UNIVERSITY OF NATURAL SCIENCES HO CHI MINH City
http://www.hcmuns.edu.vn/

Introduction to Diophantine methods:
irrationality and transcendence

Michel Waldschmidt,
Professeur, Université P. et M. Curie (Paris VI)
http://www.math.jussieu.fr/~miw/coursHCMUNS2007.html

Examen – second session
3 hours

Exercise 1. For $n \geq 1$ define

$$a_n = \begin{cases} 1 & \text{if } n \text{ is a power of } 2, \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$(a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7,\ a_8,\ a_9,\ a_{10}, \dots) = (1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0, \dots).$$

Prove that the number written in binary notation

$$0.a_1\, a_2\, a_3\, a_4\, a_5\, a_6\, a_7\, a_8\, a_9\, a_{10} \cdots = 0.1\,1\,0\,1\,0\,0\,0\,1\,0\,0\dots$$

is irrational.

Exercise 2. Which are the correct sentences? Explain your answer.
(i) The sum of two rational numbers is
(A) always rational
(B) always irrational
(C) sometimes rational, sometimes irrational.
(ii) The sum of two irrational numbers is
(A) always rational
(B) always irrational
(C) sometimes rational, sometimes irrational.
(iii) The sum of rational number and an irrational number is
(A) always rational
(B) always irrational
(C) sometimes rational, sometimes irrational.
(iv), (v), (vi) Same questions with the product instead of the sum.
(vii) If $(a_n)_{n\geq 0}$ is an infinite sequence with $a_n \in \{-1, 1\}$ for all $n \geq 0$, then the number

$$\sum_{n\geq 0} a_n 2^{-n}$$

is irrational.

Exercise 3. Define $u_0 = 0$, $u_1 = 1$, and by induction $u_n = 2u_{n-1} + u_{n-2}$ for $n \geq 2$.
a) Check, for any $n \geq 1$,

$$u_n^2 - 2u_n u_{n-1} - u_{n-1}^2 = (-1)^{n-1}.$$

b) Show that the sequence $(u_n/u_{n-1})_{n\geq 1}$ converges as $n \to \infty$. What is the limit?
c) Prove that there exists a sequence $(p_n/q_n)_{n\geq 1}$ of rational numbers such that

$$\lim_{n\to\infty} q_n \left| q_n\sqrt{2} - p_n \right| = \frac{1}{2\sqrt{2}}.$$

d) Prove that for any $\kappa > 2\sqrt{2}$, there are only finitely many $p/q \in \mathbb{Q}$ satisfying

$$\left| \sqrt{2} - \frac{p}{q} \right| \leq \frac{1}{\kappa q^2}.$$

Exercise 4. Let α be a complex number. Show that the following properties are equivalent.
(i) α is root of a polynomial of degree ≤ 3 with rational coefficients.
(ii) The $\mathbb{Q}$–vector space spanned by $1,\ \alpha,\ \alpha^2, \alpha^3 \dots$ has dimension ≤ 3.
(iii) For any integer $m \geq 1$, the number α^m is root of a polynomial of degree ≤ 3 with rational coefficients.

Exercise 5. Recall the next Theorem due to Hermite and Lindemann: *for any non–zero complex number z, one at least of the two numbers z, e^z is transcendental.* Deduce the following results.
a) For any non–zero algebraic number α, the numbers e^α, $\cos(\alpha)$ and $\sin(\alpha)$ are transcendental.
b) Let $\lambda \in \mathbb{C}$, $\lambda \neq 0$. Assume e^λ is algebraic. Then λ is transcendental.
c) The numbers $\log 2$ and π are transcendental.

Examen – Second session
Solutions

Solution exercise 1.
For $m \geq 1$ between a_{2^m} and $a_{2^{m+1}}$ there are $2^m - 1$ consecutive zeroes,

$$a_{2^m+1} = a_{2^m+2} = \cdots = a_{2^{m+1}-1} = 0.$$

Therefore the sequence $(a_n)_{n\geq 0}$ is not ultimately periodic, and it follows that the given number is irrational.

Solution exercise 2.

(i) The sum of two rational numbers is
(A) always rational
because

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

The set of rational numbers is a field.
(ii) The sum of two irrrational numbers is
(C) sometimes rational, sometimes irrational.
If x is irrational and r is rational then $y = r - x$ is irrational, while the sum of x and y is r, hence is rational.
If x is irrational then $x + x = 2x$ is also irrational.
(iii) The sum of rational number and an irrational number is
(B) always irrational.
If r is rational and $r + x$ is also rational then $x = (r + x) - r$ is rational. Hence if r is rational and x is irrational then $r + x$ is irrational.
(iv) The product of two rational numbers is
(A) always rational
because

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

The set of rational numbers is a field.
(v) The product of two irrrational numbers is
(C) sometimes rational, sometimes irrational.
If x is irrational and r is rational then $y = r/x$ is irrational, while the product of x and y is r hence is rational.
If t is rational then t^2 is also rational. Therefore if x is irrational then $\sqrt{x}$ is also irrational. Now the product of $\sqrt{x}$ with itself is x, hence irrational.
(vi) The product of rational number and an irrational number is
(C) sometimes rational, sometimes irrational.
The product of 0 and any irrational number is 0, hence rational.
If $r \neq 0$ is rational and rx is also rational then $x = rx/r$ is rational, hence if r is rational $\neq 0$ and x is irrational then rx is irrational.

(vii) If the sequence $(a_n)_{n\ge 0}$ is ultimately periodic, then the number

$$\sum_{n\ge 0} a_n 2^{-n}$$

is rational. For instance for $a_n = 1$ for all $n \ge 0$ the sum is 2.

Solution exercise 3. For $n \ge 1$ set

$$v_n = u_n/u_{n-1} \quad \text{and} \quad w_n = u_n^2 - 2u_n u_{n-1} - u_{n-1}^2$$

so that

$$w_n = u_{n-1}^2(v_n^2 - 2v_n - 1).$$

a) From the recurrence formula $u_{n+1} = 2u_n + u_{n-1}$ one deduces

$$w_{n+1} = u_{n+1}^2 - 2u_{n+1}u_n - u_n^2 = u_{n+1}(u_{n+1} - 2u_n) - u_n^2 = u_{n-1}(2u_n + u_{n-1}) - u_n^2 = -w_n.$$

Therefore $w_n = (-1)^n w_0$, and since $w_0 = 1$ we conclude $w_n = (-1)^{n-1}$.
b) The roots of the polynomial $X^2 - 2X - 1$ are $\alpha = 1 + \sqrt{2}$ and $\alpha' = 1 - \sqrt{2}$. Notice that $\alpha' < 0 < \alpha$ and

$$w_n = (u_n - \alpha u_{n-1})(u_n - \alpha' u_{n-1}).$$

From the recurrence formula we deduce $u_n > 2u_{n-1}$ for $n \ge 2$, hence $u_n \ge 2^n$ for $n \ge 0$ and

$$u_n - \alpha' u_{n-1} \ge u_n \ge 2^n.$$

Using $|w_n| = 1$ we obtain

$$|\alpha - v_n| \le \frac{1}{2^{2n-1}}.$$

Therefore the sequence $(v_n)_{n\ge 1}$ converges to $\alpha = 1 + \sqrt{2}$ as $n \to \infty$.
c) We have $w_n = u_{n-1}^2(v_n - \alpha)(v_n - \alpha')$ and the limit of the sequence $(v_n - \alpha')_{n\ge 1}$ is $\alpha - \alpha' = 2\sqrt{2}$. Hence

$$\lim_{n\to\infty} u_{n-1} \left|u_{n-1}\alpha - u_n\right| = \frac{1}{2\sqrt{2}}.$$

For $n \ge 1$ define $p_n = u_{n-1} - u_n$ and $q_n = u_{n-1}$. Then

$$\lim_{n\to\infty} q_n \left|q_n\sqrt{2} - p_n\right| = \frac{1}{2\sqrt{2}}.$$

d) For $\kappa > 2\sqrt{2}$, let $p/q \in \mathbb{Q}$ satisfy

$$\left|\sqrt{2} - \frac{p}{q}\right| \le \frac{1}{\kappa q^2}.$$

We have

$$1 \le |(p+q)^2 - 2q(p+q) - q^2| = |(p+q-q\alpha)(p+q-q\alpha')| \le \frac{1}{\kappa}\left(\alpha - \alpha' + \frac{1}{\kappa q^2}\right).$$

Hence $q^2\kappa(\kappa - 2\sqrt{2}) < 1$. Therefore q is bounded, and since p is the nearest integer to $q\sqrt{2}$ there are only finitely many solutions p/q.

Solution exercise 4.
The implication (iii) $\Rightarrow$ (i) is trivial: take $m = 1$.

Proof of (i) $\Rightarrow$ (ii). Since α is root of a polynomial of degree ≤ 3 with rational coefficients, then it is also root of a monic polynomial $X^3 - aX^2 - bX - c$ of degree 3 with rational coefficients (multiply by X or X^2 if necessary and divide by the leading coefficient). By induction, for each integer $m \geq 1$ we can write $\alpha^m = a_m\alpha^2 + b_m\alpha + c_m$ with a_m, b_m and c_m in $\mathbb{Q}$. Hence the $\mathbb{Q}$–vector space spanned by 1, α, α^2, $\alpha^3 \ldots$ is also spanned by 1, α, α^2, hence has dimension ≤ 3.

Proof of (ii) $\Rightarrow$ (iii). If the $\mathbb{Q}$–vector space spanned by 1, α, α^2, $\alpha^3 \ldots$ has dimension ≤ 3, then the four numbers 1, α^m, α^{2m}, α^{3m} are linearly dependent over $\mathbb{Q}$.

Solution exercise 5.
a) Let α be a non–zero algebraic number. Taking $z = \alpha$ in the Hermite–Lindemann Theorem shows that e^α is transcendental. Also $i\alpha$ is a non–zero algebraic number, hence $e^{i\alpha}$ is transcendental. This means that it is not root of a polynomial with rational coefficients, and this implies that it is not root of a polynomial with algebraic coefficients. Since $e^{i\alpha}$ is root of the polynomials

$$X^2 - 2X\cos(\alpha) + 1 \quad \text{and} \quad X^2 - 2iX\sin(\alpha) - 1,$$

it follows that $\cos(\alpha)$ and $\sin(\alpha)$ are transcendental.
b) Let $\lambda \in \mathbb{C}$, $\lambda \neq 0$. If e^λ is algebraic, then the Hermite–Lindemann Theorem with $z = \lambda$ shows that λ is transcendental.
c) For $\lambda = \log 2$ the number $e^\lambda = 2$ is algebraic, hence $\log 2$ is transcendental. For $\lambda = i\pi$ the number $e^\lambda = -1$ is algebraic, hence $i\pi$ is transcendental. The product of two algebraic numbers is algebraic, and i is algebraic, hence π is transcendental.