Mathematical Analysis I

Exercise sheet 2

Solutions to selected exercises

15 October 2015

3. (iii) Show that the set of all finite sequences of elements from $\mathbb{N}$ is countable. *(The case of sequences of length two is $\mathbb{N} \times \mathbb{N}$. Use this a basis for induction, together with the result, which you may assume, that a countable union of countable sets is again countable.)* A finite sequence with n terms is an element of the n-fold Cartesian product $\mathbb{N}^n$. (This is defined recursively as follows: $\mathbb{N}^1 = \mathbb{N}$ and $\mathbb{N}^{n+1} = \mathbb{N}^n \times \mathbb{N}$.)*

First we prove that $\mathbb{N}^n$ is countable. We prove this by induction. The base case $n = 1$ is true as $\mathbb{N}^1 = \mathbb{N}$. Suppose as induction hypothesis that $\mathbb{N}^n$ is countable. Then

$$\mathbb{N}^{n+1} = \mathbb{N}^n \times \mathbb{N} = \bigcup_{k=0}^{\infty} (\mathbb{N}^n \times \{k\})$$

is countable as it is a countable union of countable sets: the set $\mathbb{N}^n \times \{k\}$ (all $(n+1)$-term sequences that end in k) is countable by induction hypothesis and the obvious bijection from $\mathbb{N}^n$ to $\mathbb{N}^n \times \{k\}$ that simply appends the constant value $\{k\}$ to the end of the n-term sequence.

The set of all infinite sequences of elements from $\mathbb{N}$ is equal to

$$\bigcup_{n=1}^{\infty} \mathbb{N}^n$$

and as a countable union of countable sets is itself countable.

4. A real number is *algebraic* if it is a solution of an equation of the form

$$a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n = 0, \tag{1}$$

for some $n \in \mathbb{N}$ and $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

(i) Prove that equation (1) has at most n solutions. *(You just need the fact that if polynomial $p(x)$ has root a then $p(x) = (x - a)q(x)$ for some polynomial $q(x)$ of strictly smaller degree.)*

Let $p(x) = a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n$. If $p(a) = 0$ then by the remainder theorem for polynomials $p(x) = (x - a)q(x)$, where $q(x)$ has degree strictly less than the degree n of $p(x)$. When $p(x)$ has degree $n = 1$ then there is exactly 1 solution (namely $-a_0/a_1$ in the notation of equation (1)). This is a basis for induction. Assuming a polynomial of degree $n - 1$ has at most $n - 1$ distinct roots (solutions), the polynomial $p(x) = (x - a)q(x)$ has at most one more distinct root (equal to a) than $q(x)$, which may coincide with a root of $q(x)$, and hence at most n roots altogether.

(ii) With the help of results proved in question 3, show that the set of algebraic numbers is countable.

The coefficients of the polynomial $p(x)$ in equation (1) form a finite length sequence $\mathbf{a} = (a_0, a_1, a_2 \cdots, a_n) \in \mathbb{Z}^{n+1}$ of $n + 1$ integers.

To such a finite sequence $\mathbf{a}$ corresponds a set $A_{\mathbf{a}}$ of at most n algebraic numbers (the roots of the polynomial $p(x)$).

Claim: the set of finite sequences of integers $\bigcup_{n=0}^{\infty} \mathbb{Z}^{n+1}$ is countable.

*For the exponentiation law $\mathbb{N}^m \times \mathbb{N}^n = \mathbb{N}^{m+n}$ to hold we set $\mathbb{N}^0 = \emptyset$. This can serve as an initial definition for the recursion, starting with $n = 0$ instead of $n = 1$.

Proof of claim: there is a bijection from $\mathbb{N}^{n+1}$ to $\mathbb{Z}^{n+1}$ given by the function

$$(b_0, b_1, b_2, \dots b_n) \mapsto (g(b_0), g(b_1), g(b_2), \dots, g(b_n))$$

where $g : \mathbb{N} \to \mathbb{Z}$ is the bijection defined by

$$g(b) = \begin{cases} \frac{b}{2} & b \text{ even} \\ -\frac{b+1}{2} & b \text{ odd} \end{cases}$$

(the inverse function $g^{-1} : \mathbb{Z} \to \mathbb{N}$ sends a negative integer $-a \in \mathbb{Z}$ to $2a-1$ and a positive integer $a \in \mathbb{Z}$ to $2a$). We know $\bigcup_{n=0}^{\infty} \mathbb{N}^{n+1}$ is countable, and the bijection $\mathbb{N}^{n+1} \to \mathbb{Z}^{n+1}$ defined above establishes the claim.

The set of all algebraic numbers $\mathbb{A}$ is thus given by the countable union

$$\mathbb{A} = \bigcup_{\mathbf{a}} A_{\mathbf{a}},$$

where the union is over all finite sequences of integers $\mathbf{a}$, and each $A_{\mathbf{a}}$ is finite. Hence $\mathbb{A}$ is countable.

(iii) A real number that is not algebraic is *transcendental*. What can you conclude from (ii) about the size of the set of transcendental numbers?

The set of transcendental numbers $\mathbb{R} \setminus \mathbb{A}$ cannot be countable for otherwise $\mathbb{R} = \mathbb{A} \cup (R\backslash\mathbb{A})$ would be countable (as a union of two countable sets). But $\mathbb{R}$ is uncountable. Hence the transcendental numbers are uncountably many.

(iv) Write down what statements you would need to prove to establish that the set of algebraic numbers forms a field. *(You are not asked to prove that the algebraic numbers do indeed form a field: the standard approach is to use* resultants*, which you may wish to look up for enlightenment.)* As $\mathbb{A} \subset \mathbb{R}$ and $\mathbb{R}$ is a field it is only required to verify that the algebraic numbers are closed under addition and negation, and under multiplication and taking reciprocals (multiplicative inverse). The axioms for a field (commutative group under addition, commutative group under multiplication, together with distributivity of multiplication over addition) are inherited from $\mathbb{R}$ provided we can establish this closure property. In other words, we need to show that if $a, b \in \mathbb{A}$ then $a+b, -a, ab, \frac{1}{a} \in \mathbb{A}$. Some of these are easy: for example, if $a \in \mathbb{A}$ is the root of $p(x)$ as defined in equation (1), then $-a$ is the root of $p(-x)$, and $\frac{1}{a}$ is the root of $x^n p(\frac{1}{x})$. [*To construct the polynomials with roots $a+b$ and ab from polynomials with roots a and b is harder: for this, look up "resultants" of polynomials.*]

(v) Use the number $\sqrt{2}^{\sqrt{2}}$ to prove that there exists irrational numbers a and b such that a^b is rational. *(Hint: suppose the given number is irrational, and raise it to an appropriate power.)*

Either $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, in which case we are done ($a = \sqrt{2} = b$), or $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, and then $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ so that $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ would give an example of irrationals such that $a^b \in \mathbb{Q}$. (We don't know which is true, but we do know at least one of them is. This is an example of a non-constructive proof: showing the existence of something without being able to name a specific example, or give any algorithm to find such an example.)

(The number $\sqrt{2}^{\sqrt{2}}$ is in fact known to be transcendental, although proving this is not easy. A corollary of a theorem of Gelfond and Schneider is that when a is an algebraic number not equal to 0 or 1, and b is an irrational algebraic number then a^b is transcendental.)

8.

(i) Show that if $S \subseteq \mathbb{R}$ is bounded and $T \subseteq S$ then $\inf S \leq \inf T \leq \sup T \leq \sup S$.

Recall that u is a supremum for S if

(a) u is an upper bound for S

(b) if v is any upper bound for S then $u \leq v$.

Let $u = \sup S$. As $s \leq u$ for all $s \in S$, it follows that $t \leq u$ for all $t \in T$ ($T \subseteq S$ implies $t \in S$ whenever $t \in T$). Hence u is an upper bound for T. By definition of the supremum of T as the *least* upper bound for T, it follows that $\sup T \leq u$. This is to say $\sup T \leq \sup S$.

To prove $\inf S \leq \inf T$, either use $\inf S = -\sup(-S)$ and $\inf T = -\sup(-T)$ and by the previous $-\sup(-T) \leq -\sup(-S)$, which give the result, or argue directly that if $l = \inf S$ then $l \leq s$ for each $s \in S$ and hence for each $s \in T$, so l is a lower bound for T, whence $l \leq \inf T$ as $\inf T$ is the *greatest* lower bound for T.

That $\inf S \leq \sup S$ is clear: for each $s \in S$ we have $\inf S \leq s$ and $s \leq \sup S$, whence $\inf S \leq \sup S$ by transitivity of $\leq$.

(ii) Suppose $S \subseteq \mathbb{R}$ contains $\sup S$ as an element, i.e., $\sup S = \max S$. Show that if $x \notin S$ then $\sup(S \cup \{x\}) = \sup\{\sup S, x\}$.

If $x \geq \sup S$ then $x \geq s$ for all $s \in S$ (since $\sup S$ is *an* upper bound for S), and so x is an upper bound for $S \cup \{x\}$ which is a maximum. (The number x is a least upper bound for $S \cup \{x\}$ since any upper bound must be at least x itself.) Hence $\sup(S \cup \{x\}) = x$ in this case.

If $x < \sup S$ then x is not an upper bound for S (since $\sup S$ is the *least* upper bound for S) and hence neither for $S \cup \{x\}$. Thus $\sup(S \cup \{x\}) = \sup S$ in this case.

Together these say that $\sup(S \cup \{x\}) = \max\{\sup S, x\}$.

(iii) Deduce from (ii), using mathematical induction, that any finite set $S \subseteq \mathbb{R}$ contains its supremum, i.e., $\sup S = \max S$ when S is finite.

Let S be a finite set of n distinct reals.

When $n = 1$, where $S = \{s\}$ is a singleton, we have $\sup S = \max S = s$, since $s \leq \sup S$ ($\sup S$ is *an* upper bound for S) and s, as the maximum element of S, is an upper bound (so $s \geq \sup S$, the *least* upper bound for S).

Assume that $\sup S = \max S$ for any set $S \subset \mathbb{R}$ of size n. A set of $n+1$ reals takes the form $S \cup \{x\}$ for some $x \in \mathbb{R} \setminus S$. By (ii), $\sup(S \cup \{x\}) = \max\{\sup S, x\}$ and by induction hypothesis $\sup S = \max S$. Thus $\sup(S \cup \{x\}) = \max\{\max S, x\} = \max(S \cup \{x\})$.

For the last step we used the obvious fact that $\max\{s_1, s_2, \ldots, s_n, x\} = \max\{\max\{s_1, \ldots, s_n\}, x\}$. [*You might think how to prove this last fact, though – see Bartle & Sherbert ex. 2.2.16, which shows the base case (for min instead of max).*]