Analysis Notes 131AH

OMKAR TASGAONKAR

Winter Quarter - January-March 2026

If you are reading this...

Hello! These are my notes for analysis, which I have typed up to save to github so I can reference them in the future. Things will be written in my own words and may not be fully correct, but this is just my attempt to fully internalize everything and write it down as precisely as possible.

Contents

1 Propositional and First-Order Logic

Definition 1.1. *A proposition is a statement that takes a TRUE or FALSE value*

For example, "birds are mammals" is a valid proposition, which takes on the value of FALSE. We also define a "primitive proposition", which is one with no connectives or quantifiers.

Definition 1.2. *A connective is a unary or binary operator allowing us to chain propositions to create new propositions*

The connectives we will work with are $\neg$ (logical not), $\wedge$ (and), $\vee$ (or), $\implies$ (implies), and $\iff$ (biconditional). The $\neg$ operator is the only unary operator, which switches the value of the proposition. The others are binary, requiring two propositions and outputting one value.

We view an interesting truth table for $\implies$:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

When P is false but Q is true, the entire statement is "vacuously" true as the expected proposition Q is true no matter P. When both are false, the proposition is true as well. So in general when P is false, $P \implies Q$ is true.

Lemma 1.1. $(P \implies Q) \iff \neg(P \wedge \neg Q) \iff \neg P \vee Q$

Here the biconditional means that the propositions are equivalent. We can use the biconditional to represent when two statements imply each other or are logically the same.

This lemma highlights proof by contradiction, where we assume P and $\neg Q$ and we show some contradiction (or show that the proposition is false). Then the logical not of the proposition is true. The second equivalence is an application of DeMorgan's Laws for logic.

Lemma 1.2. $(P \implies Q) \iff \neg Q \implies \neg P$

This is the method of proof by contrapositive. This implication is called the **"only if"** direction, while the reverse is the **"if"** direction.

Definition 1.3. *We propose two quantifiers: $\forall$ (for all/for each) and $\exists$ (there exists)*

A first order statement assumes the form: (quantifier)(variable): (proposition). This is the basis of First Order Logic, an extension of propositional logic. For example:

$$\forall x : P(x)$$

translates to: for all x such that $P(x)$ is true. The terminology "some" is equivalent to $\exists$.

Lemma 1.3. $\neg(\forall x : P(x)) \iff \exists x : \neg P(x)$ *and* $\neg(\exists x : P(x)) \iff \forall x : \neg P(x)$

Here we see how the logical not operator distributes over quantifier and proposition.

Theorem 1.1. $\forall x \forall y : P(x, y) \iff \forall y, \forall x : P(x, y)$ *and* $\exists x, \exists y : P(x, y) \iff \exists y, \exists x : P(x, y)$

If the quantifiers for two variables are the same, we can switch the order of the quantifiers. This will appear in proofs involving sets and supremums/infimums. However, if they are not the same, then we cannot suggest an equivalence.

Theorem 1.2. $\exists x \forall y : P(x, y) \implies \forall y \exists x : P(x, y)$

The reason why this is a one-way implication is because the left hand statement is more specific. We will encounter this when dealing with images and preimages. We take the following example:

Mathematical Example: If there exists one x greater than all y, then for each y there exists an $x > y$. In this case that x is the same. For the converse, if each y has an $x > y$, there may not be a singular x greater than all y.

Figurative Example: If there is one building to which all apartments belong, then all the apartments belong to that building. However, if all the apartments belong to a building, not necessarily they belong to one building. We can have the apartments in multiple buildings.

2 Naive Set Theory and Zermelo Fraenkel

2.1 Naive Set Theory

Naive Set Theory was the initial proposed set theory. A set being a container for some sort of objects. To construct a set, we have the following:

Definition 2.1. *The Comprehension Principle:* $A \coloneqq \{x : P(x)\}$

The symbol $\coloneqq$ means "defined as". If we use "=" when referring to sets, that is not the same as using $\coloneqq$.

The Comprehension Principle tells us that a set is some elements x that satisfy a proposition $P(x)$. We won't dwell on this theory too much, but it has pitfalls such as Russell's paradox:

$$A \coloneqq \{x : x \notin x\}$$

Here if $x \notin x$, then we could say $A \notin A$, but the proposition tells us that $A \in A$, so we come across a contradiction.

2.2 Zermelo Fraenkel

Axiom 2.1. ***Axiom of Separation*** *Any set A can be defined as $\{x \in U : P(x)\}$.*

We see that the elements $x \in A$ are being drawn from U which in this case can be a universe (all the possible sets, but this is not itself a set), or a bigger set. By restricting elements, we can prevent self references such as those in Russell's paradox.

Axiom 2.2. ***Axiom of Extensionality*** $\forall A, B : A = B \iff \forall x : (x \in A \iff x \in B)$

We mentioned previously that $\coloneqq$ is not the same as $=$ for sets. Extensionality gives the definition of $=$ to be that the sets must have the same elements. The axiom itself is sometimes written as an implication rather than a biconditional.

Axiom 2.3. ***Empty Set:*** $\exists \varnothing : \forall x \in U : x \notin \varnothing$

We postulate the existence of the empty set, which contains none of the possible elements in the universe. Now, how do we build the set of all subsets (aka the powerset)?

Definition 2.2. $\subseteq$ *(subset relation):* $\forall A, B : A \subseteq B \implies \forall x \in A : x \in B$

Let's try to use the Axiom of Separation and this definition to construct the powerset. We can say maybe for a set A that $\mathcal{P}(A) \coloneqq \{B \in C : B \subseteq A\}$. But this definition requires a set C to exist in which B belongs, so either this is the powerset or a set containing more elements than the powerset, and so we have a circular definition.

Axiom 2.4. ***Powerset:*** $\forall A \exists \mathcal{P}(A) : (\forall B \subset A : B \in (P)(A))$

We have the same issue when we go to define a set such as $\{x, y\}$, which is called the pairset, as each element is also inherently a set.

Axiom 2.5. ***Pairset:*** $\forall x, y \exists A \forall Z \in A : x = z \vee y = z$

The pairset allows us to show the existence of a singleton set $\{x\}$ if both the elements given are the same as $\{x, x\} = \{x\}$. This can be shown by extensionality.

Axiom 2.6. ***Infinite Set:*** $I \coloneqq \{x : x \in I \implies \{x\} \in I\}$

This is one possible construction of the infinite set we will use for the naturals; however, this axiom postulates the existence of infinite sets. Many of the constructions in analysis will hinge on this axiom; without it, we fail to construct the idea of "natural numbers" let alone "real numbers".

3 Ordered Pairs and Relations

We talk about pairs (or n-tuples) of numbers such as $(1, 2)$ or (x, y). However, we also distinguish the order unlike sets, saying that $(1, 2)$ is not the same as $(2, 1)$.

Definition 3.1. ***Kuratowski Pair:*** $(x, y) \coloneqq \{\{x\}, \{x, y\}\}$

4 Isomorphisms of Dedekind Cuts and Ordered Fields

So far we have constructed the reals or $\mathbb{R}$ as the set of Dedekind cuts, which are the set of rationals less than that real number. By allowing for completeness, we can show that each cut admits an upper bound so it admits a supremum.

The supremum is the real number itself; however, quantifying the supremum will require the existence of an algebraic structure that encompasses the supremum. If we solely rely on $\mathbb{Q}$, then certain cuts may not admit supremums in $\mathbb{Q}$.

So we say there exists some complete ordered field $(F, +, 0, \cdot, 1, \leqslant)$ (completeness is important here, otherwise we cannot guarantee supremums). Each ordered field fundamentally has the $\mathbb{N}_F$. We examine a theorem:

Theorem 4.1. *If F is an ordered field, then it has characteristic* 0

We prove this by contrapositive:

Proof. Assume F does not have characteristic 0. Then $\sum_{k=1}^{n}(1) = 0$ for an arbitrary n. We then know that $0 < 1$, by ordered field properties:

$$0 < 1 \implies 0 < \sum_{k=1}^{n-1}(1) < \sum_{k=1}^{n-1}(1) + 1 = \sum_{k=1}^{n}(1)$$

Now assume the inequality to be true, then by mulitplicative property of ordered fields:

$$\implies \sum_{k=1}^{n-1}(1) \cdot \sum_{k=1}^{n-1}(1) < \sum_{k=1}^{n}(1) \cdot \sum_{k=1}^{n-1}(1)$$

$$\iff (n-1)^2 = n^2 - 2n + 1 < n(n-1) = n^2 - n \tag{1}$$

We know that n or 1 added n times repeatedly is equal to zero, so we get:

$$0 + 1 = 1 < 0$$

Which is a contradiction of a key property of ordered fields that $0 \leqslant 1$. □

So now, the addition of of 1 to an element of the field becomes our sucessor operation, and 0 becomes our zero element. If we then consider the subset of elements greater than zero, then zero is not a sucessor of any number in the set. Thus we can construct the naturals in a field as:

$$\mathbb{N}_F = \bigcap_{\alpha \in I} \{A_\alpha \subseteq F : (\forall x \in A_\alpha : x + 1 \in A_\alpha)\}$$

Now that we have the naturals in every ordered field, by field properties, we require their additive and multiplicative inverses. Furthermore any combination of these must also remain in the field, giving rise to the rationals $\mathbb{Q}_F$ (considered the "minimal" ordered field).

So currently we have the set of Dedekind cuts $\mathbb{R}$ and an ordered field structure F. One is constructed from ground up, the other's existence is assumed respectively. We aim to show the two are isomorphic. We know the following theorem proved in prior chapters:

Theorem 4.2. *The rationals of different fields are isomorphic*

So there exists an isomorphism we call $\psi : \mathbb{Q} \to \mathbb{Q}_F$. Since the Dedekind cuts are merely sets of rationals, then we can construct cuts in F which we call $\mathbb{R}_F$. We can extend $\psi : \mathbb{R} \to \mathbb{R}_F$.

Theorem 4.3. $\forall A \in \mathbb{R}_F : (\exists b \in F, \forall a \in A : a \leqslant b) : \sup : A \to F$ *and* sup *is an isomorphism*

This lemma is essentially the restatement of the completeness of F. If we take any subset bounded above, then it admits a supremum. However, here we define the supremum as a map from a set to an element in the field. We prove it is an isomorphism for a cut specifically. We require the lemma:

Lemma 4.1. $\forall A \in \mathbb{R}_F : A = \{a \in \mathbb{Q}_F : a < \sup(A)\}$

For now we only show the inclusion $A \subseteq \{a \in \mathbb{Q}_F : a < \sup(A)\}$.

Proof. If $x \in A$, then $x \leqslant \sup(A)$. If $x = \sup(A) \implies \sup(A) \in A$. By the definition of Dedekind cut's, there cannot be a maximal element, so:

$$\exists b \in A : \sup(A) < b \wedge b \leqslant \sup(A)$$

The second inequality comes from the supremum definition. We see that we get a contradiction, so $\sup(A) \notin A$, thus $\forall a \in A : a < \sup(A)$. □

We now return to proving the theorem at hand.

Proof. For the sake of brevity we assume sup is a homomorphism (which means that it respects the operations of sets and the field). We aim to show injectivity:

$$\forall A, B : \sup(A) = \sup(B) \implies A = B$$

If two cuts are not equal, then either $A \subset B \vee B \subset A$. Assume without loss of generality that $A \subset B$. Then:

$$\exists b \in B, \forall a \in A : a < b$$

This inequality we can derive from the ordering of F and the construction of the cuts. Then b is an upper bound for A and by definition of supremum $\sup(A) \leqslant b$. So by the lemma $a < \sup(A) \leqslant b < \sup(B)$. Thus $\sup(A) < \sup(B)$, proving injectivity of sup. □

Proof. We now prove the surjectivity of sup:

$$\forall x \in F, \exists A \in \mathbb{R}_F : \sup(A) = x$$

Assume for a certain $x \in F$, that there does not exist an $A \in \mathbb{R}_F$ such that $\sup(A) = x$. Then all Dedekind cuts must admit a supremum in F as they are bounded above. (The following part may be a bit hand wavy :), but in essence by means of pigeonhole principle (whose proof we detailed before), two different cuts will then share the same supremum, which breaks injectivity. □

Theorem 4.4. *For all complete ordered fields* $(F, +, 0, \cdot, 1, \leqslant)$*, we find that* $\mathbb{R} \cong F$.

The proof of this is simply a combination of the previous theorems and lemmas. We know that $\psi : \mathbb{R} \to \mathbb{R}_F$ is an isomorphism and $\sup : \mathbb{R}_F \to F$ is also an isomorphism. The composition is therefore an isomorphism:

$$\sup \circ \psi : \mathbb{R} \to F$$

So the Dedekind cut representation of the reals are isomorphic to any complete ordered field. So now instead of dealing with the reals as a set of Dedekind cuts, we can deal with it as an ordered field of the supremums of the Dedekind cuts. So $\sqrt{2}$ is a supremum of the cut, so we can explicitly refer to the cut as $\sqrt{2}$ itself even though the cut does not admit a supremum in $\mathbb{Q}$.

5 Properties of the Reals

We have determined that every complete ordered field is isomorphic to the real numbers. We now aim to show certain properties have correctly carried forward to this construction.

We dealt with rational roots and equalities such as $x^2 = 2$ that did not admit solutions in the rationals, but allowed us to construct $\sqrt{2}$ in the reals. We now see the reals hold for arbitrary roots as well:

Theorem 5.1. $\forall a \in \mathbb{R}^+, \forall n \in \mathbb{N} \setminus \{0\} : (\exists x \in \mathbb{R}^+ : x^n = a) \wedge (x^n = y^n \implies x = y)$

In essence, there exists an *nth* root for every real number, which is unique. We use the following property:

$$\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N} \setminus \{0\} : x^n - y^n = (x - y) \sum_{k=0}^{n-1} x^k y^{n-k-1}$$

Integer exponentiation can be defined by field properties as repeated multiplication of the element in the field.

HW 5 Problem: We prove the property below:

Proof. By the distributive property of multiplication in fields:

$$(x - y) \sum_{k=0}^{n-1} x^k y^{n-k-1} = x \sum_{k=0}^{n-1} x^k y^{n-k-1} - y \sum_{k=0}^{n-1} x^k y^{n-k-1}$$

$$= \sum_{k=0}^{n-1} x^{k+1} y^{n-k-1} - \sum_{k=0}^{n-1} x^k y^{n-k}$$

We can notice a pattern of cancellations here. The last term of the left term is x^n and the first term of the right term is y^n. We can then rewrite the sum as:

$$= x^n - y^n + \sum_{k=0}^{n-2} x^{k+1} y^{n-k-1} - \sum_{k=1}^{n-1} x^k y^{n-k}$$

We see that the two summations output the same terms, just that the starting and ending indices are up by 1. If our starting term is xy^{n-1}, then at $k = 0$ we sum $x^{k+1}y^{n-k-1}$, but at $k = 1$, we sum $x^k y^{n-k}$.

If our last term is $x^{n-1}y$, then the same applies. So the two summations are equal, thus their subtraction equals 0, and our resultant expression is $x^n - y^n$. □

We return to the proof of the theorem. We define the set $A \coloneqq \{y \in \mathbb{R}^+ : y^n \leqslant a\}$. Since this is a subset of the field, if it is bounded, then it admits a supremum:

$$1 + a > a \implies (1 + a)^n > (1 + a)^{n-1} a > a^n > a \quad \text{(Ordering Property of Multiplication)}$$

Thus $\forall y \in A : y \leqslant 1 + a$ so A is bounded above, thus it admits a supremum. We want to show that $\sup(A)^n = a$, thus defining the supremum of the set as the n-th root and showing its existence (as we know supremum exists).

Proof. We use the fact that $\forall y \in A : y \leqslant \sup(A)$, We first show $\sup(A)^n \leqslant A$. We also use the fact that:

$$\forall m \in \mathbb{N} \setminus \{0\} : \sup(A) - \frac{1}{m} < \sup(A) \implies \exists y \in A : \sup(A) - \frac{1}{m} \leqslant y$$

$$\sup(A)^n - a \leqslant \sup(A)^n - y^n = (\sup(A) - y) \sum_{k=0}^{n-1} \sup(A)^k y^{n-k-1}$$

Our previous implication that $\sup(A) - \frac{1}{m} \leqslant y \iff \sup(A) \leqslant y + \frac{1}{m} \implies \sup(A) \leqslant y$. Since $y \in A$, we know that $y \leqslant \sup(A)$, so $y = \sup(A)$. Our inequality becomes:

$$\sup(A)^n - a \leqslant \sup(A)^n - y^n = (\sup(A) - y) \sum_{k=0}^{n-1} \sup(A)^k y^{n-k-1} = 0 \iff \sup(A)^n \leqslant a$$

We now prove that $\sup(A)^n \geqslant a$. We note that $\forall m \in \mathbb{N} \setminus \{0\} : \sup(A) + \frac{1}{m} > \sup(A)$, so:

$$(\sup(A) + \frac{1}{m})^n > a \implies a - \sup(A)^n < (\sup(A) + \frac{1}{m})^n - \sup(A)^n$$

$$= \frac{1}{m} \sum_{k=0}^{n-1} (\sup(A) + \frac{1}{m})^k \sup(A)^{n-k-1} \leqslant \frac{n}{m} (\sup(A) + \frac{1}{m})^{n-1}$$

Thus, by dividing both sides (also the Archimedian Property is really a double implication), we see that:

$$\frac{m}{n} \frac{a - \sup(A)^n}{(\sup(A) + \frac{1}{m})^{n-1}} < 1 \implies a - \sup(A)^n \leqslant 0 \iff \sup(A)^n \geqslant a$$

So we have proven that $\sup(A)^n = a$, proving the existence of the nth root, which we will denote by $a^{1/n}$. □

Proof. We now prove the uniqueness of the $n-th$ root. Assume there are two $n-th$ roots of a such that $y^n = a = \tilde{y}^n$. Then:

$$\sup(A)^n = y^n = \tilde{y}^n = a \implies a^{1/n} = \sup(A) = y = \tilde{y}$$

Since the supremum is unique, then if $y = \sup(A) = \tilde{y}$, then y must equal $\tilde{y}$, so the nth root is unique. □

Now that we have the notion of natural powers and nth roots, we can extend this to rational roots. We know that any rational can be represented as the ratio of two integers p/q. Note the following:

Corollary 5.1. $\forall n \in \mathbb{N}, \forall a \in \mathbb{R} : a^{-n} = (a^{-1})^n = (\frac{1}{a})^n \wedge a^0 = 1$

With this corollary, we are able to define the notion of integer powers (as integers have additive inverses not accounted for by natural powers). Another property of natural powers and by extension integer powers:

Corollary 5.2. $\forall m, n \in \mathbb{N} : a^m \cdot a^n = a^{m+n} \wedge a^{m \cdot n} = (a^m)^n$

HW 5 Problem: Using this corollary, we can prove the following lemma. For this problem assume $a > 1$:

Lemma 5.1. $\forall m, n, p, q \in \mathbb{Z} : n, q > 0 \wedge \frac{m}{n} = \frac{p}{q} \implies \forall a > 1 : (a^m)^{1/n} = (a^p)^{1/q}$

Proof. If $\frac{m}{n} = \frac{p}{q}$, then we know that $mq = np$ where the two are integers. If $m/n < 0$, then $p/n < 0$ and same for $m/n \geqslant 0$. Thus the two fractions take on the same sign. Therefore $mq = np$ will either be positive or negative.

If $mq = np < 0$, we simply define their additive inverses $m'q' = n'p' > 0$ and use them to construct an equality (eg $-a = -b \iff a = b$ by field properties). So without loss of generality we proceed with $mq = np > 0$:

$$a^{mq} = a^{qm} = (a^q)^m \wedge a^{np} = a^{pn} = (a^p)^n \tag{2}$$

This is true by properties of exponentiation with respect to naturals and field multiplication. Thus, by the existence of arbitary roots:

$$(a^q)^m = (a^p)^n \implies ((a^q)^m)^{1/n} = a^p \implies ((a^m)^q)^{1/n} = a^p$$

We need to show that we can exchange the places of q and $1/n$, so we prove $(a^m)^{1/n} = (a^{1/n})^m : n > 0$:

$$((a^m)^{1/n})^n = a^m \wedge ((a^{1/n})^m)^n = (a^{1/n})^{mn} = (a^{1/n})^{nm} = ((a^{1/n})^n)^m = a^m$$

Since both expressions to raised to the $n : n > 0$ are equal, then the nth roots are also equal so $(a^m)^{1/n} = (a^{1/n})^m$.

So returning to our initial statement:

$$((a^m)^q)^{1/n} = a^p \implies ((a^m)^{1/n})^q = a^p \implies (a^m)^{1/n} = (a^p)^{1/q}$$

□

Corollary 5.3. $\forall p, q \in \mathbb{Z}, q \neq 0 : a^{\frac{p}{q}} = (a^p)^{1/q} = (a^{1/q})^p$

Lemma 5.2. $\forall r, s \in \mathbb{Q} : a^{r+s} = a^r \cdot a^s$

Proof. We let $r = \frac{m}{n}$ and $s = \frac{p}{q}$, where $m, n, p, q \in \mathbb{Z} \wedge p, q \neq 0$, then $r + s = \frac{m}{n} + \frac{p}{q} = \frac{mq+np}{pq}$. Thus by corollary 5.3:

$$a^{r+s} = a^{(mq+np)/pq} = (a^{1/pq})^{mq+np}$$

Now $mq + np$ is an integer expression, by corollary 5.2, we can rewrite the expression as:

$$= (a^{1/pq})^{mq} \cdot (a^{1/pq})^n p = (a^{mq/pq}) \cdot (a^{np/pq}) = a^{m/p} \cdot a^{n/q} = a^r \cdot a^s$$

□

The idea of multiplicative inverses can now be brought about for rational powers. Let $p, q, m, n \in \mathbb{Z} : q, n \neq 0$, then:

$$a^{p/q} \cdot a^{m/n} = (a^{1/pq})^{mq+np} = 1$$

Using corollary 5.1, we account for the sign of $mq + np$. If the expression is greater than zero, than it is a natural number. If it is less than zero, we define its additive inverse $(mq + np)' > 0$ by field properties and change the base from a to a^{-1} as per the corollary.

Without loss of generality we proceed with the first case. Once again by corollary 5.1 stating that $a^0 = 1$:

$$mq + np = 0 \implies np = -mq$$

So by Lemma 5.2, $(a^{1/pq})^{mq+np} = (a^{1/pq})^{mq} \cdot (a^{1/pq})^{np} = (a^{1/pq})^{mq} \cdot (a^{1/pq})^{-mq}$. Since $mq \in \mathbb{Z}$, we again apply corollary 5.1 and 5.3:

$$(a^{1/pq})^{mq} \cdot (a^{1/pq})^{-mq} = a^{m/p} \cdot a^{-m/p} = 1$$

So we see that $(a^{m/p})^{-1} = a^{-m/p} = (a^{-1})^{m/p}$.

Now that we have defined and proven the properties of rational powers, we need to define real powers, which we do via supremums again leveraging completeness of the underlying ordered field:

Definition 5.1. $a^x \coloneqq \begin{cases} \sup\{a^z : z \in \mathbb{Q} \wedge z \leqslant x\}, & a > 1 \\ \inf\{a^z : z \in \mathbb{Q} \wedge z \leqslant x\}, & a < 1 \\ 1, & a = 1 \end{cases}$

Proof. We prove the first case, where if $a > 1$ and $x \in \mathbb{Q}$, then $a^x = \sup\{a^z : z \in \mathbb{Q} \wedge z \leqslant x\}$. We know that $x < x + 1$. By density of the rationals:

$$\exists r \in \mathbb{Q} : x < r < x + 1$$

Since $z \leqslant q$, then $z < r$. We now need to prove the lemma:

Lemma 5.3. $\forall z, r \in \mathbb{Q} : z < r \implies a^z < a^r$.

If $z < r$, and $a > 1$, we see that $a^{r-z} > a > 1$ so by Lemma 5.2:

$$a^{r-z} = a^r \cdot a^{-z} = a^r \cdot (a^z)^{-1} > 1$$

Since $a > 1 > 0$, then $a^z > a > 0$. So if $(a^z)^{-1} < 0$. Thus:

$$a^r \cdot (a^z)^{-1} > 1 \implies 1 \cdot a^z < a^r \cdot (a^z)^{-1} \cdot a^z \iff a^z < a^r$$

Therefore a^r is an upper bound, allowing for the set to admit a supremum. We now want to show that a^x is the least upper bound. Consider any upper bound $a^p : p \in \mathbb{Q}$, then:

$$\forall z \leqslant x : a^z \leqslant a^p \implies a^x \leqslant a^p$$

If $a^p < a^x$, then $a^{x-p} > 1$. Since $a > 1$, then $a^{x-p} > a > 1$ only if $x > p$.

$$p < x \wedge z \leqslant x \implies \exists z \leqslant x : p < z \implies a^p < a^z$$

Thus, a^p is not an upper bound for all a^z, so we have proven the statement by contrapositive.

Lemma 5.4. $\forall x, y \in \mathbb{R} : a^{x+y} = a^x \cdot a^y$

We define $a^{x+y} = \sup\{a^z : z \in \mathbb{Q} \wedge z \leqslant x + y\}$.

Since $a^y = \sup\{a^p : p \in \mathbb{Q} \wedge p \leqslant y\}$ and $a^x = \sup\{a^q : q \in \mathbb{Q} \wedge q \leqslant x\}$:

$$a^x \cdot a^y = \sup\{a^q\} \cdot \sup\{a^p\} = \sup\{a^q \cdot a^p\} = \sup\{a^{q+p}\}$$

This follows from Lemma 5.2 and sup being a homomorphism. Multiplying the supremums combines the predicates in a logical $\wedge$ and results in a Minkowski product $\{a^{q+p} : q \leqslant x \wedge p \leqslant y\}$. By ordered field properties:

$$q \leqslant x \wedge p \leqslant y \implies q + p \leqslant x + y$$

By definition of the set of a^{x+y}, we see $\forall q \leqslant x, \forall p \leqslant y : a^{p+q} \in \{a^z : z \leqslant x + y\}$. Therefore:

$$\{a^{q+p}\} \subseteq \{a^z\} \implies \sup\{a^{q+p}\} \leqslant \sup\{a^z\} \iff a^x \cdot a^y \leqslant a^{x+y}$$

Thus $a^x \cdot a^y = \sup\{a^{q+p} : p \leqslant y \wedge q \leqslant x\} \leqslant \sup\{a^z : z \leqslant x + y\} = a^{x+y}$.

We now prove the opposite inequality, that $a^{x+y} \leqslant a^x \cdot a^y$. We choose a fixed $\tilde{q} \leqslant x$ and a fixed $\tilde{p} \leqslant y$, then:

$$a^{x+y} = \sup\{a^z : z \leqslant x + y\}$$

For every z, we can pick $\tilde{p}, \tilde{q}$ such that by Lemma 5.3:

$$(\forall z \in x+y : \exists \tilde{p} \leqslant y, \tilde{q} \leqslant x) : z \leqslant \tilde{p}+\tilde{q} \implies a^z \leqslant a^{\tilde{p}+\tilde{q}} = a^{\tilde{p}} \cdot a^{\tilde{q}}$$

Which means that since the choices of $\tilde{p}, \tilde{q}$ were arbitrary:

$$\forall z \leqslant x+y : a^z \leqslant a^{\tilde{p}} \cdot a^{\tilde{q}} \leqslant a^x \cdot a^y$$

By definition of supremum, a^{x+y} is the least upper bound for all a^z and we have shown that $a^x \cdot a^y$ is an upper bound, so:

$$a^z \leqslant a^x \cdot a^y \implies a^{x+y} \leqslant a^x \cdot a^y$$

Thus proving $a^{x+y} = a^x \cdot a^y$. This forces a multiplicative inverse to exist such that $a^x \cdot a^y = a^0 = 1 \implies x+y=0 \implies y=-x$. Thus $(a^x)^{-1} = a^{-x}$. □

Now that we have defined exponentiation with respect to a real valued base, along with elementary operations, we aim to define the inverse of exponentiation, which is the logarithm.

Theorem 5.2. *The exponential function: $f : \mathbb{R} \to \mathbb{R}^+ \setminus \{0\}$ is a bijection*

We define $f(x) = b^x$ for any $a \in \mathbb{R}^+$. The proof is the same if $b > 1$ or $b < 1$. Then:

Proof. f is injective if $\forall x, y \in \mathbb{R}^+ : b^x = b^y \implies x = y$. We can use Lemma 5.4 and multiplicative inverses:

$$b^x = b^y \implies b^x \cdot (b^y)^{-1} = 1 \implies b^x \cdot b^{-y} = b^{x-y} = 1$$

Since $b > 1$, then by the definition of exponentiation, $x - y = 0$, so $x = y$.

If f is surjective, then $\forall y \in \mathbb{R}^+ . \exists x \in \mathbb{R} : b^x = y$. Here x is called the logarithm of y base b.

We fix $a > 1$, then by the results of problem 1:

$$a^n - 1 = (a-1)\sum_{k=0}^{n-1} a^k \cdot 1^{n-k-1} = (a-1)\sum_{k=0}^{n-1} a^k \geqslant \sum_{k=0}^{n-1} 1^k = n(a-1)$$

Now if we let a be the nth root of b such that $a = b^{1/n} > 1$, then:

$$a^n - 1 \geqslant n(a-1) \implies b - 1 \geqslant n(b^{1/n} - 1)$$

If $t > 1$ and $n > (b-1)/(t-1)$, then $b^{1/n} < t$:

$$n(b^{1/n} - 1) \leqslant b - 1 < n(t-1) \implies b^{1/n} - 1 < t - 1 \implies b^{1/n} < t$$

If w is such that $b^w < y$, then $b^{w+(1/n)} < y$ for sufficiently large n; to see this, apply part (c) to $t = y \cdot b^{-w}$.

$$b^{1/n} < t \implies b^{1/n} < y \cdot b^{-w} \implies b^{(1/n)+w} < y$$

If $b^w > y$, then $b^{w-(1/n)} > y$ for sufficiently large n. Let $t = y^{-1} \cdot b^w > 1$:

$$b^{1/n} < t \implies b^{1/n} < y^{-1} \cdot b^w \implies y < b^{w-(1/n)}$$

Let A be the set of all w such that $b^w < y$, and show that $x = \sup(A)$ satisfies $b^x = y$.

If $b^x > y$, then $b^{x-(1/n)} > y$, which means that $x - \frac{1}{n}$ is a smaller lower bound, so b^x is not greater than y. If $b^x < y$, then $b^{x+(1/n)} < y$, so $x + \frac{1}{n} \in A$, but $x < x + \frac{1}{n} \notin A$, showing a contradiction.

Thus $b^x = y$ and $x = \sup(A)$, proving the existence of a logarithm of y base b for any $y \in \mathbb{R}^+$, showing surjection. The uniqueness of x can be derived from the injection or also through supremums:

$$b^x = b^{x'} = y \implies x = \sup(A) \wedge x' = \sup(A)$$

Since the supremum is unique, then $x = x'$, showing injectivity, thus f is a bijection and therefore has an inverse which we will call log. □

Corollary 5.4. $\log_b : \mathbb{R}^+ \setminus \{0\} \to \mathbb{R}$ *such that* $log_b(y) = x$

Then the composition of $\log_b(b^x) = x$ and $b^{\log_b(x)} = x$. Here we see the $\log_b$ acting as a left and right inverse, which is the expected behavior of the inverse of a bijective function. (Remember a surjection only has a right inverse, and an injection only has a left inverse).

6 Countability and Cardinality

The natural numbers or $\mathbb{N}$ are the backbone of the idea of "counting". When we say $0, 1, 2, 3...$ so on and so forth, we are iterating through the naturals. We define the following:

Definition 6.1. *The first n naturals are $[0, n) \coloneqq \{k \in \mathbb{N} : k < n\}$*

We can now introduce the notion of a finite set.

Definition 6.2. *A finite set A is a set such that $\exists f, \exists n \in \mathbb{N} : f : [0, n) \to A$ and f is a bijection*

An infinite set is one that is not finite, or one for which we cannot find a bijection between an interval of the first n naturals for some $n \in \mathbb{N}$.

We also introduce the notion of Dedekind infinite. A set that is Dedekind infinite is one where we can find an injective but not surjective map between the set and itself. For example:

$$S : \mathbb{N} \to \mathbb{N} : 0 \notin \text{Ran}(S) \implies S(\mathbb{N}) \subseteq \mathbb{N}$$

So the naturals are a Dedekind infinite set under the successor operation. We can also come up with other injections such as $f(n) = n^2$. We say the following:

Lemma 6.1. *Given a set A: A is Dedekind infinite $\implies$ A is infinite*

The converse requires invoking axiom of choice as we need to assume the existence of a choice function that can generate a sequence of values to which we can apply an injective function.

If we can find a bijection f between an interval $[0, n)$ and a finite set A, then the value $n \in \mathbb{N}$ is called the cardinality of A, denoted by $|A|$. We see some inequalities related to cardinality:

Lemma 6.2. *For finite sets A and b:*

1. $B \subseteq A \implies |B| \leqslant |A|$
2. $|A \cup B| \leqslant |A| + |B|$
3. $|A \times B| = |A| \cdot |B|$

We prove Lemma 6.2.1:

Proof. We define $|A|$ as $n \in \mathbb{N}, \exists f : f : [0, n) \to A \wedge \text{Im}(f) = A$. The proof is as follows:

1. $B \subseteq A \iff \forall x \in B : x \in A$ (Subset Definition)
2. $\forall x \in B : (x \in A \implies x \in \text{Im}(f))$ (By definition of f)
3. $\implies \forall x \in B \wedge A, \exists m \in [0, n) : f(m) = x$ (Definition of Preimage)
4. Thus $f^{-1}(B) = \{m \in [0, n) : f(m) = x\}$
5. Since $\forall m \in f^{-1}(B) : m \in [0, n) \implies f^{-1}(B) \subseteq [0, n)$ (Definition of Subset)
6. Therefore either $f^{-1}(B) = [0, n) = \text{Dom}(f)$ or $f^{-1}(B) \subset [0, n)$ so it does not contain all first n naturals
7. Since f is a bijection, then $f|_{f^{-1}(B)} : f^{-1}(B) \to B$ is a bijection, so by line 6: $|B| \leqslant |A|$

□

We prove Lemma 6.2.2:

Proof. The proof is as follows. Since A, B are finite, axiom of choice is not required:

1. $A \cup B \iff \forall x \in A \cup B : x \in A \vee x \in B$ (Definition of Union)
2. $f : [0, n) \to A \wedge g : [0, m) \to B$ such that f, g are bijections. Then $|A| = n, |B| = m$.
3. We define a function $p : [0, m + n) \to A \cup B$ such that $\text{Ran}(p|_{[0,n)}) = A \wedge \text{Ran}(p|_{[n,m+n)}) = B$
4. If $A \cap B \neq \varnothing$, then $\exists x : x \in A \wedge x \in B$
5. $\implies x \in \text{Im}(f) \wedge \text{Im}(g)$
6. $\implies \exists l \in [0, n) \wedge \exists k \in [m, m + n) : p|_{[0,n)}(l) = p|_{[n,m+n)} = x$, which means that p is not injective, so $|A \cup B| < m + n = |A| + |B|$
7. If $A \cap B = \varnothing$, then p is a bijection, so $|A \cup B| = m + n = |A| + |B|$
8. Thus $|A \cup B| \leqslant |A| + |B|$

□

We prove Lemma 6.2.3:

Proof. The proof is as follows:

1. We define the cartesian product of A, B as $A \times B \coloneqq \bigcup\{f : [0, 2) \to A \cup B : (f(0) \in A \wedge f(1) \in B)\}$
   (a) Remember that a function is fundamentally its graph, so each function is bijective to the set of pairs with the first element being from A and the seocnd being from B.
   (b) Let's restrict each f to a single, unique ordered pair so that all the graphs are disjoint.
2. Thus $|A \times B| = |\bigcup\{f : [0, 2) \to A \cup B : (f(0) \in A \wedge f(1) \in B)\}| = \#$ of f
3. Let $|A| = m \wedge |B| = n$
4. Fix an $a \in A : f(0) = a \wedge f(1) \in B \implies |\{f : [0, 2) \to A \cup B : f(0) = a \wedge f(1) \in B\}| = n$ as there are n elements in B
5. Since there are m elements in A, we have m sets $\{f : [0, 2) \to A \cup B : f(0) = a \wedge f(1) \in B\}$.
6. Thus in total we have m sets of n functions, so we have $m \cdot n$ functions in total, thus:
7. $|A \times B| = |A| \cdot |B|$

□

We note the relation of Axiom of Choice and Cartesian Products/Powers. Take for example the cartesian power $\mathbb{R}^{\mathbb{N}}$ which is the set of real valued sequences. The question is the same as the problem proposed in Lemma 6.1. To construct the sequence, we encounter the following collection:

1. $x_0 \in \mathbb{R}$
2. $x_1 \in \mathbb{R} \setminus \{x_0\}$
3. $x_2 \in \mathbb{R} \setminus \{x_0, x_1\}$
4. $x_3 \in \mathbb{R} \setminus \{x_0, x_1, x_2\}$
5. The sequences continues countably infinitely (for as many naturals there are)

Here we see that we are required to select real numbers from an infinite family of infinite sets. We encounter the same problem for an infinite family of finite sets.

We now consider the cartesian power $\mathbb{N}^{\mathbb{N}}$ which is the set of all natural-valued sequences. We see the following family:

1. $x_0 \in \mathbb{N}$
2. $x_1 \in \mathbb{N} \setminus \{x_0\}$
3. The sequence continues for all of $\mathbb{N}$

This case does not require axiom of choice however, due to the well ordering principle. We know that every set of naturals admits a minimum (an infinimum that exists in the set). So we know that there exists one such possible sequence which is the naturals itself. We can also take different collections of subsets of $\mathbb{N}$, combined with the well-ordering, allowing us to define different sequences and their rules.

Question to Think About: What about $\mathbb{Q}^{\mathbb{N}}$, does such construction require Axiom of Choice?

Definition 6.3. *A countable set A is one that is either finite or $\exists f$ such that $f : \mathbb{N} \to A$ is a bijection*

We now exmaine countable sets. We will show results such as $\mathbb{Q}$ being countable, or the set of algebraic reals being countable, which on surface seem counterintuitive.

Theorem 6.1. *If A is countable, then $\forall B \subseteq A : B$ infinite $\implies$ B countable*

We first see that A is infinite as well as it has an infinite subset (How can we prove this?)