ALGEBRAIC AND TRANSCENDENTAL NUMBERS (MA2316, ELEVENTH WEEK)

VLADIMIR DOTSENKO

Recall that a complex number α is called an *algebraic number* if there exist a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ for which $f(\alpha) = 0$. If there exists such a polynomial with integer coefficients and the leading coefficient equal to 1, the number α is said to be an *algebraic integer*. If α is an algebraic number, and f(x) is a non-zero polynomial with rational coefficients of smallest possible degree among the polynomials with integer coefficients having α as a root, f(x) is referred to as the *minimal polynomial* of α , and by the degree of α we mean the degree of its minimal polynomial. It is immediate to see that every polynomial with rational coefficients having α as a root is divisible by its minimal polynomial.

Complex numbers which are not algebraic are called transcendental. Our goal in this lecture is to give two different proofs of the following theorem.

Theorem 1. Transcendental numbers exist.

First proof. (Cantor) The set of algebraic numbers is countable. (Indeed, each algebraic number is a root of polynomial with *integer* coefficients, and the set of roots of all polynomials with integer coefficients of degree at most n and all coefficients at most n in absolute value is finite. Since a countable union of finite sets is countable, our claim follows.) However, the set of real numbers, as well as the set of complex numbers, is uncountable, so there must be numbers that are not algebraic.

Second proof. (Liouville) Let us first prove the following auxilliary statement.

Lemma. Suppose that α is an algebraic number of degree k > 1. Then there exist C > 0 such that for all $\frac{p}{q} \in \mathbb{Q}$ we have

$$\left|\frac{p}{q} - \alpha\right| > \frac{C}{q^k}.$$

Proof of Lemma. Indeed, let us first assume that $\left|\frac{p}{q} - \alpha\right| \leq 1$. Denote by f(x) the minimal polynomial of α with integer coefficients (obtained from any minimal polynomial by clearing denominators). By the mean value theorem from calculus, we have

$$\frac{f\left(\frac{p}{q}\right) - f(\alpha)}{\frac{p}{q} - \alpha} = f'(\xi),$$

where ξ is between $\frac{p}{q}$ and α , so in any case $\xi \in [\alpha - 1, \alpha + 1]$. Since $f(\alpha) = 0$, we have

$$\frac{p}{q} - \alpha = \frac{f\left(\frac{p}{q}\right)}{f'(\xi)}.$$

Note that $\left| f\left(\frac{p}{q}\right) \right| > \frac{1}{q^k}$ since q^k is the common denominator of the terms in $f\left(\frac{p}{q}\right)$ (and $f\left(\frac{p}{q}\right)$ is not equal to zero, since f is the minimal polynomial of α). Therefore, if $C = \frac{1}{\max(|f'(\xi)|: \xi \in [\alpha - 1, \alpha + 1])}$,

then $\left|\frac{p}{q} - \alpha\right| > \frac{C}{q^k}$. To account for the fractions with $\left|\frac{p}{q} - \alpha\right| > 1$, we replace C with $C' = \min(C, 1)$ if necessary, since $\left|\frac{p}{q} - \alpha\right| > 1$ implies $\left|\frac{p}{q} - \alpha\right| > \frac{1}{q^k}$. Back to Liouville's proof, let us consider the number

$$\beta = \sum_{k \ge 1} \frac{1}{10^{k!}}$$

Let us define

$$\frac{p_m}{q_m} = \sum_{1 \le k \le m} \frac{1}{10^{k!}}$$

so that $q_m = 10^{m!}$. We have

$$\left|\frac{p_m}{q_m} - \beta\right| = \sum_{k>m} \frac{1}{10^{k!}} < \frac{1}{10^{(m+1)!}} \left(1 + \frac{1}{10} + \frac{1}{100} + \dots\right) = \frac{\frac{10}{9}}{10^{(m+1)!}},$$

since $\frac{1}{10^{(m+k)!}} < \frac{1}{10^{(m+1)!}} \frac{1}{10^{k-1}}$. In other words,

$$\left|\frac{p_m}{q_m} - \beta\right| < \frac{\frac{10}{9}}{q_m^{m+1}}$$

Combined with the lemma above, we conclude if β were an algebraic number of degree k > 1, we would have, for some C > 0,

$$\frac{C}{q_m^k} < \frac{\frac{10}{9}}{q_m^{m+1}}$$

or $q_m^{m+1-k} < \frac{10}{9C}$, which clearly contradicts the fact $q_m \to \infty$. Also, if $\beta = \frac{p}{q}$, we have

$$\left|\frac{p_m}{q_m} - \beta\right| = \left|\frac{p_m}{q_m} - \frac{p}{q}\right| = \frac{|p_mq - pq_m|}{qq_m} > \frac{1}{qq_m},$$

which also contradicts $\left|\frac{p_m}{q_m} - \beta\right| < \frac{\frac{10}{9}}{q_m^{m+1}}.$