Analysis 1
Colloquium of Week 3

Jacob Shapiro

September 30, 2014

Abstract

We trace the procedure of constructing $\mathbb{R}$ given $\mathbb{Q}$ following Rudin's *Principles of Mathematical Analysis.*

1 Preface

- Last week we have seen how to construct $\mathbb{N}$ given the basic axioms of set theory (Halmos *Naive Set Theory* chapter 11). In essence, we defined $0 := \varnothing$, $1 := \{\varnothing\} = \{0\}$, $2 := \{\varnothing, \{\varnothing\}\} = \{0, 1\}$ and so on, and then took $\mathbb{N}$ to be the smallest set that contains all of these.
- We showed how defining $\mathbb{N}$ like this allows us to *prove* all the five Peano Axioms which we expect to be true in every respectable candidate of natural numbers (Halmos chapter 12).
- (In Halmos chapters 13 and 14) Then using this definition we can also show what it means for for two natural numbers n and m to have $n < m$ (via set inclusion), we could define what is $n + m$ as well as $n \times m$ (via recursion).
- We define a relation on a given set A as a subset R of A^2: $R \subset A^2$.
  - The relation can usually be specified with a condition, for example: $R = \left\{ (a, b) \in A^2 \,\middle|\, a = b \right\}$ stands for the relation we usually call "equality".
  - A relation R is "reflexive" iff $(a, a) \in R \forall a \in A$.
  - A relation R is "symmetric" iff $[(a, b) \in R \Longrightarrow (b, a) \in R] \,\forall\, (a, b) \in A^2$.
  - A relation R is "transitive" iff $[((a, b) \in R \wedge (b, c) \in R) \Longrightarrow (a, c) \in R] \,\forall\, (a, b, c) \in A^3$.
  - A relation R is an "equivalence relation" iff it is reflexive, symmetric, and transitive.

- Given an element $a \in A$, the equivalence class of a under R is defined as $\boxed{[a]_R \equiv \{\, b \in A \mid (a,\, b) \in R \,\}}$.
- The set of all equivalence classes of an equivalence relation partitions a set.

- Although we didn't describe it, we should have went on to construct:
  - $\mathbb{Z}$ out of $\mathbb{N}$:
    * $\mathbb{Z}$ is the set of equivalence classes of ordered pairs $(n,\, m) \in \mathbb{N}^2$ such that $(n_1,\, m_1) \sim (n_2,\, m_2) \iff n_1 + m_2 = n_2 + m_1$.
  - $\mathbb{Q}$ out of $\mathbb{Z}$:
    * $\mathbb{Q}$ is the set of equivalnce classes of ordered pairs $(n,\, m) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ such that $(n_1,\, m_1) \sim (n_2,\, m_2) \iff n_1 m_2 = n_2 m_1$.
    * You will learn more about this procedure in the course titled "algebra 2".

- On thing to note is that even though we usually write $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, the way we actually construct these objects (using set theory, bottom up) means, for example, that the elements of $\mathbb{Z}$ which we identify with $\mathbb{N}$ are not the same object (the same set):
  - $1 \in \mathbb{Z}$ is equal to $[(1,\, 0)]$ (the equivalence class of all pairs of natural numbers whose difference is $1 - 0$; thus, $1 \equiv [(1,\, 0)]$ is indeed a *set* with elements: $(1,\, 0)\,,\, (2,\, 1)\,,\, (3,\, 2)\,,\, (4,\, 3)$ and so on).
  - $1 \in \mathbb{N}$ is equal to $\{\varnothing\}$: a set whose only element is the empty set.
  - So $\underbrace{\{\varnothing\}}_{1\in\mathbb{N}} \neq \underbrace{\left\{ \left(\underbrace{\{\varnothing\}}_{1\in\mathbb{N}}, \underbrace{\varnothing}_{0\in\mathbb{N}} \right), \left(\underbrace{\{\varnothing,\, \{\varnothing\}\}}_{2\in\mathbb{N}}, \underbrace{\{\varnothing\}}_{1\in\mathbb{N}} \right), (3,\, 2)\,,\, (4,\, 3)\,,\, \ldots \right\}}_{1\in\mathbb{Z}}$ but we still identify them as the same object.
  - In the same manner, $1 \in \mathbb{Q}$ is actually equal to $\left[\left(\underbrace{1}_{\in\mathbb{Z}}, \underbrace{1}_{\in\mathbb{Z}} \right) \right]$ (the equivalence class of all pairs of integer numbers whose quotient is equal to $\frac{1}{1}$; thus, $1 \equiv [(1,\, 1)]$ is the *set* with elements which are the ordered pairs: $(1,\, 1)\,,\, (-1,\, -1)\,,\, (2,\, 2)\,,\, (-2,\, -2)\,,\, (3,\, 3)\,,\, \ldots.$ where the elements inside the ordered pairs are elements in $\mathbb{Z}$.
  - If we want to have an easy life, every time we finish a construction (for example, $\mathbb{N}$ out of set theory), we forget the technical structure of the construction (for example, that $1 = \{\varnothing\}$) and work only with the basic objects of our construction (for example, just $0,\, 1,\, 2,\, 3,\, \ldots$ when we want to construct $\mathbb{Z}$ from $\mathbb{N}$).

2 $\mathbb{R}$ out of $\mathbb{Q}$–Dedekind Cuts

2.1 Why do we need $\mathbb{R}$? Can't we do with $\mathbb{Q}$?

- $\mathbb{Q}$ is inadequate for many purposes:
  - For example, $\nexists$ a number $p \in \mathbb{Q}$ such that $p^2 = 2$.
  - We don't have π or e as rationals (but this not easy to prove). What if we need to speak about the ratio of the circumference of the circle to its radius?
- Thus $\mathbb{Q}$ has certain gaps, which $\mathbb{R}$ is supposed to fill.
- To formulate our requirement of a "proper" number system, we define a new notion:
  - A set S is said to have "the supremum property" iff

$$\boxed{\forall E \subset S \left[\left(\underbrace{E \neq \varnothing}_{\text{non-empty}} \wedge \underbrace{(\exists s \in S : \forall e \in E,\, e \leq s)}_{\text{bounded above}} \right) \implies \exists \sup(E) \in S \right]}$$

    That is, S has "the supremum property" iff given any subset of S which is not empty and is bounded above, there exists a supremum for this subset in S.
  - It is clear that $\mathbb{Q}$ does *not* have "the supremum proprety" because we can find a subset, $E := \left\{ p \in \mathbb{Q} \,\middle|\, p^2 < 2 \right\}$ which is not empty ($1 \in E$), is bounded above (1.5 is an upper bound) yet, there is no supremum for E in $\mathbb{Q}$. (in fact, $\sup(E) = \sqrt{2} \notin \mathbb{Q}$).
- Theorem 1.11: Every set with "the supremum property" also has an analogous "infimum property" (every non-empty bounded from below subset has an infimum in the set). Proof in Rudin.
- So formally we say that we are not satisified with $\mathbb{Q}$ because it doesn't have "the supremum property", and we will know that we "succeeded" in constructing $\mathbb{R}$ out of $\mathbb{Q}$ if indeed we could prove that the $\mathbb{R}$ we constructed does have have "the supremum property".
- In a way this makes intuitive sense: if a non-empty set of numbers is bounded above, surely we should be able to talk about its supremum: remember the approximation property for the supremum: $\forall \varepsilon > 0\ \exists x_\varepsilon \in E$ such that $\sup(E) - \varepsilon < x_\varepsilon \leq \sup(E)$. So we can get as close as we like to the supremum. But if the actual supremum doesn't exist in our "parent" set, then we have a "hole" in our system: a number we know is there (because we can get as close as we like to it) but is actually not there.

2.2 Dedekind Cuts

We follow a construction due to Richard Dedekind:

1. Define a "cut" as a subset of $\mathbb{Q}$, $\alpha \subset \mathbb{Q}$ such that:
   (a) $\alpha \neq \varnothing$ (non-empty) and $\alpha \neq \mathbb{Q}$ (not the whole of $\mathbb{Q}$)
   (b) $p \in \alpha \wedge q \in \mathbb{Q}$ such that $q < p$ then $q \in \alpha$ (α is "closed" from below).
   (c) $p \in \alpha \implies [(\exists r \in \alpha) : p < r]$ (α has no largest element–can always find a bigger element in it–open from above).
2. Define $\mathbb{R}$ to be the set of all possible "cuts".
3. From the second property of a "cut" we can deduce two conclusions:
   (a) *Claim 1*: If α is a "cut" and if $p \in \alpha$ and $q \notin \alpha$ then $p < q$.
   Proof:
      - Assume otherwise.
      - That is, $p \in \alpha$ and $q \notin \alpha$ and $q \leq p$.
      - Case 1: $p = q$ leads to a contradiction immediately because $p \in \alpha$ and $q \notin \alpha$.
      - Case 2: $q < p$.
         - We have a contradiction because according to the second condition $q < p$ and $p \in \alpha$ should lead to $q \in \alpha$ (α is closed from below).

   ■

   (b) *Claim 2*: If α is a "cut" and $r \notin \alpha$ and $r < s$ for some $s \in \mathbb{Q}$ then $s \notin \alpha$.
   Proof:
      - Assume otherwise, that is, assume, $r \notin \alpha$ and $r < s$ for some $s \in \mathbb{Q}$ and $s \in \alpha$.
      - This leads to a contradiction because according to the second condition, if $s \in \alpha$ and $r < s$ then $r \in \alpha$ (closed from below).

   ■
4. Define an "order" on $\mathbb{R}$: given two "cuts" α and β, define $\alpha < \beta$ to mean $\alpha \subsetneq \beta$ ("α is a *proper* subset of β").
   Claim: $<$ is an order on the set of "cuts".
   Proof:
   (a) The first condition for an order is that given two cuts α and β, we should have $\alpha < \beta \veebar \alpha = \beta \veebar \beta < \alpha$.
      i. To see this, assume that the first two conditions fail, that is $\alpha < \beta$ is false and $\alpha = \beta$ is false.
         A. That is $\alpha \subsetneq \beta$ is false and $\alpha = \beta$ is false.

B. That is ($\alpha = \beta$ or ($\alpha \subset \beta$ is false)) and $\alpha \neq \beta$.
C. That is α is not a subset of β.
D. That means that $\exists p \in \alpha \backslash \beta$.
E. β is non-empty, so $\exists q \in \beta$.
F. Because $q \in \beta$ and $p \notin \beta$, it follows that $q < p$ using *Claim 1*.
G. But because $q < p$ and $p \in \alpha$, we have that $q \in \alpha$ using the second property of "cuts".
H. Since q was an arbitrary element of β, we conclude that $\beta \subset \alpha$.
I. But according to our assumption, $\beta \neq \alpha$. As a result, $\beta \subsetneq \alpha \iff \beta < \alpha$.

ii. If $\alpha < \beta$ is false and $\beta < \alpha$ is false, then:
A. $\alpha \subsetneq \beta$ is false and $\beta \subsetneq \alpha$ is false.
B. ($\alpha = \beta$ or there is an element of α which is not in β) and ($\alpha = \beta$ or there is an element of β which is not in α).
C. Thus there are two cases:
- $\alpha = \beta$
- There is an element of α which is not in β and there is an element of β which is not in α.

D. The first case is compatible with our claim.
E. The second case is not possible because in the above claim we have shown that if $\exists p \in \alpha \backslash \beta$ then necessarily $\beta \subset \alpha$.

iii. Clearly either $\alpha < \beta$ or $\beta < \alpha$ is incompatible with $\alpha = \beta$ (because $<$ is *proper* set inclusion).
iv. Is it possible that $\alpha \subsetneq \beta$ and $\beta \subsetneq \alpha$? Clearly not, because $(\alpha \subset \beta \wedge \beta \subset \alpha) \implies \alpha = \beta$.
v. Thus we have shown that we cannot have any two of the condition simultaneously, and that if any two of the conditions fail to hold, the remaning third must hold. Thus we have proven the first condition for "order".

(b) The second condition is transitivity: If α, β, and γ are "cuts" and if $\alpha < \beta$ and $\beta < \gamma$ then we should have $\alpha < \gamma$. This is obviously true for set (proper) inclusion: $\alpha \subsetneq \beta$ and $\beta \subsetneq \gamma$ lead to $\alpha \subsetneq \gamma$, as you can verify yourself.

■

5. *Claim:* $\mathbb{R}$ has "the supremum property".
Proof:

(a) Let $A \subset \mathbb{R}$ such that $A \neq \varnothing$.

(b) Assume that A is bounded above: $\exists \beta \in \mathbb{R}$ such that $\forall \alpha \in A$, $\alpha \leq \beta$. [Don't forget that now we are one "layer" up: α and β are sets of actual rational numbers, and A is a set of *sets* of rational numbers. For A to be bounded above, we must have a *set* of sets of rational numbers which is larger (in the new sense we just defined above) than all the sets (of *sets* of rational numbers) in A.]

(c) Define $\gamma := \bigcup_{\alpha \in A} \alpha$. That is, $p \in \gamma$ iff $\exists \alpha \in A$ such that $p \in \alpha$.

(d) *Claim:* $\gamma \in \mathbb{R}$ (that is, γ is a "cut").
Proof:

i. *Claim:* γ satisfies the first property of "cuts": it's not empty and it's not the whole of $\mathbb{Q}$.
Proof:

A. Because $A \neq \varnothing$, $\exists \alpha_0 \in A$.
B. Because A is a set of "cuts", $\alpha_0 \neq \varnothing$.
C. Because $\gamma \equiv \bigcup_{\alpha \in A} \alpha$, $\alpha_0 \subset \gamma$, and so we have that $\gamma \neq \varnothing$.
D. Because $\forall \alpha \in A$, $\alpha \leq \beta$ and $\gamma \equiv \bigcup_{\alpha \in A} \alpha$, $\gamma < \beta$. That is, $\gamma \subsetneq \beta$. Thus, $\gamma \neq \mathbb{Q}$, because $\beta \neq \mathbb{Q}$.

ii. *Claim:* γ satisfies the second property for "cuts": γ is "closed" from below.
Proof:

A. Let $p \in \gamma$ (possible as $\gamma \neq \varnothing$).
B. Because $\gamma \equiv \bigcup_{\alpha \in A} \alpha$, $\exists \alpha_1 \in A$ such that $p \in \alpha_1$.
C. Pick some $q \in \mathbb{Q}$ such that $q < p$. Because α_1 is a cut, $q \in \alpha_1$.
D. But $\alpha_1 \subset \gamma$, so that $q \in \gamma$.

iii. *Claim:* γ satisfies the third property of "cuts": it has no largest element.

A. Let $p \in \gamma$ (possible as $\gamma \neq \varnothing$).
B. Because $\gamma \equiv \bigcup_{\alpha \in A} \alpha$, $\exists \alpha_1 \in A$ such that $p \in \alpha_1$.
C. Because α_1 is a "cut", $\exists r \in \alpha_1$ such that $p < r$.
D. But $\alpha_1 \subset \gamma$, so that $r \in \gamma$.

(e) *Claim:* γ is an upper bound of A.
Proof:

i. Let $\alpha_0 \in A$ be given.
ii. $\gamma \equiv \bigcup_{\alpha \in A} \alpha$, so that, in particular, $\alpha_0 \subset \gamma$.
iii. But by definition, that exactly means $\alpha_0 < \gamma$ or $\alpha_0 = \gamma$. That is, $\alpha_0 \leq \gamma$.
iv. Thus for any element α_0 of A, $\alpha_0 \leq \gamma$ and so γ is an upper bound on A.

(f) *Claim:* There is no smaller upper bound than γ on A.
Proof:

i. Let $\delta \in \mathbb{R}$ such that $\delta < \gamma$.
ii. Thus, $\delta \subsetneq \gamma$, which means that $\exists s \in \gamma \backslash \delta$.
iii. Because $\gamma \equiv \bigcup_{\alpha \in A} \alpha$ and $s \in \gamma$, $s \in \alpha_1$ for *some* $\alpha_1 \in A$.
iv. But then we found an element of A, α_1, which is *not* a subset of δ. Since $\exists s \in \alpha_1 \backslash \delta$, $\alpha_1 \neq \delta$ and as we have seen above in the proof that $<$ is an order, we also have $\delta \subset \alpha_1$: thus $\delta \subsetneq \alpha_1$ which is defined as $\delta < \alpha_1$.
v. As a result, δ is not an upper bound on A!
vi. So if $\delta < \gamma$ then δ is not an upper bound on A: γ is the least upper bound, $\gamma = \sup(A)$.

■

6. For any rational number $p \in \mathbb{Q}$, define its corresponding "cut" α_p as $\alpha_p := \{ q \in \mathbb{Q} \mid q < p \}$.
   Claim: α_p is indeed a "cut" for all $p \in \mathbb{Q}$.
   Proof:
   (a) Let $p \in \mathbb{Q}$ be given.
   (b) Clearly $\alpha_p \neq \varnothing$ because $(p-1) \in \alpha_p$. Additionally, $\alpha_p \neq \mathbb{Q}$ because $(p+1) \notin \alpha_p$. Thus the first condition for a cut is fulfilled.
   (c) It is also clear that if $r \in \alpha_p$ and $s < r$ then $s \in \alpha_p$ because $<$ is transitive for $\mathbb{Q}$.
   (d) Finally, if $r \in \alpha_p$ then $r < p$. Since both r and p are rational, so is $s := r + \frac{1}{2}(p-r)$. Clearly, $s \in \alpha_p$ and $r < s$, so that α_p has no largest element.

   ■

7. The special cut, ζ (which we will later identify as 0) is $\zeta := \{ r \in \mathbb{Q} \mid r < 0 \}$.
8. The other special cut, ω (which we will later identify as 1) is $\omega := \{ r \in \mathbb{Q} \mid r < 1 \}$.
9. For any two cuts $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$, define $+$ on them such that $\boxed{\alpha + \beta := \{ r + s \mid r \in \alpha \wedge s \in \beta \}}$.
10. For a given cut $\alpha \in \mathbb{R}$, define $-\alpha$ as $-\alpha := \{ p \in \mathbb{Q} \mid \exists r > 0 : (-p-r) \notin \alpha \}$. That is, $-\alpha$ contains all the rationals p such that there exists some rational smaller than $-p$ which is not in α.
11. *Claim:* $\alpha + (-\alpha) = \zeta$. (Proof as homework).
12. If $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$ such that $\alpha > \zeta$ and $\beta > \zeta$ then define multiplication as
    $\alpha\beta := \{ p \in \mathbb{Q} \mid p \leq rs \wedge r \in \alpha \wedge s \in \beta \wedge r > 0 \wedge s > 0 \}$
13. Define $\alpha\zeta = \zeta\alpha = \zeta$ for all $\alpha \in \mathbb{R}$

14. For all other α and β define $\alpha\beta := \begin{cases} (-\alpha)(-\beta) & \text{if} \alpha < \zeta \wedge \beta < \zeta \\ -[(-\alpha)\beta] & \text{if } \alpha < \zeta \wedge \zeta < \beta \\ -[\alpha(-\beta)] & \text{if } \zeta < \alpha \wedge \beta < \zeta \end{cases}.$

2.3 Homework

(can be found in Rudin)

1. *Claim:* The addition field axioms hold on $\mathbb{R}$ with ζ playing the role of the 'zero' element of $\mathbb{R}$.
2. *Claim:* The multiplication field axioms hold on $\mathbb{R}$ with ω playing the role of the 'one' element of $\mathbb{R}$.
3. *Claim:* The distributive law holds: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$
4. *Claim:* $\mathbb{R}$ is an ordered field ($\mathbb{R}$ is a field and an ordered set).
5. *Claim:* $\alpha_p + \alpha_q = \alpha_{p+q}$
6. *Claim:* $\alpha_p \alpha_q = \alpha_{pq}$
7. *Claim:* $\alpha_p < \alpha_q \Longleftrightarrow p < q$
8. *Claim:* Any two ordered fields with the least-upper-bound property are isomorphic.