PRINCIPLES OF ANALYSIS - LECTURE NOTES

PETER A. PERRY

1. Constructions of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

Beginning with the natural numbers $N = \{1, 2, 3, \ldots\}$ we can use set theory to construct, successively, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. We'll not give all details but discuss a few key points that arise in the constructions.

Recall that an *equivalence relation* among elements in a set S is a binary relation $\equiv$ with the following properties:

(i) (reflexivity) $a \equiv a$ for all $a \in S$
(ii) (symmetry) For all $a, b \in S$, if $a \equiv b$, then $b \equiv a$
(iii) (transitivity) For all $a, b, c \in S$, if $a \equiv b$ and $b \equiv c$, then $a \equiv c$

For a given $a \in S$, we denote by $[a]$ the *equivalence class* of a in S with respect to $\equiv$, i.e.,

$$[a] = \{b \in S : b \equiv a\}.$$

It is not too hard to see that the set of equivalence classes of elements of S partitions S into a disjoint union of subsets. Obviously, $a \in [a]$.

1.1. From $\mathbb{N}$ to $\mathbb{Z}$.

A natural way to construct $\mathbb{Z}$ from $\mathbb{N}$ is to represent elements of $\mathbb{Z}$ as formal differences $m - n$ where $m, n \in \mathbb{N}$. Of course there are many such representations, so we call two representations $m - n$ and $m' - n'$ *equivalent* if $m + n' = m' + n$. Observe that this is a statement about equality of natural numbers. The "backstory" is that we made the computation

$$\begin{aligned} m - n &= m' - n' && \text{(What we want to be true)} \\ m - n + n' &= m' && \text{(Add } n' \text{ to both sides)} \\ m + n' &= n + m' && \text{(Add } n \text{ to both sides)} \end{aligned}$$

in order to go from the statement we want to a legitimate statement about natural numbers.

Thus, to be strictly precise, we define $\mathbb{Z}$ to be the set of all *equivalence classes* $[m - n]$ of such representations where we say that

$$m - n \equiv m' - n' \text{ if } m + n' = m' + n. \tag{1.1}$$

A particular representation of $z = [m - n]$ by positive integers m and n is called *representative* of that equivalence class.

Date: August 24, 2018.

For legal purposes, be it duly noted that these notes are a gloss on the text *Introduction to Analysis* by Richard Beals. Therefore no originality is claimed for the presentation! Worse still, some of the proofs are lifted directly out of the text with trivial modifications.

These notes are for student use only in MA 575 Fall 2018 at the University of Kentucky.

From now on, if we want to define an operation on integers (addition, subtraction, multiplication) we need to be sure that our definition respects equivalence classes. Thus, for example, if we define

$$[m - n] + [p - q] = [(m + p) - (n + q)]$$

we want to be sure that the right-hand side defines the same integer, no matter which representative we pick for $[m - n]$ and $[p - q]$. That is, we need to check that if $m - n$, $m' - n'$ are two represenatives of $z = [m - n]$, and if $p - q$, $p' - q'$ are two representatives of $[p - q]$, then $[(m + p) - (n + q)] = [(m' + p') - (n' + q')]$.

Working backwards from the definition (1.1), we need to prove that

$$(m + p) + (n' + q') = (m' + p') + (n + q)$$

given that

$$m + n' = m' + n$$

and

$$p + q' = p' + q.$$

You should be able to do this using only facts about positive integers!

Similarly, we'd like to define multiplication of $z = [m - n]$ and $z' = [p - q]$ as[1]

$$z \cdot z' = [(mp + nq) - (np + mq)]$$

but we need to know that the right-hand side is the same no matter what choice of representatives we make for z and z'. In your homework you are asked to prove that this is the case.

In principle, one can *prove* all of the axioms involving addition, multiplication, and order relations among elements of $\mathbb{Z}$ from the corresponding facts of $\mathbb{N}$ and these definitions.

1.2. **From $\mathbb{Z}$ to $\mathbb{Q}$.** A natural way to construct $\mathbb{Q}$ from $\mathbb{Z}$ is to define elements of $\mathbb{Q}$ as expressions of the form m/n where $m \in \mathbb{Z}$ and $n \neq 0 \in \mathbb{Z}$. Once again, there are many ways of representing a given rational number as a quotient of integers, so we need to say when two such representations are equivalent and work with equivalence classes. Two representations of the same rational $q = m/n = m'/n'$ are *equivalent* if[2]

$$mn' = m'n. \tag{1.2}$$

Again we denote by $q = [m/n]$ the equivalence class of all representations of a given rational q as a quotient of integers m/n with $n \neq 0$.

We would like to define addition and multiplication of rationals in terms of equivalence classes. Again we have to check that our definitions respect equivalence

[1] The "backstory" here is that you use FOIL to compute

$$(m - n)(p - q) = mp + nq - np - mq = (mp + nq) - (np - mq).$$

[2] To derive this condition we compute, using the rules we want to be true (!),

$$\begin{aligned} \frac{m}{n} &= \frac{m'}{n'} \\ \frac{m}{n} \cdot nn' &= \frac{m'}{n'} \cdot nn' \\ mn' &= m'n \end{aligned}$$

classes. Thus, for example, to add two rationals $r_1 = [m/n]$ and $r_2 r = [p/q]$, we'd like to say that

$$r_1 + r_2 = [(mq + np)/nq].$$

In order for this definition to respect equivalence classes, we need to check that if m/n and m'/n' are two representatives for r_1, and if p/q and p'/q' are two representatives for r_2, then

$$\frac{mq + np}{np} = \frac{m'q' + n'p'}{n'q'} \tag{1.3}$$

provided

$$mn' = m'n, \quad pq' = p'q. \tag{1.4}$$

To state the condition(1.3) correctly in terms of properties of integers alone, we use (1.2) to rephrase (1.3) as

$$(mq + np) \cdot (n'q') = (np)(m'q' + n'p') \tag{1.5}$$

which should follow from the conditions (1.4) (does it?). Similarly, we'd like to define the multiplication of two rational $r_1 = [m/n]$ and $r_2 = [p/q]$ by the equation

$$r_1 r_2 = \left[\frac{mp}{nq}\right]. \tag{1.6}$$

For this notion to be well-defined, we need to know that if m/n, m'/n' are two representatives of r_1, and p/q, p'/q' are two representatives of r_2, then $mp/(nq) = m'p'/(n'q')$, or more precisely (recall (1.2))

$$mpn'q' = m'p'nq$$

provided (1.4) holds (check that this is so!).

1.3. **From $\mathbb{Q}$ to $\mathbb{R}$ by Dedekind Cuts.** The rationals are closed under the arithmetic operations of addition, subtraction, multiplication, and division, which means that simple linear equations like $ax + b = c$ can be solved over $\mathbb{Q}$. This is not the case for algebraic equations such as $x^2 = 2$ or $x^3 = 4$, which motivates the definition of the real numbers $\mathbb{R}$, an extension of the rational numbers $\mathbb{Q}$. Richard Dedekind[3] gave a set-theoretic construction of the real numbers from the rationals which we'll briefly describe.

For a given rational number q, consider the set

$$S_q = \{r \in \mathbb{Q} : r < q\}.$$

This set has the following properties:

(i) $S \neq \varnothing$, $S \neq \mathbb{Q}$,
(ii) If $r \in S$ and $s < R$, then $s \in S$,
(iii) S has no largest element.

Now let $S_{\sqrt{2}}$ be the set of all rationals q so that either $q \leqslant 0$ or $q^2 < 2$. You can check (carefully) that this set also has properties (i) - (iii), and might plausibly be taken as a set-theoretic definition of the *irrational* number $\sqrt{2}$. Dedekind's ideas was to *define* the real numbers as the set of all possible cuts of the rationals. It is clear that the mapping $q \mapsto S_q$ gives a one-to-one map from $\mathbb{Q}$ into the set of cuts (why is it one-to-one?) but, from the example of $S_{\sqrt{2}}$, it is clearly larger than

[3] Actually Julius Wilhelm Richard Dedekind (1831-1916), a German mathematician who worked in abstract algebra, algebraic number theory, and foundations.

$\mathbb{Q}$. As with our set-theoretic constructions of $\mathbb{Z}$ from $\mathbb{N}$ and $\mathbb{Q}$ from $\mathbb{Z}$, this gives us a plausible way to *deduce* the axioms of $\mathbb{R}$ from those of $\mathbb{Q}$ if we can define the basic operations (addition, multiplication, division, order) using the language of set theory.

Again, we won't attempt an exhaustive exposition of Dedekind's construction, but rather focus on a few highlights. For rational numbers, it clearly works to define

$$S_{q+q'} = \{r + s : r \in S_q, s \in S_{q'}\}$$

so we define addition of cuts by the set-theoretic construction

$$S + S' = \{r + s : r \in S, s \in S'\}.$$

One needs to check that $S + S'$ is in fact a cut in that it satisfies (i)-(iii) above. If so, then it is very easy to derive the commutative and associative laws of addition from those same laws for the rationals.

We can also define an order relation on real numbers "inherited" from the set-theoretic order relation on cuts. We say that $S < S'$ if $S \subset S'$ but $S \neq S'$. It is not hard to deduce from this definition the usual properties of the order relation on reals, such as trichotomy (one uses the corresponding trichotomy of sets satisfying (i)–(iii)).

We can also deduce that a monotone increasing, bounded sequence of real numbers must have a limit using the language of set theory. Such a sequence corresponds to a sequence of sets $\{S_n\}$ with the property that

$$S_1 \subset S_2 \subset \ldots \subset S_n \subset T$$

for all n and some cut T. One shows that the set

$$S = \bigcup_{n=1}^{\infty} S_n$$

is a cut, which is then defined to be the limit of the real numbers $\{S_n\}$ (where is the condition that all of the S_n contained in a fixed cut T used?).

2. The Real Numbers

Here we'd like to state the axioms of the real numbers, state the Least Upper Bound property, and derive a few basic results about the real numbers. We'll repair what appears to be a circularity in the presentation from Beals' text, section 2A.

We'll begin with a list of axioms for the real numbers and see where it leads us!

Axioms of Addition.

A1 $(a + b) + c = a + (b + c)$
A2 $a + b = b + a$
A3 There is an element 0 so that $a + 0 = a$
A4 For each $a \in \mathbb{R}$ there is an element $-a$ with $a + (-a) = 0$

Axioms of Multiplication.

M1 $(ab)c = a(bc)$
M2 $ab = ba$
M3 There is an element $1 \neq 0$ so that, for all $a \in \mathbb{R}$, $a \cdot 1 = a$
M4 For each $a \in \mathbb{R}$ with $a \neq 0$, there is an element a^{-1} so that $a \cdot a^{-1} = 1$

Distributive Law of Multiplication over Addition.

D $(a+b)c = ac + bc$; $a(b+c) = ab + ac$

Order Axioms.

O1 For any a and b, exactly one of the following is true: $a < b$, $a > b$, $a = b$
O2 If $a < b$ and $b < c$, then $a < c$
O3 If $a < b$, then $a + c < b + c$
O4 If $a < b$ and $0 < c$, then $ac < bc$
O5 (Archimedian Property) If $0 < a$ and $0 < b$, there is a positive integer n so that $b < a + a + \ldots + a$ (N summands)
O6 (Least Upper Bound Property) If A is any nonempty subset of $\mathbb{R}$ that is bounded above, then there is a least upper bound for A

2.1. **Some basic Propositions.**

(a) The elements 0 and 1 are unique
(b) For any $a \in \mathbb{R}$, $-a$ is unique
(c) For any $a \neq 0$ in $\mathbb{R}$, a^{-1} is unique
(d) For any a, $-(-a) = a$ and for any $a \neq 0$, $(a^{-1})-1 = a$
(e) For any $a \in \mathbb{R}$, $a \cdot 0 = 0$ and $(-1) \cdot a = -a$
(f) For any $a \in \mathbb{R}$, exactly one of the following is true: $0 < a$, $0 < (-a)$, or $a = 0$
(g) For any $a, b \in \mathbb{R}$, $a < b$ if and only if $0 < b - a$

Before we get started we need to prove the *additive cancellation law*: if a, b, and c are real numbers and $a + c = b + c$, then $a = b$.

Proof. Either $a = b$, $a < b$ or $b < a$ by O1. Suppose $b < a$; then by O3 $b + c < a + c$, a contradiction. Similarly, if $a < b$, then $a + c < b + c$. Hence, $a = b$. □

Using O4 you can prove a similar *multiplicative cancellation law*–it would be a good idea to state and prove it to test your understanding of the previous proof!

It's now easy to prove that the additive identity 0, the multiplicative identity 1, and additive inverse $(-a)$, and the multiplicative inverse a^{-1}, are all unique. We use a common strategy: suppose that there are two of the object to be proven unique, and show that they are equal. Here's how it works for the additive identity 0.

☞A first fundamental proof strategy

Proof. Suppose that 0 and $0'$ are both additive identities, and let a be any real number. Since $a + 0 = a + 0' = a$ we may deduce

$$\begin{aligned} a + 0 &= a + 0' && \text{Property of additive identity} \\ 0 &= 0' && \text{Cancellation law for addition} \end{aligned}$$

and conclude that 0 is unique. □

2.2. **Some Slightly Less Basic Propositions.**

(a) Given $a, b \in \mathbb{R}$, there is a unique x such that $a + x = b$
(b) Given $a \neq 0$ and b in $\mathbb{R}$, there is a unique y such that $ay = b$
(c) If a and b are positive, then $a + b$ and ab are positive
(d) If $0 < a < b$, then $0 < 1/b < 1/a$

We'll prove (a) and (b) using the additive and multiplicative cancellation laws. This proof uses a second common strategy for mathematical proof: to show than an object exists and is unique, first exhibit one such object, and then use the uniqueness proof strategy above to show that the object is uniquely defined.

☞A second fundamental proof strategy

Proof. (a) To show that such an x exists, let[4] $x = b + (-a)$. Then

$$\begin{aligned} a + x &= a + b + (-a) && \text{(definition of } x\text{)} \\ &= a + (b + (-a)) && \text{by (A1)} \\ &= a + ((-a) + b) && \text{by (A2)} \\ &= (a + (-a)) + b && \text{by (A1)} \\ &= 0 + b && \text{by (A4)} \\ &= b && \text{by (A3)} \end{aligned}$$

so we have shown the existence of such an x.

Now suppose that x' is any other solution. Then $a + x = a + x' = b$ so

$$\begin{aligned} a + x &= a + x' && \text{(hypothesis)} \\ x &= x' && \text{(cancellation property)} \end{aligned}$$

The proof of (b) is similar. □

You can easily prove (c) and (d) using O3 and O4.

2.3. A Much Less Basic Proposition.

Theorem 2.1. *Suppose that b is a positive real number and n is a positive integer. There is a unique positive real number a such that $a^n = b$.*

Proof. First, we note that for any real numbers x and y,

$$y^n - x^n = (y - x)\left(y^{n-1} + y^{n-2} + x + \ldots + yx^{n-2} + x^{n-1}\right) \tag{2.1}$$

which shows that the map $x \mapsto x^n$ preserves order, i.e., $x < y \Rightarrow x^n < y^n$. In a strategy reminiscent of Dedekind cuts, we try to construct the unique positive nth root of b as the least upper bound of the set

$$A = \{x \in \mathbb{R} : x^n < b\}.$$

The set A is bounded above: if $0 < b < 1$, any $x > 1$ has $x^n > 1$ by O4 (so 1 is an upper bound for A), while if $b > 1$ and $x > b$, then $x^n > b$ again by O4 (so b is an upper bound for A). Now let

$$a = \text{lub}(A).$$

We claim that $a^n = b$. By trichotomy, either $a^n < b$, $a^n > b$, or $a^n = b$ so it suffices to rule out the other two possibilities. We'll first show that $a^n > b$. Suppose that $x > 0$ and $x^n < b$. We claim that there is a $y > x$ so that, also, $y^n < b$. Supposing that $y \leqslant x + 1$, we can use (2.1) to estimate $y^n - x^n$, and will succeed if we can choose a y so that $y^n - x^n < (b - x^n)/2$ (why?). From (2.1) we can estimate

☞One might be tempted to use proof by contradiction here, but, with apologies to St. Paul (see Romans 12:31), Beals will show you a more excellent way!

$$y^n - x^n \leqslant (y - x)n(x + 1)^{n-1}$$

[4] Once again, the "backstory" is that we do a (suppressed) back of the envelope computation to see what x *should* be, but then prove that our suspect x actually works using the axioms for the real numbers.

since $y \leqslant x + 1$ and there are n right-hand terms in (2.1). We can make the right hand side smaller than $(b - x^n)/2$ by choosing

$$(y - x) < (b - x^n)/2(n(x + 1)^{n-1})$$

which is possible because the right-hand side is positive. Hence, no x with $x^n < b$ is an upper bound for S, and hence $a^n \geqslant b$.

On the other hand, suppose that y is positive and $y^n > b$. If we can find an $x < y$ with $b < x^n$, it will follow that y is not a least upper bound so that $a^n \leqslant b$. We can assume that $x \geqslant y - 1$ and use a similar technique to show that such an x can be chosen. □