Chapter 5

Real Numbers

5.1 Sequences and Search Sequences

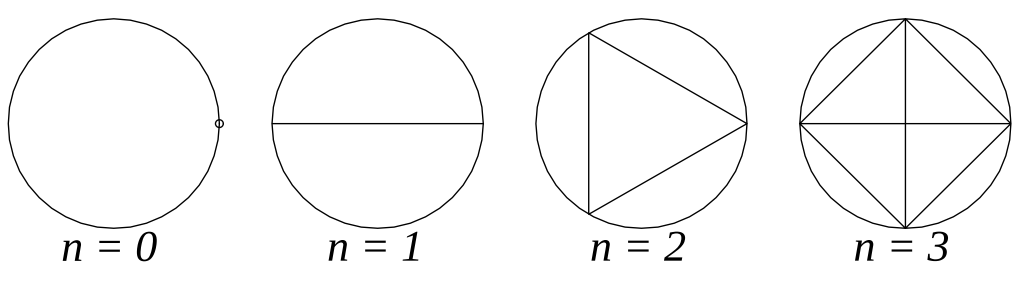
5.1 Definition (Sequence.) Let A be a set. A *sequence in* A is a function $f: \mathbf{N} \to A$. I sometimes denote the sequence f by $\{f(n)\}$ or $\{f(0), f(1), f(2), \cdots\}$. For example, if $f: \mathbf{N} \to \mathbf{Q}$ is defined by $f(n) = \dfrac{1}{n+1}$, I might write

$$f = \left\{\frac{1}{n+1}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots\right\}.$$

5.2 Warning. The notation $\{f(0), f(1), f(2), \cdots\}$ is always ambiguous. For example,

$$\{1, 2, 4, 8, 16, \cdots\}$$

might denote $\{2^n\}$. It might also denote $\{\phi(n)\}$ where $\phi(n)$ is the number of regions into which a circle is divided when all the segments joining the vertices of an inscribed regular $(n+1)$-gon are drawn.



5.3 Entertainment. Show that $\phi(4) = 2^4$, but that it is not true that $\phi(n) = 2^n$ for all $n \in \mathbf{N}$.

5.4 Warning. The notation for a sequence and a set are the same, but a sequence is not a set. For example, as sets,

$$\{1, 2, 3, 4, 5, 6, \cdots\} = \{2, 1, 4, 3, 6, 5, \cdots\}.$$

But as sequences,

$$\{1, 2, 3, 4, 5, 6, \cdots\} \neq \{2, 1, 4, 3, 6, 5, \cdots\}.$$

5.5 Notation ($\mathbf{Z}_{\geq k}$) Recall from section 3.65, that If $k \in \mathbf{Z}$, then

$$\mathbf{Z}_{\geq k} = \{n \in \mathbf{Z} : n \geq k\}.$$

Thus, $\mathbf{Z}_{\geq 0} = \mathbf{N}$. Occasionally I will want to consider sequences whose domain is $\mathbf{Z}_{\geq k}$ where $k \neq 0$. I will denote such a sequence by

$$\{f(n)\}_{n \geq k}.$$

Hence, if

$$f = \{1, 2, 3, \cdots\},$$

then $f(n) = n + 1$ for all $n \in \mathbf{N}$, and if

$$g = \{1, 2, 3, \cdots\}_{n \geq 1},$$

then $g(n) = n$ for all $n \in \mathbf{Z}_{\geq 1}$.

5.6 Remark. Most of the results we prove for sequences $\{f(n)\}$ have obvious analogues for sequences $\{f(n)\}_{n \geq k}$, and I will assume these analogues without explanation.

5.7 Examples. $\{i^n\} = \{1, i, -1, -i, 1, i, \cdots\}$ is a sequence in $\mathbf{C}_{\mathbf{Q}}$.

$$\left\{\left[0, \frac{1}{n}\right]\right\}_{n \geq 1} = \left\{[0, 1], \left[0, \frac{1}{2}\right], \left[0, \frac{1}{3}\right], \cdots\right\}$$

is a sequence of intervals in an ordered field F.

5.8 Definition (Open and closed intervals.) An interval J in an ordered field is *closed* if it contains all of its endpoints. J is *open* if it contains none of its endpoints. Thus,

$$\emptyset, [a, b], (-\infty, a], [a, \infty), (-\infty, \infty) \text{ are closed intervals.}$$

$$\emptyset, (a, b), (-\infty, a), (a, \infty), (-\infty, \infty) \text{ are open intervals.}$$

$$(a, b], [a, b) \text{ where } a < b \text{ are neither open nor closed.}$$

5.9 Definition (Binary search sequence.) Let F be an ordered field. A *binary search sequence* $\{[a_n, b_n]\}$ in F is a sequence of closed intervals with end points a_n, b_n in F such that

1) $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ for all $n \in \mathbf{N}$, and

2) $b_n - a_n = \dfrac{b_0 - a_0}{2^n}$ for all $n \in \mathbf{N}$.

Condition 1) is equivalent to

$$a_n \le a_{n+1} \le b_{n+1} \le b_n \text{ for all } n \in \mathbf{N}.$$

5.10 Warning. Note that the intervals in a binary search sequence are closed. This will be important later.

5.11 Definition (Convergence of search sequence.) Let F be an ordered field, let $\{[a_n, b_n]\}$ be a binary search sequence in F, and let $x \in F$. We say $\{[a_n, b_n]\}$ *converges* to x and write $\{[a_n, b_n]\} \to x$ if $x \in [a_n, b_n]$ for all $n \in \mathbf{N}$. We say $\{[a_n, b_n]\}$ *converges*, if there is some $x \in F$ such that $\{[a_n, b_n]\} \to x$. We say $\{[a_n, b_n]\}$ *diverges* if there is no such x.

5.12 Example. Let F be an ordered field. Then $\left\{\left[0, \dfrac{1}{2^n}\right]\right\}$ is a binary search sequence and $\left\{\left[0, \dfrac{1}{2^n}\right]\right\} \to 0$.

5.13 Exercise. Let F be an ordered field, let $a, b \in F$ with $a < b$. Let $m = \dfrac{a+b}{2}$. Show that

1) $a < m < b$.

2) $m - a = b - m = \dfrac{1}{2}(b - a)$.

(Conditions 1) and 2) say that m is the midpoint of a and b.)

5.14 Exercise. Let F be an ordered field and let $a, b \in F$ with $a \le b$ and let c, d be points in $[a, b]$. Show that

$$|c - d| \le b - a;$$

i.e., if two points lie in an interval then the distance between the points is less than or equal to the length of the interval.

5.15 Exercise. Show that $2^n \geq n$ for all $n \in \mathbf{N}$.

5.16 Example (A divergent binary search sequence.) Define a binary search sequence $\{[a_n, b_n]\}$ in $\mathbf{Q}$ by the rules

$$\begin{aligned} [a_0, b_0] &= [1, 2]. \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^2 \geq 2, \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^2 < 2. \end{cases} \end{aligned}$$

Thus,

$$\frac{a_0+b_0}{2} = \frac{1+2}{2} = \frac{3}{2}; \quad \left(\frac{a_0+b_0}{2}\right)^2 = \frac{9}{4} > 2, \text{ so } [a_1, b_1] = \left[\frac{2}{2}, \frac{3}{2}\right];$$

$$\frac{a_1+b_1}{2} = \frac{\frac{2}{2}+\frac{3}{2}}{2} = \frac{5}{4}; \quad \left(\frac{a_1+b_1}{2}\right)^2 = \frac{25}{16} < 2, \text{ so } [a_2, b_2] = \left[\frac{5}{4}, \frac{6}{4}\right];$$

$$\frac{a_2+b_2}{2} = \frac{\frac{5}{4}+\frac{6}{4}}{2} = \frac{11}{8}; \quad \left(\frac{a_2+b_2}{2}\right)^2 = \frac{121}{64} < 2, \text{ so } [a_3, b_3] = \left[\frac{11}{8}, \frac{12}{8}\right].$$

Since $\dfrac{a_n+b_n}{2}$ is the midpoint of $[a_n, b_n]$, we have

$$[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$$

and

$$b_{n+1} - a_{n+1} = \frac{1}{2}(b_n - a_n) \tag{5.17}$$

It follows from (5.17) that

$$b_n - a_n = \frac{1}{2^n}(b_0 - a_0) \text{ for all } n \in \mathbf{N}.$$

Hence $\{[a_n, b_n]\}$ is a binary search sequence. For each $n \in \mathbf{N}$, let $P(n)$ be the proposition

$$P(n) = \text{“}a_n^2 < 2 \leq b_n^2.\text{”}$$

Then $P(0)$ says $1^2 < 2 \leq 2^2$, so $P(0)$ is true. Let $n \in \mathbf{N}$.
If $\left(\dfrac{a_n+b_n}{2}\right)^2 \geq 2$, then

$$\begin{aligned} P(n) &\implies a_n^2 < 2 \leq b_n^2 \implies a_{n+1}^2 = a_n^2 < 2 \leq \left(\frac{a_n+b_n}{2}\right)^2 = b_{n+1}^2 \\ &\implies a_{n+1}^2 < 2 \leq b_{n+1}^2 \\ &\implies P(n+1). \end{aligned}$$

If $\left(\dfrac{a_n+b_n}{2}\right)^2 < 2$, then

$$\begin{aligned} P(n) &\implies a_n^2 < 2 \le b_n^2 \implies a_{n+1}^2 = \left(\frac{a_n+b_n}{2}\right)^2 < 2 \le b_n^2 = b_{n+1}^2 \\ &\implies a_{n+1}^2 < 2 \le b_{n+1}^2 \\ &\implies P(n+1). \end{aligned}$$

Hence, in all cases, $P(n) \implies P(n+1)$, and by induction, $a_n^2 < 2 \le b_n^2$ for all $n \subset \mathbf{N}$. Since $x^2 \neq 2$ for all $x \in \mathbf{Q}$, we have

$$a_n^2 < 2 < b_n^2 \text{ for all } n \in \mathbf{N}. \tag{5.18}$$

I now will show that $\{[a_n, b_n]\}$ diverges. Suppose, in order to get a contradiction, that for some $x \in \mathbf{Q}$, $\{[a_n, b_n]\} \to x$. Then

$$0 \le a_n \le x \le b_n \text{ for all } n \in \mathbf{N},$$

so

$$a_n^2 \le x^2 \le b_n^2.$$

Combining this with (5.18), we get

$$|x^2 - 2| \le b_n^2 - a_n^2 = (b_n - a_n)(b_n + a_n) \le \left(\frac{b_0 - a_0}{2^n}\right)(b_0 + b_0) = \frac{4}{2^n} \tag{5.19}$$

for all $n \in \mathbf{N}$. Since 2 is not a square in $\mathbf{Q}$, $x^2 - 2 \neq 0$. Write $|x^2 - 2| = \dfrac{p}{q}$, where $p, q \in \mathbf{Z}_{\geq 1}$. Then

$$\text{for all } n \in \mathbf{N},\ \frac{p}{q} \le \frac{4}{2^n},$$

so

$$\text{for all } n \in \mathbf{N},\ 2^n \le \frac{4q}{p} \le 4q.$$

By exercise 5.15, for all $n \in \mathbf{N}$,

$$n \le 2^n \le 4q. \tag{5.20}$$

Statement (5.20) is false when $n = 4q + 1$, and hence our assumption that $\{[a_n, b_n]\} \to x$ was false. ‖

5.2 Completeness

5.21 Definition (Completeness axiom.) Let F be an ordered field. We say that F is *complete* if it satisfies the condition:

Every binary search sequence in F converges to a unique point in F.

5.22 Example. The field $\mathbf{Q}$ is not complete, since in example 5.16 we found a binary search sequence in $\mathbf{Q}$ that does not converge.

5.23 Definition (Real field, R.) A *real field* is a complete ordered field. We will use the name $\mathbf{R}$ to denote a real field.

5.24 Remark. It is not at all clear that any real fields exist. If real fields do exist, there is a question of uniqueness; i.e., is it the case that any two real fields are "essentially the same"? I don't want to worry about what mathematical existence means, so let me formulate the questions: Are the axioms for a real field consistent; i.e., is it the case that no contradictions can be derived from them? Note that we are not entirely free to throw axioms together. If I were to make a definition that a *3-field* is an ordered field in which $3 = 0$, I would immediately get a contradiction: $3 = 0$ and $3 > 0$. All I can say about consistency is that no contradictions have been found to follow from the real field axioms. There exist proofs that any two real fields are essentially the same, cf. [35, page 129]. (This source uses a different statement for the completeness axiom than we have used, but the axiom system is equivalent to ours.) There also exist constructions of pairs of very different real fields, cf. [41].

In what follows, I am going to assume that there is a real field $\mathbf{R}$ (which I'll call *the real numbers*). Any theorems proved will be valid in all real fields.

5.25 Theorem (Archimedean property 1.) *Let* $\mathbf{R}$ *be a real field, and let* $x \in \mathbf{R}$. *Then there is an integer* $n \in \mathbf{N}$ *such that* $n > x$.

Proof: Let $x \in \mathbf{R}$, and suppose (in order to get a contradiction) that there is no $n \in \mathbf{N}$ with $n > x$. Then $x \geq n$ for all n. Now $\left\{\left[0, \dfrac{x}{2^n}\right]\right\}$ is a binary search sequence in $\mathbf{R}$. Since $x \geq 2^n$, I have $1 \leq \dfrac{x}{2^n}$ for all $n \in \mathbf{N}$. We see that $\left\{\left[0, \dfrac{x}{2^n}\right]\right\} \to 1$, but clearly $\left\{\left[0, \dfrac{x}{2^n}\right]\right\} \to 0$. Since completeness of $\mathbf{R}$ implies that a binary search sequence has a unique limit, this yields a contradiction, and proves the theorem. ‖

5.26 Corollary (Archimedean property 2.) *Let $x \in \mathbf{R}\backslash\{0\}$. Then there is some $n \in \mathbf{Z}_{\geq 1}$ such that $\frac{1}{n} < |x|$.*

Proof: By the theorem, there is some $n \in \mathbf{Z}_{\geq 1}$ with $n > \frac{1}{|x|}$. Then $\frac{1}{n} < |x|$. |||

5.27 Corollary (Archimedean property 3.) *Let x be a real number, and let C be a positive real number. Suppose*

$$|x| \leq \frac{C}{n} \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{5.28}$$

Then $x = 0$.

Proof: Let $x \in \mathbf{R}$, and let $C \in \mathbf{R}^+$ satisfy

$$|x| \leq \frac{C}{n} \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{5.29}$$

Suppose, in order to get a contradiction, that $x \neq 0$. Then by Archimedian property 2 there is some $n \in \mathbf{Z}_{\geq 1}$ such that $\frac{1}{n} < \frac{|x|}{C}$, i.e. $\frac{C}{n} < |x|$. This contradicts (5.29). |||

5.30 Theorem. *If $t \in \mathbf{R}$, then there is an integer n and a number $\varepsilon \in [0,1)$ such that $t = n + \varepsilon$.*

In order to prove this theorem, I will use the following lemma.

5.31 Lemma. *If $t \in \mathbf{R}$, then the interval $(t, t+1]$ contains an integer.*

Proof:

Case 1. $t \in [0, \infty)$: Suppose $t \in [0, \infty)$ and $(t, t+1]$ does not contain an integer. I will show that $t \geq n$ for all $n \in \mathbf{N}$. This contradicts the Archimedean property, so no such t can exist. For each $n \in \mathbf{N}$, let $P(n) =$ "$n \leq t$". Then $P(0)$ is true, since I assumed that $t \in [0, \infty)$. Let $n \in \mathbf{N}$ be a number such that $P(n)$ is true; i.e., $n \leq t$. If $n+1$ were $> t$, we'd have $t < n+1 \leq t+1$, and this cannot happen, since $(t, t+1]$ contains no integers. Hence,

$$P(n) \implies n+1 \leq t \implies P(n+1),$$

and by induction, $t \geq n$ for all $n \in \mathbf{N}$. This gives the desired contradiction.

Case 2. $t \in \mathbf{R}^-$: If $t \in \mathbf{R}^-$, then by Case 1 there is an integer n with

$$-t < n \leq -t + 1.$$

Then

$$t \leq -n + 1 < t + 1.$$

If $t < -n + 1$, then $(t, t+1]$ contains $-n + 1$. If $t = -n + 1$, then $(t, t+1] = (-n+1, -n+2]$ contains $-n + 2$. ||

Proof of theorem 5.30. Let $t \in \mathbf{R}$. By the lemma, there is an integer n with $t < n \leq t + 1$. Then

$$0 \leq t - n + 1 < 1,$$

and $t = (n-1) + (t - n + 1)$ gives the desired decomposition. ||

5.32 Theorem. *There is a number $x \in \mathbf{R}$ such that $x^2 = 2$.*

Proof: Let $\{[a_n, b_n]\}$ be the binary search sequence constructed in example 5.16. We know there is a unique $x \in \mathbf{R}$ such that $0 \leq a_n \leq x \leq b_n$ for all n. Then $0 \leq a_n^2 \leq x^2 \leq b_n^2$, and by our construction $0 \leq a_n^2 \leq 2 \leq b_n^2$ for all $n \in \mathbf{N}$, so

$$|2 - x^2| \leq b_n^2 - a_n^2 = (b_n - a_n)(b_n + a_n) \leq \frac{1}{2^n} \cdot 4 \leq \frac{4}{n} \tag{5.33}$$

for all $n \in \mathbf{Z}_{\geq 1}$.

By Archimedean property 3, we conclude that $2 - x^2 = 0$, i.e., $x^2 = 2$. ||

5.34 Theorem. *Let $x \in \mathbf{R}$. Then there is a binary search sequence $\{[a_n, b_n]\}$ in $\mathbf{R}$ such that $a_n \in \mathbf{Q}$ and $b_n \in \mathbf{Q}$ for all n, and such that $\{[a_n, b_n]\} \to x$.*

Proof: I will suppose $x \geq 0$. The case where $x \leq 0$ is left to you. By the Archimedean property of $\mathbf{R}$, there is an integer N such that $N > x$, so $x \in [0, N]$. Now build a binary search sequence $\{[a_n, b_n]\}$ as follows:

$$\begin{aligned} [a_0, b_0] &= [0, N] \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } x \leq \left[\frac{a_n+b_n}{2}\right] \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } x > \left[\frac{a_n+b_n}{2}\right]. \end{cases} \end{aligned}$$

From the construction, we have $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ and $b_n - a_n = \dfrac{b_0 - a_0}{2^n}$. A simple induction argument shows that $a_n \in \mathbf{Q}$ and $b_n \in \mathbf{Q}$ for all $n \in \mathbf{N}$, and an induction proof similar to the one in example 5.16 shows that $a_n \leq x \leq b_n$ for all $n \in \mathbf{N}$ so $\{[a_n, b_n]\} \to x$. ||

5.3 Existence of Roots

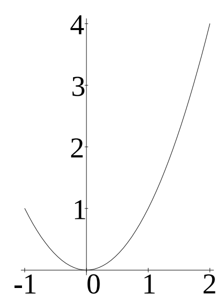
5.35 Definition (Graph.) Let $f: A \to B$ be a function. The *graph of* f is

$$\{(a, b) \in A \times B: b = f(a)\}.$$

5.36 Remark. If f is a function from $\mathbf{R}$ to $\mathbf{R}$, then graph f is

$$\{(x, y) \in \mathbf{R}^2: y = f(x)\}.$$

You may find it useful to think of $\mathbf{R}$ as points on a line, and $\mathbf{R}^2$ as points in a plane and to represent the graph by a picture. Any such picture is outside the scope of our formal development, but I will draw lots of such pictures informally.



graph of f where $f(x) = x^2$ for $x \in (-1, 2)$.

5.37 Definition (Sum and product of functions.) Let F be a field, and let $\alpha \in F$. Let A, B be sets and let $f: A \to F, g: B \to F$ be functions. We define functions $f + g$, $f - g$, $f \cdot g$, αf and $\dfrac{f}{g}$ by:

$$\begin{array}{ll}
f + g: A \cap B \to F & (f + g)(a) = f(a) + g(a) \text{ for all } a \in A \cap B. \\
f - g: A \cap B \to F & (f - g)(a) = f(a) - g(a) \text{ for all } a \in A \cap B. \\
f \cdot g: (A \cap B) \to F & (f \cdot g)(a) = f(a) \cdot g(a) \text{ for all } a \in A \cap B. \\
\alpha f: A \to F & (\alpha f)(a) = \alpha \cdot f(a) \text{ for all } a \in A. \\
\dfrac{f}{g}: D \to F & \left(\dfrac{f}{g}\right)(a) = \dfrac{f(a)}{g(a)} \text{ for all } a \in D.
\end{array}$$

where $D = \{x \in A \cap B: g(x) \neq 0\}$.

5.38 Remark. Let F be a field, let S be a set, and let $f\colon S \to F$, $g\colon S \to F$ be functions with the same domain. Then the operations $+, \cdot, -$ are binary operations on the set $\mathcal{S}$ of all functions from S to F. These operations satisfy the same commutative, associative and distributive laws that the corresponding operations on F satisfy; e.g.,

$$f \cdot (g+h) = f \cdot g + f \cdot h \text{ for all } f, g, h \in \mathcal{S}. \tag{5.39}$$

Proof of (5.39). For all $x \in S$,

$$\begin{aligned} (f \cdot (g+h))(x) &= f(x)(g+h)(x) \\ &= f(x)\left(g(x)+h(x)\right) \\ &= f(x)g(x) + f(x)h(x) \\ &= (f \cdot g)(x) + (f \cdot h)(x) \\ &= \left((f \cdot g) + (f \cdot h)\right)(x). \end{aligned}$$

Hence, $f \cdot (g+h) = (f \cdot g) + (f \cdot h)$. (Two functions are equal when they have the same domain, the same codomain, and the same rule.) $\|$

5.40 Definition (Increasing and decreasing.) Let J be an interval in $\mathbf{R}$ and let $f\colon J \to \mathbf{R}$. We say

f is increasing on J if for all $s, t \in J\,(s \le t \implies f(s) \le f(t))$.

f is strictly increasing on J if for all $s, t \in J\,(s < t \implies f(s) < f(t))$.

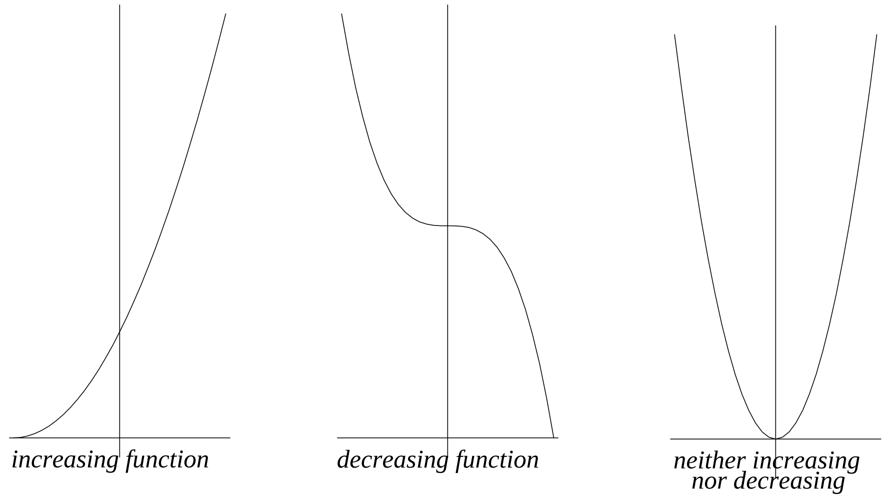
f is decreasing on J if for all $s, t \in J\,(s \le t \implies f(s) \ge f(t))$.

f is strictly decreasing on J if for all $s, t \in J\,(s < t \implies f(s) > f(t))$.

5.41 Remark. Since $s = t \implies f(s) = f(t)$, we can reformulate the definitions of increasing and decreasing as follows:

f is increasing on J if for all $s, t \in J\,(s < t \implies f(s) \le f(t))$.

f is decreasing on J if for all $s, t \in J\,(s < t \implies f(s) \ge f(t))$.



5.42 Exercise. Is there a function $f\colon \mathbf{R} \to \mathbf{R}$ that is both increasing and decreasing? If the answer is yes, give an example. If the answer is no, explain why not.

5.43 Exercise. Give an example of a function $f\colon \mathbf{R} \to \mathbf{R}$ such that f is increasing, but not strictly increasing.

5.44 Exercise. Let $f\colon \mathbf{R} \to \mathbf{R}$ and $g\colon \mathbf{R} \to \mathbf{R}$ be increasing functions. Either prove that $f + g$ is increasing or give an example to show that $f + g$ is not necessarily increasing

5.45 Exercise. Let $f\colon \mathbf{R} \to \mathbf{R}$ and $g\colon \mathbf{R} \to \mathbf{R}$ be increasing functions. Either prove that $f \cdot g$ is increasing or give an example to show that $f \cdot g$ is not necessarily increasing.

5.46 Theorem. *Let $m \in \mathbf{Z}_{\geq 1}$, let $a \in \mathbf{R}$, $a \geq 1$. Then $a^m \geq a$.*

The proof is by induction, and is omitted.

5.47 Theorem. *Let $m \in \mathbf{Z}_{\geq 1}$. Let $f_m(x) = x^m$ for all $x \in [0, \infty)$ in $\mathbf{R}$. Then f_m is strictly increasing on $[0, \infty)$.*

Proof: The proof follows from induction on m or by factoring $x^m - y^m$, and is omitted.

5.48 Exercise. Let J be an interval in $\mathbf{R}$ and let $f\colon J \to \mathbf{R}$ be a strictly increasing function on J. Show that for each $a \in \mathbf{R}$ the equation $f(x) = a$ has at most one solution x in J.

5.49 Theorem. *Let $p \in \mathbf{Z}_{\geq 1}$ and let $a \in [0, \infty)$ in $\mathbf{R}$. Then there is a unique $c \in [0, \infty)$ in $\mathbf{R}$ such that*

$$c^p = a.$$

Proof: First I will construct a binary search sequence $\{[a_n, b_n]\}$ in $\mathbf{R}$ such that

$$a_n^p \leq a \leq b_n^p \text{ for all } n \in \mathbf{N}.$$

By completeness of $\mathbf{R}$, I'll have $\{[a_n, b_n]\} \to c$ for some $c \in \mathbf{R}$. I'll show $c^p = a$, and the proof will be complete.

Let $[a_0, b_0] = [0, (1 + a)]$. Then

$$a_0^p = 0 \leq a < (1 + a) \leq (1 + a)^p = b_0^p.$$

For $n \in \mathbf{N}$, define

$$[a_{n+1}, b_{n+1}] = \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^p \geq a \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^p < a. \end{cases}$$

The proof that $\{[a_n, b_n]\}$ is a binary search sequence and that $a_n^p \leq a \leq b_n^p$ for all $n \in \mathbf{N}$ is the same as the proof given in example 5.16 for $a = p = 2$, and will not be repeated here. By completeness $\{[a_n, b_n]\} \to c$ for some $c \in \mathbf{R}$. Since $0 \leq a_n \leq c \leq b_n$, we have $a_n^p \leq c^p \leq b_n^p$. It follows that

$$|a - c^p| \leq b_n^p - a_n^p \text{ for all } n \in \mathbf{N}.$$

By the formula for factoring $b^p - a^p$ (cf. (3.78)), we have

$$\begin{aligned} |a - c^p| &\leq (b_n - a_n) \sum_{j=0}^{p-1} b_n^j a_n^{p-1-j} \leq (b_n - a_n) \sum_{j=0}^{p-1} b_n^j b_n^{p-1-j} \\ &= (b_n - a_n) p b_n^{p-1} \leq \frac{b_0 - a_0}{2^n} \cdot p b_0^{p-1} \leq \frac{(b_0 - a_0) p b_0^{p-1}}{n} \end{aligned}$$

for all $n \in \mathbf{Z}_{\geq 1}$. By Archimedean property 3 (cf corollary 5.28), it follows that $a - c^p = 0$, i.e $c^p = a$.

Let $f_p(x) = x^p$. Since f_p is strictly increasing on $\mathbf{R}$, it follows from exercise 5.48 that $x^p = a$ has at most one solution in $\mathbf{R}^+$ and this completes the proof of the theorem. ‖

5.50 Notation ($a^{\frac{1}{p}}$.) If $p \in \mathbf{Z}_{\geq 1}$ and $a \in [0, \infty)$, then the unique number c in $[0, \infty)$ such that $c^p = a$ is denoted by $a^{\frac{1}{p}}$, and is called the *pth root of a*. An alternative notation for $a^{\frac{1}{2}}$ is $\sqrt{a}$.

5.51 Exercise. Let $a \in [0, \infty)$, let $q, r \in \mathbf{Z}_{\geq 1}$, and let $p, s \in \mathbf{Z}$.

a) Show that $\left(a^{\frac{1}{q}}\right)^p = (a^p)^{\frac{1}{q}}$.

b) Show that if $\dfrac{p}{q} = \dfrac{s}{r}$, then $\left(a^{\frac{1}{q}}\right)^p = \left(a^{\frac{1}{r}}\right)^s$.

5.52 Definition (a^r.) If $a \in \mathbf{R}^+$ and $r \in \mathbf{Q}$ we define $a^r = \left(a^{\frac{1}{q}}\right)^p$ where $q \in \mathbf{Z}_{\geq 1}$, $p \in \mathbf{Z}$ and $r = \dfrac{p}{q}$. The previous exercise shows that this definition does not depend on what representation we use for writing r.

5.53 Theorem (Laws of exponents.) *For all $a, b \in [0, \infty)$ and all $r, s \in \mathbf{Q}$,*

a) $(ab)^r = a^r b^r$.

b) $a^r a^s = a^{r+s}$.

c) $(a^r)^s = a^{(rs)}$.

Proof: [of part b)] Let $r = \dfrac{p}{q}$, $s = \dfrac{u}{v}$ where u, v are integers and q, v are positive integers. Then (by laws of exponents for integer exponents),

$$\begin{aligned}(a^r a^s)^{q\cdot v} &= \left(a^{\frac{p}{q}} \cdot a^{\frac{u}{v}}\right)^{q\cdot v} = \left(a^{\frac{p}{q}}\right)^{(q\cdot v)} \cdot \left(a^{\frac{u}{v}}\right)^{(q\cdot v)} \\ &= \left(\left((a^p)^{\frac{1}{q}}\right)^q\right)^v \cdot \left(\left((a^u)^{\frac{1}{v}}\right)^v\right)^q = (a^p)^v \cdot (a^u)^q = a^{(pv)} a^{(uq)} \\ &= a^{pv+uq}.\end{aligned}$$

Also,

$$\begin{aligned}(a^{r+s})^{q\cdot v} &= \left(a^{\left(\frac{p}{q}+\frac{u}{v}\right)}\right)^{q\cdot v} \\ &= \left(a^{\left(\frac{pv+uq}{qv}\right)}\right)^{(qv)} = \left(\left(a^{(pv+uq)}\right)^{\frac{1}{qv}}\right)^{qv} \\ &= a^{pv+uq}.\end{aligned}$$

Hence, $(a^r a^s)^{q\cdot v} = (a^{r+s})^{q\cdot v}$, and hence $a^r a^s = a^{r+s}$ by uniqueness of $q \cdot v$ roots.

5.54 Exercise. Prove parts a) and c) of theorem 5.53.

5.55 Entertainment. Show that of the two real numbers

$$\sqrt{\tfrac{9}{2}+\sqrt{8}}+\sqrt{\tfrac{9}{2}-\sqrt{8}}, \quad \sqrt{\tfrac{9}{2}+\sqrt{8}}-\sqrt{\tfrac{9}{2}-\sqrt{8}},$$

one is in $\mathbf{Q}$, and the other is not in $\mathbf{Q}$.

5.56 Note. The Archimedean property was stated by Archimedes in the following form:

> $\cdots$ the following lemma is assumed: that the excess by which the greater of (two) unequal areas exceeds the less can, by being added to itself, be made to exceed any given finite area. The earlier geometers have also used this lemma.[2, p 234]

Euclid indicated that his arguments needed the Archimedean property by using the following definition:

> Magnitudes are said to *have a ratio* to one another which are capable, when multiplied, of exceeding one another.[19, vol 2, p114]

Here "multiplied" means "added to itself some number of times", i.e. "multiplied by some positive integer".

Rational exponents were introduced by Newton in 1676.

> Since algebraists write a^2, a^3, a^4, etc., for $aa, aaa, aaaa$, etc., so I write $a^{\frac{1}{2}}, a^{\frac{3}{2}}, a^{\frac{5}{3}}$, for $\sqrt{a}, \sqrt{a^3}, \sqrt{ca^5}$; and I write a^{-1}, a^{-2}, a^{-3}, etc. for $\frac{1}{a}, \frac{1}{aa}, \frac{1}{aaa}$, etc.[14, vol 1, p355]

Here $\sqrt{ca}$ denotes the cube root of a.

Buck's *Advanced Calculus*[12, appendix 2] gives eight different characterizations of the completeness axiom and discusses the relations between them.

The term *completeness* is a twentieth century term. Older books speak about the *continuity* of the real numbers to describe what we call completeness.