MATH 215 Mathematical Analysis, Spring 2012

Handout 3: Construction of the Real Numbers

Laurence Barker, Mathematics Department, Bilkent University,
version: 17 April 2012.

These notes summarize some material that was presented with more background narrative in lectures. All of the material below is of fundamental importance to the so-called "conceptual" approach to mathematics. The parts on the syllabus for this Mathematical Analysis course are:

Section 2: Equivalence Relations.

Section 5: Construction of the real numbers.

Section 6: Completion of a metric space (omitted from this version of the notes, but discussed in class, and outlined in a step-by-step way in Exercise 3.24 of the textbook).

The parts not on the syllabus are:

Section 1: Axiomatic definition of the real numbers (because memorizing the axioms would be a waste of time).

Section 3: Construction of congruence classes of integers (but it is a nice model for a technique that is used frequently throughout mathematics, and I advise reading it in preparation for Sections 5 and 6).

Section 4: Construction of the natural numbers, the integers and the rational numbers (perhaps not "analysis", but still a necessary part of the story).

Note: in this draft, I find that I have included quite a lot of material, but it was written in haste, and there are sure to be many minor mistakes.

1: Axiomatic definition of the real numbers

The following two very general definitions will be needed. A **binary operation** $*$ on a set S, often simply called an **operation** on S, is defined to be a function $* : S \times S \to S$. Often, we write the value at (s,t) not as $*(s,t)$ but as $s * t$. A **relation** $\sim$ on S is formally defined to be a subset of $S \times T$. Usually, we write $s \sim t$ instead of $(s,t) \in \sim$. Thus, $\sim$ associates each element $(s,t) \in S \times T$ with a statement $s \sim t$.

We may understand the set of real numbers $\mathbb{R}$ to be equipped an operation called addition, written $(x,y) \mapsto x+y$, an operation called multiplication, written $(x,y) \mapsto xy$ and a relation $\leq$ called the ordering, such that the following axioms hold:

F1: Additive Associativity Axiom: $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{R}$.

F2: Zero Axiom: There is an element $0 \in \mathbb{R}$ such that $0 + x = x$ for all $x \in \mathbb{R}$.

F3: Negation Axiom: For all $x \in \mathbb{R}$, there is an element $-x \in \mathbb{R}$ such that $x + (-x) = 0$.

F4: Additive Commutativity Axiom: $x + y = y + x$ for all $x, y \in \mathbb{R}$.

F5: Distributivity Axiom: $x(y + z) = xy + xz$ for all $x, y, z \in \mathbb{R}$.

F6: Multiplicative Associativity Axiom: $x(yz) = (xy)z$ for all $x, y, z \in \mathbb{R}$.

F7: Unity Axiom: There is an element $1 \in \mathbb{R}$ such that $1x = x$ for all $x \in \mathbb{R}$.

F8: Inversion Axiom: For all non-zero $x \in \mathbb{R}$, there is an element $x^{-1} \in \mathbb{R}$ such that $x^{-1}x = 1$.

F9: Multiplicative Commutativity Axiom: $xy = yx$ for all $x, y \in \mathbb{R}$.

T1: Reflexivity Axiom: $x \leq x$ for all $x \in \mathbb{R}$

T2: Anti-symmetry Axiom: For all $x, y \in \mathbb{R}$ satisfying $x \leq y$ and $y \leq x$, we have $x = y$.

T3: Transitivity Axiom: For all $x, y, z \in \mathbb{R}$ satisfying $x \leq y$ and $y \leq z$, we have $x \leq z$.

T4: Commensurability Axiom: $x \leq y$ or $y \leq x$ for all $x, y \in \mathbb{R}$.

O1: Additive Ordering Axiom: For all $x, y, z \in \mathbb{R}$ satisfying $y \leq z$, we have $x + y \leq x + z$.

O2: Multiplicative Ordering Axiom: For all $x, y \in \mathbb{R}$ satisfying $0 \leq x$ and $0 \leq y$, we have $0 \leq xy$.

O3: Least Upper Bound Axiom: Any non-empty subset of $\mathbb{R}$ with an upper bound has a least upper bound.

All of these axioms, except for the last three, crop up in many different kinds of important mathematical structures. For instance, anything satisfying F1, F2, F3, F4 is called an **abelian group**. Anything satisfying F1 to F6 is called a **ring**. Anything satisfying F1 to F9 is called a **field**. Anything satisfying T1, T2, T3 is called a **partial ordering**. Those four concepts appear very frequently throughout most of mathematics. Anything satisfying T1, T2, T3, T4 is called a **total ordering**.

Of course, there are some other important features of $\mathbb{R}$, such as subtraction $x-y$, division x/y, absolute value $|x|$, taking limits $\lim_n x_n$. But these can be defined in terms of the equipment specified above. For instance, subtraction is defined to be the operation on $\mathbb{R}$ sending (x, y) to the real number $x - y = x + (-y)$.

It can be shown that, given two structures $\mathbb{R}_1$ and $\mathbb{R}_2$ satisfying all the above axioms, then there exists a unique bijection $\theta : \mathbb{R}_1 \to \mathbb{R}_2$ such that $\theta(x+y) = \theta(x)+\theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in \mathbb{R}_1$. It can also be shown that θ satisfies $x \leq y$ if and only if $\theta(x) \leq \theta(y)$. Thus, $\mathbb{R}_1$ and $\mathbb{R}_2$ are copies of each other. That allows us to avoid the metaphysical question as to what, exactly, the real numbers are. All copies of $\mathbb{R}$ are copies of each other, and no practical meaning can be assigned to any notion of, so to speak, the genuine original $\mathbb{R}$. Our concern, essentially, is with the common structure shared by all the copies of $\mathbb{R}$.

Below, we shall give a construction of $\mathbb{R}$, starting from the notion of a set. The motive for doing this is not just to check that such a structure $\mathbb{R}$ exists. The construction is useful in itself. It also illustrates various techniques that are often employed elsewhere in mathematics.

2: Equivalence Relations

A relation $\equiv$ on a set S is called an **equivalence relation** provided it satisfies the following four conditions for all $x, y, z \in S$.

Reflexivity Axiom: We have $x \equiv x$.

Symmetry Axiom: If $x \equiv y$ then $y \equiv x$.

Transitivity Axiom: If $x \equiv y$ and $y \equiv z$ then $x \equiv z$.

Plenty of examples will be given in later sections. Given an equivalence relation $\equiv$ on a set S and an element $x \in S$, the set

$$[x] = \{y \in S : y \equiv x\}$$

is called the **equivalence class** of x under $\equiv$.

Remark 2.1: *With the notation above, S is the disjoint union of the equivalence classes under $\equiv$. In other words, each element of S belongs to a unique equivalence class.*

Proof: Given $x \in S$ then, by reflexivity, $x \in [x]$. So S is the union of the equivalence classes. To show that the union is disjoint, it suffices to show that, given an equivalence class $[z]$ then, for all $y \in [z]$, we have $[y] = [z]$. For all $x \in [y]$, we have $x \equiv y$ and $y \equiv z$ hence, by transitivity, $x \equiv z$, in other words, $x \in [z]$. We have shown that $[y] \subseteq [z]$. By the symmetry condition, $z \in [y]$. Repeating the above argument with z and y interchanged, we deduce that $[z] \subseteq [y]$. Therefore $[y] = [z]$, as required. $\square$

3: Construction of congruence classes of integers

In this section, we presume familiarity with the set $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ of integers, and we shall discuss the set $\mathbb{Z}/n$ of integers modulo n, where n is a positive integer. We shall equip this set with addition and multiplication operations.

The definition of $\mathbb{Z}/n$ is based on the relation $\equiv_n$ on $\mathbb{Z}$ such that, given $x, y \in \mathbb{Z}$ then $x \equiv_n y$ if and only if n divides $x - y$. We claim that $\equiv_n$ is an equivalence relation. Consider $x, y, z \in \mathbb{Z}$. If $x \equiv y$ and $y \equiv z$, in other words, if n divides $x - y$ and $y - z$, then n divides the integer $x - y + y - z = x - z$, in other words, $x \equiv z$. We have shown that $\equiv_n$ satisfies the Transitivity Axiom. Similar and easier arguments show that $\equiv_n$ satisfies the Reflaxivity and Symmetry Axioms. The claim is established.

We define $\mathbb{Z}/n$ to be the set of equivalence classes under $\equiv$. That is to say,

$$\mathbb{Z}/n = \{[x]_n : x \in \mathbb{Z}\}$$

where $[x]_n$ denotes the equivalence class of x under $\equiv_n$. We define an operation on $\mathbb{Z}/n$, called addition, given by

$$[x]_n + [y]_n = [x + y]_n$$

and another operation on $\mathbb{Z}/n$, called multiplication, given by

$$[x]_n \, [y]_n = [xy]_n \; .$$

We must show that these operations are well-defined, in other words, unambiguous. Before doing so, let us be clear about what the problem is. We defined addition to be such that, given elements X and Y of $\mathbb{Z}/n$, then $X + Y$ is to be the element of $\mathbb{Z}/n$ such that, choosing x and y satisfying $X = [x]$ and $Y = [y]$, then $X + Y = [x + y]$. What we must check is that, if we had chosen different integers x' and y' such that $X = [x']$ and $Y = [y']$, then we would have arrived at the same element $X + Y = [x' + y']$. Now, since $[x] = [x']$ and $[y] = [y']$, the integers $x - x'$ and $y - y'$ are divisible by n, hence $(x + y) - (x' + y')$ is divisible by n. Therefore $[x + y] = [x' + y']$, as required. The well-definedness of the multiplication is almost as easy. Again assuming that $[x] = [x']$ and $[y] = [y']$, then n divides the integer $(x - x')y = xy - x'y$, so

$[xy] = [x'y]$. Similarly, $[x'y] = [x'y']$. We conclude that $[xy] = [x'y']$ and that the multiplication operation is well-defined.

Let us point out that $\mathbb{Z}$ and $\mathbb{Z}/n$ are rings, we mean to say, they satisfy Axioms F1 to F6. In fact, they also satisfy Axioms F7 and F9. It is not hard to see that, furthermore, $\mathbb{Z}/n$ is a field if and only if n is prime.

Exercise 3.A: Let X be a set and let $d : X \times X \to \mathbb{R}$ be a function such that, for all $x, y, z \in X$, we have: $d(x, y) \geq 0$ and $d(x, x) = 0$; also $d(x, y) = d(y, x)$; also $d(x, z) \leq d(x, y) + d(y, z)$. Consider the relation $\equiv$ on X such that $x \equiv y$ if and only if $d(x, y) = 0$.
(1) Show that $\equiv$ is an equivalence relation.
(2) Letting $\mathcal{X}$ denote the set of equivalence classes under $\equiv$, show that there is a well-defined function $\delta : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ such that $\delta([x], [y]) = d(x, y)$.
(3) Show that δ is a metric on $\mathcal{X}$.

One application of the latest exercise is in the notion of the Hilbert space $L^2(\mathbb{R})$. Often, $L^2(\mathbb{R})$ is casually described as the metric space consisting of the functions $f : \mathbb{R} \to \mathbb{C}$ such that $\int_{-\infty}^{\infty} |f(x)|^2 \, dx$ is defined and finite, the metric being given by $d(f, g) = \int_{-\infty}^{\infty} \overline{g(x)} \, f(x) \, dx$. But, letting c run over the real numbers, consider the functions f_c such that $f_c(x) = 1$ when $x = c$ and $f_c(x) = 0$ otherwise. These functions are mutually distinct but mutually equivalent in the sense of the above exercise, $d(f_c, f_{c'}) = 0$ for any $c, c' \in \mathbb{R}$. Strictly speaking, the metric space $L^2(\mathbb{R})$ is the set of equivalence classes under that equivalence relation.

4: Construction of the natural numbers, the integers and the rational numbers

Let us start from the notion of a set. A set S is said to be **finite** provided every injection $S \to S$ is a bijection. Two finite sets are said to be **equipotent** provided there is a bijection between them. Ignoring some deep roubles with set theory (the notion of the "set of finite sets" is logically tricky), equipotency of finite sets is an equivalence relation. Let $\mathbb{N}$ be the set of equivalence classes here. We write $|X|$ to denote the equivalence class of a finite set X. The elements of $\mathbb{N}$ are $0 = |\emptyset|$ and $1 = |\{0\}|$ and $2 = |\{0, 1\}|$ and so on. Addition on $\mathbb{N}$ is defined to be such that $|X| + |Y| = |X \cap Y|$ when X and Y are disjoint. Multiplication on $\mathbb{N}$ is defined to be such that $|X| \, |Y| = |X \times Y|$. The ordering on $\mathbb{N}$ is defined to be such that $|X| \leq |Y|$ provided there exists an injection $X \to Y$. It is laborious but easy to check that, equipped with that structure, $\mathbb{N}$ satisfies Axioms F1, F2 and F4 to F7, also F9 and T1 to T4 and O1 to O3.

We define $\mathbb{Z}$ to be the set of equivalence classes under the equivalence relation on $\mathbb{N} \times \mathbb{N}$ whereby $(a, b) \equiv (a', b')$ provided $a + b' = a' + b$. To check that $\equiv$ is an equivalence relation, note that reflexivity and symmetry are obvious, and transitivity holds because, if $a + b' = a' + b$ and $a' + b'' = a'' + b'$ then

$$a + b' + b'' = a' + b + b'' = a'' + b + b'$$

hence $a + b'' = a'' + b$. Write $[a, b]$ for the equivalence class of (a, b). We define addition and multiplication operations on $\mathbb{Z}$ such that

$$[a, b] + [c, d] = [a + b, c + d] \ , \qquad [a, b][c, d] = [ac + bd, ad + bd] \ .$$

Proof of the well-definedness of addition is very easy. In class, we took the trouble to show that the multiplication is well-defined.

We impose an ordering relation $\leq$ on $\mathbb{Z}$ such that $[a, b] \leq [c, d]$ provided $a + d \leq b + c$. Via some long but easy arguments, it can be shown that the relation $\leq$ on $\mathbb{Z}$ is well-defined and that $\mathbb{Z}$ satisfies many but not all of the axioms listed in Section 1.

We regard $\mathbb{N}$ as a subset of $\mathbb{Z}$ by identifying each element $a \in \mathbb{N}$ with the element $[a, 0] \in \mathbb{Z}$. Note that the addition and multiplication operations on $\mathbb{N}$ extend to the addition and multiplication operations on $\mathbb{Z}$. There is an evident way of defining a subtraction operation on $\mathbb{Z}$ and, under the identification we have made,

$$[a, b] = a - b \ .$$

It may be felt that the elements of $\mathbb{N}$, as defined above, are not the usual natural numbers that we have always known, and likewise for the elements of $\mathbb{Z}$. There are many different ways of defining copies of $\mathbb{N}$, but any copy will do just as well as any other copy, likewise for $\mathbb{Z}$.

Variants of the above construction of $\mathbb{N}$ occasionally appear elsewhere in mathematics, and variants of the above construction of $\mathbb{Z}$ appear frequently. (As it happens, the day after presenting some of the above material in class, I was giving a seminar where both of those constructions were adapted as part of the definition of a mathematical object called the monomial Burnsider ring.) Variants of the next construction, too, are frequently applied in many different contexts.

We follow the same approach to constructing the set of rational numbers $\mathbb{Q}$. Let S be the set of pairs (α, β) where $\alpha, \beta \in \mathbb{Z}$ and $\beta > 0$. We define an equivalence relation on S such that (α, β) is equivalent to (α', β') provided $\alpha\beta' = \alpha'\beta$. Writing $[\alpha, \beta]$ for the equivalence class of (α, β), we define

$$[\alpha, \beta] + [\gamma, \delta] = [\alpha + \gamma, \beta\delta] \qquad\qquad [\alpha, \beta]\, [\gamma, \delta] = [\alpha\gamma, \beta\delta] \ .$$

We define $\leq$ on $\mathbb{Q}$ such that $[\alpha, \beta] \leq [\gamma, \delta]$ provided $\alpha\delta \leq \gamma\beta$. The rest of the discussion for $\mathbb{Q}$ proceeds much as for $\mathbb{Z}$. We omit the details. Eventually, $\mathbb{Q}$ is shown to satisfy all of the axioms in section 1 except for Axiom O3, and $\mathbb{Z}$ is realized as a subset of $\mathbb{Q}$ by means of the identification

$$[\alpha, \beta] = \alpha/\beta \ .$$

We point out that the addition, multiplication and ordering on $\mathbb{Q}$ extend the addition, multiplication and ordering on $\mathbb{Z}$.

There are, of course, other ways of constructing $\mathbb{Q}$. For instance, instead of constructing $\mathbb{Z}$ followed by $\mathbb{Q}$, we could have constructed the set of non-negative rational numbers $\mathbb{Q}^+$ from $\mathbb{N}$ using a variant of the latest construction, and then we could have constructed $\mathbb{Q}$ from $\mathbb{Q}^+$ using a variant of the penultimate construction. That would yield a different copy of $\mathbb{Q}$ and, strictly speaking, we perhaps ought to denote it by a different symbol, say, $\mathbb{Q}'$. However, a long but routine argument shows that there is a bijective correspondence $\mathbb{Q} \leftrightarrow \mathbb{Q}'$ preserving the addition operations, the multiplication operations and the ordering operations on the two sets. Thus, $\mathbb{Q}$ and $\mathbb{Q}'$ have the same structure, and they amount to the same thing.

5: Construction of the real numbers

We now apply the above techniques to construct a copy of the real numbers. A sequence $\underline{a} = (a_0, a_1, ...)$ of rational numbers is called a **Cauchy sequence** provided, for all positive rational numbers E, there exists a natural number N such that, for all natural numbers n and m with $n \geq N \leq m$, we have $|a_n - a_m| < E$. As another way of saying this: for all rational $E > 0$, we have $|a_n - a_m| < E$ for sufficiently large n and m.

Let $\mathcal{R}$ be the set of Cauchy sequences. Given $\underline{a}, \underline{b} \in \mathcal{R}$, we define

$$\underline{a} + \underline{b} = (a_0 + b_0, a_1, b_1, ...) \;, \qquad \underline{a} \,.\, \underline{b} = (a_0 b_0, a_1 b_1, ...) \;.$$

As we saw in class, it is easy to check that $\underline{a} + \underline{b}$ is a Cauchy sequence. A little more work is needed to arrive at the same conclusion for $\underline{a} \,.\, \underline{b}$. For that, we need the following lemma. Let us mention that variants of the following proof appear several times in the course material.

Lemma 5.1: *Let $\underline{a}$ be a Cauchy sequence of rational numbers. Then $\underline{a}$ has an upper bound. In other words, there exists a positive rational number A such that $a_n < A$ for all n.*

Proof: Choose $N \in \mathbb{N}$ such that $|a_n - a_m| < 1$ for all $n \geq N \leq m$. Then $|a_n - a_N| < 1$ for all $n \geq N$. Put $A = 1 + \max\{a_0, a_1, ..., a_N\}$. $\square$

For $\underline{a}$ and $\underline{b}$ be as above, choose upper bounds A and B, respectively. Given rational $E > 0$, we have $|a_n - a_m| < E/2B$ and $|b_n - b_m| < E/2A$ for sufficiently large n and m, whence

$$|a_n b_n - a_m b_m| = |a_n b_n - a_m b_n + a_m b_n - a_m b_m| \leq |a_n b_n - a_m b_n| + |a_m b_n - a_m b_m|$$

$$\leq |a_n - a_m| B + A |b_n - b_m| < \frac{E}{2B} B + A \frac{E}{2A} = E \;.$$

We have shown that $\underline{a} + \underline{b}$ is a Cauchy sequence.

Let $\equiv$ be the relation on $\mathcal{R}$ such that $\underline{a} \equiv \underline{a'}$ provided, for all rational $E > 0$, we have $|a_n - a'_n| < E$ for sufficiently large N. We claim that $\equiv$ is an equivalence relation. Suppose that $\underline{a} \equiv \underline{a'}$ and $\underline{a'} \equiv \underline{a''}$. Then, for all rational $E > 0$, we have $|a_n - a'_n| < E/2 > |a'_n - a''_n|$, whence $|a_n - a'_n| < E$. We have established transitivity. The proof of the claim is completed by observing that $\equiv$ is plainly reflexive and symmetric.

We write $[\underline{a}] = [a_0, a_1, ...]$ to denote the equivalence class of $\underline{a}$. We define $\mathbb{R}$ to be the set of equivalence classes,

$$\mathbb{R} = \{[\underline{a}] : \underline{a} \in \mathcal{R}\} \;.$$

We define addition and multiplication to be such that

$$[\underline{a}] + [\underline{b}] = [\underline{a} + \underline{b}] = [a_0 + b_0, a_1 + b_2, ...] \;, \qquad [\underline{a}]\,[\underline{b}] = [\underline{a} \,.\, \underline{b}] = [a_0 b_0, a_1 b_2, ...] \;.$$

Exercise 5.A: Show that the addition and multiplication operations on $\mathbb{R}$ are well-defined.

We define a relation $<$ on $\mathbb{R}$ such that $[\underline{a}] < [\underline{b}]$ provided $[\underline{a}] \neq [\underline{b}]$ and $a_n < b_n$ for sufficiently large n. We define $\leq$ on $\mathbb{R}$ such that $\underline{a} \leq \underline{b}$ provided $\underline{a} < \underline{b}$ or $\underline{a} = \underline{b}$.

Exercise 5.B: Show that the relation $<$ is well-defined.

Exercise 5.C: Show that $\underline{a} \leq \underline{b}$ if and only if, for all rational $E > 0$, we have $b_n - a_n < E$ for all sufficiently large n.

There is a long list of further exercises in checking that $\mathbb{R}$, as defined in this section, satisfies all the axioms listed in Section 1. For all except one of those axioms, the argument is straightforward and makes use of the fact, noted above, that the axiom is satisfied by $\mathbb{Q}$. The exception is the Axiom O3, which we shall deal with below.

We regard $\mathbb{Q}$ as a subset of $\mathbb{R}$ by identifying each rational number a with the element $[a, a, a, ...]$ of $\mathbb{R}$. Plainly, the addition, multiplication and ordering on $\mathbb{R}$ are extensions of those operations and that relation on $\mathbb{Q}$.

Before demonstrating that our constructed $\mathbb{R}$ satisfies O3, the Least Upper Bound Axiom, we prove another fundamental property. Let us take it as granted, now, that $\mathbb{R}$, as constructed above, satisfies all of the other specified axioms. Let us also take it for granted that all necessary preliminary features, such as the subtraction operation $(x, y) \mapsto x - y$ and the absolute value $x \mapsto |x|$ have been defined and have had their basic properties established: for instance, the Triangle Inequality $|x - z| \leq |x - y| + |y - z|$.

We define a **Cauchy sequence** of real numbers to be a sequence $\underline{x} = (x_0, x_1, ...)$ of real numbers such that, for all $\epsilon > 0$, we have $|x_n - x_m| < \epsilon$ for sufficiently large n. Evidently, this extends the notion of a Cauchy sequence of rational numbers.

Theorem 5.2: (Completeness of the Real numbers; also called Cauchy's Criterion for Convergence.) *A sequence of real numbers is convergent if and only if it is a Cauchy sequence.*

Proof: Let $\underline{x}$ be a sequence of real numbers. An easy application of the Triangle Inequality shows that, if $\underline{x}$ is convergent, then $\underline{x}$ is Cauchy. The converse is similar to an argument in the next section. $\square$

6: Completion of a metric space

This section is omitted, for the time-being.