Discrete Mathematics lecture notes 7-1

December 20, 2013

22. Algebraic and transcendental numbers

Let's solve one of the more involve homework problems in detail:

Definition 1. A number $\alpha \in \mathbb{R}$ is *algebraic* if there is some nonzero polynomial $p(x) = q_n x^n + q_{n-1}x^{n-1} + \ldots + q_1 x + q_0$ with $q_i \in \mathbb{Q}$[1] such that $p(\alpha) = 0$. This latter condition is often stated "α is a root of p" or "α is a zero of p."

A real number $\tau \in \mathbb{R}$ is *transcendental* if τ is not algebraic.

It is not *a priori* obvious that transcendental number exist, which is why asking you to show it makes for such a good homework problem.

Exercise. Show that there are real transcendental numbers.

Let $A \subseteq \mathbb{R}$ denote the set of algebraic numbers and $T \subseteq \mathbb{R}$ the set of transcendentals. The solution will involve the following steps:

1. Show that, in general, the countable union of countable sets is countable.
2. Show that we can write $A = \bigcup_{i=1}^{\infty} A_i$ for a certain countable collection $\{A_i\}_{i\in\mathbb{N}}$ of subsets of A.
3. Show that the A_i of part 2 are all countable.
4. Conclude that A is countable.
5. Conclude that $A \neq \mathbb{R}$, as $\mathbb{R}$ is uncountable.
6. Conclude that $T \neq \emptyset$, as $T := \mathbb{R} - A$.

We will provide further elaboration here for steps 1, 2, and 3.

Proposition 2. *If $\{X_i\}_{i=1}^{\infty}$ is a countable set, where for each $i \in \mathbb{N}$ the element X_i is* itself *a countable set, then $\bigcup_{i=1}^{\infty} X_i$ is countable.*

Proof. Write out all the elements of the union in a doubly infinite array:

$$\begin{array}{lcccccccc} X_1 & = & \{ & x_1^1 & x_2^1 & x_3^1 & x_4^1 & \ldots & \} \\ X_2 & = & \{ & x_1^2 & x_2^2 & x_3^2 & x_4^2 & \ldots & \} \\ X_3 & = & \{ & x_1^3 & x_2^3 & x_3^3 & x_4^3 & \ldots & \} \\ X_4 & = & \{ & x_1^4 & x_2^4 & x_3^4 & x_4^4 & \ldots & \} \\ \vdots & & & \vdots & \vdots & \vdots & \vdots & \ddots & \end{array}$$

Clearly every element of the union is listed somewhere on this array: If $x \in \bigcup_{i=1}^{\infty} X_i$, then there is some i such that $x \in X_i$, and if $x \in X_i$, there must be some $j \in \mathbb{N}$ such that $x = x_j^i$, which occurs in the ith row, jth column of the array. Now define a surjection from $\mathbb{N}$ to this union by counting elements along diagonals of slope 1, just as in the proof that $\mathbb{Q}$ is countable. To turn this surjection into a bijection (again as in the rational case), simply skip over any terms that we come across more than once. □

[1] The such of all such polynomials with coefficients in $\mathbb{Q}$ is denoted $\mathbb{Q}[x]$.

Next, define

$$A_i := \{\alpha \in \mathbb{R} | \exists\ 0 \neq p(x) \in \mathbb{Q}[x] \text{ s.th. } \deg(p) \leq i, \text{ and } p(\alpha) = 0\}.$$

In other words, A_i consists of those algebraic numbers that are roots of a nonzero polynomial of degree at most i. I claim $A = \bigcup_{i=1}^{\infty} A_i$.

Indeed, each A_i is by construction a subset of A, so we have $A \supseteq \bigcup_{i=1}^{\infty} A_i$. On the other hand, if $\alpha \in A$, then α is a root of some nonzero polynomial $p(x)$, which has some finite degree n. Thus $\alpha \in A_n$ and $A \subseteq \bigcup_{i=1}^{\infty} A_i$, showing equality.

Finally, we need to show that each A_i is a countable set. We will do this by writing A_i as a countable union of countable[2] sets, which, with another application of Proposition 2, will yield the desired result.

To accomplish this last goal, we first identify the countable *indexing set*[3] we will need to write A_i as a countable union of countable sets. Let P_i be the set of nonzero polynomials of degree at most i; I claim that P_i is countable. Indeed, consider the function $f : P_i \to \mathbb{Q}^{n+1} - \{\mathbf{0}\}$[4] defined by

$$f : q_n x^i + q_{i-1} x^{i-1} + \ldots + q_1 x + q_0 \mapsto (q_i, q_{i-1}, \ldots, q_1, q_0).$$

In other words, f takes a polynomial of degree at most i and assigns to it the ordered list of $n+1$ rational numbers that are its coefficients. Either convince yourself directly that f is a bijection, or explicitly write down an inverse.[5]

Thus we've shown that $|P_i| = |\mathbb{Q}^{i+1} - \{\mathbf{0}\}| = |\mathbb{Q}^{i+1}|$.[6] We saw in class that $\mathbb{Q}$ is countable, and you proved in the homework that a product of two countable sets is countable, from which it follows that $\mathbb{Q}^n$, is countable for all n.[7] In other words, P_i is countable for all i.

Finally finally, we'll use P_i as an indexing set for a union that will equal A_i. I claim:

$$A_i = \bigcup_{p(x) \in P_i} \{\text{roots of } p(x)\}.$$

In fact this is clear: The containment $\supseteq$ is obvious, and if $\alpha \in A_i$, α is a root of a nonzero polynomial $p(x)$ of degree at most i, so $p(x) \in P_i$, so the containment $\subseteq$ follows. But as $\deg p \leq i$ whenever $p(x) \in P_i$, we have $|\{\text{roots of } p(x)\}| \leq i$. Thus we have written A_i as a countable union of finite sets, forcing A_i to be countable and completing the exercise.

22. The Binomial Theorem

Let's return to the world of finite combinatorics. Last time we introduced the binomial coefficients $\binom{n}{i}$ as the number of i-element subsets of a set with n elements. What we didn't do was explain where the name came from. Let's fix that omission.

Theorem 3 (Binomial Theorem)**.** *For $n \in \mathbb{N}$ and $a, b \in \mathbb{R}$,*[8] *we have*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

[2] In fact, finite.

[3] That is, the set that contains the names of the sets whose union will be A_i.

[4] Here $\mathbb{Q}^{n+1}$ is the $(n+1)$-fold Cartesian product of $\mathbb{Q}$ and $\mathbf{0}$ represents the n-tuple of rational numbers that are all zero.

[5] As with most questions that we deal with: If you have difficulty proving or understanding a statement in full generality, pick a small value for i, like 2 or 3, and examine that special case in more detail.

[6] Why is this last equality true?

[7] Prove this explicitly, using induction.

[8] Or $\mathbb{Z}$ or $\mathbb{N}$ or $\mathbb{Z}/n$ or.... See if you can figure out what are the essential structure and axioms we're using to guarantee the truth of this Theorem.

Proof. Let's prove this in two different ways: First by a standard induction (this is an $\mathbb{N}$-indexed collection of claims, after all): If $n = 0$ or $n = 1$, it is immediately clear that the formula holds.

Let's suppose that for some given k the conclusion of the Theorem holds for k. That is, for any $a, b \in W$,[9] the equality

$$(a+b)^k = \sum_{i=0}^{k} \binom{n}{i} a^i b^{k-i}$$

holds. We calculate:

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)(a+b)^k \\
&= (a+b) \cdot \left(\sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i} \right) \\
&= a \cdot \left(\sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i} \right) + b \cdot \left(\sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i} \right) \\
&= \left(\sum_{i=0}^{k} \binom{k}{i} a^{i+1} b^{k-i} \right) + \left(\sum_{i=0}^{k} \binom{k}{i} a^i b^{k+1-i} \right) \\
&= \left(\sum_{j=1}^{k+1} \binom{k}{j-1} a^j b^{k-(j+1)} \right) + \left(\sum_{i=0}^{k} \binom{k}{i} a^i b^{k+1-i} \right) \\
&= \left(\sum_{j=0}^{k+1} \binom{k}{j-1} a^j b^{k+1-j} \right) + \left(\sum_{i=0}^{k+1} \binom{k}{i} a^i b^{k+1-i} \right) \\
&= \sum_{\ell=0}^{k+1} \left(\binom{k}{\ell-1} + \binom{k}{\ell} \right) a^\ell b^{k+1-\ell} \\
&= \sum_{\ell=0}^{k+1} \binom{k+1}{\ell} a^\ell b^{k+1-\ell},
\end{aligned}$$

where the first equality is by definition, the second by the inductive hypothesis, the third and fourth the Distributive Axiom, the fifth by reindexing $j = i + 1$, the sixth by observing that we can increase the limits of summation without changing the sums (as the extra terms are secretly 0), the seventh by realizing that the names of dummy variables are immaterial, and the eighth by Pascal's Lemma. But putting these all together is precisely the content of the Theorem's holding for $k + 1$, and induction finishes the job for us.

Alternate proof: Write

$$(a+b)^n = \underbrace{(a+b)(a+b)\dots(a+b)}_{n \text{ times}}$$

and expand out using repeated applications of the Distributive axiom. The result will be a sum of many terms of the form $a^i b^j$ (using the fact that multiplication is commutative), which we should think of as coming from picking i as and j bs from the totality of n choices of a or b. Note that this forces $i + j = n$. But now the question is *how many* copies of $a^i b^j$ do we have for fixed i, j? Well, we get one copy for each possible way of selecting i as from a total of n choices, which (by your homework identifying $\mathcal{P}(S) \xrightarrow{\sim} \{0,1\}^S$ for any set S)[10] is the same thing as the number of i element subsets of a set of n elements. But this is just $\binom{n}{i}$ by definition. The result follows. □

[9] For "whatever."

[10] In general, if A and B are sets, write B^A for the set of functions $\{f : A \to B\}$.