## MASTER WORKSHOP

## EXERCISES XI ( THE HERMITE-LINDEMANN TRANSCENDENCE THEOREM)

MATANIA BEN-ARTZI

**Definition.** A complex number $\alpha$ is called **algebraic** if it is a zero of a real polynomial $p(x)$ with rational coefficients. It is **algebraic integer** if it is the root of a monic (leading coefficient=1) polynomial with integer coefficients.
In problem 8 of Exercise Set VI you proved that the set of algebraic numbers is a field.The set of algebraic integers is a ring.

(1) Prove the **Hermite-Lindemann Transcendence Theorem**:
Let $\alpha_1, ..., \alpha_n$ be distinct algebraic numbers and let $A_1, ..., A_n$ be algebraic numbers such that

$$A_1 e^{\alpha_1} + ... + A_n e^{\alpha_n} = 0.$$

Then $A_1 = A_2 = ... = A_n = 0$.
**Suggestion.**
- (a) Extend the set $\{A_k\}_{k=1}^n$ by algebraic numbers $A_{n+1}, ..., A_N$, so that the extended set is the set of all roots of a polynomial of degree $N$ with rational coefficients.
- (b) Take the product $\Gamma$ of all sums of the form $A_{\sigma(1)} e^{\alpha_1} + ... + A_{\sigma(n)} e^{\alpha_n}$ where $\sigma$ is any permutation in $S_N$. Show that $\Gamma = 0$ and can be written as
$$\Gamma = A'_1 e^{\beta_1} + ... + A'_l e^{\beta_l},$$
where the $A'_k$ are rational and not all zero. Multiplying by the common denominator you can assume they are all integer.
- (c) Extend the set $\{\beta_k\}_{k=1}^l$ by algebraic numbers $\beta_{l+1}, ..., \beta_M$, so that the extended set is the set of all roots of a polynomial of degree $M$ with rational coefficients.
- (d) Take the product $\Phi$ of all sums of the form $A'_{\sigma(1)} e^{v\beta_1} + ... + A'_{\sigma(l)} e^{v\beta_l}$ where $\sigma$ is any permutation in $S_M$, and $v$ is a variable. Show that the resulting product can be written as
$$\Phi(v) = C_1 e^{v\gamma_1} + ... + C_J e^{v\gamma_J},$$
where the $C_k$ are integers and not all zero.
- (e) Conclude (symmetry of $\Phi$...) that for every nonnegative integer $m = 0, 1, 2, ...$ the sum
$$D_m = C_1 \gamma_1^m + ... + C_J \gamma_J^m$$
is a rational number.

*Date*: February 5, 2007.

(f) Conclude that for every polynomial $g(x)$ with integer coefficients the sum

$$C_1 g(\gamma_1) + ... + C_J g(\gamma_J)$$

is a rational number.

(g) Show that

$$\Phi(1) = C_1 e^{\gamma_1} + ... + C_J e^{\gamma_J} = 0.$$

(h) Extend the set $\{\gamma_j\}_{j=1}^J$ by algebraic numbers $\gamma_{J+1}, ..., \gamma_L$, so that the extended set is the set of all roots of a polynomial $r(x) = x^L + r_1 x^{L-1} + ... + r_L$ with rational coefficients.

(i) Multiply by the ($L$-power of) common denominator of the $r_i$ to obtain the equation(with integer coefficients)

$$(Hx)^L + Hr_1(Hx)^{L-1} + ... + H^L r_L = 0,$$

and set $X = Hx$ to get

$$f(X) = H^L r(x) = X^L + Hr_1 X^{L-1} + ... + H^L r_L = (X - \Lambda_1)...(X - \Lambda_L),$$

where $\Lambda_j = H\gamma_j, \quad j = 1, ..., L.$

(j) Conclude from (f) that

$$C_1 g(\Lambda_1) + ... + C_J g(\Lambda_J)$$

is an integer.

(k) Show that the polynomial

$$\phi(X) = \frac{f(X)}{X - \Lambda_1} + ... + \frac{f(X)}{X - \Lambda_L} = LX^{L-1} + ...$$

has integer coefficients and does not vanish at $\Lambda_1, ..., \Lambda_L$.

(l) Show that for some integer $0 \le h < J$ we have

$$C_1 \Lambda_1^h \phi(\Lambda_1) + ... + C_J \Lambda_J^h \phi(\Lambda_J) \neq 0.$$

(m) Take a "symbol" $\mho$ and use the convention that, for every integer $\nu$, with $H$ as above, we have $\mho^\nu = \nu! H^\nu$, so that

$$e^x \mu! H^\mu = e^x \mho^\mu = (\mho + X)^\mu + X^\mu[\frac{x}{\mu + 1} + \frac{x^2}{(\mu+1)(\mu+2)} + ...].$$

Denote $\xi = |x|$ to obtain, with $0 \le \varepsilon < 1$,

$$e^x \mho^\mu = (\mho + X)^\mu + e^\xi \varepsilon X^\mu.$$

(n) Let $V(X) = X^k + K_1 X^{K-1} + K_2 X^{K-2} + ... + K_k$ be a polynomial with integer coefficients . Show that , with the above notation, $e^x V(\mho) = V(X + \mho) + e^\xi \overline{V}(X)$, where $\overline{V}(X) = \sum_{j=0}^{k} \varepsilon_j K_j X^{k-j}$ and $0 \le \varepsilon_j < 1, \quad 0 \le j \le k$.
Let $\Delta_1, ..., \Delta_k$ be the roots of $\overline{V}(X)$ and let $d \ge \max_{1 \le j \le k} [|X| + |\Delta_j|]$. Then $|\overline{V}(X)| \le d^k$.

(o) For $V$ as above take now $V(X) = F(X)^q \Phi(X)$ where

$$F(X) = X^h f(X), \quad \Phi(X) = X^h \phi(X), \quad f, \phi, \quad \text{as in (k)}, \quad h \quad \text{as in (l)},$$

and $q = p - 1$ where $p$ is a prime number to be determined. ($\Phi$ not the same as in (d)).
Note that $k = degV = (L+h)q + h + L - 1$.

(p) Take $1 \leq \nu \leq J$ and let $x = \gamma_\nu, X = \Gamma_\nu$. Let $\xi_\nu = |x|, d_\nu = \max_{1\leq j\leq k}[|X| + |\Delta_j|]$, and define $D = \max_{1\leq\nu\leq J}(d_\nu^{L+h}, e^{\xi_\nu} d_\nu^{2(L+h)-1})$. Show that, for every $1 \leq \nu \leq J$,

$$e^{\gamma_\nu} V(\mho) = V(\Gamma_\nu + \mho) + \eta_\nu D^q, \quad |\eta_\nu| < 1.$$

(q) Show that for $1 \leq \nu \leq J$,

$$V(\Gamma_\nu + \mho) = \psi_0 \mho^q + \psi_1 \mho^{q+1} + \psi_2 \mho^{q+2} + ...,$$

where the $\psi_i = \psi_i(\Gamma_\nu)$ are integers and $\psi_0 = \Phi(\Gamma_\nu)^p$. Now multiply by $C_\nu$ and sum, using the result in (g), to get,

$$(*) \quad 0 = G_0 \mho^q + G_1 \mho^p + G_2 \mho^{p+1} + ... + G_{k-q} \mho^k + \lambda D^q,$$

where the integers $G_s$ are given by,

$$G_s = C_1 \psi_s(\Gamma_1) + C_2 \psi_s(\Gamma_2) + ... + C_J \psi_s(\Gamma_J),$$

and $|\lambda| \leq J \max_{1\leq\nu\leq J} |C_\nu|$.

(r) Use the convention for $\mho^r$ from (m) and divide (*) by $H^q$ to obtain, with $E = \frac{D}{H}$,

$$G_0 q! + G' p! = -\lambda E^q,$$

where $G'$ is an integer.

(s) Define (the nonzero integer by (l))

$$G = C_1 \Phi(\Gamma_1) + C_2 \Phi(\Gamma_2) + ... + C_J \Phi(\Gamma_J),$$

and show that

$$G^p = C_1^p \Phi(\Gamma_1)^p + C_2^p \Phi(\Gamma_2)^p + ... + C_J^p \Phi(\Gamma_J)^p + \delta p,$$

where $\delta$ is an integer.

(t) Show that there exist integers $g, c_1, ..., c_J$ such that

$$\begin{aligned} G + gp = (C_1 + c_1 p)\Phi(\Gamma_1)^p + C_2^p \Phi(\Gamma_2)^p + ... + (C_J + c_J p)\Phi(\Gamma_J)^p + \delta p \\ = G_0 - \delta' p, \end{aligned}$$

where $-g' = \delta' + g$ is an algebraic integer and hence integer since it is rational $(= \frac{G_0 - G}{p})$.

(u) Rewrite the equation in (r) as

$$Gq! + g'p! + G'p! = -\lambda E^q,$$

or

$$G + (g' + G')p = -\lambda \frac{E^q}{q!}.$$

(v) Obtain a contradiction by taking $p > |G|$ and also such that the right-hand side of the last equality is of absolute value smaller than one.

(2) Show that the numbers $\pi, e$ are transcendental (i.e., not algebraic).

(3) Show that the curves of the functions $y = e^x$ and $y = \sin x$ contain no algebraic points except the one at $x = 0$.
(an algebraic point in the plane is a point whose two coordinates are algebraic).

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
*E-mail address*: mbartzi@math.huji.ac.il