Real Analysis Math 452 [1]

Go over policies. Go over handout on groups, rings, fields, order relations and vector spaces. You should know or have seen somewhere most of Chapter 1 except Section 2. I will cover Section 2. Read all of Chapter 1 carefully. Read all the exercises. We will then cover Chapters 2, 3, 4 and maybe some of 6.

1. Rational Numbers

We take the integers, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$, as a given ordered commutative ring with a unit. The natural numbers $\mathbb{N}$ are the positive integers. Then we define the *rational numbers* by

$$\mathbb{Q} = \{(p, q) \,|\, p \in \mathbb{Z} \,\&\, q \in \mathbb{Z}\backslash\{0\}\}/\sim$$

where $(p_1, q_1) \sim (p_2, q_2)$ iff $p_1q_2 = p_2q_1$. We then define field operations by

$$\begin{aligned} (p_1, q_1) + (p_2, q_2) &= (p_1q_2 + p_2q_1, q_1q_2) \\ (p_1, q_1) \cdot (p_2, q_2) &= (p_1p_2, q_1q_2). \end{aligned}$$

One checks that $\mathbb{Q}$ is a field. We identify $\mathbb{Z}$ with the subring $\{(p, 1) \,|\, p \in \mathbb{Z}\}$. It is customary to write

$$\text{“}\frac{p}{q}\text{”} \text{ for } \text{“}(p, q)\text{”}.$$

We can always express $\frac{p}{q}$ in *reduced form* where $q > 0$ and p and q have no prime factors in common[2].

We define an order on $\mathbb{Q}$ by

$$\frac{p_1}{q_1} < \frac{p_2}{q_2} \Longleftrightarrow p_1q_2 < p_2q_1,$$

assuming reduced form. One checks this is an order and that the induced order on $\mathbb{Z}$ is equivalent to its original order. One can show that $\mathbb{Q}$ is an ordered field and $\mathbb{Z}$ is an ordered subring.

We know that $\sqrt{2}$ is not in $\mathbb{Q}$. In fact for p prime and $n \geq 2$ there is no member $k/m \in \mathbb{Q}$ such that $(k/m)^n = p$.

Give some history. How to fix this?

[2]The proof that this can be done is nontrivial and can be found in books on number theory.

There are basically two ways, *Dedekind cuts* and *Cauchy completion.* These start with $\mathbb{Q}$ and build a new set $\mathbb{R}$ called the *real numbers.* The results are isomorphic. We do cuts first.

2. Dedekind Cuts

Definition. A *cut* of $\mathbb{Q}$ is a pair of subsets A and B of $\mathbb{Q}$ such that
(a) $A \cup B = \mathbb{Q}$, $A \neq \emptyset$, $B \neq \emptyset$, $A \cap B = \emptyset$.
(b) If $a \in A$ and $b \in B$, then $a < b$.
(c) A contains no largest element.
A cut is denoted by the symbol $A|B$.

Examples.
1. $A = (-\infty, 2)_{\mathbb{Q}}$, and $B = [2, \infty)_{\mathbb{Q}}$. This is clear.
2. $A = \{r \in \mathbb{Q} \,|\, r^2 < 2 \,\text{or}\, r \leq 0\}$, and $B = \mathbb{Q} \backslash A$.

Proof for 2. (a) is clear. (b) is easy. (c) will take some work. Let $r \in A$ and suppose it is the largest element. Clearly $r > 0$. Let $n \in \mathbb{N}$. Consider $r + \frac{1}{n}$. We will show there exists and n such that $(r + \frac{1}{n})^2 < 2$. This will imply that $r + \frac{1}{n} \in A$ and hence that r was not the largest element of A. It follows that A has no largest element. For this we need the following.

Fact. For every $r \in \mathbb{Q}$ with $r > 0$, there exists $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < r$.

Proof. Let $r = p/q$ with p and q in $\mathbb{N}$. If $p > 1$ use $n = q$. If $p = 1$ use $n = 2q$. In both cases $\frac{1}{n} < \frac{p}{q}$. $\square$

Continuation of Proof for 2. We see $(r + \frac{1}{n})^2 = r^2 + \frac{2r}{n} + \frac{1}{n^2}$. We know $r^2 < 2$. If $\frac{2r}{n} + \frac{1}{n^2} < 2 - r^2$, then we will have $(r + \frac{1}{n})^2 < 2$. Choose n such that $0 < \frac{1}{n} < \frac{2 - r^2}{2r+1}$. Then,

$$\frac{1}{n} < \frac{2 - r^2}{2r + 1} \leq \frac{2 - r^2}{2r + \frac{1}{n}} \implies \frac{2r}{n} + \frac{1}{n^2} < 2 - r^2.$$

We are done. $\square$

Definition. If $A|B$ has $A = \{r \in \mathbb{Q} \,|\, r < \frac{p}{q}\}$ then we say $A|B$ is a *rational cut*; it is denoted by $(\frac{p}{q})^*$.

Thus, if we identify $(\frac{p}{q})^*$ with $\frac{p}{q}$, the set of all rational cuts is a copy of $\mathbb{Q}$ sitting inside the set of all cuts.

Definition. The set of all cuts is called the *real numbers* and is denoted $\mathbb{R}$.

We have to define the field operations and an order relation such that $\mathbb{Q}$ is an ordered subfield. We will then show that $\mathbb{R}$ is *complete*. For example, $\sqrt{2} \in \mathbb{R}$.

Definition. The cut $A|B$ is $<$ the cut $C|D$ if A is a proper subset of C.

You can check that this is an order relation and that the induced order on $\mathbb{Q}$ is the same as the original.

Addition. Let $x = A|B$ and $y = C|D$ be members of $\mathbb{R}$. Then $x + y = E|F$ where

$E = \{r \in \mathbb{Q} \,|\, \exists a \in A, c \in C \text{ s.t. } r = a + c\}$ and
$F = \mathbb{Q} \backslash E$.

Claim. $E|F$ is a cut of $\mathbb{Q}$.

Proof. (a) Since A and C are bounded above so is E. Hence $E \neq \mathbb{Q}$ and it is obvious that $E \neq \emptyset$, $F \neq \emptyset$, $E \cup F = \mathbb{Q}$ and E and F are disjoint.

(b) Let $e \in E$ and $f \in F$. We need to show $e < f$. Clearly $e \neq f$. Suppose $f < e$. Assume $e = a + c$ where $a \in A$ and $c \in C$. Let $\delta = e - f > 0$. Then $f = e - \delta = a - \delta + c$. Since $a - \delta < a$, we have $a - \delta \notin B$ which implies $a - \delta \in A$. Thus $(a - \delta) + c \in E$, contradicting that $f \in F$. Thus, $e < f$.

(c) Suppose $e \in E$ is the largest element of E. Assume $e = a + c$ with $a \in A$ and $c \in C$. Since A does not have a greatest element $\exists a' \in A$ s.t. $a' > a$. Then $e' = a' + c \in E$ and is larger than e. Thus E does not have a largest element.

We conclude that $E|F$ is a cut. $\square$

Claim. $x + y = y + x$.

Proof. Let $x = A|B$ and $y = C|D$ be real numbers, that is let them be cuts. Let $E|F = x + y$ and $E'|F' = y + x$. Then $E = \{r \in \mathbb{Q} \,|\, \exists a \in A, c \in C \text{ s.t. } r = a + c\} = \{r \in \mathbb{Q} \,|\, \exists c \in C, a \in A \text{ s.t. } r = c + a\} = E'$. Thus $E = E'$ so $E|F = E'|F'$. $\square$

Claim. $x + 0^* = x$.

Proof. Let $x = A|B$ and recall $0^* = (-\infty, 0)_{\mathbb{Q}}|[0, \infty)_{\mathbb{Q}}$. Let $E|F = x + 0^*$. Then

$$E = \{r \in \mathbb{Q} \,|\, \exists a \in A, c \in (-\infty, 0)_{\mathbb{Q}} \text{ s.t. } r = a + c\}.$$

We will show $E = A$.

If $r \in E$ then $r = a + c$ for some $a \in A$ and $c \in (\infty, 0)_{\mathbb{Q}}$. Since $c < 0$, $r < a$. But $r < a$ implies $r \in A$. Hence $E \subset A$.

Let $a \in A$. Since A does not have a largest member, there exists a positive rational number δ such that $a + \delta \in A$. Then $-\delta \in (-\infty, 0)_{\mathbb{Q}}$. Since $a = (a + \delta) - \delta$ we get that $a \in E$. Hence $A = E$. This shows that as cuts $A|B = E|F$ and hence that $x + 0^* = x$. $\square$

Claim. For rational cuts

$$\left(\frac{p}{q}\right)^* + \left(\frac{r}{s}\right)^* = \left(\frac{p}{q} + \frac{r}{s}\right)^*.$$

Proof. Let $E|F = (p/q)^* + (r/s)^*$. Then

$$E = \{x \in \mathbb{Q} \,|\, x = a + c \text{ for } a < p/q, c < r/s, a, c \in \mathbb{Q}\}.$$

Let $E' = \{y \in \mathbb{Q} \,|\, y < p/q + r/s\}$. Them the cut $E'|(\mathbb{Q} - E') = (p/q + r/s)^*$. We claim $E = E'$.

If $x \in E$ then $x < p/q + r/s$. Thus $x \in E'$ and we have that $E \subset E'$. Now suppose $y \in E'$. Let $\delta = p/q + r/s - y$. So $\delta > 0$ and is rational. Now

$$y = p/q + r/s - \delta = (p/q - \delta/2) + (r/s - \delta/2) \in E.$$

Thus $E' \subset E$.

Therefore $E = E'$ and we are done. $\square$

Minus. Let $x = A|B$. Define $-x = A'|B'$ by
$A' = \{r \in \mathbb{Q} \,|\, \exists b \in B,$ not the smallest element of B, s.t. $r = -b\}$, and
$B' = \mathbb{Q}\backslash A'$.

Example. Let $A = (-\infty, 5)_{\mathbb{Q}}$, $B = [5, \infty)_{\mathbb{Q}}$, and $x = A|B$. Then you can check that $-x = A'|B'$ where $A' = (-\infty, -5)_{\mathbb{Q}}$ and $B' = [-5, \infty)_{\mathbb{Q}}$.

Claim. If $x \in \mathbb{R}$, then $-x$ is indeed a cut.

Punt. You try this.

Claim. $x + (-x) = 0^*$.

Proof. Let $x = A|B$ and $-x = A'|B'$. Let $Z = (-\infty, 0)_{\mathbb{Q}}$ and $E = \{r \in \mathbb{Q} \,|\, r = a + b, a \in A, b \in A'\}$. Then $0^* = Z|(\mathbb{Q} - Z)$ and $x + (-x) = E|(\mathbb{Q} - E)$. We will show $E = Z$.

Let $r \in E$. Then $r = a + b$ for some $a \in A$ and $b \in A'$. Thus $-b \in B$. Hence $a < -b$, which implies $a + b < 0$. Therefore, $r \in Z$ and we have shown that $E \subset Z$.

Let $z \in Z$. We shall find an $a \in A$ such that $a + (-z) \in B$ and is not the smallest element of B. Then since $z = a - (a - z)$ we will have $z \in E$. Suppose for every $a \in A$ that $a - z \notin B$. Since this means $a - z \in A$ we can use induction to show that $a - nz \notin B$ for all positive integers n. But, we claim that for every $b \in B$ there is an n s.t. $b < a - nz$, forcing $a - nz \in B$. Proof: There exists an positive integer n s.t. $0 < \frac{1}{n} < \frac{-z}{b-a}$. It follows that $b < a - nz$.

Thus, $\exists\ a \in A$ s.t. $a - z \in B$. If $a - z$ is the smallest member of B replace a with $a' \in A$ s.t. $a' > a$. Such an a' exists because A has no largest member. Then $a' - z$ is in B and is not the smallest member. Thus, we may assume $a - z$ is not the smallest member of B. Hence $-a + z \in A'$.

Now, $z = a + (-a + z)$ implies $z \in E$. Thus $Z \subset E$ and so $Z = E$ as claimed. $\square$

Claim. Addition in $\mathbb{R}$ is associative.

Punt. See textbook[3].

[3] *Real Mathematical Analysis*, by Charles Pugh, Springer 2002.

Claim. If $x < y$ then $x + z < y + z$, for all x, y, z in $\mathbb{R}$.

Punt. See textbook.

So far we have that $\mathbb{R}$ is an ordered abelian group with $\mathbb{Q}$ an ordered subgroup.

Multiplication. Multiplication is more complicated because the definition depends on the signs. First suppose $0^* < x = A|B$ and $0^* < y = C|D$. Then we define $x \cdot y = E|F$ where

$E = \{r \in \mathbb{Q} \,|\, r \leq 0 \text{ or } \exists a \in A \& c \in C \text{ s.t. } a > 0, c > 0 \text{ and } r = ac\}$.

$F = \mathbb{Q} \setminus E$.

For the other cases do the following.

If $0^* < x$ & $y < 0^*$, define $x \cdot y = -(x \cdot (-y))$.
If $x < 0^*$ & $0^* < y$, define $x \cdot y = -((-x) \cdot y)$.
If $x < 0^*$ & $y < 0^*$, define $x \cdot y = (-x) \cdot (-y)$.
And of course $x \cdot 0^* = 0^* \cdot x = 0^*$.

Theorem. With this definition $\mathbb{R}$ is an ordered field, with $\mathbb{Q}$ an ordered subfield.

Punt. See reference in textbook.

What did we gain by all of this?

Definition. Let X be an ordered set and let S be a nonempty subset. An *upper bound* for S is any $x \in X$ s.t. $\forall s \in S$ we have $s \leq x$. A *least upper bound* for S is an $x' \in X$ s.t. x' is an upper bound of S and for any other x that is an upper bound of S we have $x' < x$. When a least upper bound exists it is unique; it is called the supremum of S and denoted $\sup S$.

There are parallel definitions for lower bounds, greatest lower bounds and the infimum of S, denoted $\inf S$. If $S \neq \emptyset$ and has no upper bound we define $\sup S = \infty$. If $S \neq \emptyset$ and has no lower bound then we define $\inf S = -\infty$. We also define $\sup \emptyset = -\infty$ and $\inf \emptyset = \infty$.

Example. Sup $\{1 - \frac{1}{n} \,|\, n \in \mathbb{N}, n \geq 1\} = 1$, while the infimum is zero.

Definition. An ordered set X has the *least upper bound property* if for all nonempty subsets S with an *upper bound* there is a *least upper bound.*

There is a parallel definition of the *greatest lower bound property.*

Theorem. The set of real numbers has the least upper bound property.

Proof. Let $\mathcal{C} \subset \mathbb{R}$ be nonempty and bounded by $X|Y$. Let
$C = \{a \in \mathbb{Q} \,|\, \exists A|B \in \mathcal{C}$ with $a \in A\}$, and
$D = \mathbb{Q} \backslash C$.

Claim. $C|D$ is a cut.

Proof. (a) If $A|B \in \mathcal{C}$ then $A \subset C$, so $C \neq \emptyset$. Let $y \in Y$. $\forall\, A|B \in \mathcal{C}$, $A \subset X$, and so y is bigger than every $a \in A$. Thus $y \notin C$ and thus $D \neq \emptyset$.
(b) Let $c \in C$ and $d \in D$. $\exists A^*|B^* \in \mathcal{C}$ s.t. $c \in A^*$. Since $d \notin A$ $\forall\, A|B \in \mathcal{C}$ we know $d \notin A^*$. Thus $d \in B^*$. This means $c < d$.
(c) Let $c \in C$. By definition $\exists\, A|B \in \mathcal{C}$ s.t. $c \in A$. $\exists\, a \in A$ s.t. $c < a$. Then $a \in C$, so c could not be the largest element of C.

Claim. $C|D$ is a the least upper bound of $\mathcal{C}$.

Proof. Let $z = C|D$ and let $z' = C'|D'$ be any upper bound of $\mathcal{C}$. $\forall\, A|B \in \mathcal{C}$, we know that $A|B \leq C'|D'$ implies $A \subset C'$. Thus $C \subset C'$ and $z \leq z'$ as required.

These two Claims prove the Theorem. $\square$

Theorem. The $\sqrt{2}$ exists as a real number. That is, there exists $x \in \mathbb{R}$ s.t. $x^2 = 2$.

Proof. Let $A = \{r \in \mathbb{Q} \,|\, r \leq 0$ or $r^2 < 2\} \subset \mathbb{R}$. Then A is bounded above by 2, for if not $\exists\, a \in A$ s.t. $a^2 < 2$ and $a > 2$, implying $4 < 2$. Let $x = \text{l.u.b. } A$. Clearly $x > 0$.

Suppose $x^2 < 2$. We will show $\exists\, n \in \mathbb{N}$ s.t. $\left(x + \frac{1}{n}\right)^2 < 2$; hence $x + \frac{1}{n} \in A$, contradicting that $x = \text{l.u.b. } A$. We need the following.

Fact. If x is any real positive number, there exists an $n \in \mathbb{N}$ s.t. $0 < \frac{1}{n} < x$.

Proof. Suppose x equals the cut $P|Q$. Since $x > 0$ there exists a positive rational number r in P. Then, identifying r with r^* we have $r < x$. Then choose n so that $0 < \frac{1}{n} < r < x$.

You can check that $\dfrac{2-x^2}{2x+1} > 0$. Thus $\exists\ n \in \mathbb{N}$ s.t. $\dfrac{1}{n} < \dfrac{2-x^2}{2x+1}$. Thus $\dfrac{2x+1}{n} < 2 - x^2$. Therefore,

$$\left(x + \frac{1}{n}\right)^2 = x^2 + \frac{2x}{n} + \frac{1}{n^2} = x^2 + \frac{2x + \frac{1}{n}}{n} \leq x^2 + \frac{2x+1}{n} < x^2 + 2 - x^2 = 2.$$

Suppose $x^2 > 2$. Choose $m \in \mathbb{N}$ s.t. $\dfrac{1}{m} < \dfrac{x^2-2}{2x}$. Thus $\dfrac{2x}{m} < x^2 - 2$. Since $x = $ l.u.b. A, $\exists\ x_0 \in A$ s.t. $x - \frac{1}{m} < x_0$. Thus,

$$2 < x^2 - \frac{2x}{m} < x^2 - \frac{2x}{m} + \frac{1}{m^2} = \left(x - \frac{1}{m}\right)^2 < x_0^2.$$

Thus, $2 < x_0^2$, which contradicts that $x_0 \in A$.

We conclude that $x^2 = 2$ and are thus justified in defining $\sqrt{2} = x$. $\square$

Fact. $\forall\ x \in [0, \infty)$ and $n \in \mathbb{N}$ $\exists!\ y \in [0, \infty)$ s.t. $y^n = x$. See Exercise 15 in Chapter 1 of the textbook. We write $y = \sqrt[n]{x}$ or $y = x^{\frac{1}{n}}$.

Fact. For even $n \in \mathbb{N}$ and $x > 0$ there are two solutions to $y^n = x$, and each is the negative of the other. For odd $n \in \mathbb{N}$ the solution to $y^n = x$ is unique.

Remark. To see the connection between cuts and the usual decimal representation of real numbers see Exercise 16 in Chapter 1 of the textbook.

3. Cauchy Sequences

Definition. Let $(a_n) = (a_1, a_2, a_3, ...)$ be an infinite sequence in $\mathbb{R}$ and let $b \in \mathbb{R}$. We say

$$\lim_{n\to\infty} a_n = b \text{ or just } a_n \to b$$

if $\forall \epsilon > 0 \quad \exists N \in \mathbb{N}$ s.t. $n \geq N$ implies $|a_n - b| < \epsilon$. In words (a_n) converges to b.

Definition. An infinite sequence (a_n) satisfies the *Cauchy condition* and is call a *Cauchy sequence* if $\forall \epsilon > 0\ \exists N \in \mathbb{N}$ s.t. $n, m \geq N \implies |a_n - a_m| < \epsilon$.

Theorem. A sequence (a_n) converges to a limit iff it is Cauchy.

Proof. Suppose $a_n \to b$. Let $\epsilon > 0$ be given. Then $\exists N \in \mathbb{N}$ s.t. $n \geq N \implies |a_n - b| < \epsilon/2$. Thus, if $n, m \geq N$ we have

$$|a_n - a_m| = |(a_n - b) - (a_m - b)| \leq |a_n - b| + |a_m - b| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Thus, (a_n) is Cauchy.

The other direction is harder. Suppose (a_n) is Cauchy. Let $A = \{a_n \,|\, n \geq 1\}$. This is called the *underlying set* for (a_n).

Claim. A is bounded (above and below).

Proof. Let $\epsilon = 1$. Then $\exists n \in \mathbb{N}_1$ s.t. $n, m \geq N_1$ implies $|a_n - a_m| < 1$. Thus $\forall n \geq N_1$ we have $|a_n - a_{N_1}| < 1$. Clearly $A_{N_1} = \{a_1, a_2, \ldots, a_{N_1}\}$ is bounded, and so is $A'_{N_1} = A_{N_1} \cup \{a_{N_1} - 1, a_{N_1} + 1\}$. Assume $A'_{N_1} \subset [-M, M]$. Since for $n \geq N_1$ we have $a_{N_1} - 1 < a_n < a_{N_1} + 1$ we know that $A \subset [-M, M]$. $\square$

Now, what is a good candidate for the limit?

Let $S = \{s \in [-M, M] \,|\, a_n \geq s \text{ for infinitely many } n\}$. Since $-M \in S$ we know $S \neq \emptyset$. Since M is an upper bound for S, $\exists$ a l.u.b. of S. Let $b = \text{l.u.b. } S$.

Claim. $a_n \to b$.

Proof. Let $\epsilon > 0$ be given. What do we need? We need to find $N \in \mathbb{N}$ s.t. $n \geq N \implies |a_n - b| < \epsilon$. What do we know? There exists $N_2 \in \mathbb{N}$ s.t. $n, m \geq N_2 \implies |a_n - a_m| < \epsilon$.

We have to use the fact that $b = \text{l.u.b. } S$. This means $b + \epsilon \notin S$ no matter how small ϵ is. Thus, only finitely many of the a_n are greater than $b + \epsilon$. Thus for some $N_3 \in \mathbb{N}$, $n \geq N_3 \implies a_n \leq b + \epsilon$. We may assume $N_3 > N_2$.

$\exists\ s \in S$ s.t. $s > b - \epsilon$. Thus $a_n \geq s > b - \epsilon$ for infinitely many n. $\exists$ $N \geq N_3$ s.t. $a_N > b - \epsilon$. But then also $a_N < b + \epsilon$. Let $n \geq N$. We have

$$|a_n - b| \leq |a_n - a_N| + |a_N - b| < \epsilon + \epsilon = 2\epsilon.$$

Back up and replace ϵ with $\epsilon/2$ as needed. This proves the Claim and the Theorem. □

An alternative to cuts is to use Cauchy sequences in $\mathbb{Q}$ to define $\mathbb{R}$. Basically you take the collections of all Cauchy sequences and identify two if $|a_n - b_n| \to 0$. Then define $+$, $\cdot$ and $<$ to get $\mathbb{R}$. This $\mathbb{R}$ is isomorphic to the $\mathbb{R}$ we get from Dedekind cuts by a map that preserves order. This will be covered in the more general setting of *metric spaces* in section 2.7 of the textbook.