Real Analysis
Lecture Notes

Set Theory & The Real Number System

September 14 2016
Last update: October 7, 2016

1 Well-Ordering Principle

Recall the well-ordering principle we introduced last class: Every set X can be well-ordered. That is, there exists a ordering relation $\prec$ that well orders X.

Proposition: There exists an uncountable set X that is well-ordered by a relation $\prec$ so that:

(i) There is a largest element $\Omega \in X$.

(ii) If $x \in X$ and $x \neq \Omega$ then x has only a countable number of predecessors. That is, the set $\{y \in X \ : \ y < x, x \in X, x \neq \Omega\}$ is countable.

Proof. Take any uncountable set Y. By the well-ordering principle, there exists some well-ordering, say $<$, on Y. If Y has a largest/last element then call this element α. If Y does not have a last element, then take some $\alpha \notin Y$ and form the union $Y \cup \{\alpha\}$ such that $y < \alpha$ for all $y \in Y$.

We should first confirm that this set new set $Y \cup \{\alpha\}$ well-ordered. To verify this we must verify that any nonempty subset has a least element. To this end, take an arbitrary nonempty subset $S \subseteq Y$. We now consider two cases for possible subsets S:

Case 1: $S = \{\alpha\}$. Clearly this has a least element.

Case 2: $S \neq \{\alpha\}$ (S contains at least one element that is not α). Take the intersection $S \cap Y$. Since $S \neq \emptyset$ and $S \subseteq Y$ we have that $S \cap Y$ cannot be empty. Additionally, it is clear that $S \cap Y \subseteq Y$ by the definition of intersection. By our initial assumption that Y is well-ordered we find that $S \cap Y$ is well-ordered since a subset of a well-ordered set inherits its well-order.[1] Hence, $S \cap Y$ has a least element. Label this least element β. If we take S to be the entire set Y, we see that some β is also the least element of S. Thus, $Y \cup \{\alpha\}$ is indeed well-ordered.

[1] This was established in the first lecture.

Basically, we've shown that this process of appending some last element α to our original set Y doesn't damage its well-ordering.

Moving on, we note that α has an uncountable number of predecessors since Y has an uncountable number of elements. That is, we have essentially placed a largest α ahead of an uncountable number of elements.

Let F be the set of *all* the elements of $Y \cup \{\alpha\}$ which have an uncountable number of predecessors. Clearly F is not empty since we have just established that $\alpha \in F$. However, note that $Y \cup \{\alpha\}$ is well-ordered and so every nonempty subset has a least element. Therefore, our set $F = \{$elements with an uncountable number of predecessors$\}$ must have a least element since F is itself a subset of $Y \cup \{\alpha\}$.

Let Ω be this least element of F. So, Ω has an uncountable number of predecessors. In fact, Ω is the "smallest" element with an uncountable number of predecessors in our uncountable set $Y \cup \{\alpha\}$.

Finally, construct the set X such that

$$X = \big\{y \in Y \ : \ y \leq \Omega\big\}$$

Clearly $\Omega \in X$, satisfying our first goal in the proof. Furthermore, if we consider the subset, for $x \in X$ and $x \neq \Omega$,

$$\{y \in X \ : \ y < x\}$$

then since Ω was the smallest element with an uncountable number of predecessors, the all elements of $\{y \in X \ : \ y < x\}$ must have only a countable number of predecessors, and so the set itself must be countable,[2] which satisfies our second goal, as desired. □

We call the last element $\Omega \in X$ to be the first *uncountable ordinal*, and the set X is called the set of ordinals less than or equal to the first uncountable ordinal. The elements $x < \Omega$ are called *countable ordinals*. If the set $\{y \ : \ y < x\}$ is finite, then x is called a *finite ordinal*. Suppose ω is the first *nonfinite ordinal*. Then the set $\{x \ : \ x < \omega\}$ is the set of finite ordinals and is equivalent (in the sense of an ordered set), to the set of naturals $\mathbb{N}$.[3]

2 A Review of Basic Algebra

2.1 Groups

A group is some set G with a binary operation θ defined for elements $g \in G$ such that

[2] I'm a little shaky on this final point: Is it immediately obvious that if all x in this set have a countable number of predecessors then the set must be countable?

[3] i.e. It is countable?

(1) If $g_1, g_2 \in G$ then $g_1 \ \theta \ g_2 \in G$ (θ-closure).

(2) $(g_1 \ \theta \ g_2) \ \theta \ g_3) = g_1 \ \theta \ (g_2 \ \theta \ g_3)$ (associativity).

(3) $\exists \, z$ such that z is unique and $g_1 \ \theta \ z = z \ \theta \ g_1 = g_1$ (identity element).[4]

(4) $\forall \, g \in G, \ \exists \, h_1$ such that h_1 is unique and $g_1 \ \theta \ h_1 = h_1 \ \theta \ g_1 = z$ (inverse element).

If we stop at criteria (1) and (2) then we form a semigroup. Stopping at criteria (1) through (3) form the definition of a monoid. If our group also satisfies $g_1 \ \theta \ g_2 = g_2 \ \theta \ g_1$ then we call our group an *Abelian* group.

2.1.1 Rings

Let R be an Abelian group and let $r_1, r_2 \in R$ with operation $+$, identity element 0, and inverse element $-r$. We say that R is a ring if it equipped with two binary operators $+$ and $\cdot$ which satisfy the following: R is an Abelian group under addition, the second operation (say, multiplication) satisfies

(1) $\forall \, r_1, r_2 \in R, \ r_1 \cdot r_2 \in R$ (closure under multiplication).[5]

(2) $\exists \, e \in R, \ \forall \, r_1 \in R$ such that $r_1 \cdot e = e \cdot r_1 = r_1$ (multiplicative identity).

(3) For technical reasons we also require associativity under multiplication: $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$.

That is, R is a monoid under multiplication $\cdot$. Finally, a ring R must also satisfy multiplicative distributivity with respect to addition:

$$\begin{aligned} r_1 \cdot (r_2 + r_3) &= r_1 \cdot r_2 + r_1 \cdot r_3 \quad \text{(left distributivity)} \\ (r_1 + r_2) \cdot r_3 &= r_1 \cdot r_3 + r_2 \cdot r_3 \quad \text{(right distributivity)} \end{aligned}$$

There exists a distinction within rings where we may wish to consider commutative rings (if multiplication commutes: $\forall \, r_1, r_2 \in R, \ r_1 \cdot r_2 = r_2 \cdot r_1$) and noncommutative rings.

Example: (*Commutative ring)* The set $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$. We can verify that this set equipped with the natural addition and multiplication is satisfies all the criteria of a commutative ring.

Example *(Noncommutative ring)* The set of 2×2 matrices over $\mathbb{Z}$ under matrix multiplication. We can verify that the set of 2×2 matrices over $\mathbb{Z}$ is a noncommutative ring with additive identity (Abelian group identity)

$$z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

[4] "It is easy to prove that such a z must be unique."

[5] Presumably this is generalized to closure under our second operation.

and multiplicative identity (monoid identity)

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Example: *(Boolean rings)* A boolean ring is a ring for which the set R satisfies $R = \{r \in \mathbb{R} \ : \ r^2 = r\}$.

Example: Consider the set of continuous real-valued functions $\mathcal{C}(x) = \{f \ : \ X \to \mathbb{R}\}$. Is this set a ring? Recall that if $f, g \in \mathcal{C}$ then $f + g \in \mathcal{C}$. Also, we have our additive identity $\overline{0}(x) = 0 \in \mathcal{C}$ such that $f + \overline{0} = f$. We also have the multiplicative identity $\overline{1}(x) = 1$ such that $f \cdot \overline{1} = f$. We can verify the remaining criteria to conclude that the set of continuous real-valued functions form a ring.

We can introduce the following requirement:

$$\forall\, x \neq 0, \ \exists\, y \in R \text{ such that } x \cdot y = 1$$

When this criteria is satisfies in a ring we say that this ring is a *division ring*.

It turns out that you don't need to satisfy commutativity in order to have an identity element: Hamilton quaternions have an identity element under multiplicative but fail commutativity.

2.1.2 Fields

A <u>field</u> is a commutative ring with identity element e in which all nonzero elements have a multiplicative inverse: $x \cdot x^{-1} = e$.

Example: *(Examples of fields)* $\mathbb{Z}$? No! We fail to have inverse elements such that $z_1 \cdot z_1 = 1$. $\mathbb{Q}$? Yes! For all $\frac{a}{b} \in \mathbb{Q}$, $a, b \neq 0$, we have an inverse element $\frac{b}{a} \in \mathbb{Q}$ such that $\frac{a}{b} \cdot \frac{b}{a} = 1$.

We also have examples of finite fields: $\mathbb{Z}_2 = \{0, 1\}$ the set of integers modulo 2. In fact, we can show (but we won't) that $\mathbb{Z}_2$ is the smallest finite field. We can also show that $\mathbb{Z}_p = \{0, 1, ..., p-1\}$, p prime, is also a (finite) field. However, $\mathbb{Z}_n$, $n \in \mathbb{N}$, is not a field. For example, if we consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ then we may note that we generate the following multiplication table (mod 6):

$(\mathbb{Z}_6, \cdot)$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Note that we fail to have a multiplicative inverse for 2 since there is no element in $z \in \mathbb{Z}_6$ such that $2 \cdot z = 1$.

3 The Real Number System

Although we will be constructing the real numbers $\mathbb{R}$ from the bottom-up, it turns out that $\mathbb{R}$ is a field.

Note that we can break up the real line into 3 part: positives, zero, and negatives. From this, note that $\exists\, P \subset \mathbb{R}$ such that

(1) $x, y \in P \implies x + y \in P$ (additive closure).

(2) $x, y \in P \implies xy \in P$ (multiplicative closure).

(3) $x \in P \implies -x \notin P$.

(4) If $x \in \mathbb{R}$ then exactly one of the following hold:

- (i) $x = 0$.
- (ii) $x \in P$.
- (iii) $x \notin P$.

If a set X satisfies the above criteria, in addition to the field axioms (not introduced in this lecture), then we say that X is an <u>ordered field</u>, and so $\mathbb{R}$ is indeed an ordered field.