p(x)$ is an irreducible polynomial in the field extension $K[x]$, take the quotient of the ideal $K[x]/(p)$ is a field. This is obviously a ring. This a ring, now we check existence of inverses, suppose $q(x)$ is in $K(x)/(p)$, $q(x)$ is nonzero, then $q$ and $p$ are coprime since $p(x)$ is irreducible. Therefore, $a(x)q(x) + b(x)p(x) = 1$ can be found by Euclidean algorithm, so $a(x)$ is inverse of $q(x)$ in $K(x)/((p(x)))$. Since $a$ is a root of $p(x)$ in $K[x]$, where $p$ is irreducible, so $K[x]/p(x)$ is a map to $L$ taking $x$ to $a$. The image of $K[x]/(p)$ is in $L$. □

**Lemma 0.13.** *Sums, products, quotients and differences of algebraic integers are algebraic. Consequently, roots of polynomials are algebraic.*

*Proof.* Consider chain of extensions by pairs of algebraic integers, these are finite extensions. Polynomials are finite sums and products of algebraic integers so these are algebraic as well. □

## *Rings*

*Notation*

-

# *Bibliography*

Evan Chen. *Napkin Project*. Self-Published, May 2025.