NCKU 112.1
Rudin

Eric Liu

Contents

Chapter 1

The Real and Complex Number System

1.1 Introduction

In this section, we will define the concept of ordered sets, and give a close look of the completeness property of real numbers, by showing the "uncompleteness" of rational numbers. First, we prove an elementary and classic theorem of rational numbers.

Theorem 1.1.1. There exists no rational p such that $p^2 = 2$

Proof. Assume there is, and we write p in the form $p = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and one of a, b is odd. Observe that $p^2 = 2 \implies a^2 = 2b^2 \implies 2$ divides $a \implies 2$ divides b CaC ■

For the sake of our discussion below, we will use $\mathbb{Q}^+$ instead of $\mathbb{Q}$ as our universal. Now, we divide the "rational numbers line" in half at the point $\sqrt{2}$, and have two subdivisions $A = \{x \in \mathbb{Q}^+ : x^2 < 2\}, B = \{x \in \mathbb{Q}^+ : x^2 > 2\}$

Axiom 1.1.2. Let S be an ordered set and X be a subset of S. Axiomatically define

$$\max X \in X \text{ and } \forall x \in X, x \leq \max X \tag{1.1}$$

$$\min X \in X \text{ and } \forall x \in X, \min X \leq x \tag{1.2}$$

Theorem 1.1.3. $\max A$ and $\min B$ both doesn't exist.

Proof. We wish to construct a function $q(p)$ on $\mathbb{Q}^+$ such that for all $p \in \mathbb{Q}^+$, we have $p^2 < 2 \implies p^2 < q^2 < 2$ and have $2 < p^2 \implies 2 < q^2 < p^2$. Notice $p < q \iff p^2 < q^2$, so we can translate the wanted property of q into

$$p^2 < 2 \implies p < q \text{ and } q^2 < 2 \tag{1.3}$$

$$p^2 > 2 \implies q < p \text{ and } 2 < q^2 \tag{1.4}$$

Let a, b be two function of p on $\mathbb{Q}^+$. To satisfy the above properties, we can let the below equation first be true and then solve for a, b.

$$q - p = \frac{2-p^2}{a} \tag{1.5}$$

$$q^2 - 2 = \frac{p^2-2}{b} \tag{1.6}$$

Now we solve for a, b

$$q - p = \frac{2-p^2}{a} \text{ and } q^2 - 2 = \frac{p^2-2}{b} \implies q = \frac{2-p^2}{a} + p \text{ and } q^2 = \frac{p^2-2}{b} + 2 \tag{1.7}$$

$$\iff [\frac{2-p^2}{a} + p]^2 = \frac{p^2-2}{b} + 2 \tag{1.8}$$

$$\iff \frac{(2-p^2)^2}{a^2} + \frac{2p(2-p^2)}{a} + p^2 = \frac{p^2-2}{b} + 2 \tag{1.9}$$

$$\iff (p^2-2)^2(\frac{1}{a^2}) + (p^2-2)(-\frac{2p}{a} + 1 - \frac{1}{b}) = 0 \tag{1.10}$$

$$\iff \frac{p^2-2}{a^2} - \frac{2p}{a} + 1 - \frac{1}{b} = 0 \text{ (because } p^2 - 2 \neq 0) \tag{1.11}$$

$$\iff \frac{p^2 - 2 - 2ap + a^2}{a^2} = \frac{1}{b} \tag{1.12}$$

$$\iff b = \frac{a^2}{p^2 - 2 - 2ap + a^2} = \frac{a^2}{(p-a)^2 - 2} \tag{1.13}$$

Define $a := p + c$ where $c^2 > 2$, and we are finished. ■

Now, we come back to define the concept of ordered set.

Definition 1.1.4. (Ordered Set Axioms) S is an ordered set if there is a relation $\sim$ on it that satisfy

$$\forall x \in S, x \not\sim x \tag{1.14}$$

$$\forall x, y \in S, x \neq y \implies x \sim y \text{ exclusively or } y \sim x \tag{1.15}$$

$$\forall x, y, z \in S, x \sim y \text{ and } y \sim z \implies x \sim z \tag{1.16}$$

From now on, we write this relation as $<$ and if we write $x > y$, we mean $y < x$.

To discuss the uncompleteness of rational numbers, which is an ordered set, we first define a few concepts brought by concept of ordered set.

Definition 1.1.5. Let S be an ordered set and $E \subseteq S$. E is bounded above if

$$\exists a \in S, \forall b \in E, a \geq b \tag{1.17}$$

In this case, we say a is an upper bound of E and E is bounded above by a. On the other hand, E is bounded below by c if

$$\forall b \in E, c \leq b \tag{1.18}$$

Before we give the definition of supremum, aka least upper bound, we first prove a theorem about it.

Theorem 1.1.6. If x is the smallest upper bound of a bounded above nonempty set E, then any number smaller than x is not an upper bound of E, and every upper bound of E is greater than or equal to x.

Proof. Let A be the set of upper bounds of E. Arbitrarily pick an m such that $m < x$. Assume $\forall z \in E, m > z$. We see $m \in A$, and because $x = \min A$, we see $x \leq m$ CaC . Assume $\exists n \in A, n < x$. Then $\exists z \in E, n < z$, which implies $n \notin A$ CaC ■

Definition 1.1.7. (Definition of Supremum and Infimum) Let A, B respectively be the set of upper bounds of E and the set of lower bounds of E. We define

$$\sup E := \min A \tag{1.19}$$

and

$$\inf E := \max B \tag{1.20}$$

if they ever exist.

Theorem 1.1.8. Let A be a subset of ordered set S. If $\max A$ exists, then $\max A = \sup A$. Similarly, if $\min A$ exists, then $\min A = \inf A$

Proof. $\max A$ is an upper bound and $\min A$ is an lower bound hold true by definition. Any number smaller than $\max A$ can not be an upper bound since $\max A \in A$. Similarly, and number greater than $\min A$ can not be an lower bound since $\min A \in A$ ■

Now, we look back to our subdivisions $A = \{x \in \mathbb{Q}^+ : x^2 < 2\}, B = \{x \in \mathbb{Q}^+ : x^2 > 2\}$. We first show that B is exactly the set of all upper bounds of A.

Theorem 1.1.9. Given $A = \{x \in \mathbb{Q}^+ : x^2 < 2\}, B = \{x \in \mathbb{Q}^+ : x^2 > 2\}$. We have

$$B = \{x \in \mathbb{Q}^+ : \forall y \in A, y \leq x\} \tag{1.21}$$

Proof. Arbitrarily pick $x \in B$, and we see $\forall y \in A, y^2 < 2 < x^2$. Then $\forall y \in A, y < x$. This implies $B \subseteq \{x \in \mathbb{Q}^+ : \forall y \in A, y \leq x\}$. Let x satisfy $\forall y \in A, y \leq x$. Assume $x^2 < 2$. We immediately see $x = \max A$, but $\max A$ doesn't exist CaC ■

By Theorem 1.1.3, we then can see that $\sup A$ does not exist. Now, we give this idea a name.

Definition 1.1.10. (Definition of Completed Ordered Set) An ordered set S satisfy least-upper-bound property if

$$E \subseteq S \text{ and } E \neq \varnothing \implies \sup E \text{ exists} \tag{1.22}$$

Also, we say S is completed.

Obviously, we can see $\mathbb{Q}$ as an ordered set doesn't satisfy the least-upper-bound property. Before we close this section, we reveal the face of the twin brother of the least-upper-bound property. In fact, it is more like the mirror self of the property, since they are equivalent.

Theorem 1.1.11. (LUB $\iff$ GLB) If S satisfy the least-upper-bound property, then S satisfy the greatest-lower-bound property; that is, every bounded below nonempty subset of S have an infimum.

Proof. Let B be the bounded below nonempty subset of S. Let L be the set of lower bounds of B; that is $L = \{x \in S : \forall y \in B, x \leq y\}$. Because B is bounded below, we know L is nonempty. Thus, because S satisfy the least-upper-bound property, we know $\sup L$ exists. Now, we show $\inf B = \sup L$. Assume $\exists b \in B, \sup L > b$. By the definition of L we see b is an upper bound of L CaC . This indicate that $\sup L$ is an lower bound of B, since $\forall b \in B, \sup L \leq b$. Assume $\exists c, \forall b \in B, \sup L < c \leq b$. Because $\forall b \in B, c \leq b$, so we know $c \in L$ CaC . This indicate that $\sup L$ is the greatest lower bound of B. (done) ∎

1.2 Ordered Fields

In this section, we first give the definition of ordered fields, and prove basic result concerning positivity. Notice in this section that x, y, z are all in $\mathbb{F}$.

Definition 1.2.1. (Ordered Field Axioms) An ordered field $\mathbb{F}$ is a field that is not only a ordered set, but also satisfy the following axioms

$$y < z \implies x + y < x + z \tag{1.23}$$

$$x > 0 \text{ and } y > 0 \implies xy > 0 \tag{1.24}$$

Theorem 1.2.2. (Negate reverse positivity) $(x > 0 \iff -x < 0)$ and $(x < 0 \iff -x > 0)$

Proof. Observe $0 < x \implies 0 + (-x) < x + (-x) \implies -x < 0$, and observe $-x < 0 \implies -x + x < 0 + x \implies 0 < x$. Obviously $x = 0 \iff -x = 0$. Then $x < 0 \iff -x > 0$ follows. ∎

Theorem 1.2.3. (Multiply a negative number reverse positivity) Given $y < 0$, we have

$$(x > 0 \iff xy < 0) \text{ and } (x < 0 \iff xy > 0) \tag{1.25}$$

Proof. First observe $y < 0 \implies -y > 0$. Now observe $x > 0 \implies x(-y) > 0 \implies -xy > 0 \implies xy < 0$. Observe $x < 0 \implies x(-y) < 0 \implies -xy < 0 \implies xy > 0$. Obviously $xy = 0 \iff x = 0$. Then the Theorem follows. ■

Theorem 1.2.4. (Multiply on both side) Given $y < z$, we have

$$(x > 0 \iff xy < xz) \text{ and } (x < 0 \iff xy > xz) \tag{1.26}$$

Proof. First observe $y < z \implies z - y > 0$. Now observe $x > 0 \implies x(z-y) > 0 \implies xz - xy > 0 \implies xz > xy$. Observe $x < 0 \implies x(z-y) < 0 \implies xz < xy$. Obviously $x = 0 \iff xy = xz$. Then the Theorem follows. ■

Theorem 1.2.5. (Squares are nonnegative) $x \neq 0 \implies x^2 > 0$

Proof. If $x > 0$, then $x^2 > 0$ follows from the axiom. If $x < 0$, then $x^2 < 0$ follows from Theorem 1.2.2. ■

Corollary 1.2.6. $1 > 0$

Notice that the definition of natural power is given arithmetically; that is, the definitions of $x^2 := (x)(x), x^3 := (x)(x)(x)$, etc, are of no dispute. However, if we were to define $x^{-2} := x^{-1}x^{-1}$, we must realize 0^{-1} does not exist and realize we have not yet prove some common inequalities concerning integer powers before the following definition. These common inequality will be proven after the definition of negatives power and the proof of some properties of integer power inherited from those of natural power. Notice that those properties of natural power are arithmetic and that the base of power x can be any nonzero number.

Definition 1.2.7. (Definition of Inverse) For all nonzero x and naturals p, we define $x^{-p} := (x^{-1})^p$, and define $x^0 := 1$

Theorem 1.2.8. (Integer Power addition written in multiplication) For all nonzero x and integers p, q, we have

$$x^{p+q} = x^p x^q \tag{1.27}$$

Proof. If p, q are both positive, this is arithmetically true. If p, q are both negative, observe $x^p x^q = (x^{-1})^{-p}(x^{-1})^{-q} = (x^{-1})^{-(p+q)} = x^{p+q}$, where the last equality hold true because $p + q < 0$. If $p > 0 > q$ and $p + q > 0$, observe $x^p x^q = x^p (x^{-1})^{-q} = x^{p-(-q)} = x^{p+q}$. If $p > 0 > q$ and $p + q < 0$, observe $x^p x^q = x^p (x^{-1})^{-q} = (x^{-1})^{-(q+p)} = x^{p+q}$, where the last equality hold true because $p + q < 0$. ■

Theorem 1.2.9. (Integer Power multiplication written in power of power of base) For all nonzero x and integers p, q, we have

$$x^{pq} = (x^p)^q = (x^q)^p \tag{1.28}$$

Proof. If p, q are both positive, this is arithmetically true. If any of p, q are zero, the proof is trivial. If $p < 0 < q$, observe $(x^p)^q = ((x^{-1})^{-p})^q = (x^{-1})^{-pq} = x^{pq}$, where the last equality hold true because $pq < 0$, and observe $(x^q)^p = ((x^q)^{-1})^{-p} = ((x^{-1})^q)^{-p} = (x^{-1})^{-qp} = x^{qp}$, where the second equality hold true algebraically. ■

Now we prove the common inequalities concerning only positive base, unlike the above properties concerning all nonnegative base.

Theorem 1.2.10. (Inequality when base is fixed) Given a positive a and two integer x, y where $x < y$, we have

$$\begin{cases} a^x < a^y \iff a > 1 \\ a^x = a^y \iff a = 1 \\ a^x > a^y \iff 0 < a < 1 \end{cases} \tag{1.29}$$

Proof. Observe by Theorem 1.2.3, we know $1 < a \iff 1 < a < a^2 \iff 1 < a < a^2 < a^3 \iff \cdots \iff 1 < a < \cdots < a^{y-x} \iff a^x < a^y$. If $a = 1$, we know $a^x = 1 = a^y$. And again by Theorem 1.2.3, we know $a < 1 \iff a^2 < a < 1 \iff \cdots \iff a^{y-x} < \cdots < 1 \iff a^y < a^x$. ■

Theorem 1.2.11. (Inequality when integer power is fixed) Given $0 < b < c$ and $z \in \mathbb{Z}$, we have

$$\begin{cases} b^z < c^z \iff 0 < z \\ b^z = c^z \iff 0 = z \\ b^z > c^z \iff 0 > z \end{cases} \tag{1.30}$$

Proof. Observe that because b, c are positive and $b < c$, we can deduce $b^z < c^z \iff 1 < (\frac{c}{b})^z \iff 0 < z$ and deduce $b^z > c^z \iff 1 > (\frac{c}{b})^z \iff z < 0$. Then the Theorem follows. ■

Theorem 1.2.12. (Positivity of integer power) If $a > 0$, then $\forall x \in \mathbb{Z}, a^x > 0$. If $a < 0$, then $a^x > 0 \iff 2|x$

Proof. If $a > 0$, then by axiom we know for all nonnegative integer x that $a^x > 0$, and to see $a^{-x} > 0$, assume a^{-x} is not positive, and see $a^x a^{-x} = 1 > 0$ draw a contradiction. The latter result is a direct consequence of Theorem 1.2.4 and Theorem 1.2.2. ■

Notice that if the base is negative, the inequalities can all be deduced by the above theorems with a little effort, although the results are quite messy.

1.3 Real Numbers Field

Although the title of this section is "Real Numbers Field", here, we will not construct the real numbers field, nor use any common property of real numbers. In fact, we will not even use the symbol $\mathbb{R}$ in this section, since we are merely proving theorems about an ordered field with least-upper-bound property. We don't know if there exists any ordered field with least-upper-property. Let's say there does; yet, we don't know if such structure is unique. Let's say it is unique; yet, we don't know if that structure have relation with $\mathbb{R}$. Here, we will use the symbol $\mathbb{F}$ to denote an ordered field with least-upper-bound property. One should realize that we can use algorithm to define a subset containing $1 \in \mathbb{F}$ that is isomorphic to $\mathbb{N}$, and thereby we abuse the notation to denote that subset $\mathbb{N}$. A subfield of $\mathbb{F}$ isomorphic to $\mathbb{Q}$ can also be defined after we define $\mathbb{Z}$, so we also thereby abuse the notation to denote that subfield $\mathbb{Q}$.

Theorem 1.3.1. $\mathbb{N}$ is unbounded above.

Proof. Assume $\mathbb{N}$ is bounded above. Because $1 > 0$, we know $\sup \mathbb{N} - 1 < \sup \mathbb{N}$. Then $\sup \mathbb{N} - 1$ is not an upper bound of $\mathbb{N}$. Arbitrarily pick any $m \in \mathbb{N}$ greater than $\sup \mathbb{N} - 1$. We see $m > \sup \mathbb{N} - 1 \implies m + 1 > \sup \mathbb{N}$, where $m + 1 \in \mathbb{N}$ CaC ■

Corollary 1.3.2. Both $\mathbb{Z}$ and $\mathbb{Q}$ are unbounded both above and below.

Corollary 1.3.3. Given any $x \in \mathbb{F}$, there exists $n \in \mathbb{Z}$ such that $n \leq x < n + 1$

Proof. If $x > 0$, let $S = \{n \in \mathbb{N} : n > x\}$. Notice $S = \varnothing$ implies $\mathbb{N}$ is bounded above by x, so S is nonempty. Then by well-ordering principle, we know $\min S$ exists. We now show $(\min S - 1) \leq x < (\min S - 1) + 1$.

Observe that $\min S \in S \implies x < \min S \implies x < (\min S - 1) + 1$.

Assume $\min S - 1 > x$. We immediately see $\min S - 1 \in S$ CaC (done) .

If $x < 0$, let $S = \{n \in \mathbb{N} : n \geq -x\}$. Again, $S = \varnothing$ implies $\mathbb{N}$ is bounded above by $-x$, so S is nonempty. Then by well-ordering principle, we know $\min S$ exists. We now show $-\min S \leq x < -\min S + 1$.

Observe that $\min S \in S \implies \min S \geq -x \implies x \geq -\min S$.

Assume $-\min S + 1 \leq x$. Then $\min S - 1 \geq -x > 0$; thus $\min S - 1 \in S$ CaC (done)

If $x = 0$, then we let $n = 0$. ■

Theorem 1.3.4. (Archimedean Property) Given $x, y \in \mathbb{F}$ and $0 < x$, there exists $n \in \mathbb{N}$ such that $nx > y$

Proof. Because $\mathbb{N}$ is unbounded above, we know $\frac{y}{x}$ can not be an upper bound of $\mathbb{N}$, so we know $\exists n \in \mathbb{N}, n > \frac{y}{x}$. Then because $x > 0$, we can deduce $nx > y$. ■

Theorem 1.3.5. ($\mathbb{Q}$ is dense in $\mathbb{F}$) Given $x, y \in \mathbb{F}$ and $x < y$, we know there exists $p \in \mathbb{Q}$ such that $x < p < y$

Proof. Every rational, positive or negative, can be expressed in the form $\frac{m}{n}$ for some integer m and naturals n. We seek to find some integer m and n such that $x < \frac{m}{n} < y$. Notice that $x < \frac{m}{n} < y \iff nx < m < ny$. Because m has to be an integer, we know for $nx < m < ny$ to hold true, we must first have $ny - nx > 1$. Because $y - x > 0$, by Archimedean Property, there exists $n \in \mathbb{N}$ such that $ny - nx = n(y - x) > 1$. By Corollary 1.3.2, we know there exists $m \in \mathbb{Z}$ such that $m \leq ny < m + 1$.

Notice $m = ny$ if and only if $y \in \mathbb{Q}$. So we can split the proof into two cases.

Case 1: $y \in \mathbb{Q}$

We see that the set $\{r \in \mathbb{Q} : r < y\}$ have supremum y, since if there exists upper bound less than y, say q, we know $\frac{q+y}{2}$ is in the set and greater than its upper bound q. Then $x < y$ tell us x is not an upper bound of the set, then we can pick some rational r in the set greater than x, so $x < r < y$ (done) .

Case 2: $y \notin \mathbb{Q}$

We know $m < ny < m + 1$. $ny < n + 1$ tell us $nx < ny - 1 < m$, so $nx < m < ny$ (done) ■

Theorem 1.3.6. (Positive root of power uniquely exists) For all natural n and $y > 0$, there exists one and only one positive x such that $x^n = y$

Proof. By Theorem 1.2.5, we know for two different positive numbers $0 < x < x'$, their n-th power are different, being $0 < x^n < (x')^n$, so if such positive power exists, it must be unique.

We have handled the uniqueness part of the proof. Denote $E := \{m \in \mathbb{F}^+ : m^n < y\}$ and $x := \sup E$. Now we do the existence part by proving x exists and $x^n = y$.

To show $x = \sup\{m \in \mathbb{F}^+ : m^n < y\}$ exists, we only have to show the set $\{m \in \mathbb{F}^+ : m^n < y\}$ is nonempty and bounded above. In other word, we wish to construct function $a \in \mathbb{F}^+$ and b of y such that for all positive input $y > 0$, we have $a^n < y$ and $(m^n < y \longrightarrow m < b)$.

In the followings, the domain of a and b are only positives.

First we construct a. By Theorem 1.2.7, we know if $a < \min\{1, y\}$, then $a^n < a < y$, so we construct a such that $0 < a < \min\{1, y\}$. Notice that a must be positive because we are constructing a number in E, where E contain only positives. Express a in the form $a = \frac{p}{q}$ where p, q are both function of y. In the process of construction, We must be careful to make sure a exists for all positive y.

To satisfy $0 < a$, we need only guarantee p, q are always of the same sign for all positive y. Obviously, if such p, q exists, we can change both sign of p, q when they are negative, and we will get two nonnegative function, so we can just require p, q to be positive for all positive y.

To satisfy $a < 1$, observe $a < 1 \iff \frac{p}{q} < 1 \iff p < q$, since we require q to be positive when y is positive. The easiest construction is to let $q = p + c$ where c is positive.

To satisfy $a < y$, observe $a < y \iff \frac{p}{q} < y \iff p(y-1) + cy = qy - p > 0$. The easiest construction is to let $p(y-1) + cy = y^2$, which is possible, if we let $p = y$ and $c = 1$. In this case $p = y > 0$ and $q = y + 1 > 0$, and $a = \frac{y}{y+1}$. We finished proving E is nonempty. **(Notice $c = y^2, p = y^3, q = y^3 + y^2, a = \frac{y^3}{y^3+y^2}$ also do the trick)**

Now we construct b. By Theorem 1.2.5, we know if $0 < b$ and $0 < m^n < b^n$, then $m < b$, so we construct b such that $y < b^n$ which lead to $0 < m^n < y < b^n$ if $m^n < y$. Because $y > 0$, this is fairly easy. Simply let $b = y + 1$, so we have $b > 1$ and $b > y$; thus by Lemma 1.3.1, we have $b^n > b > y$, finishing proving E is bounded above, where $b = y + 1$ is an upper bound. (done)

To show $x^n = y$, we show $x^n \not< y$ and $x^n \not> y$. Obviously we are going to assume the $x^n < y$ or $x^n > y$, but before we do such, let's see what property from which can we possibly draw contradiction. Notice that because we just prove the existence of the supremum of E, we haven't use the fact that $x = \sup E$ in anywhere of our proof. We know

$$x = \sup E \iff \forall d > 0, \begin{cases} x + d \notin E \text{ (x is an upper bound)} \\ \text{and} \\ x - d \text{ is not an upper bound of } E \text{ (the \textit{least} upper bound)} \end{cases}$$

So, you see, we wish to construct h and k such that if we assume $x^n < y$ or $x^n > y$ we can draw $x + h \in E$ or $x - k$ is an upper bound of E.

Observe $x + h \in E \iff (x+h)^n < y \iff (x+h)^n - x^n < y - x^n$, and observe $x - k$ is an upper bound of $E \iff (m^n < y \longrightarrow m < x - k) \iff (m \geq x - k \longrightarrow m^n \geq$

$y) \iff (m \geq x-k \longrightarrow x^n - m^n \leq x^n - y)$.

Notice that the act of subtracting x^n at the both side of the inequality play an important role in our proof: not only does the act allow us to use the identity $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$, and the act also tell us between $x+h \in E$ and $x-k$ is an upper bound of E, which contradiction statement should we draw from $x^n > y$. If $y - x^n < 0$, then $y - x^n < 0 < (x+h)^n - x^n$, so we can not possibly draw $x+h \in E$ from $x^n > y$.

Assume $x^n > y$. We wish to construct positive k such that $m \geq x-k \longrightarrow x^n - m^n \leq x^n - y$, so we can draw the contradiction $x-k$ is an upper bound of E.

Notice that $m \geq x-k \implies x^n - m^n \leq x^n - (x-k)^n$, so if $x^n - (x-k)^n \leq x^n - y$, our proof at this part is finished. Now our job is to single out the k in the inequality to give an condition such that $x^n - (x-k)^n \leq x^n - y$ hold if the condition hold. It is easy to see that computing the polynomial of k on left hand side of inequality and to prove such positive k exists for all n is almost impossible. Thus, we take a possible but actually non-existing risk in our next step of the proof. Use the identity and that $x-k < x$ to deduce

$$x^n - (x-k)^n = k(x^{n-1} + x^{n-2}(x-k) + \cdots + (x-k)^{n-1}) \leq knx^{n-1} \tag{1.31}$$

So, if we have $knx^{n-1} \leq x^n - y$, which is equivalent to $k \leq \frac{x^n - y}{nx^{n-1}}$, our proof is partially finished. Notice that $x^n - y > 0$ and $nx^{n-1} > 0$, so $\frac{x^n-y}{nx^{n-1}} > 0$; thus the positive k we desire has been constructed. (done) CaC **(The reason I use the word "possible risk" is that if we use an identity that show us $x^n - (x-k)^n$ smaller than a quantity greater than $x^n - y$, the proof can not be done.)**

Assume $x^n < y$. We wish to construct positive h such that $(x+h)^n - x^n < y - x^n$, so we can draw the contradiction $x + h \in E$.

Again, we use the same identity to deduce

$$(x+h)^n - x^n = h((x+h)^{n-1} + (x+h)^{n-2}x + \cdots + x^{n-1}) < hn(x+h)^{n-1} \tag{1.32}$$

To single out the h in the $hn(x+h)^{n-1}$, notice that we can take the risk to add the constraint $h < 1$ at the end of our construction to have $(x+h)^n - x^n < hn(x+h)^{n-1} < hn(x+1)^{n-1}$. Then, if we have $hn(x+1)^{n-1} < y - x^n$, which is equivalent to $h < \frac{y-x^n}{n(x+1)^{n-1}}$, our proof is finished. To sum up, any h satisfy $h < \min\{1, \frac{y-x^n}{n(x+1)^{n-1}}\}$ does the trick, and such h exists, since $0 < \min\{y - x^n, n(x+1)^{n-1}\}$. (done) CaC (done) ■

Definition 1.3.7. The number x in Theorem 1.3.4 is written $x = \sqrt[n]{y}$ or $x = y^{\frac{1}{n}}$.

The above theorem is by far the trickiest we have seen. Often the theorem is proven only in special case $\sqrt{2}$ as a classical example in the first class of analysis. Here, we prove a general result. The following theorem is to make sure the definition of rational power make sense. Like in the last section that after we define integer power we prove some properties inherited from those of natural power, we here prove some properties inherited from those of integer power. And of course, the common inequalities of rational power, also inherited from those of integer power, will be proven after those properties.

About the coverage of definition, notice that we didn't and won't define $y^{\frac{1}{n}}$ when y is negative. Also, notice that for all nonzero rational s, we can define $0^s = 0$.

Theorem 1.3.8. Given $m, p \in \mathbb{Z}$ and $n, q \in \mathbb{N}$ and $a > 0$ and $\frac{m}{n} = \frac{p}{q}$, we have

$$(a^m)^{\frac{1}{n}} = (a^p)^{\frac{1}{q}} \tag{1.33}$$

Proof. Observe

$$\begin{align} x &= (a^m)^{\frac{1}{n}} \tag{1.34}\\ \iff x^n &= a^m \tag{1.35}\\ \iff (x^n)^q &= (a^m)^q \tag{1.36}\\ \iff x^{nq} &= a^{mq} = a^{np} \text{ (because } n, m, q \in \mathbb{Z}) \tag{1.37}\\ \iff (x^q)^n &= (a^p)^n \text{ (again, because } n, p, q \in \mathbb{Z}) \tag{1.38}\\ \iff x^q &= a^p \text{ (by Theorem 1.3.4)} \tag{1.39}\\ \iff x &= (a^p)^{\frac{1}{q}} \text{ (by Theorem 1.3.4)} \tag{1.40}\\ \iff (a^m)^{\frac{1}{n}} &= x = (a^p)^{\frac{1}{q}} \tag{1.41} \end{align}$$

■

Definition 1.3.9. (Definition of Rational Powers) Given a rational $r = \frac{p}{q}$, where $q \in \mathbb{N}$. For all a, we define $a^r = (a^p)^{\frac{1}{q}}$

Theorem 1.3.10. (Rational Power addition written in multiplication, inherited form Theorem 1.2.5 and Theorem 1.2.6) Given $r, s \in \mathbb{Q}$ and $a > 0$, we have

$$a^{r+s} = a^r a^s \tag{1.42}$$

Proof. Express r, s in the form $r = \frac{p}{q}, s = \frac{m}{n}$ where $q, n \in \mathbb{N}$ and $p, m \in \mathbb{Z}$. Observe

$$\begin{align} (a^{r+s})^{nq} &= (a^{\frac{np+mq}{nq}})^{nq} \tag{1.43}\\ &= a^{np+mq} \tag{1.44} \end{align}$$

And observe

$$
\begin{aligned}
(a^r a^s)^{nq} &= (a^{\frac{p}{q}} a^{\frac{m}{n}})^{nq} && (1.45)\\
&= (a^{\frac{p}{q}})^{nq}(a^{\frac{m}{n}})^{nq} \text{ (because } nq \in \mathbb{N}) && (1.46)\\
&= ((a^{\frac{p}{q}})^q)^n((a^{\frac{m}{n}})^n)^q && (1.47)\\
&= (a^p)^n(a^m)^q && (1.48)\\
&= a^{np+mq} = (a^{r+s})^{nq} \text{ (by Theorem 1.2.5 and Theorem 1.2.6)} && (1.49)
\end{aligned}
$$

Because the rational power of a positive must also be positive, we can deduce $a^r a^s = a^{r+s}$ by Theorem 1.3.4 ■

Theorem 1.3.11. (Rational Power of Rational Power written in power multiplication, inherited from Theorem 1.2.6) Given $r, s \in \mathbb{Q}$ and $a > 0$, we have

$$(a^r)^s = a^{rs} \tag{1.50}$$

Proof. Express r, s in the form $r = \frac{p}{q}, s = \frac{m}{n}$ where $q, n \in \mathbb{N}$ and $p, m \in \mathbb{Z}$. Observe

$$
\begin{aligned}
(a^{rs})^{nq} &= (a^{\frac{mp}{nq}})^{nq} && (1.51)\\
&= a^{mp} && (1.52)
\end{aligned}
$$

And observe

$$
\begin{aligned}
((a^r)^s)^{nq} &= (((a^{\frac{p}{q}})^{\frac{m}{n}})^n)^q && (1.53)\\
&= ((a^{\frac{p}{q}})^m)^q && (1.54)\\
&= (a^{\frac{p}{q}})^{mq} \text{ (by Theorem 1.2.6)} && (1.55)\\
&= ((a^{\frac{p}{q}})^q)^m \text{ (by Theorem 1.2.6)} && (1.56)\\
&= (a^p)^m = a^{mp} = (a^{rs})^{nq} \text{ (by Theorem 1.2.6)} && (1.57)
\end{aligned}
$$

■

Corollary 1.3.12. $a^{\frac{q}{p}} = (a^{\frac{1}{p}})^q$

Now comes the inequalities about rational power concerning only positive base, since there is no definition of rational power on negative base.

Theorem 1.3.13. (Inequality when base is fixed) Given a positive a and two rational x, y where $x < y$, we have

$$
\begin{cases}
a^x < a^y \iff a > 1\\
a^x = a^y \iff a = 1\\
a^x > a^y \iff 0 < a < 1
\end{cases} \tag{1.58}
$$

Proof. Express $y-x=\frac{q}{p}$ where p is an natural and q is an integer. Observe that $a>1 \implies a^{\frac{1}{p}}>1$, since if $a^{\frac{1}{p}}<1$, by Theorem 1.2.7, we can deduce $a=(a^{\frac{1}{p}})^p<(a^{\frac{1}{p}})^0=1$. Then, we can deduce $a>1 \implies a^{\frac{1}{p}}>1 \implies a^{\frac{q}{p}}>1 \implies a^{y-x}>1 \implies a^y>a^x$, where at second implication, Theorem 1.2.7 again kick in again. It is clear that if $a=1$, then $a^x=a^y$. Observe that $a<1 \implies a^{\frac{1}{p}}<1$, since if $a^{\frac{1}{p}}>1$, by Theorem 1.2.7, we can deduce $a=(a^{\frac{1}{p}})^p>(a^{\frac{1}{p}})^0=1$. Then, we can deduce $a<1 \implies a^{\frac{1}{p}}<1 \implies a^{\frac{q}{p}}<1 \implies a^{y-x}<1 \implies a^y<a^x$. The Theorem then follows the three implications. ■

Theorem 1.3.14. (Inequality when rational power is fixed) Given $0<b<c$ and $z\in\mathbb{Q}$, we have

$$\begin{cases} b^z<c^z \iff 0<z \\ b^z=c^z \iff 0=z \\ b^z>c^z \iff 0>z \end{cases} \tag{1.59}$$

Proof. Express $z=\frac{q}{p}$, where q is an integer and p is a natural. Notice q and z are of the same sign. If $q>0$, we can deduce $0<b<c \implies 1<\frac{c}{b} \implies 1<(\frac{c}{b})^{\frac{1}{p}}$, since if $(\frac{c}{b})^{\frac{1}{p}}>1$, then by Theorem 1.2.7, we can deduce $\frac{c}{b}=((\frac{c}{b})^{\frac{1}{p}})^p>(\frac{c}{b})^{\frac{1}{p}}>1$. Again by Theorem 1.2.7, we can deduce $1<(\frac{c}{b})^{\frac{1}{p}} \implies 1<(\frac{c}{b})^{\frac{q}{p}} \implies 1<(\frac{c}{b})^z \implies b^z<c^z$. If $q=0$, it is clear $b^z=1=c^z$. If $q<0$, we can deduce $0<b<c \implies 1<\frac{c}{b} \implies 1<(\frac{c}{b})^{\frac{1}{p}} \implies 1=((\frac{c}{b})^{\frac{1}{p}})^0>((\frac{c}{b})^{\frac{1}{p}})^q=(\frac{c}{b})^{\frac{q}{p}} \implies 1>(\frac{c}{b})^z \implies b^z>c^z$. ■

After the rational power, we now try to define real power, which of course heavily rely on completeness property. The definition will be split into two parallel part, each definition have a lemma beforehand to guarantee the definition exists. The properties inherited from those of rational power will be proven as soon as it can be proven, and the common inequalities will be proven last. Notice that we still don't define $y^{\frac{1}{n}}$ when y is negative.

Lemma 1.3.15. Given $b>1$, for $x\in\mathbb{F}$, define $B(x):=\{b^t : t\in\mathbb{Q}, t\leq x\}$. Then $\forall x\in\mathbb{F}, \sup B(x)$ exists.

Proof. For all x, we know $B(x)$ is nonempty, since if not, $\mathbb{Q}$ is bounded below. Because $\mathbb{Q}$ is nonbounded above, we can pick a rational y greater than x, and observe that $t\leq x \implies t\leq y$. Then because $b>1$, we deduce $\forall b^t\in B(x), b^t\leq b^y$; thus b^y is an upper bound of $B(x)$. ■

Definition 1.3.16. (The First Half of Real Power Definition) For all $b,x\in\mathbb{F}$ where $b>1$, we define $b^x:=\sup B(x)$, where B is the function in Lemma above.

The above definition is in fact not very appropriate, since we have already define b^x where $x\in\mathbb{Q}$. We don't know if the above definition is consistent with our old definition. The next theorem is to show they are.

Theorem 1.3.17. (Consistency of power definitions) If $b > 1$ and $r \in \mathbb{Q}$, then $b^r = \sup B(r)$

Proof. Because $1 < b$, we know $b^r = \max B(r)$, then $\sup B(r) = \max B(r) = b^r$ ■

Now, we are going to prove that the definition of real power do inherit the properties of rational power (i.e. Theorem 1.3.6 and Theorem 1.3.7), but before that, we will prove a general result about supremum.

Lemma 1.3.18. Let A, B and be two bounded above subset of $\mathbb{F}$, containing only nonnegative numbers. Define $AB := \{ab : a \in A, b \in B\}$. We have

$$\sup AB = \sup A \sup B \tag{1.60}$$

Proof. Because A, B contain only nonnegative numbers, we know $a \leq \sup A$ and $b \leq \sup B$ implies $ab \leq \sup A \sup B$, so $\sup A \sup B$ is an upper bound of AB. Now we show $\sup A \sup B$ is the *least* upper bound of AB.

Assume there is an upper bound x of AB smaller than $\sup A \sup B$. Express x in the form $x = \sup A \frac{x}{\sup A}$. Because $x < \sup A \sup B$, we know $\frac{x}{\sup A} < \sup B$, which implies there is a number $b \in B$ greater than $\frac{x}{\sup A}$. Observe $b > \frac{x}{\sup A} \implies \frac{x}{b} < \sup A$, which implies that there is a number $a \in A$ greater than $\frac{x}{b}$. Observe $\frac{x}{b} < a \implies x < ab$ CaC (done) ■

Theorem 1.3.19. (Power addition written in multiplication, inherited from Theorem 1.3.6 and Theorem 1.3.7) Given $r, s \in \mathbb{F}$ and $b > 1$, we have

$$b^{r+s} = b^r b^s \tag{1.61}$$

Proof. We prove $B(r + s) = \{xy : x \in B(r) \text{ and } y \in B(s)\}$. Denote the set on right side E. Observe that $xy \in E \implies \exists q \leq r \in \mathbb{Q}$ and $m \leq s \in \mathbb{Q}, x = b^q$ and $y = b^m \implies xy = b^{q+m} \leq b^{r+s} \implies xy \in B(r + s)$. Then we know $E \subseteq B(r + s)$. Given $b^d \in B(r + s)$, we know $d \leq r + s$, so if we express $b^d = b^r b^{d-r}$, we are sure $b^{d-r} \in B(s)$ and $b^r \in B(r)$, which implies $b^d \in E$. Then we can deduce $B(r + s) \in E$. (done)

By Lemma 1.3.2, our proof is finished. ■

Before we prove $(b^r)^s = b^{rs}$ if $b > 1$, we must finish the definition of the reals power, since b^r may be less than 1. Notice that the function A below, is identical to B above.

Lemma 1.3.20. Given $0 < a < 1$, for all $x \in \mathbb{F}$, define $A(x) := \{a^t : t \in \mathbb{Q}, t \leq x\}$. Then $\forall x \in \mathbb{F}, \inf A(x)$ exists.

Proof. For all x, we know $A(x)$ is nonempty, since if not, $\mathbb{Q}$ is bounded below. Because $\mathbb{Q}$ is nonbounded above, we can pick a rational y greater than x, and observe that $t \leq x \implies t \leq y$. Then because $0 < a < 1$, we deduce $\forall a^t \in A(x), a^t \geq a^y$; thus a^y is an lower bound of $A(x)$. ■

Definition 1.3.21. (The Second Half of Real Power Definition) For all $a, x \in \mathbb{F}$ where $0 < a < 1$, we define $a^x := \inf A(x)$, where A is the function in Lemma above.

Theorem 1.3.22. (Consistency of power definitions) If $0 < a < 1$ and $r \in \mathbb{Q}$, then $a^r = \inf A(r)$

Proof. Because $0 < a < 1$, we know $a^r = \min A(r)$, then $\inf A(r) = \min A(r) = a^r$ ■

Lemma 1.3.23. Let A, B and be two bounded below subset of $\mathbb{F}$, containing only nonnegative numbers. Define $AB := \{ab : a \in A, b \in B\}$. We have

$$\inf AB = \inf A \inf B \tag{1.62}$$

Proof. Because A, B contain only nonnegative numbers, we know $a \geq \inf A$ and $b \geq \inf B$ implies $ab \geq \inf A \inf B$, so $\inf A \inf B$ is an lower bound of AB. Now we show $\inf A \inf B$ is the *greatest* lower bound of AB.

If $\inf A = 0$, we know $\inf AB = 0$, since if not, we can arbitrarily pick nonzero $b \in B$ and see for all $a \in A$, we have $a > (\inf AB)b > 0$. Assume there is an lower bound x of AB greater than $\inf A \inf B$. Express x in the form $x = \inf A \frac{x}{\inf A}$. Because $x > \inf A \inf B$, we know $\frac{x}{\inf A} > \inf B$, which implies there is a number $b \in B$ less than $\frac{x}{\inf A}$. Observe $b < \frac{x}{\inf A} \implies \frac{x}{b} > \inf A$, which implies that there is a number $a \in A$ less than $\frac{x}{b}$. Observe $\frac{x}{b} > a \implies x > ab$ CaC (done) ■

Theorem 1.3.24. (Power addition written in multiplication, inherited from Theorem 1.3.6 and Theorem 1.3.7) Given $r, s \in \mathbb{F}$ and $0 < a < 1$, we have

$$a^{r+s} = a^r a^s \tag{1.63}$$

Proof. We prove $A(r+s) = \{xy : x \in A(r) \text{ and } y \in A(s)\}$. Denote the set on right side E. Observe that $xy \in E \implies \exists q \leq r \in \mathbb{Q}$ and $m \leq s \in \mathbb{Q}, x = a^q$ and $y = a^m \implies xy = a^{q+m} \geq a^{r+s} \implies xy \in A(r+s)$. Then we know $E \subseteq A(r+s)$. Given $a^d \in A(r+s)$, we know $d \leq r+s$, so if we express $a^d = a^r a^{d-r}$, we are sure $a^{d-r} \in A(s)$ and $a^r \in A(r)$, which implies $a^d \in E$. Then we can deduce $A(r+s) \in E$. (done)

By Lemma 1.3.4, our proof is finished. ■

Theorem 1.3.25. (Power of Power written in power multiplication, inherited from Theorem 1.3.7) Given $r, s \in \mathbb{F}$ and $a > 0$, we have

$$(a^r)^s = a^{rs} \tag{1.64}$$

Proof. If $a > 1$ and $r, s > 0$, then $(a^r)^s = \sup\{(\sup\{a^t : t \in \mathbb{Q}, t < r\})^u : u \in \mathbb{Q}, u < s\}$ ■

1.4 Exercises

Question 1

Given a nonzero rational r, prove that $r + x$ and rx are irrational.

Question 2

Prove that no rational r satisfy $r^2 = 12$

Question 3

Let E be a nonempty subset of an ordered set; suppose α is a lower bound and β is an upper bound of E. Prove $\alpha < \beta$

Question 4

Let A be a nonempty subset of real numbers which is bounded below. Define $-A := \{-x : x \in A\}$. Prove that

$$\inf A = -\sup(-A) \tag{1.65}$$