A Collection of my Undergraduate Course Notes

Yunhai Xiang

February 23, 2020

Contents

Chapter 1

Foundations of Mathematics

1.1 Motivation

In the 1930s, a group of mainly French mathematicians under the pseudonym *Bourbaki* decided to reformulate mathematics on an extremely abstract, formal and rigorous manner. They undertook arduous efforts and publish the treatise called *Éléments de mathématique*, the first book of which, *Théorie des ensembles* or *Theory of Sets* in English, is the foundation of all mathematics.

One of our objectives for axiomatic set theory is to avoid paradoxes such as the **Russell paradox**, which comes from the very naive intuition that if formula F about x does not use w then

$$\exists w \, \forall x \, [(x \in w) \leftrightarrow F]$$

and this obviously creates a paradox, since if we take $F \equiv (x \notin x)$, then $(w \in w) \leftrightarrow (w \notin w)$. As an analogy, consider a barber who shaves all those, and those only, who do not shave themselves, then does the barber shave himself? Chang and Keisler's book on Model Theory is dedicated to all those model theorists who have never dedicated a book to themselves.

1.2 Formal Languages

In this section, we will introduce the most basic concept in the theory of sets: **formal languages**, specifically, the **propositional language** and the **first order language**. A string in propositional language consists of the following symbols

i. Proposition Symbols: $A, B, C, D, \ldots$

ii. Negation Symbols: $\neg$ (not)

iii. Binary Logic Symbols: $\wedge$ (and), $\vee$ (or), $\rightarrow$ (implies), $\leftrightarrow$ (if and only if)

iv. Auxiliary Symbols: $(,), [,]$

and a **formula** in propositional language is a string that follows the following rules

1. If A is a proposition symbol, A is a formula
2. If F is a formula, then $\neg F$ is a formula
3. If F, G are formulas, then $F \wedge G, F \vee G, F \rightarrow G, F \leftrightarrow G$ are formulas
4. The auxiliary brackets $(,)$ are often used to clearify the structure of the formula.

Let F be a formula with proposition symbols $A_1, \ldots, A_n$, then each proposition symbol can be assigned a **boolean** value: true or false, represented by 1 and 0 respectively. Therefore, for a specific assignment of $A_1, \ldots, A_n$ we can obtain a **valuation** of F through reduction by the reduction rules specified in the following tables

A	$\neg A$
1	0
0	1

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

A	B	$A \rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

A	B	$A \leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Example 1.2.1. Consider the following formulas

(a) $((A \vee B) \wedge A) \rightarrow \neg B$

(b) $((A \rightarrow B) \rightarrow A) \rightarrow A$

(c) $(\neg A \rightarrow \neg B) \leftrightarrow \neg(A \rightarrow \neg B)$

A valuation of (a) by assigning both A and B as true would be

$$\begin{aligned} & ((A \vee B) \wedge A) \rightarrow \neg B \\ \Rightarrow & ((1 \vee 1) \wedge 1) \rightarrow \neg 1 \\ \Rightarrow & ((1 \vee 1) \wedge 1) \rightarrow 0 \\ \Rightarrow & (1 \wedge 1) \rightarrow 0 \\ \Rightarrow & 1 \rightarrow 0 \\ \Rightarrow & 0 \end{aligned}$$

As an exercise, obtain the valuations of (a),(b) and (c) of all assignments for A, B.

Formulas such as (b) in Example 1.2.1 that are always valued to be true no matter what boolean values its variables is assigned is called a **tautology**. We write $\vDash F$ to denote that F is a tautology.

Example 1.2.2. Here are some examples of tautologies,

1. (Law of Identity) $\vDash A \leftrightarrow A$
2. (Law of Double Negativity) $\vDash \neg\neg A \leftrightarrow A$
3. (Law of Excluded Middle) $\vDash A \vee \neg A$
4. (Law of Idempotence) $\vDash A \leftrightarrow (A \wedge A)$
5. (Law of Idempotence) $\vDash A \leftrightarrow (A \vee A)$
6. (Law of Commutativity) $\vDash (A \vee B) \leftrightarrow (B \vee A)$
7. (Law of Commutativity) $\vDash (A \wedge B) \leftrightarrow (B \wedge A)$
8. (Law of Associativity) $\vDash ((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$
9. (Law of Associativity) $\vDash ((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$
10. (Law of Distributivity) $\vDash ((A \wedge B) \vee C) \leftrightarrow ((A \vee C) \wedge (B \vee C))$
11. (Law of Distributivity) $\vDash ((A \vee B) \wedge C) \leftrightarrow ((A \wedge C) \vee (B \wedge C))$
12. (Law of Absorption) $\vDash (A \wedge (A \vee B)) \leftrightarrow A$
13. (Law of Absorption) $\vDash (A \vee (A \wedge B)) \leftrightarrow A$
14. (De Morgan's Law) $\vDash \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$
15. (De Morgan's Law) $\vDash \neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
16. (Law of Implication) $\vDash (A \to B) \leftrightarrow (\neg A \vee B)$
17. (Law of Implication) $\vDash \neg(A \to B) \leftrightarrow (A \wedge \neg B)$
18. (Law of If and Only If) $\vDash (A \leftrightarrow B) \leftrightarrow ((A \to B) \wedge (B \to A))$
19. (Law of Tautology) $\vDash (A \wedge (B \vee \neg B)) \leftrightarrow A$
20. (Law of Tautology) $\vDash (A \vee (B \vee \neg B)) \leftrightarrow (B \vee \neg B)$
21. (Law of Contradiction) $\vDash (A \wedge (B \wedge \neg B)) \leftrightarrow (B \wedge \neg B)$
22. (Law of Contradiction) $\vDash (A \vee (B \wedge \neg B)) \leftrightarrow A$
23. (Law of Contrapositive) $\vDash (A \to B) \leftrightarrow (\neg B \to \neg A)$
24. (Peirce's Law) $\vDash ((A \to B) \to A) \to A$
25. (Proof by Contradiction) $\vDash (\neg A \to (B \wedge \neg B)) \to A$
26. (Principle of Syllogism) $\vDash ((A \to B) \wedge (B \to C)) \to (A \to C)$

First order language can be seen as a extension to propositional language. It is much more complicated as it introduces quantification of variables, which means that a variable in first order language is either a **free variable** or a **bound variable**. First order language is a major topic of this chapter, and it will be the primary formal language we will use in this book. We will also formulate the **ZFC axioms** in first order language, which you will see in the next section. A string in first order language consists of the following symbols,

i. Variable Symbols: $a, b, c, d, \ldots$

ii. Predicate Symbols: $\in$ (in), $=$ (equals)

iii. Quantifier Symbols: $\forall$ (forall), $\exists$ (exists)

iv. Negation Symbols: $\neg$ (not)

v. Binary Logic Symbols: $\wedge$ (and), $\vee$ (or), $\to$ (implies), $\leftrightarrow$ (if and only if)

vi. Class Builder Symbols: $\{, |, \}$

vii. Auxiliary Symbols: $(,), [,]$

A formula in first order language is a string that follows the following rules

1. If a, b are variables then $a \circ b$ is a formulas where $\circ$ is one of the predicate symbols $\in$ or $=$. The free variables of $a \circ b$ are a and b, and $a \circ b$ does not have any bound variables.

2. If F is a formula then so is $\neg F$. The free variables of $\neg F$ is the same as the free variables of F, and the bound variables of $\neg F$ is the same as the bound variables of F.

3. If F, G are formulas such that any free variable in F is not a bound variable in G, and any bound variable in F is not a free variable in G, then $F \circ G$ is a formula where $\circ$ is one of the binary logic symbols $\wedge$, $\vee$, $\to$, or $\leftrightarrow$. The free variables of $F \circ G$ are the free variables of F and G, and the bound variables $F \circ G$ are the bound variables of F and G.

4. If a is a free variable of the formula F then $\forall a\, F$ and $\exists a\, F$ are formulas. The free variables $\forall a\, F$ are the free variables of F except a, and the bound variables of $\forall a\, F$ are a and the bound variables of F. The same applies to $\exists a\, F$.

5. A term is a string that follows the following ruless

   (a) If a is a variable symbol then a is a term with one free variable a and no bound variables.

   (b) Let $a_1, \ldots, a_n$ where $n \geq 1$ be variables symbols distinct from $x_1, \ldots, x_m$ where $m \geq 0$. If ϕ is a term such that $a_1, \ldots, a_n$ are its only free variables and none of $x_1, \ldots, x_m$ is its bound variable, and φ is a formula with $a_1, \ldots, a_n, x_1, \ldots, x_m$ as its only free variables, then $\{\phi \mid \varphi\}$ is a term. The free variables of $\{\phi \mid \varphi\}$ are $x_1, \ldots, x_m$, and the bound variables of $\{\phi \mid \varphi\}$ are the bound variables of φ and ϕ and also the variables $a_1, \ldots, a_n$.

   If s, t are terms such that any free variable in s is not a bound variable in t, and any bound variable in s is not a free variable in t, then $s \circ t$ is a formula where $\circ$ is one of the predicate symbols $\in$ or $=$. The free variables of $s \circ t$ are the free variables of the terms s and t, and the bound variables of $s \circ t$ are the bound variables of the terms s and t.

6. The auxiliary brackets $(,)$ and $[,]$ are often used to clearify the structure of the formula.

Example 1.2.3. Consider the following strings

(a) $\forall x\,\exists y\,[\neg((x=y)\to(z\in y))\vee\exists a\,(z\in a\leftrightarrow z\in z)]$

(b) $\forall x\,[(\forall z\,[(z\in a)\to(z\in z)])\leftrightarrow(\exists x\,(x\in y))]$

(c) $\exists a\,[\forall b\,[b\in\{x\mid(a\in x)\wedge(x\in c)\}]\leftrightarrow\forall b\,[(a\in b)\vee(b=c)]]$

(d) $(x\in y)\to\forall a\,[(\forall b\,[(b\in a)\to(b=c)])\wedge(\forall z\,(z\in b))]$

(e) $\{\{x\mid x=a\vee x=b\}\mid x\in y\wedge b\in y\}=\{\{g\mid g\in i\vee g\in j\vee g\in k\}\mid\exists l[l\in\{x\mid x\in i\to x\in j\}]\}$

and we can easily verify that string (a) is a valid formula with free variable z and bound variables x, y and a. The string (b), however, is not a valid formula, since $\exists x$ appeared within $\forall x$ which violates rule 4. As an exercise, check whether the strings (c),(d) and (e) are valid formulas, and if so, what are its free and bound variables? If not, which rule does it violate?

The notion of free and bound variables extends beyond formal language and can be applied to expressions you are probably more familiar with, for example, in the expression

$$\lim_{n\to\infty}\left[\left(\prod_{k=1}^{n}\frac{2k}{2k-1}\right)\int_{-1}^{\infty}\frac{(\cos x)^{2n}}{2^x}\,\mathrm{d}x\right]=\frac{\pi 2^\pi}{2^\pi-1}$$

the variables n, k, x are all bound variables and there are no free variables, hence it is a proposition[1].

Exercise 1.2.4. Let $\{\cdot\}$ be the fractional part function, and consider the expression

$$\int_0^1\cdots\int_0^1\left\{\frac{1}{\prod_{n=1}^{k}x_n}\right\}\mathrm{d}x_1\cdots\mathrm{d}x_k=1-\sum_{n=0}^{k-1}\left[\frac{1}{n!}\lim_{m\to\infty}\left[\sum_{\ell=1}^{m}\frac{(\ln\ell)^n}{\ell}-\frac{(\ln m)^{n+1}}{n+1}\right]\right]$$

what are the free variables and what are the bound variables? Try proving this as a challenge.

Remark 1.2.5. We introduce the following terminologies

1. A formula with $x_1,\ldots,x_n$ as is its only free variables is a **property** of $x_1,\ldots,x_n$,
2. A term with $x_1,\ldots,x_n$ as its only free variables is a **mapping** of $x_1,\ldots,x_n$,
3. A formula without free variables is a **proposition**,
4. A term without free variables is called a **class**,
5. If a variable is neither free nor bound in a formula, it is **unused** in that formula,
6. If a variable is neither free nor bound in a term, it is **unused** in that term,
7. Let $a_1,\ldots,a_n$ where $n\geq 1$ be variables symbols distinct from $x_1,\ldots,x_m$ where $m\geq 0$. If ϕ is a mapping of $a_1,\ldots,a_n$ and none of $x_1,\ldots,x_m$ is its bound variable, and φ is a property of $a_1,\ldots,a_n,x_1,\ldots,x_m$, we say that the term $\{\phi\mid\varphi\}$ **ranges over** $a_1,\ldots,a_n$.
8. If F is a string, x is a variable symbol and s is another string, we use $[F][x\mapsto s]$ represents the string obtained by replacing every occurence of x in F by s.

[1] This is a problem taken from the 2013 Stanford Math Tournament. See appendix for proof.

As the formulas we are considering gets longer and more complicated, we need to introduce the notion of **definitions**. Definitions are abbriviations of terms and formulas. There are two types of definitions, **extensional definitions** and **intensional definitions**. An extensional definition is an abbriviation of a mapping by introducing a new notation or terminology. To declare an extensional definition, we either write a string of the form

$$[a_1, \ldots, a_n] := \{\phi(x_1, \ldots, x_m) \mid \varphi(a_1, \ldots, a_n, x_1, \ldots, x_m)\}$$

where $[a_1, \ldots, a_n]$ is some notation for the variables $a_1, \ldots, a_n$ where $n \geq 0$, and the term on the right hand side is a mapping of $a_1, \ldots, a_n$ ranging over $x_1, \ldots, x_m$ where $m \geq 1$; or we could write a sentence similar to "for $a_1, \cdots, a_n$, let $[a_1, \cdots, a_n]$ be the class of all $\phi(x_1, \ldots, x_m)$ such that $\varphi(a_1, \ldots, a_n, x_1, \ldots, x_m)$". Note that for the case $n = 0$, the notation has no variable, it is therefore only a symbol that cannot be used as a variable symbol, and we call it a **notational symbol**. Examples of common notational symbols include $\emptyset, \mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \aleph_0, \pi, e, 0, 1, 2, 3$ and etc.

Definition 1.2.6 (Empty Set)**.** $\emptyset := \{x \mid \neg(x = x)\}$

Definition 1.2.7 (Pairing Set)**.** $\{a, b\} := \{x \mid x = a \vee x = b\}$

Definition 1.2.8 (Singleton)**.** $\{a\} := \{a, a\}$

Definition 1.2.9 (Tuple)**.** $(a, b) := \{\{a\}, \{a, b\}\}$

Definition 1.2.10 (Cartesian Product)**.** $a \times b := \{(x, y) \mid x \in a \wedge y \in b\}$

Definition 1.2.11 (Set Difference)**.** $a \setminus b := \{x \mid x \in a \wedge \neg(x \in b)\}$

Definition 1.2.12 (Union Set)**.** $\bigcup a := \{x \mid \exists b\, [b \in a \wedge x \in b]\}$

Definition 1.2.13 (Intersection Set)**.** $\bigcap a := \{x \mid \forall b\, [b \in a \to x \in b]\}$

Definition 1.2.14 (Union)**.** $a \cup b := \bigcup\{a, b\}$

Definition 1.2.15 (Intersection)**.** $a \cap b := \bigcap\{a, b\}$

Definition 1.2.16. Let the **first coordinate** of the tuple x be $\bigcap\bigcap x$

Definition 1.2.17. Let the **second coordinate** of the tuple x be $(\bigcap\bigcup x) \cup ((\bigcup\bigcup x) \setminus (\bigcup\bigcap x))$

Definition 1.2.18 (Power Set)**.** $\mathcal{P}(a) := \{x \mid \forall y\, [y \in x \to y \in a]\}$

Definition 1.2.19 (Succesor)**.** $a^+ := a \cup \{a\}$

Definition 1.2.20 (Arabic Numerals)**.** Define the notational symbols $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ as

$$\begin{aligned} 0 &:= \emptyset & 5 &:= 4^+ \\ 1 &:= 0^+ & 6 &:= 5^+ \\ 2 &:= 1^+ & 7 &:= 6^+ \\ 3 &:= 2^+ & 8 &:= 7^+ \\ 4 &:= 3^+ & 9 &:= 8^+ \end{aligned}$$

Definition 1.2.21 (Natural Numbers)**.**

$$\mathbb{N} := \bigcap\{z \mid (\emptyset \in z) \wedge (\forall w\, [w \in z \to w^+ \in z])\}$$

An intentional definition is an abbriviation for a property by introducing a new predicate or terminology. To declare a intentional definition, we either write a string of the form

$$\langle a_1, \ldots, a_n \rangle :\Longleftrightarrow P(a_1, \ldots, a_n)$$

where $a_1, \ldots, a_n$ with $n \geq 1$ are variables, $\langle a_1, \ldots, a_n \rangle$ is some predicate and $P(a_1, \cdots, a_n)$ is a property of $a_1, \cdots, a_n$; or we could write a sentence similar to "$a_1, \ldots, a_n$ is said to have blah blah relation or property if and only if (usually we omit 'only if') $P(a_1, \ldots, a_n)$". Note that unlike intentional definitions, we do not allow $n = 0$.

Definition 1.2.22. $a \notin b :\Longleftrightarrow \neg(a \in b)$

Definition 1.2.23. $a \neq b :\Longleftrightarrow \neg(a = b)$

Definition 1.2.24. $a \subseteq b :\Longleftrightarrow \forall z \, [(z \in a) \to (z \in b)]$

Definition 1.2.25. a is a **subset** of b if $a \subseteq b$

Definition 1.2.26. $a \subset b :\Longleftrightarrow (a \neq b) \wedge a \subseteq b$

Definition 1.2.27. a is a **proper subset** of b if $a \subset b$

Definition 1.2.28. R is a **relation** between X and Y if $R \subseteq X \times Y$

Definition 1.2.29. R is a relation on X if $R \subseteq X \times X$ and define $aRb :\Longleftrightarrow (a, b) \in R$

Definition 1.2.30. The relation R is **symmetric** if $\forall a \, \forall b \, [aRb \leftrightarrow bRa]$

Definition 1.2.31. The relation R is **antisymmetric** if $\forall a \, \forall b \, [(aRb \wedge bRa) \to (a = b)]$

Definition 1.2.32. The relation R is **reflexive** on X if $\forall a \, [a \in X \to aRa]$

Definition 1.2.33. The relation R is **transitive** if $\forall a \, \forall b \, \forall c \, [(aRb \wedge bRc) \to aRc]$

Definition 1.2.34. The relation R is **total** on X if $\forall a \, \forall b \, [(a \in X \wedge b \in X) \to (aRa \vee bRa)]$

Definition 1.2.35. X has a **minimal element** under the relation R if $\exists a \, (a \in X \wedge \forall b \, (aRb))$

Definition 1.2.36. X has a **maximal element** under the relation R if $\exists a \, (a \in X \wedge \forall b \, (bRa))$

Definition 1.2.37. A reflexive and transitive relation on some X is a **preorder**.

Definition 1.2.38. A symmetric preorder is an **equivalence relation**.

Definition 1.2.39. An antisymmetric preorder is a **partial order**.

Definition 1.2.40. A total partial order is a **total order**.

Definition 1.2.41. The relation R is a **well order** on X if R is a total order on X such that S has a minimal element under R for all $S \subseteq X$.

Definition 1.2.42. We say that the relation f between X and Y is a **function** from its **domain** X to its **codomain** Y if for $x \in X$ there exists a unique $y \in Y$ with $(x, y) \in f$. In other words,

$$(f : X \to Y) :\Longleftrightarrow (f \subseteq X \times Y) \wedge (\forall x \, [x \in X \to \exists y \, [(x, y) \in f \wedge \forall z \, [(x, z) \in f \to z = y]]])$$

Exercise 1.2.43. Consider the definitions from Definition 1.2.44 to Definition 1.2.71. Which ones are intentional definitions? Which ones are extensional definitions?

Definition 1.2.44. $f(x) := \bigcap\{y \mid (x, y) \in f\}$

Definition 1.2.45. $*$ is an **operation** on X if $* : X \times X \to X$ and define $a * b := *((a, b))$

Definition 1.2.46. Let the **image** of A under f be $f[A] := \{f(x) \mid x \in A\}$

Definition 1.2.47. Let the **preimage** of B under f be $f^{-1}[B] := \{x \mid f(x) \in B\}$

Definition 1.2.48. f is **one-to-one** on S if $\forall a \, \forall b \, [((a \in S) \wedge (b \in S)) \to (f(a) = f(b) \to (a = b))]$

Definition 1.2.49. f is **onto** S if $\forall y \, [y \in S \to \exists x \, (f(x) = y)]$

Definition 1.2.50. A function is **injective** if it is one-to-one on its domain

Definition 1.2.51. A function is **surjective** if it is onto its codomain

Definition 1.2.52. A function is **bijective** if it is injective and surjective

Definition 1.2.53. Let the **inverse** of f be $f^{-1} := \{(y, x) \mid (x, y) \in f\}$

Definition 1.2.54. Let the **composite** of f and g be $f \circ g := \{(x, z) \mid \exists y \, [(x, y) \in f \wedge (y, z) \in g]\}$

Definition 1.2.55. Define the **equivalence class** of x under R as $[x]_R := \{y \mid xRy\}$

Definition 1.2.56. $|a| \leq |b| :\iff \exists f \, [f : a \to b \wedge f \text{ is injective}]$

Definition 1.2.57. $|a| \geq |b| :\iff \exists f \, [f : a \to b \wedge f \text{ is surjective}]$

Definition 1.2.58. $|a| = |b| :\iff \exists f \, [f : a \to b \wedge f \text{ is bijective}]$

Definition 1.2.59. $|a| \neq |b| :\iff \exists f \, [f : a \to b \wedge f \text{ is not bijective}]$

Definition 1.2.60. $|a| < |b| :\iff |a| \leq |b| \wedge |a| \neq |b|$

Definition 1.2.61. $|a| > |b| :\iff |a| \geq |b| \wedge |a| \neq |b|$

Definition 1.2.62. a is **finite** if $|a| < |\mathbb{N}|$

Definition 1.2.63. a is **countable** if $|a| \leq |\mathbb{N}|$

Definition 1.2.64. a is **countably infinite** if $|a| = |\mathbb{N}|$

Definition 1.2.65. a is **uncountable** if $|a| > |\mathbb{N}|$

Definition 1.2.66. a is **inductive** if $\emptyset \in a \wedge \forall x \, [x \in a \to x^+ \in a]$

Definition 1.2.67 (Finite Set)**.** $\{a_1, \ldots, a_{n^+}\} := \{a_1, \ldots, a_n\} \cup \{a_{n^+}\}$

Definition 1.2.68 (Ordered List)**.** $(a_1, \ldots, a_{n^+}) := ((a_1, \ldots, a_n), a_{n^+})$

Definition 1.2.69 (Cartesian Product)**.** $a_1 \times \cdots \times a_{n^+} = (a_1 \times \cdots \times a_n) \times a_{n^+}$

Definition 1.2.70 (Finite Union)**.** $a_1 \cup \cdots \cup a_{n^+} := (a_1 \cup \cdots \cup a_n) \cup a_{n^+}$

Definition 1.2.71 (Finite Intersection)**.** $a_1 \cap \cdots \cap a_{n^+} := (a_1 \cap \cdots \cap a_n) \cap a_{n^+}$

To make our lives easier, we will introduce a few abbriviations in formulas. If F is a formula,

1. $\exists! x\, F$ abbriviates $\exists x\, [F \wedge ((\exists y\, F) \to (x = y))]$
2. $\{t \in s \mid F\}$ abbriviates $\{t \mid (t \in s) \wedge F\}$ for terms s, t
3. $F_1 \wedge \cdots \wedge F_{n^+}$ abbriviates $(F_1 \wedge \cdots \wedge F_n) \wedge F_{n^+}$ for formulas F_i
4. $F_1 \vee \cdots \vee F_{n^+}$ abbriviates $(F_1 \vee \cdots \vee F_n) \vee F_{n^+}$ for formulas F_i
5. $t_1, \ldots, t_n \in s$ abbriviates $t_1 \in s \wedge \cdots \wedge t_n \in s$ for terms s and t_i
6. $(\forall f : X \to Y)\, F$ abbriviates $\forall f\, ((f : X \to Y) \to F)$
7. $(\exists f : X \to Y)\, F$ abbriviates $\exists f\, ((f : X \to Y) \wedge F)$
8. $\{f : X \to Y \mid F\}$ abbriviates $\{f \mid (f : X \to Y) \wedge F\}$
9. $(\forall z_1, \ldots, z_n \in s)F$ abbriviates $\forall z_1 \cdots \forall z_n\, ([z_1, \ldots, z_n \in s] \to F)$ for term s and variables z_i
10. $(\exists z_1, \ldots, z_n \in s)F$ abbriviates $\exists z_1 \cdots \exists z_n\, ([z_1, \ldots, z_n \in s] \wedge F)$ for term s and variables z_i
11. $t_1 \circ_1 t_2 \circ_2 \cdots \circ_n t_{n^+}$ abbriviates $t_1 \circ_1 t_2 \wedge \cdots \wedge t_n \circ_n t_{n^+}$ for terms t_i and relations $\circ_i$

It is important to note that in these abbriviations, as well as intentional and extensional definitions, it is often the case that a few bound variables are omitted. Take, for example, the term $\{x \mid \forall y\, [y \in x \to y \in a]\}$ that has free variable a and bound variables x, y. After we defined $\mathcal{P}(a) := \{x \mid \forall y\, [y \in x \to y \in a]\}$, the term $\mathcal{P}(a)$ has a free variable a and no bound variables. Therefore, the string $\forall y\, \exists x\, [a \in \mathcal{P}(a)]$ is a valid formula while the string $\forall y\, \exists x\, [a \in \{x \mid \forall y\, [y \in x \to y \in a]\}]$ is not. As another example, the abbriviation $\exists! x\, F$ has an implicit bound variable y since it abbriviates $\exists x\, [F \wedge ((\exists y\, F) \to (x = y))]$. We need to be careful when we expand these abbriviations during proofs to avoid bound variable collisions, as we will elaborate in the next section.

1.3 Zermelo–Fraenkel Axioms

Now that we have established the fundamentals of formal languages, it is time to introduce the rules for **formal proofs**. If F, G are formulas in first order language, the string $F \Longrightarrow G$ is called an **argument**, where the arrow $\Longrightarrow$ denotes **logical consequence** or **semantic implication**. A proof of the argument $F \Longrightarrow G$ is a sequence of **arguments** which ends with $F \Longrightarrow G$ and follows the **Rules of Inference and Logic**, which we accept axiomatically. An argument with a proof is called a **theorem**, and an argument mathematicians have not yet found a proof for is a **conjecture**; a auxiliary theorem used subsequently as a stepping stone to a larger result is a **lemma**; and a minor theorem that is a special case of or can be proved straightforwardly by a larger theorem is called a **corollary**. The proof rules are as following,

1. If the formula F is a ZFC axiom or a formula derived from an ZFC axiom schema, then you can append the string $\mathbf{ZFC} \Longrightarrow F$ to the sequence
2. If F and G are formulas in propositional language with propositional variables $A_1, \ldots, A_n$ and we know for a fact that $\vDash F \to G$, you can append $F' \Longrightarrow G'$ where F' and G' are formulas in first order language such that F' is obtained by replacing $A_1, \ldots, A_n$ in F by first order formulas $B_1, \ldots, B_n$, and so is G'.

3. If $F :\Longleftrightarrow G$ then you can append $F \Longrightarrow G$ or $G \Longrightarrow F$
4. If $F \Longrightarrow G$ and $G \Longrightarrow H$ are in the sequence, you can append $F \Longrightarrow H$ to the sequence
5. If $F \Longrightarrow G$ and $F \Longrightarrow H$ are in the sequence, you can append $F \Longrightarrow G \wedge H$ to the sequence

Bear in mind that so far we have not assigned truthness to formulas. To introduce truthness into first order language, we first have to state a list of **axioms**. A list of axioms is a list of independent and non-contradictory propositions that are taken to be true for granted. Any proposition inferred from the list of axioms is considered true, and any proposition whose negation is true is considered false. Note that a proposition can be neither true or false, but cannot be both true and false. In fact, the logician Kurt Gödel proved that almost all meaningful formal axiomatic system contains a proposition that is neither true or false, which is known as Gödel's incompleteness theorem.

Axiom 1.3.1 (Axiom of Empty Set)**.** $\exists w \, \forall x \, (x \notin w)$

Axiom 1.3.2 (Axiom of Extensionality)**.** $\forall x \, \forall y \, [(x = y) \leftrightarrow \forall z \, [(z \in x) \leftrightarrow (z \in y)]]$

Axiom 1.3.3 (Axiom of Pairing)**.** $\forall a \, \forall b \, \exists w \, \forall x \, [(x \in w) \leftrightarrow (x = a \vee x = b)]$

Axiom 1.3.4 (Axiom of Union)**.** $\forall a \, \exists w \, \forall x \, (x \in w \leftrightarrow \exists b \, [b \in a \wedge x \in b])$

Axiom 1.3.5 (Axiom of Power Set)**.** $\forall a \, \exists w \, \forall x \, [x \in w \leftrightarrow x \subseteq a]$

Axiom 1.3.6 (Axiom of Infinity)**.** $\exists w \, (\emptyset \in w \wedge \forall x \in w \, [x^+ \in w])$

Axiom 1.3.7 (Axiom of Regularity)**.** $\forall x \, (x \neq \emptyset \to \exists y \in x \, (y \cap x = \emptyset))$

The last two of the ZF "axioms", however, cannot be formulated as first order propositions, as they involve in formulas as variables. The only way to formulate them as real propositions is to introduce extensions of ZFC such as Von Neumann-Bernays-Gödel set theory or Morse-Kelley-Tarski set theory, which are not topics of our discussion. Therefore, we will instead write "for all such and such formulas" as an informal substitude. Rigorously speaking, they are not two single axioms in first order language, but "a lot of" axioms. We call them **axiom schemas**.

Axiom 1.3.8 (Axiom Schema of Specification)**.** For all formulas φ about $x, a, w_1, \ldots, w_n$,

$$\forall w_1 \cdots \forall w_n \, \forall a \, \exists b \, \forall x \ (x \in b \leftrightarrow [x \in a \wedge \varphi])$$

We allow $n = 0$, in which case there is no variable w_i.

Axiom 1.3.9 (Axiom Schema of Replacement)**.** For all formulas φ about $a, x, y, w_1, \ldots, w_n$

$$\forall w_1, \ldots, \forall w_n \, \forall a \ ([\forall x \in a \, \exists! y \, \varphi] \to \exists b \, \forall y \ [y \in b \leftrightarrow \exists x \in a \, \varphi])$$

where b is unused in φ. We allow $n = 0$, in which case there is no variable w_i.

If $\mathcal{S} := \{\phi \mid \varphi\}$ where $\{\phi \mid \varphi\}$ ranges over $a_1, \ldots, a_n$ is a class, and we proved that

$$\mathbf{ZFC} \Longrightarrow \exists x \, \forall y \, [y \in x \leftrightarrow \ \exists a_1 \cdots \exists a_n \, (y = \phi \wedge \varphi)]$$

then we say that $\mathcal{S}$ is a set. Natural Numbers, Integers and induction

Definition 1.3.10. For $n, m \in \mathbb{N}$, define $n <_{\mathbb{N}} m :\Longleftrightarrow n \in m$

1.4 Introduction to Algebraic Structures

In mathematics, **algebraic structures** are sets with operations that follows a list of properties that originated from our intuitions of elementary and common mathematical objects, namely,

1. the set of **integers** $\mathbb{Z} = \{\dots, -2, -1, 1, 0, 1, 2, \dots\}$,
2. the set of **rational numbers** $\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \wedge q \neq 0 \right\}$,
3. the set of **real numbers** $\mathbb{R} = \{\text{all decimals, terminating, repeating, or otherwise}\}$,
4. the set of **complex numbers** $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ where $i^2 = -1$

However, bear in mind that the above are not rigorous definitions. Later in this chapter, we will discuss the contruction of these sets rigorously. There are a few properties of these sets that we can state straightforwardly,

Definition 1.4.1. Let $+, \times$ be operations on S and $Q \subseteq S$, then

1. Q is **closed** under $+$ if $\forall a, b \in Q\,[(a + b) \in Q]$,
2. S is **associative** under $+$ if $\forall a, b, c \in S\,[(a + b) \circ c = a + (b + c)]$,
3. The elements $a, b \in S$ **commute** under $+$ if $a + b = b + a$,
4. S is **commutative** under $+$ if $\forall a, b \in S\,[a + b = b + a]$,
5. S is **left distributive** under addition $+$ and product $\times$ if $\forall a, b, c \in S\,[a\times(b+c) = a\times b+a\times c]$,
6. S is **right distributive** under addition $+$ and product $\times$ if $\forall a, b, c \in S\,[(b+c)\times a = b\times a+c\times a]$,
7. S is **distributive** if it is both left and right distributive under the same addition and product,
8. S has a **left identity** $e \in S$ under $+$ if $\forall a \in S\,[e + a = a]$,
9. S has a **right identity** $e \in S$ under $+$ if $\forall a \in S\,[a + e = a]$,
10. S has an **identity** $e \in S$ under $+$ if e is both a left and a right identity under $+$,
11. $a \in S$ has an **left inverse** $b \in S$ under $+$ if $b + a = e$ where e is an identity under $+$,
12. $a \in S$ has an **right inverse** $b \in S$ under $+$ if $a + b = e$ where e is an identity under $+$,
13. $a \in S$ has an **inverse** $b \in S$ under $+$ if b is both a left and right inverse of a under $+$

Exercise 1.4.2. Let $*$ be an operation on S, prove that

1. if S has more than one left (right) identity, it has no right (left) identity,
2. if S has a left identity e_L and a right identity e_R then $e_L = e_R$,
3. if S has an identity, then it is unique.
4. if S is associative under $*$ and $a \in S$ has a left inverse b, then b is a right inverse of a
5. if S is associative under $*$ and $a \in S$ has an inverse, then it is unique

Definition 1.4.3. If G be a set and $*$ an operation on G such that

1. G is associative under $*$,
2. G has an identity under $*$,
3. All $g \in G$ has an inverse

then we say that G is a **group** under $*$. If the group G is commutative under its operation then we say G is **abelian**.

Definition 1.4.4. Define two operations **addition** $(+)$ and **multiplication** $(\cdot)$ on R such that

1. R is an abelian group under $(+)$ with identity 0 and inverse $-a$ for $a \in R$.
2. for $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
3. for $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$,
4. exists **multiplicative identity** $1 \in R$ such that for $a \in R$, $1 \cdot a = a \cdot 1 = a$,

then R is called a **ring** under the addition $(+)$ and the multiplication $(\cdot)$. Further, consider

8. for $a, b \in R$, $a \cdot b = b \cdot a$,
9. for $a \in R$, exists **multiplicative inverse** $a^{-1} \in X$ such that $aa^{-1} = a^{-1}a = 1$

If a ring R satisfies property 8 then it is a **commutative ring**. If a ring R satisfies property 9 then it is a **division ring**. A commutative division ring is called a **field**. A **pseudo-ring** is a set R with two operations addition $(+)$ and multiplication $(\cdot)$ such that properties 1,2,3 are satisfied but not necessaily property 4.

Proposition 1.4.5. If G is a group then

1. $e \in G$ is unique
2. for $g \in G$, g^{-1} is unique
3. for $g \in G$, $(g^{-1})^{-1} = g$
4. for $g, \ldots, g_n \in G$, $(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}$

Proposition 1.4.6. If R is a ring and $a, b, c \in R$, then

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $(-1)a = -a$
5. $(-1)(-1) = 1$
6. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$

Example 1.4.7. Here are some examples of groups

1. $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ are groups under addition
2. The **cyclic group** of degree n, $\mathrm{C}_n = \{1, g, \ldots, g^{n-1}\}$ where $g^n = 1$.
3. The **dihedral group** of degree n, $\mathrm{D}_n = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ where $s^2 = r^n = 1$.
4. The **permutation group** of degree n is
$$\mathrm{S}_n = \{f : \mathbf{Z}^+ \to \mathbf{Z}^+ \mid f \text{ is bijective and } f(m) = m \text{ for } m > n\}$$
where the operation is function composition.
5. The **quaternion group**, $\mathrm{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ where $(-1)^2 = 1$ and
$$i^2 = j^2 = k^2 = ijk = -1$$
6. If R is a ring, define $R^\times = \{r \in R \mid \exists s \in R\,(rs = sr = 1)\}$, then $R^\times$ is a group under the multiplication operation of R, which we call the **multiplicative group of** R.
7. If $G_1, \ldots, G_n$ are groups, then $G_1 \times \cdots \times G_n$ is a group under the operation
$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$
for $a_1, b_1 \in G, \ldots, a_n, b_n \in G_N$, which we call the **product group** of $G_1, \ldots, G_n$.

Example 1.4.8. Here are some examples of rings

1. $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ are rings under the usual operations, and $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are also fields.
2. If $R_1, \ldots, R_n$ are rings then $R_1 \times \cdots \times R_n$ is the called the **product ring** of $R_1, \ldots, R_n$ where
$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$
for $a_1, b_1 \in R_1, \ldots, a_n, b_n \in R_n$.
3. If G is a group and R is a ring, then the **group ring** of R over G
$$R[G] = \{f : G \to R \mid |f^{-1}(R \setminus \{0\})| < \aleph_0\}$$
is a ring under the operations
$$(f_1 + f_2)(g) = f_1(g) + f_2(g)$$
$$(f_1 f_2)(g) = \sum_{h \in G} f_1(h) f_2(h^{-1} g)$$
for $g \in G$ and $f_1, f_2 \in R[G]$. We typically write an element $f \in R[G]$ as the formal polynomial
$$a_1 g_1 + \cdots + a_n g_n$$
where $\{g_1, \ldots, g_n\} = f^{-1}(R \setminus \{0\})$ and $a_i = f(g_i)$ for $1 \le i \le n$. Define the group $\langle x \rangle = \{x^n \mid n \in \mathbf{Z}\}$, then we abbriviate $R[\langle x \rangle]$ as $R[x]$, which we call the **polynomial ring** of R.

4. Let R be a ring, then $R[[x]] = \{f \mid f : \mathbf{N} \to R\}$ is called the **power series ring** of R under

$$(f_1 + f_2)(n) = f_1(n) + f_2(n)$$
$$(f_1 f_2)(n) = \sum_{i=0}^{n} f_1(i) f_2(n-i)$$

for $n \in \mathbf{N}$. We typically write an element $f \in R[[x]]$ as the formal power series

$$a_0 + a_1 x + a_2 x^2 + \cdots$$

where $a_i = f(i)$ for $i \geq 0$.

5. If R is a ring then $\mathcal{M}_n(R) = \{f \mid f : \{1, \ldots, n\}^2 \to R\}$ is called the **matrix ring** under

$$(f_1 + f_2)(i, j) = f_1(i, j) + f_2(i, j)$$
$$(f_1 f_2)(i, j) = \sum_{k=1}^{n} f_1(i, k) f_2(k, j)$$

for $1 \leq i, j \leq n$ and $f_1, f_2 \in \mathcal{M}_n(R)$. We typically write an element $f \in \mathcal{M}_n(R)$ as

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

where $a_{i,j} = f(i, j)$ for $1 \leq i, j \leq n$.

Definition 1.4.9 (Integers)**.** Define $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/ =_{\mathbb{Z}}$ and $a -_{\mathbb{N}} b := [(a, b)]_{=_{\mathbb{Z}}}$ where

$$=_{\mathbb{Z}} := \{((a, b), (c, d)) \in (\mathbb{N} \times \mathbb{N})^2 \mid a +_{\mathbb{N}} d = c +_{\mathbb{N}} b\}$$

The set $\mathbb{Z}$ is called the **set of integers**.

Definition 1.4.10. Define the relation $<_{\mathbb{Z}}$ on $\mathbb{Z}$ as

$$<_{\mathbb{Z}} := \{((a -_{\mathbb{N}} b), (c -_{\mathbb{N}} d)) \in \mathbb{Z} \times \mathbb{Z} \mid a +_{\mathbb{N}} d <_{\mathbb{N}} c +_{\mathbb{N}} b\}$$

and define operations $+_{\mathbb{Z}}, -_{\mathbb{Z}}, \times_{\mathbb{Z}}$ on $\mathbb{Z}$ by

$$(a -_{\mathbb{N}} b) +_{\mathbb{Z}} (c -_{\mathbb{N}} d) = (a +_{\mathbb{N}} c) -_{\mathbb{N}} (b +_{\mathbb{N}} d)$$
$$(a -_{\mathbb{N}} b) -_{\mathbb{Z}} (c -_{\mathbb{N}} d) = (a +_{\mathbb{N}} d) -_{\mathbb{N}} (b +_{\mathbb{N}} c)$$
$$(a -_{\mathbb{N}} b) \times_{\mathbb{Z}} (c -_{\mathbb{N}} d) = (a \times_{\mathbb{N}} c +_{\mathbb{N}} b \times_{\mathbb{N}} d) -_{\mathbb{N}} (a_{\mathbb{N}} \times d_{\mathbb{N}} +_{\mathbb{N}} b_{\mathbb{N}} \times c_{\mathbb{N}})$$

for all $a, b, c, d \in \mathbb{N}$

Definition 1.4.11 (Rationals)**.** Define $\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0 -_{\mathbb{Z}} 0\}))/ =_{\mathbb{Q}}$ and $\frac{a}{b} := [(a, b)]_{=_{\mathbb{Q}}}$ with

$$=_{\mathbb{Q}} := \{((a, b), (c, d)) \in (\mathbb{Z} \times (\mathbb{Z} \setminus \{0 -_{\mathbb{Z}} 0\}))^2 \mid a \times_{\mathbb{Z}} d = b \times_{\mathbb{Z}} c\}$$

The set $\mathbb{Q}$ is called the **set of rational numbers**.

Definition 1.4.12. Define the relation $<_{\mathbb{Q}}$ on $\mathbb{Q}$ as

$$<_{\mathbb{Q}} := \left\{ \left(\frac{a}{b}, \frac{c}{d} \right) \mid \right\}$$

and define the operation $+_{\mathbb{Q}}, -_{\mathbb{Q}}, \times_{\mathbb{Q}}, \div_{\mathbb{Q}}$ on $\mathbb{Q}$ by

$$\begin{aligned}
\frac{a}{b} +_{\mathbb{Q}} \frac{c}{d} &= \frac{a \times_{\mathbb{Z}} d +_{\mathbb{Z}} b \times_{\mathbb{Z}} c}{b \times_{\mathbb{Z}} d} \\
\frac{a}{b} -_{\mathbb{Q}} \frac{c}{d} &= \frac{a \times_{\mathbb{Z}} d -_{\mathbb{Z}} b \times_{\mathbb{Z}} c}{b \times_{\mathbb{Z}} d} \\
\frac{a}{b} \times_{\mathbb{Q}} \frac{c}{d} &= \frac{a \times_{\mathbb{Z}} c}{b \times_{\mathbb{Z}} d} \\
\frac{a}{b} \div_{\mathbb{Q}} \frac{c}{d} &= \frac{a \times_{\mathbb{Z}} d}{b \times_{\mathbb{Z}} c}
\end{aligned}$$

for all $a, b, c, d \in \mathbb{Z}$

1.5 Real Numbers and Complex Numbers

There are two ways to

Definition 1.5.1. A set $\emptyset \subset r \subset \mathbb{Q}$ is a **Dedekind cut** on $\mathbb{Q}$ if

$$(\forall p \in r)\,(\forall q \in \mathbb{Q} \setminus r)\,[p < q] \quad \text{and} \quad (\forall p \in r)\,(\exists q \in r)\,[p < q]$$

Definition 1.5.2. Define the set of **real numbers** as $\mathbb{R} := \{r \mid r \text{ is a Dedekind cut on } \mathbb{Q}\}$

0.9999=1
Least Upper Bound Archimedian Property Denseness Cantor Set Sylvester–Gallai theorem

1.6

Definition 1.6.1. For $n, m \in \mathbf{N}$, define the **rising factorial** and **falling factorial** of n to m as

$$\begin{aligned}
n^{\overline{m}} &:= n(n+1)(n+2)\cdots(n+m-1) \\
n^{\underline{m}} &:= n(n-1)(n-2)\cdots(n-m+1)
\end{aligned}$$

where $n^{\overline{0}} = n^{\underline{0}} = 1$, and define $m! := 1^{\overline{m}} = 1 \cdot 2 \cdot 3 \cdots m$.

Definition 1.6.2. Define the **binomial coefficient** $\binom{n}{m}$ where $n, m \in \mathbf{N}$ as

$$\binom{n}{m} := \begin{cases} \dfrac{n^{\underline{m}}}{m!} & \text{if } m \leq n \\ \\ 0 & \text{if } m > n \end{cases}$$

Exercise 1.6.3. Let R be a ring. Prove that for $a, b \in R$ and $n \in \mathbf{N}$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$$

and if n is odd, prove that

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots \pm ab^{n-2} \mp b^{n-1})$$

1.7 Ordinal Numbers and Cardinal Numbers

Transfinite induction Continuum Hypothesis Schurodiner Burnsiein Grothendieck Universe Von Neumann Universe

1.8 Axiom of Choice and Zorn's Lemma

Zorn Lemma Tukey Lemma Hausdorff Maximal principle Well ordering theorem For every set there is an operation on it making it a group Tychonoff's Theorem Tarski's theorem Every surjection has an injective inverse Every commutative ring with a unity has a maximal ideal Every two cardinals is comparable Every vector space has a basis Banach-Tarski paradox

1.9 Algorithms and Turing Computability

Eucildean Algorithm Boolean satisfiabililty problem Entscheidungsproblem

Chapter 2

Introduction to Algebra

2.1 Motivation

2.2 Irreducibles and Primes

2.3 ED, PID, and UFD

Chapter 3

Finite Dimensional Vector Spaces

3.1 Motivation

Chapter 4

Metric Space and Topology

discrete calculus

4.1 Motivation

4.2 Metric Space and Metric Topology

Herschfeld's Convergence Theorem

Chapter 5

Measure and Integration

5.1 Motivation

Chapter 6

Combinatorics and Graph Theory

6.1 Motivation

6.2