Foundations of Analysis

Daisuke Natthaworn Sakai

April 15, 2019

Contents

“Excellent!” I cried. “Elementary,” said he.

Praeambulum

The current elementary monograph emerged from the author's desire to create a comprehensive treatment on mathematical analysis from a purely theoretical and unified standpoint, and systematically summarize results necessary and sufficient for the treatment of more advanced subjects with foundations in analysis, or have much use from theorems of analysis, such as Riemannian geometry, complex geometry, manifold theories, functional analysis, spectral theory, analytic and algebraic number theory, probability theory, and differential equations. Indeed, almost every facet of mathematics is in some way reliant on analysis, and obviously the much used real and complex number systems is an analyitcal construction from the rationals.

In the first section, we give preliminaries. Although these preliminaries are given with a view toward developing analysis, there is In the third section, we give a foundational exposition to further topics in analysis. The text may also be of use to physicists who would want to build a foundational understanding of Analysis.

We build every fact from scratch, assuming no knowledge other than a working knowledge of set theory, and first order logic. For these, P. D. Magnus's text (or its alternative version modified by Tim Button), ForAllx, would be necessary for a full understanding, the usual undergraduate courses in mathematics would suffice for a more or less smooth read. If the reader has taken beginning graduate level courses in functional analysis or complex analysis, this text perhaps would be most appropriate as a reference. No exercises are given; one may instead try to complete a proof without looking at the text.

Analysis is a theory on its own with its own way of thinking to obtain results. For example, for a function $f : A \to B$, suppose we are given t in A. When reasoning with $f(t)$, we must first acknowledge $\forall x(x \in A \to (\exists y((x, y) \in f)))$. we first use universal elimination to obtain $t \in A \to (\exists y((t, y) \in f))$, then use conjuction elimination to obtain $\exists y((t, y) \in f)$ and use existential elimination, by substituting $f(t)$ for y and obtain the sentence $(t, f(t)) \in f$. Although a formal linguistic proof would look something like what was described, it is of major inconvenience to consider proofs with all these details, and doing so can only hinder the progress of mathematics. Therefore we only start with the logical basis, and then quickly (quickly, here, means after two or three months of continuous grappling with the idea) progress to our apropos theory. A theory itself is a system of valid symbolic manipulations that can essentially be reduced to logical manipulations of axioms.

The author is also planning to write a short text on the foundations of common foundational notions in mathematics, apropos the discussion in the previous paragraph, such as functions, ordered pairs, algebraic operations, in a set theoretic point context, which would serve as a useful guide that will bridge logical gap between ForAllx and this text. The text will first treat ZFC and obtain completely self contained results from a computational perspective; that is, it will emphasize the fact that the results given in the text can in principle be entirely reduced to symbolic/linguistic manipulations which means that they

can be verified by a computer. The author also intends for this upcoming text to treat other theories in more or less detail as well, such as NBG, ZFC + Grothendieck universes, SEAR and ETCS which are more useful or convenient in discussing certain facets of mathematics, but unwieldy or incompatible for others. As of 2019, unfortunately it is not agreed upon as to which axiomatic system is all encompassing and most convenient to use. In any case, we will proceed our discussion on the theory of analysis assuming that some kind of set theory underlies our usage of the symbol $\in$.

A text on the foundations of analysis is not meant to be a text for an introduction to analysis. In this text, we present only the underpinnings of the subject and develop ideas systematically, formally, and concisely. The presentation of facts, and notations are to make proofs as easy flowing as possible. In particular, this collection of notes will reflect the author's not-so-subtle Bourbakian, and particularly algebraic and set theoretic leaning, and penchance for logical exactness and elegance.

The current text can be used as a reference for graduate students on the basic foundations of analysis, who want a text that summarizes the basic results of undergraduate analysis, or as a self study text for so called "advanced undergrates," who specialize in analysis. A graduate student or working mathematician may also find this a convenient text to review the subject from a self contained and axiomatic mathematical standpoint. The text is written with the assumption that the reader already has studied analysis, algebra, and topology and has already sufficient motivation for the material, but wants a concise text summarizing necessary results on the theory behind analysis. For this reason, examples are given only when necessary to develop further theory, and no motivation is given for theorems. For example, the existence (and its necessary reliance on the axiom of choice, given certain assumptions), of a non-Lebesgue measureable set is considered off topic, and so is the existence of a continuous function differentiable nowhere, as well as the irrationallity (or transcendentality) of π, e, and $\sqrt{2}$.

Analysis is taught at the introductory level in most universities courses, as it provides much motivation to general topology and its immediate use in the sciences and engineering fields; rigorous analysis, often in a sparce and incoherent manner. Those who are logically or set theoretically minded would find it more comforting to have the theory built from scratch, starting from the general and proceeding to the specific.

It is a mild inconvenience that the order of motivation and logical consequences are contrary in direction. As such, most texts on analysis do not state theorems in too specific a form, and are not rigorous or formal to satisfactory degree. Further, as such, it is logically and aesthetically unappealing to do so, for the definition of a field and a vector space is algebraic, the conversation of limits and continuity are topological in its essence, and analysis can be most elegantly derived from these mathematical foundations. This text attempts to give the algebraic and topological foundations of analysis, and treats theorems in a more or less general way without being inconvenient, so that theorems may be applied to real, complex, p-adic, metric, uniform, or other spaces, when apro-

pos. The specific is then deduced from the general. We explain the intuition when it is not immediately self evident.

Finally, it is also unforunate that too many texts are instructive rather than referential in nature, too lengthy and at times unwieldy, both physically and oganizationally. Further, the subject is large and sparse, and results are scattered all over the literature. This text tries to integrate all these results in a coherent and concise whole, and give a fast route to more advanced mathematics, starting from the very definitions in algebra and topology.

As such, we assume that the reader has already mastered the theory of algebra and the theory of topology. The foundations of the algebra and topology that we use can be reduced to ZFC, if we ignore or conveniently circumvent certain parts. We only view ZFC as a language that can make rigorus most of what we discuss in this text.

My deepest gratitude to Alfred Tarski, P. D. Magnus, Tim Button, Walter Rudin, Y. Miyamoto, Jonathan K. Hodge, Steven Schlicker, Ted Sundstrom, James Munkres, Serge Lang, and of course, Wikipedia, ProofWiki, and nLab for my education.

Any mathematical mistakes, gaps in logic, or improvements in content, exposition, or formatting are greatly thanked; please email them to DNsakai1729@gmail.com. Any one who would like the original tex/lyx file is also welcome ask for them via the aforementioned address.

General Remarks

The text is in the standard definition-theorem-proof format. Remarks are not used in further development of theory but may serve to better understand an idea. It may reference defintions which are not yet introduced. Therefore they can be freely skipped without obstruction to the logical flow of the book. We only number theorems.

Obviously, mastery of the logical foundations of the definition of functions and ordered pairs, are assumed, as in virtually any treatement of mathematics. Proofs and definitions are given formally and concisely and may be terse when it is easy, and sometimes omitted when the method of proof is trivial, or is a quick routine logical manipulation. Otherwise, proofs perhaps tend to be more explanatory than most texts. The reader is expected to have the so called mathematical maturity to fill these out, when the reader so desires, but note that this can always be done; we leave no gaps in this treatement of mathematical analysis.

The only assumption in this text is the existence of $\mathbb{N}$, whose algebraic characterization is given in chapter 1.

When we give a long or short list of "obvious" or "immediate" properties which follow from a certain definition, the author suggests to the reader to actually go through the algebraic manipulations to obtain the above results. We will be implicitely relying on them; and to have them memorized would facilitate the mental process of verifying a statement (or proof); by being much quicker and automated. Although these properties would be all too familiar, we state them so that we can immediately appeal to these properties when developing further theory, without technically having small gaps.

Part I
Prerequisites

When we use the symbol "$\in$", we do not necessarily denote set theoretic inclusion but a general meaning of inclusion, which may be axiomatized in a more general theory or more encompassing theory, such as NBG, ZFC + Grothendieck Universes, or some other theory that gives a definition of "collection." As such, when we use the word "set" we do not mean a set in ZFC, but rather a general object belonging in a more general theory or theory, that does not need to be ZFC. All objects that we treat are to be considered a collection of some sort.

We will say "set," to mean an object that exists in some set theory. Further, we assume a theory that can treat the collection of all "sets," which can include entities that may not be "sets," themselves. One such example would be NBG theory, where the collection of all "sets" exists, and is called a "class" or "proper class." Another axiomatization is ZFC + Grothendieck Universes. In whatever case, it is very common to simply use the term "set," to mean an object that can be operated by the axioms in ZFC (note that this does not necessarily mean that we need a theory containing ZFC, like NBG, but we can also use Grothendieck Universes, which only locally looks like ZFC, so all the theory in ZFC still make sense).

We will use the axiom of choice (abbreviated as AC) in the apropos form (that is we can apply it without assuming that what we are chosing from need not be a "set" of "sets" but can also be so called "classes"). We will write (AC) when it is used.

Assuming usual ZF, the axiom of choice, the well ordering theorem, and Zorn's lemma are equivalent. Refer to Lang's Algebra, revised third edition, Appendix 2 and 4.

We will assume that the reader understands and has mastered the logical and set theoretic foundations of algebraic theory and has furthermore understands and has mastered algebraic theory itself. This section serves only as a reminder of these things, but it is suggested to be worked through as well.

When f is a function, and $(x, y) \in f$, we will denote the element y as $f(x)$. When U is a subset of the domain of f, we will write $f[U]$ to denote the set $\{f(x) \mid x \in U\}$, called the "image of f under U"; when U is the domain, one may also denote $f[U]$ as $Im(f)$, and this set is called the "image of f." We denote the restriction of f on U as $f\mid_U$.

In denoting unions, when Θ is a set of sets, we write $\bigcup \Theta$, or $\bigcup_{T\in\Theta} T$, or to denote the set $\{x \mid \exists T \in \Theta : x \in T\}$, which we assume to exist in whatever underlying set theory we use. If the elements of Θ are indexed by a set S, that is, we have a surjection $f : S \to \Theta$, then we denote $\bigcup_{T\in U} T$ or $\bigcup_{s\in S} f(s)$ to denote $\bigcup f[S]$, which is, of course by definition equal to $\bigcup \Theta$.

We write WLOG to state "without loss of generality."

Remark. We make the following general remarks.

1. There is much overlap between the beginning of this part and chapter

1 of Munkres' "Topology," and chapter 1 and 2 of Rudin's "Principles of Mathematical Analysis." However, we start from the very beginning definitions of algebra.

2. The purpose of part I of this text is manifold: it serves as a logical base from which proceeding claims can be actually defined in a purely linguistic standpoint. However, it also serves as a reminder of the basics of many topics of mathematics, such as sets, relations, functions, groups, rings, categories, and elementary arithmetic.

3. On the same note as 2, this part can be taken as a "foundation of mathematics" in general.

1 Structural Prerequisites

We recall categories, relations, order relations, well order and induction. These are, of course, pertitent to almost all fields of mathematics.

1.1 Categories

$\mathbb{A} = (Ob(\mathbb{A}), Mor(\mathbb{A}), Mor, \circ)$ is a "category" iff:

1. $Mor : Ob(\mathbb{A}) \times Ob(\mathbb{A}) \to Mor(\mathbb{A})$ is a partition (One may use the weaker condition that Mor is a surjection). We call elements in $Mor(\mathbb{A})$, "morphisms."

2. $\circ$ maps from $Ob(\mathbb{A}) \times Ob(\mathbb{A}) \times Ob(\mathbb{A})$ to $\mathcal{P}(Mor(\mathbb{A}) \times Mor(\mathbb{A}) \times Mor(\mathbb{A}))$, where:

   (a) $A, B, C \in Ob(\mathbb{A})$, we have that $\circ_{(A,B,C)} : Mor(A, B) \times Mor(B, C) \to Mor(A, C)$. In this case, we will simply write "$\circ$" instead of "$\circ_{(A,B,C)}$" by abuse of notation.

   (b) Given (a) hence, for all $A \in Ob(\mathbb{A})$ there exists an identity morphism $1_A \in Mor(A, A)$ such that for all $B \in Ob(\mathbb{A})$, we have $\forall f \in Mor(A, B) : 1_A \circ f = f$ and $\forall f \in Mor(A, B) : f \circ 1_A = f$. It is immediately verified that the identity morphism is unique. (If we assume that in condition 1, Mor is a partition.)

   (c) For all $A, B, C, D \in Ob(\mathbb{A})$, and for all $f \in Mor(A, B)$, $g \in Mor(B, C)$, and $h \in Mor(C, D)$, we have $(f \circ g) \circ h = f \circ (g \circ h)$. (Note that if (a) holds, then both sides of the equality must exist; that is, it is in fact, "defined")

When we are given a category that satifies the weaker condition of 1, we can always associate the objects with the original morphisms to create a partition, in the following way. Suppose $\overline{Mor}$ is a surjection. Define $Mor(A, B) := \{(A, f, B) \mid f \in \overline{Mor}(A, B)\}$. If $\overline{\circ}$ is the original composition, define a new composition by $(A, f, B) \circ (B, g, D) := (A, g \overline{\circ} f, D)$. It is routine verification to

obtain that the new composition then satisfies condition 2. When we discuss categories we will always implicitely assume this construction hence, but will not explicitely mention it, and will write f for (A, f, B), and $g \circ f$ for $(A, g \circ f, D)$, by abuse of notation.

An element in $Ob(\mathbb{A})$ is called an "object of $\mathbb{A}$," and an element in $Mor(\mathbb{A})$ is called a "morphism of $\mathbb{A}$," or an "arrow of $\mathbb{A}$."

An arrow f is called an "automorphism," iff there exists object A such that $f \in Mor(A, A)$.

For morphism $f \in Mor(A, B)$, when $g \in Mor(B, A)$ and $f \circ g = id_A$ and $g \circ f = id_B$, we say that "g is an inverse of f." If an inverse of f exists, then f is said to be an "isomorphism." An inverse is immediately verified to be unique.

We say that "A is isomorphic to B" when such a function f exists. Clearly, if A is isomorphic to B, then B is isomorphic to A, so we simply say that "A and B are isomorphic."

Proposition 1. *We note the following:*

1. *The identity morphism is an isomorphism*
2. *The compositions of two isomorphisms is an isomorphism*
3. *The inverse of an isomorphism is an isomorphism*

For an object A in a category:

- A is called universally repelling iff: for all objects B the collection $Mor(A, B)$ is a singleton
- A is called universally attracting iff: for all objects B the collection $Mor(B, A)$ is a singleton

It is immediately verified that universally repelling or attracting objects are unique under isomorphism.

1.1.1 Category of Sets

Denote $Ob(Sets)$ as the collection of all "sets" within a certain theory that allows the existence of the collection of all "sets." We denote the collection $Mor(Sets)$ as the collection of all functions between sets. For two sets, we map $Mor(A, B)$ to the set of all maps which map from A to B. Denote $\circ$ as usual function composition. Then $Sets = (Ob(Sets), Mor(Sets), Mor, \circ)$ is a category.

1.2 Commonly Used Relations

For collection S, we say that R is a relation on S iff $R \subseteq S \times S$. When considering relations, we write, as a logical sentence: "xRy" iff $(x, y) \in R$. The restriction of R on subset U of S denoted R_U is defined as $R_U := R \cap (U \times U)$.

We note that for a relation R on S, and subset U of S, for any elements $x, y \in U$, the statement $xR_Uy \iff xRy$ is true.

We also note that for relation R on S, and subset U and D such that $D \subset U \subset S$, we have that $(R_U)_D = R_D$.

A relation R on S is called "Well-founded," iff for all non-empty subsets U of S, the statement $\exists x \in U : \neg yRx$ is true.

Remark. Well-foundedness is a generalization of well-order. Replace R with $<$ to obtain the statement.

1.2.1 Equivalence Relations

A relation $\sim$ on a set S is called an "equivalence" iff:

1. $\forall x \in S : x \sim x$
2. $\forall x, y \in S : x \sim y \Rightarrow y \sim x$
3. $\forall x, y, z \in S : x \sim y \wedge y \sim z \Rightarrow x \sim z$

For $x \in S$, the set $[x] := \{y \in S \mid x \sim y\}$ is called an equivalence class of x, and the set of all equivalence classes is denoted $S/\sim$. When x and y are in the same equivalence class, we say that "x and y are equivalent." It is immediately verified that equivalence classes are pairwise disjoint, that is, two distinct classes are disjoint. Further, it is immediately verified that $[x] = [y]$ iff $x \sim y$.

If R is an equivalence on S, and $U \subset S$, then the restriction of R on U is an equivalence, with the notation $\sim_U$. In this case, we will write $U/\sim$ to mean $U/\sim_U$ in order to abbreviate notation.

1.2.2 Order relations

The ordered pair $(S, \leq)$ is called a "partially ordered set," which will be shortened as "poset," iff:

- $\leq$ is a relation on S

1. $\forall x \in S : x \leq x$
2. $\forall x, y \in S : (x \leq y \wedge y \leq x) \Rightarrow x = y$
3. $\forall x, y, z \in S : (x \leq y \wedge y \leq z) \Rightarrow x \leq z$

The first condition is called "reflexivity," the second is called "antisymmetry," because the relation is never symmetric for distinct elements, and the third condition is called "transitivity."

In the context of a poset, we state "x is smaller than or equal to y" to mean that $x \leq y$.

The ordered pair $(S, \leq)$ is called a "non-strict totally ordered set," which can be shortened as "non-strict toset," iff:

- $\leq$ is a relation on S

1. $\forall x, y \in S : x \leq y \vee y \leq x$

2. $\forall x, y \in S : (x \leq y \wedge y \leq x) \Rightarrow x = y$

3. $\forall x, y, z \in S : (x \leq y \wedge y \leq z) \Rightarrow x \leq z$

We call $\leq$ the partial order on S.

A non-strict totally ordered set is also often called a "totally ordered set." This is bad convention because we also have a "strictly totally ordered set," defined below, which cannot be a non-strictly totally ordered set, by definition, unless the set on which there is order, is itself empty, in which case, the order relations are also empty and satisfy the same axioms. However, note that if a collection is non-strictly totally ordered then it is also partially ordered.

The ordered pair $(S, <)$ is called a "strictly totally ordered set," or a "strict toset," iff

- $<$ is a relation on S

1. $\forall x, y \in S : x \neq y \Rightarrow (x < y \vee y < x)$

2. $\forall x, y \in S : x < y \Rightarrow (x \neq y)$

3. $\forall x, y, z \in S : (x < y \wedge y < z) \Rightarrow x < z$

We call $<$ the total order on S.

It is immediately verified that a strict total order defines a non-strict total order by defining $x \leq y$ iff $x < y \vee x = y$, and vice versa, by $x < y$ iff $x \leq y \wedge x \neq y$. In this case, we say that $\leq$ is induced by $<$ and vice versa. Further, if $<$ is induced by $\leq$, and $<'$ is induced by $\leq$, then $<'$ and $<$ are equal. Similarly, if $\leq$ is induced by $<$ and $\leq'$ is induced by $<$, then $\leq$ and $\leq'$ are equal. Therefore reasoning with tosets is the same as reasoning with posets, and in a principle we only need to define terms regarding strict and non-strict relations in terms of one or the other. To use only one for our definitions is in fact not necessarily convenient, and we will proceed apropos of context.

In the context of a total order $<$, when we use the symbol $\leq$, we always use it assuming that it is the partial order induced by the total order. Similarly, in the context of a partial order $\leq$, when we use the symbol $<$, we always use it assuming that it is the total order induced by the partial order.

It is an immediately verified that the restriction if $U \subset S$, then if $(S, \leq)$ is a poset, then $(U, \leq_U)$ is a poset; if $(S, \leq)$ is a non-strict toset then $(U, \leq_U)$ is a non-strict toset; and if $(S, \leq)$ is a strict toset then $(U, \leq_U)$ is a strict toset.

When we have strict totally ordered set $(S, <)$, or a partially ordered set $(S, \leq)$, for subset D of S and element x of S, we will write:

1. $D < x$ to mean that $\forall t \in D : t < x$

2. $x < D$ to mean that $\forall t \in D : x < t$

Similarly, we write:

1. $D \leq x$ to mean that $\forall t \in D : t \leq x$

2. $x \leq D$ to mean that $\forall t \in D : x \leq t$

Proposition 2. *For poset $(S, \leq)$, and subset D of S, and subset U of D, and element $x \in D$, the following properties hold:*

1. $U \leq_D x \iff U \leq x$
2. *In particular,* $D \leq_D x \iff D \leq x$

Proof. Omitted. □

Remark. For a toset or poset S, we will invariably use upper case letters for subsets of S and lower case letters for elements in S to avoid confusion. There will be no cases when the and element of a poset is also a poset or toset, and hence there will be no ambiguity in this notation in this text.

Proposition 3. *For poset $(S, \leq)$, denoting subsets of S as D and E, and elements of S as x, and y, the following properties hold:*

1. $D \leq x \leq y \Rightarrow D \leq y$
2. $x \leq y \leq D \Rightarrow x \leq D$
3. $E \subset D \wedge D \leq x \Rightarrow E \leq x$
4. $E \subset D \wedge x \leq D \Rightarrow x \leq E$

Proof. Omitted. □

Proposition 4. *For toset $(S, <)$, denoting subsets of S as D and E, and elements of S as x, and y, the following properties hold:*

1. $D < x < y \Rightarrow D < y$
2. $x < y < D \Rightarrow x < D$
3. $E \subset D \wedge D < x \Rightarrow E < x$
4. $E \subset D \wedge x < D \Rightarrow x < E$
5. $x < D \vee D < x \Rightarrow x \notin D$

Proof. Omitted. □

For a strict toset $(S, <)$, and elements $a, b \in S$, and denoting $\leq$ as the induced non-strict order, we will use the following notation to denote certain sets:

1. $[a, b]_S := \{x \in S \mid a \leq x \leq b\}$
2. $]a, b[_S := \{x \in S \mid a < x < b\}$
3. $[a, b[_S := \{x \in S \mid a \leq x < b\}$

4. $]a, b]_S := \{x \in S \mid a < x \leq b\}$
5. $[a, \infty[_S := \{x \in S \mid a \leq x\}$
6. $]a, \infty[_S := \{x \in S \mid a < x\}$
7. $]-\infty, a]_S := \{x \in S \mid x \leq a\}$
8. $]-\infty, a[_S := \{x \in S \mid x < a\}$

These sets are called "intervals." When the context is clear, and we are considering a toset $(S, <)$, we will omit the subscript. For example, we will simply write $[a, b] := \{x \in S \mid a \leq x \leq b\}$. However, when dealing with two tosets, or when considering a subset of a toset, we will use subscript to be clear with our notation. For example, if we have subset U of S, and elements $a, b \in U$, we will write $[a, b]_U := \{x \in U \mid a \leq_U x \leq_U b\} = \{x \in U \mid a \leq x \leq b\}$.

Remark. Using curved brackets to denote openness is highly unadvised, for (a, b) is already used to denote an ordered pair.

For poset $(S, \leq)$, and subset U of S:

1. An element $x \in U$ is called "maximal" iff $\forall y \in U : (x \leq y \Rightarrow x = y)$
2. An element $x \in U$ is called "minimal" iff $\forall y \in U : (y \leq x \Rightarrow y = x)$
3. An element $x \in U$ is called "greatest" iff $U \leq x$.
4. An element $x \in U$ is called "smallest" or "least" iff $x \leq U$

Remark. These elements may or may not exist in a given poset.

In the context of a strictly totally ordered set $(S, <)$, subset U of S, and an element $x \in S$, we will say that it is "greatest," or "smallest," elements of S, we mean those which are, respectively, "greatest," or "smallest," elements of S with respect to the non-strict toset induced by the strict total order in the set S. Immediately, one sees that greatest and smallest elements are maximal and minimal, respectively. It is immediately verified that the smallest and greatest elements are unique, and further, if the partial order is a non-strict total order, then maximal elements are greatest, and minimal elements are smallest.

When referring to a subset U of poset S, where $(S, \leq)(U, \leq_U)$, where $\leq_U$ refers to the restriction of $\leq$ on U. Therefore:

Proposition 5. *For poset $(S, \leq)$, and subset U of S, the following are consequences of the above definitions:*

1. *An element $x \in U$ is maximal in $(U, \leq_U)$ iff $\forall y \in U : (x \leq y \Rightarrow x = y)$*
2. *An element $x \in U$ is minimal in $(U, \leq_U)$ iff $\forall y \in U : (y \leq x \Rightarrow y = x)$*
3. *An element $x \in U$ is greatest in $(U, \leq_U)$ iff $U \leq x$*
4. *An element $x \in U$ is least in $(U, \leq_U)$ iff $x \leq U$*

Proof. We simply use the fact that when dealing with elements in U, $\leq$ and $\leq_U$ are interchangeable. □

In the context of a strict toset $(S, <)$, and a subset U of S, when we use the words "maximal," "minimal," "greatest," or "smallest," elements in U, we use those words in the context of the non-strict total order induced by the strict total order $<$, by abuse of language. The non-strict total order will be denoted as $\leq$.

For a non-strict toset $(S, \leq)$, or strict toset $(S, <)$:

1. A subset U of S is called "bounded above" or is said to "have an upper bound," iff: $\exists b \in S : U \leq b$
2. A subset U of S is called "bounded below" or is said to "have an lower bound," iff: $\exists b \in S : b \leq U$

A non-strict toset $(S, \leq)$ or strict toset $(S, <)$, is said to have the "least upper bound property" (LUB property) iff for every non empty subset U of S, if the set $B_{upp}(U) := \{x \in S \mid U \leq x\}$ of all upper bounds is non-empty, then it has a least element. This element is called the "least upper bound of U."

A non-strict toset $(S, \leq)$ or strict toset $(S, <)$, is said to have the "greatest lower bound property" (GLB property) iff for every non empty subset U of S, if the set $B_{low}(U) := \{x \in S \mid x \leq U\}$ of all lower bounds is non-empty, then it has a greatest element. This element is called the "greatest lower bound of U."

Proposition 6. *An ordered set has the least upper bound property iff it has the greatest lower bound property.*

Proof. If a poset has the least upper bound property, then for non empty U bounded below, consider the set $B_{low}(U)$. It is bounded above, so it has a least upper bound. This element is the greatest lower bound of U. The converse is similar. □

In the context of a strict toset $(S, <)$, we will say that it is "bounded above," or "bounded below," to mean that the non-strict toset $(S, \leq)$, where $\leq$ is induced by $<$, is bounded above or bounded below.

Proposition 7. *Given a non-strict total order $\leq$, and strict order induced by $<$ or vice versa, on a set S, the following properties hold for elements in S:*

1. $a < b \leq c \Rightarrow a < c$
2. $a \leq b < c \Rightarrow a < c$
3. $a \leq b \wedge a \neq b \Rightarrow a < b$
4. $a \leq b \vee b < a$
5. $\neg(a \leq b \wedge b < a)$

Proof. Omitted. □

1.3 Induction and Well order

A non-strict toset $(S, \leq)$ is called "well ordered" iff for every non empty subset U of S, U has a least element. A strict toset, $(S, <)$, is called "well ordered," iff it is well ordered with respect to the induced non-strict order. In the context of a poset or toset S, given a subset U of S, we will say that U is "well ordered," iff, $(U, \leq_U)$ is well ordered.

Proposition 8. *A subset of a well ordered poset is well ordered.*

Proof. Suppose U is a subset of well ordered toset S. Then suppose $D \subset U$ and $D \neq \varnothing$. Then $D \subset S$ so take μsuch that $\mu \leq D$ and $\mu \in D$. Then □

Proposition 9. *Given toset $(S, <)$, and subset U of S, U is well ordered iff every non-empty subset D of U contains an element μ such that $\mu \leq D$.*

Proof. This is due to the fact that $\leq$, $\leq_U$, and $(\leq_U)_D$ are all interchangeable when we only consider elements in, and subsets of D. □

Remark. Therefore hence, we can essentially regard the above proposition as a definition of well order of subsets of tosets. However, when we discuss Zorn's lemma it is easier to use the one we stated.

Given a strict toset $(S, <)$, and elements $a, b \in S$, we will state that "a is an immediate successor of b" and likewise state that "b is an immediate predecessor of a" iff the set $]a, b[$ is empty. An immediate successor or an immediate predecessor of an element is immediately verified to be unique. We will also abbreviate "immediate successor," and "immediate predecessor," as "successor," and "predecessor," respectively.

Proposition 10. *For well ordered set $(S, <)$, any element a in S is either greatest or there exists $b \in S$ such that b is an immediate succesor of a.*

Proof. Suppose $a \in S$ is not greatest. There $B_{upp}(U)$, the set of all upper bounds of a is non-empty and hence has a least element; denote it as b. Then if $]a, b[$ is non-empty, b is not least in $B_{upp}(U)$; a contradiction. □

Corollary 11. *For well ordered set $(S, <)$, if S does not have a greatest element, then every element in S has an immediate successor.*

Proof. Omitted. □

Given strict toset $(S, <)$, it is said to "obey the principle of strong induction," iff for all subsets U of S, the statement $\forall x \in S((\ ] - \infty, x[_S \subset U) \Rightarrow x \in U)$ implies that $U = S$.

Proposition 12. *A strict toset $(S, <)$, if well ordered, obeys the principle of strong induction.*

Proof. Suppose $(S, <)$ is well ordered. $\forall x \in S(\ ]-\infty, x[_S \subset U) \Rightarrow x \in U)$ holds. Further suppose $U \neq S$. The set $K := S \setminus U$ has a least element, μ, for it must be non-empty. If $t \in S$ satisfies $t < \mu$, then t is not in K, otherwise μ is not the least element. So t is in U. So $]-\infty, \mu[_S \subset U$. Hence $\mu \in U$, a contradiction. □

Remark. Notice that we did not require S to be non-empty (for otherwise the conclusion is then trivial), nor did we require that U be non-empty. At a cursory glance it may seem like U need be non-empty, but indeed, if S is non-empty, then the condition $\forall x \in S((]-\infty, x[_S \subset U) \Rightarrow x \in U)$ obtains that U must be non-empty. Indeed, S itself has a least element, denote it as μ. Then clearly, $]-\infty, x[_S = \varnothing \subset U$ hence $\mu \in U$, so indeed, the "base case," is in fact, implied.

A strict toset $(S, <)$, where every element in S has an immediate successor, and S has a least element, is said to "obey the principle of induction," iff:

The following two statements

1. If μ is a least element in S, and $\mu \in U \subset S$
2. For every element in $x \in S$, the statement $\forall x \in U(\forall y(\ ]x, y[= \varnothing \Rightarrow y \in U) \Rightarrow y \in U)$ is true

together imply that $U = S$.

2 Algebraic Prerequisites

We first show the existence of the real numbers and its algebraic properties. We then define the extended reals, and the complex numbers. We then recall basic properties of integers and other algebraic structures and define cardinality. Since integers are the basis of sequences, summations, series, and countability on the one hand, and modular arithmetic, p-adic numbers, number theory on the other, we will be rather detailed in our discussion.

We assume that the reader is familiar with the foundations of algebraic theory, and has a working knowledge of it.

2.1 Group Theoretic Definitions

For set M, a map $\cdot : M \times M \to M$ is said to be a "law of composition," or "composition." In this case, for $a, b \in M$ we denote the element $a \cdot b := \cdot(a, b)$.

When we denote a composition as "$\cdot$," or "$\times$," we will call it "multiplication," and when we denote a composition as "$+$," we will call it "addition." We will use the same terminology even when we adorn these symbols; for example, the compositions "$+'$," "$\overline{+}$," will also be called "addition." For $x, y \in M$, we call $x \cdot y$ as the composition of x and y, or the the multiplication of x and y, the addition of x and y, according to the above context mentioned. We often interchangeably use the symbols $\cdot$ and $\times$, and omit them, and write ab for $a \cdot b$ or $a \times b$.

Given set M, and law of compositon $+$, and subset U of M, we write $+_U$ to denote the set $\{((x,y),z) \mid (x,y) \in U \times U, z \in M\}$ and we will call $+_U$ the "restriction of $+$ on U."

Given set U, if $U \times U$ is within the domain of a law of composition $+$, we will state that the composition is "closed" under U iff the image of $U \times U$, $+[U \times U]$, is a subset of U. When this is true, then the restriction of the composition on U is a composition.

If $+$ is a composition on A, and $+'$ is a composition on B, a function $f : A \to B$ is said to "preserve operation":

- $\forall x, y \in A : f(x + y) = f(x) +' f(y)$

$(S, \cdot)$ is called a "Semi-group" iff

- $\cdot$ is a law of composition of S; and

1. For all $a, b, c \in S : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

For semigroups $(A, +)$ and $(B, +')$, a function $f : A \to B$ is called a "semi-group" homomorphism iff:

- $\forall x, y \in A : f(x + y) = f(x) +' f(y)$

that is, it preserves operation.

A law of composition on a set M is called "commutative" or "Abelian" iff:

- For all $a, b \in M : a \cdot b = b \cdot a$

A law of composition on a set M is called:

1. "right cancellable" iff: for all $a, b, c \in M : a \cdot c = b \cdot c \Rightarrow a = b$
2. "left cancellable" iff: for all $a, b, c \in M : c \cdot a = c \cdot b \Rightarrow a = b$
3. Simply "cancellable" iff: M is both left and right cancellable

Clearly if a composition is commutative, and it is left cancellable, then it is also right cancellable, and vice versa.

$(M, \cdot)$ is called a "Monoid" iff

- $\cdot$ is a law of composition of M; and

1. For all $a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. There exists $e \in M$ such that $\forall a \in M : a \cdot e = e \cdot a = a$

That is, it is a semigroup with identity. It is immediately shown that an identity element, e, mentioned in condition 2, is unique. We hence usually use e to denote the identity element in a group.

When we say that "e is the identity," what we in fact mean is that "e an identity". The deviation from formal precision is so as to accomodate our informal linguistic expressions. In a purely logical context, when we are given

two elements x, y, for example, and we write $x \cdot y = e$, we mean the sentence: $\exists e \in M[\forall a \in M[e \cdot a = a \cdot e = a] \wedge x \cdot y = e]$. A fully correct sentence, (assuming that we have defined ordered pairs set theoretically), would be as follows: $\exists y \in M[\forall a \in M[((e, a), a) \in \cdot \wedge ((a, e), a) \in \cdot] \wedge ((x, y), e) \in \cdot]$.

When the operation is additive, the identity is denoted as 0; when it is multiplicative, it is denoted as 1. f is a monoid homomorphism when it is a function between monoids that is a semi-group homomorphism.

It is customary to write hg to denote $h \cdot g$, and at times we will do this.

We also must note that in fact a monoid can be viewed as a category in the following manner. Given category $(Ob(\mathbb{A}), Mor(\mathbb{A}), Mor, \circ)$, when $Ob(\mathbb{A})$ is a singleton, we have $(Mor(\mathbb{A}), \circ)$ is a monoid. Note that the information of the object in the category is irrelevant information. For indeed, all arrows are automorphisms and hence can be composed with any other arrow. Hence $\circ : Ob(\mathbb{A}) \times Ob(\mathbb{A}) \to Ob(\mathbb{A})$. By definition of a category, we hence have a semi-group. Further, the identity morphism is the identity element in the composition, hence we have a monoid. Conversely, given monoid $(M, \times)$, we can give define a corresponding category, $\mathbb{A}$, in the following manner. We can simply put the object of A as the set M, although this is irrelevant information. The morphisms of $\mathbb{A}$ are all the elements in M, and the composition $\circ$ maps the (M, M) to the map $\times$. $Mor(\mathbb{A})$ maps from a single element, that is, (M, M), to the element M, which has an identity morphism, the identity element in M.

A monoid $(G, \cdot)$ is called a "Group" iff every element in the monoid is invertible, that is:

1. For all $g \in G$ there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$

It is immediately shown that any element in a group has a unique inverse, and therefore we can regard the inversion of an element as a function. For subsets A and B of a semigroup S, we denote $A \cdot B := \{a \cdot b \mid a \in A \wedge b \in B\}$. For an element $g \in G$ and subset H of G, we denote $g \cdot H := \{g\} \cdot H$. Obviously $e \cdot H = H$ for identity e.

Clearly, for subsets A, B, C of a semigroup M, we have $(AB)C = A(BC)$. Further, if G is commutative, then $AB = BA$.

H is a subgroup of G iff it is a subset of G and the restriction of the composition of G on H is a group.

For subgroup H, we denote $G/H := \{g \cdot H \mid g \in G\}$. When H is a subgroup, we say that H is "normal " iff:

- $\forall x \in G : xHx^{-1} \subset H$

Proposition 13. *H is normal iff $\forall x \in G : xHx^{-1} = H$*

Proof. Omitted. □

Proposition 14. *If H is a normal subgroup of G, if we define $x \sim y$* iff *$xy^{-1} \in H$*, then this is an equivalence on G, and the set of all equivalence classes is G/H, the quotient group, and conversely, if $\sim$ is and equivalence on G, then $[e] = \{y \in S \mid e \sim y\}$ is a normal subgroup of G, and $G/H = G/\sim$.

Proof. Omitted. □

When H is normal the set G/H forms a group under the definition of composition: $xH \cdot yH = xyH$, which is immediately verified to be a unique assignment. G/H is called a "quotient group."

f is a group homomorphism when it is a function between groups that is a semi-group homomorphism.

Denote $Ob(Mon)$ as the collection of all monoids, and denote $Mor(Mon)$ as the collection of all monoid homomorphisms. Denote the function Mor as mapping from two groups A, B to the set of all monoid homomorphisms of A to B. Denote $\circ$ as function composition. Then $(Ob(Mon), Mor(Mon), Mor, \circ)$ is a category, which we denote as Mon, and call it the category of monoids.

When the objects $Ob(Grp)$ are groups, and the morphisms $Mor(Grp)$ are group homomorphisms, and Mor is the mapping from two groups A, B to the set of all group homomorphisms of A to B, and $\circ$ is function composition, then $(Ob(Grp), Mor(Grp), Mor, \circ)$ is a category and is called the category of groups.

When the objects $Ob(Ab)$ are Abelian groups, and the morphisms $Mor(Ab)$ are group homomorphisms, and Mor is the mapping from two groups A, B to the set of all group homomorphisms of A to B, and $\circ$ is function composition, then $(Ob(Ab), Mor(Ab), Mor, \circ)$ is a category and is called the category of Abelian groups.

2.2 Elementary Properties of Group-like Structures

In this section we recall elementary properties of groups, and in particular commutative groups; these properties will be used freely in the following sections.

Proposition 15. *In a group $(G, \cdot)$, the following properties hold for elements in G:*

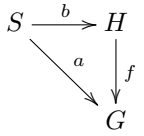
1. $x \cdot z = y \cdot z \Rightarrow z = y$, *and* $z \cdot x = z \cdot x \Rightarrow z = y$
2. *If e is an additive identity, then* $\forall x, a, b \in G : (xa = ax = e \wedge xb = bx = e) \Rightarrow a = b$. *That is, the inverse is unique. We will denote the inverse of an element a as a^{-1}, when the operation is multiplication, and $-a$ when the operation is addition.*
3. $(ab)^{-1} = b^{-1}a^{-1}$
4. $e^{-1} = e$

Proof. Omitted. □

By the above proposition, from number 2 we can consequently regard taking an inverse element in a group as a function.

Suppose S is a semigroup. Consider the following category, which we denote as ζ. The objects of ζ are semigroup homomorphisms from S to an Abelian group G. Suppose a and b are objects in ζ such that they are semigroup homomorphisms from S to Abelian groups H and G, respectively. The morphisms

of ζ are the collection of all semigroup homomorphisms (which are necessarily group homomorphisms) from H to G such that the diagram



commutes. For a universally repelling object, $f \in Mor(S, K(S))$, we call $K(S)$ the "Grothendieck completion" of S, or the "Grothendieck group" of S.

Theorem 16. *For any commutative monoid $(M, +)$, the Grothendieck group exists.*

Proof. Consider the set $M \times M$ with componentwise addition. This is a commutative monoid. The relation $\sim$ by $(x, y) \sim (x', y')$ iff $\exists k \in M : x + y' + k = y + x' + k$ is an equivalence. Then the composition on $(M \times M)/\sim$ by $[(x, y)] + [(x', y')] = [(x + x', y + y')]$ is in fact a function and is commutative. $[(0, 0)]$ is the additive identity, and the inverse of $[(x, y)]$ is $[(y, x)]$. So we have an abelian group. Denote this group as $K(M)$. For x in M, map $\phi(x) = [(x, 0)]$. Then ϕ is a semigroup homomorphism, and is the universal object that was required. For suppose $\alpha : M \to G$, for a commutative group G. It is quickly verified that $f : K(M) \to G$ by $f([(x, y)]) = \alpha(x) - \alpha(y)$ is a semigroup homomorphism such that $\alpha = f \circ \phi$. Futher, f is unique, because if $\alpha = g \circ \phi$, then $g([(x, y)]) = g([(x, 0)] - [(y, 0)]) = \alpha(x) - \alpha(y)$. □

Remark. The reader may be familiar with the proof using the free group generated by M, which generalizes the theorem to: "For any semigroup S, the Grothendieck group exists." However, this proof uses the existence of the free group generated by S, which in turn relies on the existence of the integers. Since we have not yet deduced the existence of the integers, nor have we discussed their properties, we avoid this method in this instance.

2.3 Ring-like structures

$(S, +, \cdot)$ is a near-semiring iff:

1. $(S, +)$ is a commutative monoid
2. $(S, \cdot)$ is a semigroup
3. Multiplication distributes over addition, that is, $\forall x, y, z \in R : z \cdot (x + y) = z \cdot y + z \cdot x$ and $(x + y) \cdot z = x \cdot z + y \cdot z$
4. When we denote 0 as the additive identity, $\forall x \in S : 0 \cdot x = x \cdot 0 = 0$

$(S, +, \cdot)$ is a semiring iff:

1. $(S, +)$ is a commutative monoid

2. $(S, \cdot)$ is a commutative monoid

3. Multiplication distributes over addition

4. When we denote 0 as the additive identity, $\forall x \in S : 0 \cdot x = x \cdot 0 = 0$

The ordered triple $(R, +, \cdot)$ is a "ring" iff:

1. $(R, +)$ is an Abelian group

2. $(R, \cdot)$ is a semigroup

3. Multiplication distributes over addition

Remark. We do not assume that a ring has identity nor do we assume that it is commutative. Therefore a ring is not necessarily a semiring, but is necessarily a near-semiring.

For two near semi-rings, R, S, a function $f : R \to S$ is called a "near-semiring homomorphism" iff it preserves addition and multiplication. We similarly define "semi-ring homomorphisms," and "ring homomorphisms." Near-semirings, semi-rings, and rings are categories with their morphisms being the respective homomorphisms.

An element x in a ring R is called a "zero divisor" iff there exists $y \in R : x \cdot y = 0 \vee y \cdot x = 0$. It is called a unit iff there exists $y \in R$ such that $x \cdot y = 1$.

A ring $(R, +, \cdot)$ is called "commutative" iff multiplication is commutative, and it is said to "have identity" iff multiplication has identity that is distinct from the additive identity. We note that a ring R is with identity, then it is a monoid under multiplication. If, further it is commutative, then it is a commutative monoid under multiplication.

It is verified that ring with identity is necessarily a semiring.

Near semi-rings, semirings, and rings all form categories.

Proposition 17. *The following operational statements hold for elements in a ring* $(R, +, \cdot)$.

1. *When we denote 0 as the additive identity,* $0x = x0 = 0$

2. $-a = (-1)a$

3. $(-a)b = (-b)a = -(ab)$

Proof. Omitted. □

An integral domain $(R, +, \cdot)$, is a commutative ring with identity such that every non-zero element is cancellable, that is:

- If $z \in R$ and $z \neq 0$ then $\forall x, y \in R : xz = yz \Rightarrow x = y$

It is verified that $(R, +, \cdot)$ is a commutative ring with identity iff the multiplication of non-zero elements in an integral domain is nonzero.

The ordered triple $(F, +, \cdot)$ is a "Field" iff:

- $+$ and $\cdot$ are laws of compositions on F; and

1. $(F, +)$ is an Abelian group
2. When we denote the additive identity as 0, and the restriction of $\cdot$ on $F \setminus \{0\}$, is denoted as $\tilde{\cdot}$, we have that $(F \setminus \{0\}, \tilde{\cdot})$ is an Abelian group
3. Addition distributes over multiplication.

In condition 2, we use 1 to denote the identity element in $(F \setminus \{0\}, \tilde{\cdot})$.

A field is verified to be an integral domain.

Proposition 18. *In the non-strict order $\leq$ induced by the strict order $<$, $\mathbb{N}$ is not bounded above by any element in $\mathbb{N}$.*

Proof. Because $0 < 1$, any greatest element m is smaller than $m + 1$. □

If $(R, +, \cdot, <)$ is called an "ordered ring" iff:
If $(R, +, \cdot)$ is a ring, and the strict total order satisfies:

1. $\forall a, b, c \in R : a < b \Rightarrow a + c < b + c$
2. $\forall a, b, c \in R : 0 < a \wedge 0 < b \Rightarrow 0 < a \cdot b$

It is here strongly emphasized that when we say that a ring R is ordered, we do not only mean that there is an order on the ring R, but we also mean that the order on R satisfies the two conditions above conditions.

Proposition 19. *If R is an ordered ring that is commutative and with identity;*

1. Then similar properties hold for the non-strict order induced by the strict total order:
   (a) $\forall a, b, c \in R : a \leq b \Rightarrow a + c \leq b + c$
   (b) $\forall a, b, c \in R : 0 < a \wedge 0 \leq b \Rightarrow 0 \leq a \cdot b$
   (c) $\forall a, b, c \in R : 0 \leq a \wedge 0 \leq b \Rightarrow 0 \leq a \cdot b$
2. Further, the following order property holds in R:
   (a) $0 < 1$
3. Further, for elements in R, the following additive properties hold with respect to order:
   (a) $0 < c \iff -c < 0$
   (b) $c < 0 \iff 0 < -c$
   (c) $a < b \iff -b < -a$
   (d) $x < y \wedge x' < y' \Rightarrow x + x' < y + y'$
4. Further, for elements in R, the following multiplicative properties hold with respect to the induced non-strict total order:

(a) $0 \leq c \iff -c \leq 0$

(b) $c \leq 0 \iff 0 \leq -c$

(c) $a \leq b \iff -b \leq -a$

(d) $x \leq y \wedge x' \leq y' \Rightarrow x + x' \leq y + y'$

5. Further, for elements in R, the following multiplicative properties hold with respect to the strict total order:

(a) $a < b \wedge 0 < c \Rightarrow ac < bc$

(b) $a < b \wedge c < 0 \Rightarrow bc < ab$

(c) $ac < bc \wedge 0 < c \Rightarrow a < b$

(d) $ac < bc \wedge c < 0 \Rightarrow b < a$

(e) $0 < a < b \wedge 0 < a' < b' \Rightarrow 0 < aa' < bb'$

(f) $a < b < 0 \wedge a' < b' < 0 \Rightarrow 0 < bb' < aa'$

(g) $0 < a \wedge 0 < ab \Rightarrow 0 < b$

(h) $0 < a \wedge ab < 0 \Rightarrow b < 0$

(i) $a < 0 \wedge 0 < ab \Rightarrow b < 0$

(j) $a < 0 \wedge ab < 0 \Rightarrow 0 < b$

(k) $a < 0 \wedge 0 < b \Rightarrow ab < 0$

(l) $a < 0 \wedge b < 0 \Rightarrow 0 < ab$

6. Further, for elements in R, the following multiplicative properties hold with respect to the induced non-strict total order:

(a) $a \leq b \wedge 0 < c \Rightarrow ac \leq bc$

(b) $a \leq b \wedge c < 0 \Rightarrow bc \leq ab$

(c) $ac \leq bc \wedge 0 < c \Rightarrow a \leq b$

(d) $ac \leq bc \wedge c < 0 \Rightarrow b < a$

(e) $0 \leq a \leq b \wedge 0 \leq a' \leq b' \Rightarrow 0 \leq aa' \leq bb'$

(f) $a \leq b < 0 \wedge a' \leq b' < 0 \Rightarrow 0 \leq bb' \leq aa'$

(g) $0 < a \wedge 0 \leq ab \Rightarrow 0 \leq b$

(h) $0 < a \wedge ab \leq 0 \Rightarrow b \leq 0$

(i) $a < 0 \wedge 0 \leq ab \Rightarrow b \leq 0$

(j) $a < 0 \wedge ab \leq 0 \Rightarrow 0 \leq b$

(k) $a \leq 0 \wedge 0 \leq b \Rightarrow ab \leq 0$

(l) $a \leq 0 \wedge b \leq 0 \Rightarrow 0 \leq ab$

7. Further, for elements $c, x \in R$, and subset D of R, the following properties hold with respect to order and multiplication:

(a) $0 < D \iff -1 \cdot D < 0$

(b) $D < 0 \iff 0 < -1 \cdot D$

(c) $D < 0 \wedge 0 < c \Rightarrow 0 < c \cdot D$

(d) $D < 0 \wedge c < 0 \Rightarrow c \cdot D < 0$

(e) $0 < D \wedge x < D \wedge 0 < c \Rightarrow c \cdot x < c \cdot D$

(f) $0 < D \wedge x < D \wedge c < 0 \Rightarrow c \cdot D < c \cdot x$

(g) In particular, in 6, we have $0 < D \wedge x < D \Rightarrow -1 \cdot D < -x$

(h) $c \in D \wedge D < x \Rightarrow c < x$

8. Further, for elements $c, x \in R$, and subset D of R, the following properties hold with respect to order and addition:

   (a) $x < D \rightarrow x + c < D + c$

   (b) In particular, $x < D \Rightarrow 0 < D - x$

   (c) $c \in D \wedge D < x \Rightarrow c < x$

9. Further, for elements $c, x \in R$, and subset D of R, the following properties hold with respect to the induced non-strict order:

   (a) $0 \leq D \iff -1 \cdot D \leq 0$

   (b) $D \leq 0 \iff 0 \leq -1 \cdot D$

   (c) $D < 0 \wedge 0 \leq c \Rightarrow 0 \leq c \cdot D$

   (d) $D \leq 0 \wedge c < 0 \Rightarrow c \cdot D \leq 0$

   (e) $0 < D \wedge x \leq D \wedge 0 < c \Rightarrow c \cdot x \leq c \cdot D$

   (f) $0 < D \wedge x \leq D \wedge c < 0 \Rightarrow c \cdot D \leq c \cdot x$

   (g) In particular, in 6, we have $0 < D \wedge x \leq D \Rightarrow -1 \cdot D \leq -x$

   (h) $c \in D \wedge D \leq x \Rightarrow c \leq x$

10. Further, for elements $c, x \in R$, and subset D of R, the following properties hold with respect to order and addition:

    (a) $x \leq D \rightarrow x + c \leq D + c$

    (b) In particular, $x \leq D \Rightarrow 0 \leq D - x$

    (c) $c \in D \wedge D \leq x \Rightarrow c \leq x$

11. Further, for elements $c, x \in R$, and subset D of R, the following properties hold with respect to order and addition: $c \in D \iff c + x \in D + x$

Proof. Omitted. □

2.3.1 The Natural Numbers

We will call the set $(\mathbb{N}, +, \cdot, <)$, "the set of natural numbers," iff $(\mathbb{N}, +, \cdot)$ is a semiring and $<$ is a strict total order on $\mathbb{N}$, satisfying the following properties:

1. Addition is cancellable
2. The multiplicative identity, denoted 1, is distinct from the additive identity
3. $\forall a, b \in \mathbb{N} : a < b$ iff $\exists k \in \mathbb{N} : k \neq 0 \wedge a + k = b$
4. $a < b \wedge c \neq 0 \Rightarrow a \cdot c < b \cdot c$
5. $\mathbb{N}$ is well ordered

Further, we will always refer to a semiring with a strict total order satisfying the above five properties as the "the set of natural numbers," and denote the algebraic structure as $\mathbb{N}$. We leave it to the set theorists to show the existence of $\mathbb{N}$ from ZFC (In fact, it can be shown in ZF.)

Proposition 20. *For elements in $\mathbb{N}$, the following cancellation properties hold with regard to order:*

1. $a + c < b + c \Rightarrow a < b$
2. $a \cdot c < b \cdot c \wedge c \neq 0 \Rightarrow a < b$
3. $a \cdot c = b \cdot c \wedge c \neq 0 \Rightarrow a = b$

Proof. Omitted. □

Proposition 21. *For elements in $\mathbb{N}$, the following order properties hold:*

1. $a < b \Rightarrow a \cdot c \leq b \cdot c$
2. *If a, b are non-zero, then $a, b < a + b$*

Proof. Omitted. □

Lemma 22. *The following order properties hold in $\mathbb{N}$:*

1. *The smallest element in $\mathbb{N}$ is 0*
2. *In particular, $0 < 1$.*
3. *If $a \neq 0$ and $b \neq 0$, then $0 < ab$*
4. *If $a < 1$ and $b < 1$ then $ab < 1$*

Proof. 1. Immediate from the property 3 of $\mathbb{N}$.

3. We have $0 < a, b$, so $0 = 0 \cdot b < ab$

4. It is immediate when either a, or b are zero. Therefore suppose the contrary. Take non-zero k, k' such that $a + k = 1$ and $b + k' = 1$. Then $ab + bk + ak' + kk' = 1 \cdot 1 = 1$; and bk, ak', kk' are all greater than 0. Hence their addition is greater than zero, hence non-zero, hence $ab < 1$.

The rest is omitted. □

Proposition 23. *1 is the immediate successor of 0.*

Proof. Suppose $]0,1[$ is non-empty. It therefore has a smallest element. Suppose m is the smallest element. Then since $m < 1$, and $m \neq 0$, we have by property 4 of the natural numbers, that $m \cdot m < m < 1$. Further, from the above lemma, we have $0 < m \cdot m$, so $m \cdot m$ is in $]0,1[$, and is smaller than m, a contradiction. □

Remark. Note that at a glance it may seem that the set $\{0, 0.5, 1, 1.5, 2, ...\}$ might satisfy the axioms of the natural numbers, but the proof of the above proposition clearly shows the import of the interaction between well orderedness and the closure of multiplication.

Corollary 24. *For any element $n \in \mathbb{N}$, the immediate successor of n is $n + 1$.*

Proof. We have $n < n + 1$. Suppose $]n, n + 1[$ is non-empty. Take m such that $n < m < n + 1$. Take k such that $m = n + k$, hence we have $n < n + k < n + 1$. By cancellation, $0 < k < 1$; a contradiction. □

For a set T, and natural number n, we will write T^n to denote the set $\{f \mid f : [1, n] \to T\}$. An element in T^n can be represented $(a_1, \ldots, a_n)$, and we can reason with these objects in such a format. However, it is noted that this is technically very informal, but since writing fully formal proofs dealing with such objects becomes often unwieldy and obscure, we take it for granted that our informal proofs may be rewritten formally. In the first few proofs we reason using only set theoretic means, but eventually when it becomes reasonably convincing, we will simply use the notation $(a_1, \ldots, a_n)$.

2.3.2 The Integers

We will call the set $(\mathbb{Z}, +, \cdot, <)$, "the set of integers," iff $(\mathbb{Z}, +, \cdot, <)$ is an ordered ring that is commutative and with identity, such that:

1. The set $\mathbb{W} := \{x \in \mathbb{Z} \mid 0 \leq x\}$ is well ordered

In condition 3, we will call the set $\mathbb{W} := \{x \in \mathbb{Z} \mid 0 \leq x\}$ the "whole numbers," or the "wholes."

Further in condition 3, note that this means, by proposition 9, that every nonempty subset D of $\mathbb{W}$ has in it μ such that $\mu \leq D$, where $\leq$ is the order on $\mathbb{Z}$.

Further, we will always refer to a commutative ring with identity, with a strict total order satisfying the above three conditions as the "the set of integers," and denote the algebraic structure as $\mathbb{Z}$.

Theorem 25. *The integers exists.*

Proof. Take the natural numbers $\mathbb{N}$. Denote the set $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$ as the construction of the Grothendieck completion as in the proof of theorem 17. Thus $\mathbb{Z}$ is an Abelian group.

We define multiplication by $[(x, y)] \cdot [(x', y')] = [(xx' + yy', yx' + xy')]$. Multiplication is indeed well defined: if $(x, y) \sim (a, b)$ and $(x', y') \sim (a', b')$, then

$x'(x+b)+y'(y+a)+a(x'+b')+b(y'+a') = x'(y+a)+y'(x+b)+a(y'+a')+b(x'+b')$. Hence expanding and cancelling we get $xx'+yy'+ab'+ba' = aa'+bb'+yx'+xy'$. So we have a commutative monoid with additive identity $[(0,0)]$, multiplicative identity $[(1,0)]$, distinct from $[(0,0)]$, where 1 is the multiplicative identity and 0 is the additive identity in $\mathbb{N}$.

We define the order relation $<$ by $[(x,y)] < [(x',y')]$ iff $x+y' < y+x'$. It is verified that the relation $<$ is without ambiguity because of cancellability in $\mathbb{N}$. It is easily shown that it is a strict total order. We note that since for any $x \in \mathbb{Z}$ such that $[0,0] \leq x$, there exists $n \in \mathbb{N}$ such that $[(n,0)] = z$, it is immediately verified that the order relation satisfies the desired the order properties of 1. and 2.

Finally, for property 3 of the strict total order, it is clear that the map $f : \mathbb{N} \to \mathbb{W}$ by $f(n) = [(n,0)]$ is bijective, preserves addition, multiplication, and order. For nonempty $A \subset \mathbb{W}$ denote $B := f^{-1}[A]$. Then taking smallest element μ in B, we have that $f(\mu)$ is the smallest element in A in the restricted order on $\mathbb{W}$. So all the desired properties are satisfied. □

Remark. We note that on $\mathbb{N}\times\mathbb{N}$: $\exists k \in \mathbb{N} : x+y'+k = y+x'+k$ iff $x+y' = y+x'$, because addition is cancellable.

We note that our construction of the integers is entirely within the axioms of ZFC. Since the natural numbers is constructed from ZFC, the above theorem is a theorem in ZFC.

The integers is clearly an integral domain, due to its ordering properties.

2.3.3 Properties of the Integers and Natural Numbers

Although the most "natural" system of numbers, whatever that phrase may mean, is $\mathbb{N}$, or the variation of $\mathbb{N}$ which does not include zero, the algebraic characterization of $\mathbb{N}$ is rather unwieldy, and it is easier to reason with the integers, and consider the natural numbers a subset of the integers.

Proposition 26. *The restriction of the operations of $\mathbb{Z}$ on addition and multiplication on the wholes, $\mathbb{W}$, is closed. Denoting $+_{\mathbb{W}}$ and $\cdot_{\mathbb{W}}$ as the respective restrictions, and denoting the $<_{\mathbb{W}}$ as the restriction of order on $\mathbb{W}$, the algebraic structure $(\mathbb{W}, +_{\mathbb{W}}, \cdot_{\mathbb{W}}, <_{\mathbb{W}})$ is the natural numbers. That is, they satisfy the conditions for them to be called the natural numbers.*

Proof. The first statement is by definition of $\mathbb{W}$.

The second statement is routine verification. For indeed, $(\mathbb{W}, +_{\mathbb{W}}, \cdot_{\mathbb{W}})$ is a semi-ring. $<_{\mathbb{W}}$ is a strict total order on $\mathbb{W}$. We verify the conditions:

1. Addition is cancellable: from the fact that addition is cancellable in $\mathbb{Z}$.
2. $1 \neq 0$, from the fact that both elements are in $\mathbb{Z}$.
3. If $\forall a, b \in \mathbb{N} : a < b$, then $b - a \in \mathbb{W}$ and $b - a \neq 0$. So we have $\exists k \in \mathbb{W} : k \neq 0 \wedge a + k = b$. Suppose $\exists k \in \mathbb{W} : k \neq 0 \wedge a + k = b$. Then $0 < k$, so $a < a + k = b$.

4. $a < b \wedge c \neq 0 \Rightarrow a \cdot c < b \cdot c$, by the fact that if $c \neq 0$, then $0 < c$.

5. $\mathbb{W}$ is well ordered by the partial order induced by the strict total order: by definition of $\mathbb{Z}$.

□

Remark. We remark the following.

1. The reader may note that we have not given a bijection from our construction of the wholes to the natural numbers, but simply noted that a subset of the integers is the wholes, although in the proof of the construction of the integers, we did give an explicit bijection.

2. Although in the proof we state routine verification, the author feels like that there should be some meta-algebraic/meta-mathematical theorem or theorem in category theory that immediately obtains the result.

Proposition 27. *The following ordering properties hold in $\mathbb{Z}$:*

1. *$\mathbb{Z}$ is not bounded above*

2. *$\mathbb{Z}$ is not bounded below.*

Proof. 1. Because $\mathbb{W}$ is not bounded above.
2. Because $-1 < 0$. □

2.4 Induction and Recursion on the Integers

2.4.1 Principles of Induction on the Integers

Proposition 28. *In the context of the order on the integers, the immediate succesor of* 0 *is* 1.

Proof. If not, then $\{x \in \mathbb{Z} \mid 0 < x < 1\}$ is non-empty. This set is equal to $\{x \in \mathbb{W} \mid 0 <_{\mathbb{W}} x <_{\mathbb{W}} 1\}$, and therefore 1 is not the immediate successor of 0 in $\mathbb{W}$, which is the natural numbers. □

Corollary 29. *For any $x \in \mathbb{Z}$, its immediate successor exists and is equal to $x + 1$.*

Proof. Indeed, $x + 1$ is in $\mathbb{Z}$ and $x < x + 1$. Suppose $]x, x + 1[$ is non-empty. Then taking an element in the set as z, we have $x < z < x + 1$, and hence $0 < z - x < 1$. □

Corollary 30. *For any $x \in \mathbb{Z}$, its immediate predecessor exists and is equal to $x - 1$.*

Proof. From the previous corollary. □

Proposition 31. *The following properties hold for elements x, y in $\mathbb{Z}$, and subset D of $\mathbb{Z}$:*

1. $x < y \Rightarrow x + 1 \leq y$

2. $x < y \Rightarrow x \leq y - 1$

3. $x < D \Rightarrow x + 1 \leq D$

4. $x < D \Rightarrow x \leq D - 1$

Proof. 1. Suppose $y < x + 1$. Then $x < y < x + 1$; a contradiction.
The rest are omitted, as they follow the same idea. □

Theorem 32. *For any element $x \in \mathbb{Z}$, the set $[x, \infty[$ is well ordered.*

Proof. Suppose D is a subset of $[x, \infty[$. By proposition 9, it therefore suffices to show existence of $d \in D$ such that $d \leq D$, where $\leq$ is the order on $\mathbb{Z}$. If $0 \leq D$, then $D \subset \mathbb{W}$, so the result is immediate. Suppose D has an element below zero. Then obviously $x \leq D$ so $0 \leq D - x$. Thus $D - x$ has a least element; denote it as μ. That is, $\mu \in D - x$ and $\mu \leq D - x$. Hence $\mu - x \in D$, and $\mu - x \leq D$. □

Corollary 33. *If D is a non-empty subset of $\mathbb{Z}$, and is bounded below, it has a least element.*

Proof. Suppose D is bounded below. By definition this means that there exists $x \in \mathbb{Z}$ such that $x < D$. Then $D \subset [x, \infty[$ hence has a least element. □

We will call the set $\mathbb{Z}_+ :=]0, \infty[= \{z \in \mathbb{Z} \mid 0 < z\} = \mathbb{W} \setminus \{0\} = [1, \infty[$ the "positive integers." It is well ordered.

Corollary 34. *The following properties hold:*

1. $\mathbb{N} \setminus \{0\}$ has a bijection to $\mathbb{Z}_+$ that which preserves addition, multiplication, and order

2. *$\mathbb{Z}_+$ is not bounded above*

Proof. Omitted. □

Theorem 35. *(Principles of Induction) For element $x \in \mathbb{Z}$ and U such that $U \subset [x, \infty[$:*

1. *If $x \in U$ and the sentence $\forall t \in U : t + 1 \in U$ holds true, then $U = [x, \infty[$.*

2. *If $x \in U$, and the sentence $\forall k \in [x, \infty[: (\forall n \in \mathbb{Z}(x \leq n \leq k \Rightarrow n \in U)) \Rightarrow k + 1 \in U$ holds true, then $U = [x, \infty[$.*

Proof. 1. Suppose the antecedent and $U \neq [x, \infty[$. Then $[x, \infty[\setminus U \neq \varnothing$ so has a least element, μ; which satisifies $x < \mu$. Then $x \leq \mu - 1$, so if $\mu - 1$ is not in U, then it is in $[x, \infty[\setminus U$, a contradiction. So $\mu - 1 \in U$, so $\mu \in U$, a contradiction.

2. Denote $A := [x, \infty[$. Since A is well ordered, it obeys the principle of strong induction. That is, for all subsets U of A, the statement $\forall k \in A : ((]-\infty, k[_A \subset U) \Rightarrow k \in U)$ implies that $U = A$.

We see that $]-\infty, k[_A = [x, k[_{\mathbb{Z}}$. Suppose the sentence $\forall k \in [x, \infty[: (\forall n \in \mathbb{Z}(x \leq n \leq k \Rightarrow n \in U)) \Rightarrow k+1 \in U$ holds true. Then suppose $k \in A$, (that is, $x \leq k$), and further suppose $[x, k[_{\mathbb{Z}} \subset U$.

If $[x, k[_{\mathbb{Z}} = \varnothing$, then $k = x$, so $k \in U$. If $[x, k[_{\mathbb{Z}} \neq \varnothing$ then $k-1$ is the immediate predecessor of k and hence $[x, k[_{\mathbb{Z}} = [x, k-1]$. Hence $k-1+1 = k \in U$. Therefore by the principle of strong induction, $U = A$. □

In the treatement of basic analysis (and virtually any other area of mathematics) it is very often that one encounters induction and strong induction on the integers. When context is clear (that is, we know that we are discussing the integers), the first statement of theorem 35 is called "the principle of induction" or simply "induction." The second statement of theorem 35 is called "the principle of strong induction" or simply "strong induction."

In both statements 1 and 2 in theorem 35, with the same notation, the statement $x \in U$ is called the "base case." The statements $\forall t \in U : t+1 \in U$ and $\forall k \in [x, \infty[: (\forall n \in \mathbb{Z}(x \leq n \leq k \Rightarrow n \in U)) \Rightarrow k+1 \in U$ are both called the "inductive case," when context is clear.

Remark. We remark the following.

1. Note that in number 2 of the above theorem, we require that $x \in U$, otherwise U may be empty, even though the sentence $\forall k \in [x, \infty[: (\forall n \in \mathbb{Z}(x \leq n \leq k \Rightarrow n \in U)) \Rightarrow k+1 \in U$ is true (vacuously).

2. Note our statements allow induction starting from any integer, which is of great convenience, and is essentially implicitely assumed by almost all expositions of principles of induction after showing the particular case of induction on $\mathbb{Z}_+$ or $\mathbb{N}$. Of course the general case can be derived from the specific, but here we take the route of immediately deducing the general.

3. In some expositions, one states the principle of induction as follows: If $P(x)$ is a sentence, where x is an unbound variable wherein an integer can be substituted, then if given some integer z, $P(z)$ is true and for all integers t such that $z \leq t$, the sentence $P(t)$ implies $P(t+1)$, the sentence $P(x)$ is true for all integers x greater or equal to z. However, this is a meta-mathematical statement, for "sentences" are not treated set theoretically, hence we do not discuss this here. However, it is indeed more convenient to look at the theorem meta-mathematically.

The first statement in the above theorem is known as the "principle of induction," and the second is known as the "principle of strong induction."

2.4.2 Principles of Recursive Definition on the Integers

Theorem 36. *For $n, m \in \mathbb{Z}$ such that $n \leq m$, set T, and $\alpha \in T$, and function $R : T \to T$, there exists a function $f : [n, m] \to T$ such that:*

1. $f(n) = \alpha$

2. *For all* $k \in [n, m[$, we have $f(k+1) = R(f(k))$

Further, such a function is unique.

Proof. We first show existence. We use the first statement of theorem 35. Suppose $n, m \in \mathbb{Z}$ such that $n \leq m$, set T and $\alpha \in T$, and further suppose $R : T \to T$ is a function.

Denote $A := [n, \infty[$. Then denote $U := \{t \in A \mid \exists f : [n, t] \to T, \text{ such that } f(n) = \alpha \wedge \forall k \in [n, t[: f(k+1) = R(f(k))\}$.

We would like to show that $U = A$. Now $n \in U$; for simply take $f := \{(n, \alpha)\}$. Note that $\forall k \in [n, t[: f(k+1) = R(f(k))$ is vacuously true in this case. Now, suppose t is in U. Take $f : [n, t] \to T$, such that $f(n) = \alpha \wedge \forall k \in [n, t[: f(k+1) = R(f(k))$. Then put $g := f \cup \{(t+1, R(f(t)))\}$, a union of pairwise disjoint sets; hence g is a function. Then indeed $g : [n, t+1] \to T$, satisfying the conditions required, so $t + 1 \in U$. So $U = A$. Since m is in A, and existence is shown.

For uniqueness, suppose functions f and g both satisfy the conditions 1 and 2 as given. Denote $A := [n, \infty[$, and $U := \{t \in A \mid f(t) = g(t) \vee m < t\}$. Then by induction, $U = A$. □

Remark. Note the vacuousness of $\forall k \in [n, t[: f(k+1) = R(f(k))$ is from the fact that this sentence says $\forall k \in \varnothing : f(k+1) = R(f(k))$. It comes to mind whether the logical sentence $f(k+1) = R(f(k))$ makes sense when we are discussing no elements. However, rephrasing the sentence in a more precise form, we get $\exists y \in T : (\exists s \in \mathbb{Z}((k, 1), s) \in + \wedge (s, y) \in f) \wedge (\exists z \in T : (k, z) \in f \wedge (z, y) \in R)$, with free variable k, assuming that 1 is named. This sentence is indeed "well-formed," and our doubts are cleared.

Theorem 37. *For $n \in \mathbb{Z}$, set T, $\alpha \in T$, function $R : T \to T$, such that $n \leq m$, , if $R : T \to T$, given $m \in \mathbb{Z}$, denote $f_m : [n, m] \to T$ as a function satisfying*

1. $f_m(n) = \alpha$
2. *For all* $k \in [n, m[$, we have $f_m(k+1) = R(f_m(k))$

then if $m \leq m'$, then $f_m \subset f_{m'}$.

Proof. We again use induction. We have that $f_n = \{(n, \alpha)\}$. Define $A := [n, \infty[$. Suppose $t \in [n, \infty[$. As in the proof of the previous theorem, put $g := f_t \cup \{(t+1, R(f_t(t)))\}$. Then by the uniqueness statement in the previous theorem, $g = f_{t+1}$ thus the statement $f_t \subset f_{t+1}$ holds true. Suppose $m \leq m'$. Define $B := [m, \infty[$, and $U := \{t \in B \mid f_m \subset f_t\}$. By induction $U = B$. □

Remark. We remark the following:

1. In a similar manner as we remarked previously, $U := \{t \in A \mid f(t) = g(t) \vee m \leq t\}$ in the proof of uniqueness, one might feel that it is rather bad to write $f(t) = g(t)$, within a sentence that defines a subset of elements which are not even in the domains of f nor g. However, writing the logical

sentence fully, this becomes: $(\exists y \in T : (t, y) \in f \wedge (t, y) \in g) \vee m \leq t$. This justifies our seemingly logically fallacious sentence. Indeed, we note that when we write $f(n) = \alpha$, we mean $(n, \alpha) \in f$.

2. To exhibit the import of set theory we have chosen to use induction set theoretically rather than meta-mathematically in our above proof. In future cases, since induction is very common, we may simply give an informal summary of the inductive process, which may be reframed in a formal way, especially when the proof becomes very long or complex.

3. The current theorem, although used in the following theorem, is useful in itself.

Theorem 38. *(Principle of Recursive Definition on the Integers) For set T and $\alpha \in T$ and $x \in \mathbb{Z}$, if $R : T \to T$, then there exists a function $f : [x, \infty[\to T$ such that:*

1. $f(x) = \alpha$
2. *For all $n \in [x, \infty[$,* we have $f(n + 1) = R(f(n))$

Further, such a function is unique.

Proof. Denote $A := [x, \infty[$. The set $U := \{t \in A \mid \exists f : [x, t] \to T,$ such that $f(x) = \alpha \wedge \forall k \in [x, t[: f(k + 1) = R(f(k))\}$ is equal to A, by theorem 37. For m such that $x \leq m$, denote $f_m : [x, m] \to T$ the function such that:

1. $f(x) = \alpha$
2. For all $k \in [x, m[$, we have $f(k + 1) = R(f(k))$

Denote Θ as the set of all such functions. Then put $\Gamma := \bigcup \Theta$. We show that Γ is a function. Clearly, we have that Γ consists only of ordered pairs (t, y) where t is an integer such that $n \leq t$ and $y \in T$. Then suppose $(t, y), (t, y') \in \Gamma$. Then take f_m and $f_{m'}$ in Θ such that $(t, y) \in f_m$, and $(t, y') \in f_{m'}$. Then WLOG, $m \leq m'$, so $(t, y) \in f_{m'}$, so $y = y'$; that is, Γ is a function. Then we have $\Gamma : [x, \infty[\to T$. Clearly, $(x, \alpha) \in \Gamma$, and for $n \in [x, \infty[$, we have that $f_{n+1}(n+1) = R(f_{n+1}(n))$, and since $f_{n+1} \subset \Gamma$, we have that $\Gamma(n + 1) = R(\Gamma(n))$. □

Theorem 39. *(General Principle of Recursive Definition on the Integers) For set T and $\alpha \in T$ and $x \in \mathbb{Z}$, if $R : \bigcup_{n \in \mathbb{Z}_+} T^n \to T$, then there exists a function $f : [1, \infty[\to T$ such that:*

1. $f(1) = \alpha$
2. *for k such that $1 \leq k$, we have $f(k+1) = R(f \mid_{[1,k]})$.* In informal notation, this means that $f(k + 1) = R(f(1), f(2), \ldots, f(k))$.

Further, such a function is unique.

Proof. We deduce this from the previous theorem. Suppose and $\alpha \in T$ and take $1 \in \mathbb{Z}$. if $R : \bigcup_{n\in\mathbb{Z}_+} T^n \to T$. Define function $* : \bigcup_{n\in\mathbb{Z}_+} T^n \times T \to \bigcup_{n\in\mathbb{Z}_+} T$ as follows: For a function f mapping from $[1, n']$ to T, for $a \in T$, define $*(f, a) = f \cup \{(n'+1, a)\}$, which is indeed a map from $[1, n'+1]$ to T. Then informally, this means that the function $*$ maps from $(a_1, \ldots, a_{n'})$ to $(a_1, \ldots, a_{n'+1})$. Define the function $\rho : \bigcup_{n\in\mathbb{Z}_+} T^n \to \bigcup_{n\in\mathbb{Z}_+} T^n$ by $\rho(t) = *(t, R(t))$. Indeed, informally, the function ρ maps from $(a_1, \ldots, a_{n'})$ to $(a_1, \ldots, a_{n'+1})$.

Then by the previous theorem, take function $\phi : [1, \infty[\to \bigcup_{n\in\mathbb{Z}_+} T^n$ such that: $\phi(1) = (1, \alpha)$, and for all $\gamma \in [1, \infty[$, we have $\phi(\gamma + 1) = \rho(\phi(\gamma))$. Clearly, by induction that for all k, we have $\phi(k) : [1, k] \to T$ and $\phi(k) \subset \phi(k + 1)$.

We finally define $f : [1, \infty[\to T$ by $f(k) = (\phi(k))(k)$, which clearly satisfies the property 1 in the theorem. For the second property, suppose $1 \leq k$. Then $f(k + 1) = (\phi(k + 1))(k + 1) = (\rho(\phi(k))(k + 1)$. Noting that $(\rho(\phi(k)) = *(\phi(k), R(\phi(k)))$, and $\phi(k) : [1, k] \to T$, so we have $*(\phi(k), R(\phi(k))) = \phi(k) \cup \{(k + 1, R(\phi(k)))\}$. Hence $(\rho(\phi(k))(k + 1) = R(\phi(k))$.

It hence suffices to show that $\phi(k) = f \mid_{[1,k]}$. We do this by induction. The base case is by definition. Suppose $\phi(k) = f \mid_{[1,k]}$. Then since $\phi(k) \subset \phi(k + 1)$, we have $\phi(k+1) = \phi(k) \cup \{(k+1, ((\phi(k+1))(k+1)))\}$. By definition of f, this is equal to $\phi(k) \cup (k + 1, f(k + 1)) = f \mid_{[1,k]} \cup (k + 1, f(k + 1)) = f \mid_{[1,k+1]}$.

To show uniqueness, this is also by induction. Suppose both f and f' satisfy the conditions. □

Remark. We remark the following.

1. It is of course possible to deduce the general principle of recursion on its own, but for expositional purposes, we use the specific recursion case to deduce the general case.

2. The above theorem does not need generalization to recursion starting from an arbitrary integer as we have done in the previous theorem, for in virtually all cases there is only need to recursively define a function starting from 1, and further, generalizing obscures rather than elucidates, and makes the proof unnecessarily convoluted, in this case.

2.5 Definition of Sums and Products

We rigorously define of the notion of what are called "sums" and "products."

Definition 40. Given category $\mathbb{A}$, and element $n \in \mathbb{Z}$, and a map $\gamma : [n, \infty[\to Mor(\mathbb{A})$, such that for all $m \in [n, \infty[$, we have that $\gamma(m)$ can be composed with $\gamma(m + 1)$ by $\gamma(m + 1) \circ \gamma(m)$. Define map $R : Mor(\mathbb{A}) \to Mor(\mathbb{A})$ as follows. When $f \in Im(\gamma)$, denote $\gamma(m) = f$, and put $R(f) = R(\gamma(m)) = \gamma(m+1) \circ \gamma(m)$. Otherwise put $R(f) = f$.

We will denote the function $\Gamma : [n, \infty[\to Mor(\mathbb{A})$ as the function such that $\Gamma(n) = \gamma(n)$, and for all $m \in [n, \infty[$, we have $\Gamma(m + 1) = R(\gamma(n))$. Define the function $\sum_{k=n}^{k=()} \gamma(k) : [n-1, \infty[\to Mor(\mathbb{A})$, which we call the "sum" or "product" as follows. Define $\sum_{k=n}^{k=m} \gamma(k) := \Gamma(m)$ for all $k \in [n, \infty[$, and denoting id as the

identity composible with $\gamma(n)$ from the left. Define $\sum_{k=n-1}^{k=m} \gamma(k) := id$. The function evaluated at m is called the "sum of γ from n to m."

Proposition 41. *Given category $\mathbb{A}$, and element $n \in \mathbb{Z}$, and a map $\gamma : [n, \infty[\to Mor(\mathbb{A})$, such that for all $m \in [n, \infty[$, we have that $\gamma(m)$ can be composed with $\gamma(m+1)$ by $\gamma(m+1) \circ \gamma(m)$. Then the following properties hold:*

1. *For all $p, q, r \in [n, \infty[$ such that $p \leq q \leq r$, the equality*

Remark. There are two generalizations of monoids that come to mind, one of them is the category, and other is the semigroup. We introduce the summation in terms of categories, for semigroups appear rarely, while categories appear very often.

2.6 Ordered Fields and Their Existences

An ordered field $\mathbb{F}$, refers to a field, with a strict total order such that:

1. $\forall a, b, c \in \mathbb{F} : a < b \Rightarrow a + c < b + c$
2. $\forall a, b, c \in \mathbb{F} : 0 < a \wedge 0 < b \Rightarrow 0 < a \cdot b$

Proposition 42. *Notice that an ordered field is an ordered, commutative ring with identity, and therefore satisfies identical properties.*

Proof. Immediate from definition. □

Theorem 43. *An ordered field exists.*

Proof. Take the integers $\mathbb{Z}$. Define the equivalence $(x, y) \sim (x', y')$ iff $xy' = yx'$ on $\mathbb{Z}$. Consider the set $\mathbb{A} := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 < y\}$ with componentwise multiplication with the restriction of the equivalence. Denote $\mathbb{Q} := \mathbb{A}/\sim$.

We define addition on the set $\mathbb{Q}$ by $[(x, y)] \cdot [(x', y')] = [(x \cdot y' + y \cdot x', y \cdot y')]$. Then addition is well defined, for if $[(x, y)] = [(a, b)]$ and $[(x', y')] = [(a', b')]$, then since $ay = bx$ and $a'y' = b'x'$, we have $ab'yy' + ba'yy' = bb'xy' + bb'yx'$, that is, $[(x, y)] \cdot [(a, b)] = [(x, y)] \cdot [(a, b)]$. Therefore $\mathbb{Q}$ is an abelian group with respect to addition, with additive identity $[(0, 1)]$.

Now consider $\mathbb{Q}^\times := \mathbb{Q} \setminus [(0, 1)]$. It is clearly a commutative monoid with the identity $[(1, 1)]$. Suppose $[(x, y)]$ is in $\mathbb{Q}^\times$. Then $x \neq 0$ and $y \neq 0$, so $[(y, x)]$ is in $\mathbb{Q}^\times$ and we get $[(x, y)] \cdot [(y, x)] = [(1, 1)]$, so $\mathbb{Q}^\times$ is an Abelian group under multiplication.

We note that the multiplication distributes over addition, and we get that $\mathbb{Q}$ is a field.

Define $(x, y) < (x', y')$ iff $xy' < yx'$. It is immediately verified that the first two conditions for a strict total order are satisfied. For the third condition, first note that $[(x, y)] < [(0, 1)]$, iff $x < 0$; $[(0, 1)] < [(x, y)]$, iff $0 < x$, and $[(x, y)] = [(0, 1)]$ iff $x = 0$.

Suppose $[(x, y)] < [(x', y')] < [(x'', y'')]$. Suppose $0 \leq x$, then $0 \leq xy' < yx'$ hence $0 < x'$ hence $0 < x'y'' < y'x''$ hence we have $xy'x'y'' < yx'y'x''$ so

$xy'' < yx''$. Now suppose $x < 0$, and further, $0 \leq x'$. Then $0 < x''$, so $xy'' < 0 < yx''$. Therefore given $x < 0$, instead suppose $x' < 0$. Further suppose that $0 \leq x''$. Then immediately, $xy'' < 0 \leq yx''$. Therefore given $x < 0$, and $x' < 0$ instead suppose that $x'' < 0$. Then since $xy' < yx' < 0$ and $x'y'' < y'x'' < 0$, we have $0 < yx'y'x'' < xy'x'y''$. Since $x'y' < 0$, we have $xy'' < yx'' < 0$.

It finally suffices to verify that this total order is compatible with addition and multiplication in the field. Suppose $[(x, y)] < [(x'y')]$. Then $xy' < yx'$. Then for $[(a, b)] \in \mathbb{Q}$, we have $0 < b$ so $xy'bb + yy'ab < yx'bb + yy'ab$, hence $(xb + ya)(y'b) < (yb)(bx' + y'a)$, that is, $(xb + ya, yb) < (bx' + ya', y'b)$, so $[(x, y)] \cdot [(a, b)] < [(x'y')] \cdot [(a, b)]$. Now suppose $[(0, 1)] < [(a, b)]$. Then $0 < a$, so $xy'ab < yx'ab$, so $[(x, y)] \cdot [(a, b)] < [(x', y')] \cdot [(a, b)]$. □

Remark. We remark the following three points.

1. Although in we proceed similarly to the construction of the Grothendieck group when considering multiplication, there are theoretical considerations which necessitate an slightly altered treatment. In a purely theoretical perspective, we desired to make the additive operation invertible in 1.1.2, but in 1.1.3, we desired to make the multiplicative operation invertible, which is essentially what we want in a ring. However, we cannot simply first consider the construction in 1.1.1 with respect to multiplication using the equivalence, for doing so results in exactly one equivalence class in $\mathbb{Z} \times \mathbb{Z}/\sim$, which is, of course, $\mathbb{Z} \times \mathbb{Z}$ itself, because if we define $(x, y) \sim (x', y')$ iff $\exists k \in \mathbb{Z} : xy'k = yx'k$ the equivalence always holds when $k = 0$. This even makes $0 = 1$, which does not allow it to be a field. We cannot remedy this by restricting $\sim$ on the set $\mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\}$ because zero cannot exist. A simple solution is to restrict it on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. However for defining the order relation it is most convenient to consider the more restrictive set $\mathbb{A}$ as in the proof.

2. The idea behind well definedness of multiplication is to manipulate using familiar methods and reduce the problem in the original set of integers. Put $a/b = x/y$, and $a'/b' = x'/y'$, and then obtain $(ab' + ba', bb) = (xy' + yx', yy)$. Then it now is clear that we only need to show $ab'yy' + ba'yy' = bb'xy' + bb'yx'$.

3. The ordered field that we have exhibited in the above proof is not well ordered. Indeed, consider $\{x \in \mathbb{Q} \mid 0 < x\}$.

Proposition 44. *The following order properties hold for elements in an ordered field, which we denote as $\mathbb{Q}$:*

1. *There does not exist y such that $0 \cdot y = 1$*
2. $0 < c \Rightarrow 0 < c^{-1}$
3. $c < 0 \Rightarrow c^{-1} < 0$

4. $0 \cdot c = c \cdot 0 = 0$

5. $\mathbb{Q}$ *is not bounded above*

6. $\mathbb{Q}$ *is not bounded below*

7. $\forall x, y \in \mathbb{Q}(x < y \Rightarrow \exists t \in \mathbb{Q}(x < t < y))$

Proof. Omitted. □

Lemma 45. *For a subset A of an ordered field $\mathbb{Q}$, we say that A is "inductive" iff $0 \in A$ and $\forall x \in A : x + 1 \in A$. Denote Θ as the set of all inductive subsets of $\mathbb{Q}$. Denote $N := \bigcap \Theta$. Then:*

1. *N is inductive*

2. *If $U \subset N$, and U is inductive, then $U = N$.*

Proof. Omitted. □

Lemma 46. *We observe the following:*

1. *Taking N as in the previous lemma, the immediate successor of k is $k+1$.*

2. *If $0 < k$, then $k - 1 \in N$.*

Proof. 1. Denote $U := \{k \in N \mid]k, k+1[_N = \varnothing\}$. It is quickly verified that U is inductive.

2. Denote $U := \{k \in N \mid 0 < k \Rightarrow k - 1 \in N\}$. We have $0 \in U$. Suppose $k \in U$, and further, $0 < k+1$. Then obviously $(k+1)-1 \in N$, so the implication holds true; hence $k + 1 \in U$. □

Note that that the second statement means that the immediate predecessor of a positive element k in N exists and is $k - 1$.

Remark. In the previous lemma, 2 is particularly deceptive, for it may seem to immediately follow from 1, but this is not the case.

Proposition 47. *There exists a subset $\mathbb{Z}$ of an ordered field which, with the restriction of addition, multiplication, and order on the set $\mathbb{Z}$, satisfies the axioms of the integers.*

Proof. Take the set N as in the previous lemma.

Denote $-N := -1 \cdot N = \{-1 \cdot n \mid n \in N\}$. Now we show that the desired subset is $N \cup -N$, and denote this set as Z. We have that $0 \leq N$.

We first need to show closure of addition. Suppose $x \in N$. Denote the set $U := \{t \in N \mid t + x \in N\}$. Clearly U is inductive, so addition is closed under N. From this it is immediately obtained that $-N$ is closed under addition as well.

Now suppose $x \in N$. Define the set $U := \{t \in N \mid t \leq x \Rightarrow x - t \in N\}$. Obviously $0 \in U$. Suppose $t \in U$. Further suppose $t < x$. Then by the previous

lemma, we have $t+1 \leq x$, and $1 \leq x-t$. Hence by the previous lemma, $x-t-1$ is in N. So $U = N$.

Now suppose $x, y \in N$. By the previous paragraph, if $y \leq x$, then $x - y \in N \subset Z$. If $x \leq y$, then $x - y = -(y - x) \in -N \subset Z$.

Therefore addition is closed. We immediate obtain that Z is an additive abelian group under the addition restricted on Z.

For closure of multiplication, we do the same thing; suppose $x \in N$. Then the set $U := \{t \in N \mid t \cdot x \in N\}$ contains 0 and if $t \in U$, then $(t+1)x = tx + x \in N$ by closure of addition.

From this, immediately, multiplication is closed under Z. We immediately obtain that Z is a monoid under the multiplication restricted on Z. Therefore Z is a commutative ring with identity. Indeed we also see that the order on Z makes it an ordered ring. Now we will show well order using the inductive property of N. Indeed, N is the set of all non-negative elements of Z.

Lemma 48. *If $U \subset N$ and $0 \in U$, and the sentence $\forall t \in U : ((\forall k \in N : k \leq t) \Rightarrow t + 1 \in U)$ holds true, then $U = N$.*

Proof. Because U is inductive. □

Denote $U := \{t \in N \mid$ for all subsets D of N we have $t \in D \Rightarrow (\exists m \in D : m \leq D)\}$. Then clearly $0 \in U$. Then suppose $t \in U$. Suppose $\forall k \in N : k \leq t$. Suppose D is a subset of N, and further suppose that $t + 1 \in D$. Then if D contains an element smaller than $t + 1$, that element must be smaller than or equal to t, so D has a minimal element. If not, then $t+1$ is the minimal element in D. □

The real numbers, denoted $\mathbb{R}$, refers to an ordered field such that the non-strict total order induced by the strict total order has the least upper bound property.

Remark. We remark the following.

1. We give two proofs of the next theorem, which is the existence of the real numbers. We give two proofs, one via Dedekind cuts, and one via equivalence classes of Cauchy sequences, both of which are most historically relevant, of theoretical interest, and most well known of various proofs that have been discovered. They rest on the same underlying idea once we consider limit points. This will be observed in chapter 2. We first give definitions for use in the proofs.

2. The construction of $\mathbb{R}$ from $\mathbb{Q}$ is often called a "completion." Using terminology not yet defined, a "completion of a metric space," is the construction of a new metric space to which there exists an injective map, call if f, from the old metric space that obtains an isomorphism (preserving algebraic and order properties, whatever apply), and in which all Cauchy sequences converge. However to define "Cauchy sequence," and "metric space," in the usual sense of the terms, we would need to define metrics,

and also show the existence of the real numbers, which we have not done yet.

In the context of an ordered field, which we will denote as $\mathbb{Q}$, a subset D of $\mathbb{Q}$ is called a "cut," iff:

1. $D \neq \varnothing$
2. $D \neq \mathbb{Q}$
3. $\forall x, y \in D : y \in D \wedge x < y \Rightarrow x \in D$
4. D has no greatest element.

Lemma 49. *We note the following:*

1. *A cut D is bounded above, and not bounded below*
2. *For $d \in \mathbb{Q}$, we have $d \in D \vee D \leq d$.*

Proof. Omitted. □

Theorem 50. *An ordered field with the least upper bound property exists.*

Proof. First proof (from Dedekind).

Denote the set $\mathbb{R}$ as the set of all cuts in an ordered field, which we will denote as $\mathbb{Q}$. We will define addition and multiplication on $\mathbb{R}$ such that the desired properties are satisfied.

Let 0 and 1 denote the additive and multiplicative identities in $\mathbb{Q}$, respectively. Denote the set $\overline{0} := \{x \in \mathbb{Q} \mid x < 0\}$.

Before defining our operations we must first note the following. There is, here, an unfortunate clash in notation. When discussing a group G, and subsets A, B, of G, and $\cdot$ is the composition on G, we defined $A \cdot B = AB := \{x \cdot y \mid x \in A, y \in B\}$. Now if we have subsets A, B which do not contain 0, then it is a subset of the group $\mathbb{Q}$, but this is will not be our definition of multiplication of two elements on the reals. To resolve this, we will henceforth, we will denote $A(+)B$ and $A(\times)B$ to denote the addition and product, respectively, on the ring $\mathbb{Q}$, and also use the same notation for the addition and multiplication on the subsets of $\mathbb{Q}$, and will denote negation and inverse of element $q \in \mathbb{Q}$ as $(-)q$ and $q^{(-1)}$ respectively. We will define addition on $\mathbb{R}$ using the symbol $+$ and multiplication using the symbol $\cdot$.

We define the addition on $\mathbb{R}$, in the form of addition of subsets of groups; that is, $D + C := D(+)C = \{x(+)y \mid x \in D, y \in C\}$. Then $D + C$ is a cut. We clearly have commutativity and associativity of our composition, so we have a commutative semigroup. $\overline{0}$ is the additive identity, so we have a commutative monoid.

For the inverse element, given cut D, denote the set of upper bounds of D, for convenience, as $\overline{D} := B_{upp}(D) = \{x \in \mathbb{Q} \mid D \leq x\}$. It is clearly non-empty. For the inverse of addition on $\mathbb{R}$, define $-D := \{a(-)b \mid a \in \overline{0} \wedge b \in \overline{D}\} = \{a(-)b \mid a < 0 \wedge D \leq b\}$. Then $-D$ is clearly non-empty, and is bounded above,

and therefore satisifies conditions 1 and 2 for the definition of a cut. For the third condition, suppose $a(-)b \in -D$, where $a \in \overline{0} \wedge b \in \overline{D}$. If $t < a(-)b$, then $t(+)b \in \overline{0}$, and $t = t(+)b(-)b \in -D$. Finally, it clearly has no greatest element; therefore it is a cut. We now show that $-D$ is indeed the additive inverse of D.

Clearly, we have that $D+(-D) \subset \overline{0}$. Now suppose $\beta \in \overline{0}$. Denote $\alpha = -\beta/2$. The set of upper bounds, $\overline{D}$ is non-empty, and clearly, $D \cup \overline{D} = \mathbb{Q}$; this is a disjoint union. Now obviously $\bigcup_{q\in\mathbb{Q}}[q, q+\alpha] = \mathbb{Q}$, hence $\bigcup_{q\in\mathbb{Q}}([q, q+\alpha] \cap D) = D$.

Suppose that if $q \in \mathbb{Q}$ such that $[q, q+\alpha] \cap D \neq \varnothing$, then $[q, q+\alpha] \cap D = [q, q+\alpha]$. Take an element $q \in D$. Clearly $[q, q+\alpha] \cap D \neq \varnothing$. We will define a function recursively on the integer subset of our ordered field. Recursively define $f(1) = q$, and $f(n+1) = f(n) + \alpha$, and define $I_n := [f(n), f(n+1)]$. By induction, clearly, we have that for all n greater than or equal to 1 in our integer subset of the ordered field, $f(n) = q + (n-1)\alpha$, for any element in for elements in n. Furthermore, by induction, we have $I_n \subset D$. Hence $Im(f)$ is equal to $q + \alpha\mathbb{W}$, which is not bounded above. Hence $\bigcup_n I_n$ is not bounded above. But $\bigcup_n I_n \subset D$, a contradiction.

Remark. Note that we needed to define the function recursively on the integer subset of our ordered field, and not an arbitrary integer system, otherwise the statement $f(n) = q + (n-1)\alpha$ does not make sense.

Hence take $q \in \mathbb{Q}$ such that $[q, q+\alpha] \cap D \neq \varnothing$, and $[q, q+\alpha] \cap D \neq [q, q+\alpha]$. Clearly, $q \in D$. Take element η such that $q \leq \eta \leq q + \alpha$ that is not in D. So $0 \leq \eta - q \leq \alpha$, so $0 < \alpha + \eta - q \leq 2\alpha = -\beta$. On the other hand, since D is a cut, we have $D < \eta$, so $\eta \in \overline{D}$. We have $-\alpha < 0$, so $-\alpha - \eta \in -D$. Hence $q + (-\alpha - \eta) \in D + (-D)$. From this, we have $\beta \leq q + (-\alpha - \eta)$, from which it follows that $\beta \in D + (-D)$.

For cut D, we will denote its additive inverse as $-D$.

For the following discussion, it is useful to note that if $0 \in D$ then $0 \notin -D$, and $-D < 0$; and conversely, if $0 \notin D$ then $0 \in -D$, and $0 < D$.

We define multiplication on $\overline{\mathbb{R}}$ as follows. Suppose D and C are cuts. We examine four cases.

1. Suppose $0 \notin D, C$. Then $D, C < 0$. Define $D \cdot C := \{(-)x(\times)y \mid x \in D, y \in C\} = (-)1(\times)D(\times)C$. Clearly, conditions 1 and 2 of a cut are satisfied. Suppose $(-)x(\times)y \in D \cdot C$, where $x \in D, y \in C$. Then suppose that $t < (-)x(\times)y$. Then $(-)t(\times)y^{(-1)} < x$, so $(-)t(\times)y^{(-1)} \in D$. So $t = (-)((-)t(\times)y^{(-1)})(\times)y \in C$. Clearly $D \cdot C$ has no greatest element. So $D \cdot C$ is a cut.

2. Now supposing $0 \notin D$, instead suppose $0 \in C$. Then $0 \notin -C$. So we can now define $D \cdot C := -(D \cdot -C)$ using 1, so we obtain a cut.

3. When $0 \in D$, and $0 \notin C$, this is the same as in 2.

4. When $0 \in D, C$, then we define $D \cdot C := (-D) \cdot (-C)$.

Now we need to show that $\mathbb{R} \setminus \{\overline{0}\}$ is an abelian group under multiplication. When verifiying the group properties, we reduce all cases to the definition of multiplication for sets bounded above by 0. We first note the following lemmata before proceeding further.

Lemma 51. *We note the following.*

1. If $0 \notin D, C$, then $0 \notin D \cdot C$
2. If $0 \in D$, then $0 \notin -D$
3. If $0 \notin D$, then $0 \in -D$
4. If $0 \notin D, 0 \in C$, then $0 \in D \cdot C$
5. If $0 \in D, 0 \notin C$, then $0 \in D \cdot C$

Proof. Omitted. □

Lemma 52. *For all cuts $D, C \in \mathbb{R}$, we have:*
$(-D) \cdot C = D \cdot (-C) = -(D \cdot C)$.

Proof. 1. If $0 \notin D, C$, then $(-D) \cdot C = -((- - D) \cdot C)) = -(D \cdot C) = -(D \cdot - - C) = D \cdot -C$.

2. If $0 \notin D, 0 \in C$, then $(-D) \cdot C = (- - D) \cdot (-C) = D \cdot -C$. Now $(D \cdot C) = -(D \cdot -C)$. Performing addition, we get $(D \cdot C) + (D \cdot -C) = -(D \cdot -C) + (D \cdot -C) = \overline{0}$ by definition.

3. If $0 \in D, 0 \notin C$; the proof is the same as in 2.

4. If $0 \in D, C$, then $(-D) \cdot C = -(-D \cdot -C) = -(D \cdot C) = D \cdot -C$ □

Now we show associativity. Suppose $A, B, C, \in \mathbb{R}$.

Suppose $0 \notin A$.

If $0 \notin B, C$, then we have $(AB)C = \{xyz \mid x \in A, y \in B, z \in C\} = A(BC)$. If $0 \notin B, 0 \in C$, then by the previous line of proof, $(AB)C = -((AB) \cdot -C) = -(A(B \cdot -C)) = A(-(B \cdot -C)) = A(BC)$. If $0 \in B, 0 \notin C$, then since $0 \in AB$, we have $(AB)C = -(-(AB))(C)) = (-(AB))(-C) = (A \cdot -B)(-C)$; noting that $0 \notin -B$, and $0 \in -C$, by the previous line, we have $(A \cdot -B)(-C) = A((-B) \cdot -C) = A(-(-B \cdot C)) = A(BC)$. If $0 \in B, 0 \in C$, then by what was already proved, $(AB)C = (-(A \cdot -B))C = (A \cdot -B) \cdot -C = A(-B \cdot -C) = A(BC)$.

Suppose $0 \in A$. We simply note that $0 \notin -A$, and the proofs are straightforeward:

If $0 \notin B, C$, then $(AB)C = -((-(AB)) \cdot C)) = (-A \cdot B) \cdot -C) = -(-A \cdot (B \cdot -C)) = (-A \cdot -(B \cdot C)) = -(-A \cdot (BC)) = A(BC)$. If $0 \notin B, 0 \in C$, then $(AB)C = -(-(AB) \cdot C) = (-(AB) \cdot -C) = (((-A) \cdot B) \cdot -C) = (-A \cdot (B \cdot -C)) = (-A \cdot -(BC)) = A(BC)$. If $0 \in B, 0 \notin C$, then $(AB)C = (-A \cdot -B) \cdot C) = -A \cdot (-B \cdot C) = (-A) \cdot -(BC) = A(BC)$. If $0 \in B, C$, then $(AB)C = -((AB) \cdot -C) = -((-A \cdot -B) \cdot -C) = -(-A \cdot (-B \cdot -C)) = A(BC)$.

We now show that the identity element exists in the semi-group $\mathbb{R} \setminus \{\overline{0}\}$. Denote the set $\overline{1} := \{x \in \mathbb{Q} \mid x < 1\}$. Then $\overline{1}$ is a cut, and $0 \in \overline{1}$. We note

now, that $-\overline{1} = \{x \in \mathbb{Q} \mid x < -1\}$. Suppose D is a cut. Suppose $0 \in D$. Then $\overline{1} \cdot D = (-\overline{1})(-D)$. We straightforewardly obtain that $\overline{1} \cdot D \subset D$. Then clearly,

We now show commutativity. Suppose $A, B \in \mathbb{R}$. Then suppose $0 \notin A, B$. Then immediately, $AB = BA$. Now suppose $0 \notin A, 0 \in B$. Then $AB = -(A \cdot -B) = -\{-x \cdot y \mid x \in A, y \in -B\} = -\{-x \cdot y \mid x \in -B, y \in A\} = -(-B \cdot A) = B \cdot A$. The previous equation also shows that when $0 \in A, 0 \notin B$, we have $AB = BA$. Finally, when $0 \in A, B$, then $AB = (-A)(-B) = (-B)(-A) = BA$.

For invertibility, □

Remark. Cuts are of course open sets, and their boundaries are not within them. When considering lower cuts, as we have in the above proof, in a sense, it is the same as considering all sequences that are bounded above by a certain boundary. It suggests that instead of using equivalence classes of all rational Cauchy sequences, it suffices to consider equivalence classes of monotonically increasing sequences (or monotonically decreasing sequences, whichever one pleases).

Proof. Second proof. (Via Cauchy Sequences).

We note that since \mathbb{R} is an ordered field, it contains the integers as a subset. □

2.7 Elementary algebra of $\mathbb{R}$ and $\overline{\mathbb{R}}$

2.8 Elementary algebra of $\mathbb{C}$

3 Arithmetic on the Integers and Natural Numbers

This section develops the usual arithemetic on the integers in a formally algebraic way. Although this section will be of use in p-adic analysis, it is not disadvantageous for one to understand the underlying principles of the usual "numbers" that are used in a simply "intuitive," or "obvious way." For example, one may say that 2 and 3 are prime, but it certainly begs the question of the definition of "prime."

4 Cardinalities

In the category $\mathbb{A}$, we can define the equivalence on $Ob(\mathbb{A})$. For ease, denote it $\mathbb{U}$. In this case, the relation $\{(A, B) \in \mathbb{U} \mid A \text{ and } B \text{ are isomorphic}\}$ is obviously an equivalence by proposition 1.

In particular, consider the category of sets. The equivalence classes of $Ob(Sets)$ are called "cardinalities," and when two sets A and B are in the same equivalence class, we say that A and B have same cardinality. We denote the equivalence class of a set A as $Card(A)$, or $\#(A)$.

Remark. Unfortunately, although age old, the discussion of sets (and a great many other facets of mathematics) is not quite settled. If we define cardinalities

in this method, there may be objects in our underlying axiomatic theory which cannot be assigned cardinalities. For example, if there are proper classes, then if we take classes C and C', we do not have a definition of the cardinality of the class $\{C, C'\}$, for it is not a set, but a proper class in the sense of NBG. That is, we cannot say that $Card(\{C, C'\}) = Card(\{1, 2\})$, where 1 and 2 are integers (which are indeed sets in ZFC). Since this is restrictive, we will hence define cardinality in a more general sense, and assume that there is some underlying set theoretical axiomatization that allows our statements to make sense.

More generally, however, we will be metamathematical in our definition of cardinality. For sets X, Y, in the more general sense of the term, we will state, as a logical proposition, that "X and Y have the same cardinality," iff there exists a function $f : X \to Y$ such that f is bijective.

Remark. Note here, that in a theory equipped with proper classes, for example, we can now discuss the cardinality of the proper classes. In this case, then, functions are defined to be subsets of classes, and not the more restrictive "sets."

Here we enter into a discussion of statements regarding cardinality, and we progress onto discussion on countability.

4.1 Cardinality of the Positive Integers

Since the positive integers is The cardinality of the positive integers is of particular interest. Set theorists use the notation $\aleph_0$ to denote $Card(\mathbb{Z}_+)$.

5 Modules

6 Finite Vector Spaces and Linear Maps

7 General Topological Definitions and Prerequisites

We only assume a working knowledge of set theory.

A pair (X, τ) is called a "topological space" iff:

1. $\varnothing, X \in \tau$
2. $T \subset \tau \Rightarrow \bigcup T \in \tau$
3. If $T \subset \tau$ and T is finite, then $\bigcap T \in \tau$

Continuous maps

Topological Ring

Topological Group

Nets

Part II
Fundamental Objects

8 Uniform Spaces

Uniform spaces are the foundational objects that we will treat hence. Here, we define and discuss uniform spaces in a general setting and summarize their properties.

// Write this after completing the chapter on metric spaces, up to analytic properties of number systems, and topological groups, rings, and vector spaces, which provide motivation for uniform spaces.

Remark. Metric spaces, along with topological groups and rings, which are discussed later, are uniform spaces.

9 Metric Spaces

10 Normed Vector Spaces

11 Analytic Properties of $\mathbb{R}^n$

12 Analytic Properties of $\mathbb{C}$

13 Analytic Properties of $\mathbb{R}$

14 The Derivative

15 The Riemann and Riemann-Steiltjes Integrals

16 Analytic Properties of the P-adic Numbers

In this chapter we develop modular arithmetic and recall its basic properties. We then proceed to algebraically and analytically define the p-adic numbers and show their algebraic isomorphism. We then define the p-adic norm and topology on the p-adic numbers, and discuss their properties.

17 Topological Groups and Rings

18 Topological Vector Spaces

18.1 Normed Vector Spaces

Theorem 53. $\mathbb{R}$ *and* $\mathbb{C}$ *are complete.*

18.2 Banach Space

18.3 Hilbert Space

19 Sigma Algebras and Measure

An ordered pair $(X, \mathbb{A})$ is called an "Algebra of Sets," or simply, in an abridged way, an "Algebra," iff

1. $X \in \mathbb{A}$
2. for all $A, B \in \mathbb{A}$, we have $A \cup B, A \cap B, X \setminus B \in \mathbb{A}$.

It is highly advised to use the full term "Algebra of Sets," to lessen confusion,

Proposition 54. *We note the following properties of an algebra of sets* $(X, \mathbb{A})$.

Part III

Foundations for Further Topics in Analysis