NOTES ON IRRATIONALITY AND TRANSCENDENCE

Frits Beukers

October 9, 2007

5 Linear Forms in Logarithms

5.1 Generalisation of Hilbert 7

A reformulation of the Gel'fond-Schneider theorem reads as follows

Theorem 5.1.1 (Gel'fond, Schneider, 1934) *Let α_1, α_2 be non-zero algebraic numbers. Choose $\log \alpha_1, \log \alpha_2$. Then, if $\log \alpha_1$ and $\log \alpha_2$ are $\mathbb{Q}$-linear independent, we have*

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0$$

for any $\beta_1, \beta_2 \in \overline{\mathbb{Q}}$ not both zero. In other words, $\mathbb{Q}$-linear independence of $\log \alpha_1$ and $\log \alpha_2$ implies their $\overline{\mathbb{Q}}$-linear independence.

A natural question to ask whether $\log \alpha_1$ and $\log \alpha_2$ are algebraically independent over $\mathbb{Q}$. By this we means that for any $P(X, Y) \in \mathbb{Z}[X, Y]$ the equality $P(\log \alpha_1, \log \alpha_2) = 0$ implies that P is identically zero. In general, $\gamma_1, \ldots, \gamma_n$ are said to be algebraically independent if for any $P \in \mathbb{Z}[X_1, \ldots, X_n]$ the equality $P(\gamma_1, \ldots, \gamma_n) = 0$ implies that P vanishes identically. In particular a single number is said to algebraically independent over $\mathbb{Q}$ if it is transcendental.
A field extension L of $\mathbb{Q}$ is said to have transcendence degree n the maximal set of algebraically independent elements of L has size L. Notation: $\mathrm{degtr}_{\mathbb{Q}}(L) = n$. When L is an algebraic extension its transcendence degree is zero.
Remarkably enough, nothing is known about algebraic independence of two logarithms of algebraic numbers. It is not even known if $\log(2)\log(3)$ is transcendental or not. It is very likely that it is transcendental. In general we have the following conjecture discussed in the exercises of the previous Section.

Conjecture 5.1.2 (Schanuel) *Suppose that $b_1, \ldots, b_m$ are $\mathbb{Q}$-linearly independent. Then*

$$\mathrm{degtr}_{\mathbb{Q}}\mathbb{Q}(b_1, \ldots, b_m, e^{b_1}, \ldots, e^{b_m}) \geq m.$$

It entails that logarithms of algebraic numbers which are $\mathbb{Q}$-linear independent, are also algebraically independent.
The case $n = 1$ of Schanuel's conjecture follows from the Lindeman-Weierstrass Theorem. However, note that the case $n = 2$ is not verified in its generality.

5.2 A.Baker's results

It was only in 1966 that A.Baker succeeded in extending the Gel'fond-Schneider theorem to more than two logarithms. He proved the following Theorem.

Theorem 5.2.1 *Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers. If $\log \alpha_1, \ldots, \log \alpha_n$ are $\mathbb{Q}$-linear independent, then the numbers $1, \log \alpha_1, \ldots, \log \alpha_n$ are $\overline{\mathbb{Q}}$-linear independent.*

Baker's proof of this theorem is reminiscent to the Gel'fond solution of Hilbert's 7th problem, except that Baker used interpolating functions of several variables. It also became clear very soon that a variant of Baker's approach could also be used to obtain lower bounds for linear forms in logarithms.
In these lower bounds also the heights of algebraic numbers occur. By this we mean the following. Let α be a non-zero algebraic number with minimal polynomial $a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d$. Then the height of α is defined by $\max(|a_0|, \ldots, |a_d|)$. Notation: $H_\infty(\alpha)$ indicating that we take the sup-norm of the coefficient vector of the minimal polynomial.
Here is the general shape of a lower bound for linear forms in logarithm.

Theorem 5.2.2 *Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and heights at most A. Let $\beta_0, \beta_1, \ldots, \beta_n$ be algebraic numbers of degree at most d and height at most $B(\geq 2)$. Let*

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \cdots + \alpha_n \log \alpha_n.$$

Then, either $\Lambda = 0$ or $|\Lambda| > B^{-C}$ where C is an explicitly computable number which depends only on n, d, A and the choice of the logaritms.

Lower bounds of this form were found earlier by Gel'fond in 1935 for the case $n = 2$ and $\beta_0 = 0$. Because of the potential application of these lower bounds an enormous amount of energy has gone into the actual determination of the value of C. In particular we mention

Theorem 5.2.3 (Baker-Wüstholz, 1993) *Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers which generate a number field of degree d over $\mathbb{Q}$. Let $b_1, \ldots, b_n \in \mathbb{Z}$. Let $A_i = \max(e, H_\infty(\alpha))$ and $B = \max(|b_1|, \ldots, |b_n|, e)$. For each i we choose $\log \alpha_i$ such that $-\pi i < \mathrm{Im}(\log \alpha_i) \leq \pi i$. Let*

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n.$$

Then either $\Lambda = 0$ or

$$|\Lambda| > \exp\left(-(16nd)^{2n+4} \log A_1 \times \cdots \times \log A_n \times \log B\right).$$

Notice that the lower bound in this theorem has the form B^{-C} where $C = (16nd)^{2n+4} \log A_1 \times \cdots \times \log A_n \times \log B$.
The importance of these lower bounds becomes clear from the following Corollary of Theorem 5.2.3 or 5.2.2.

Corollary 5.2.4 *Let notations be as in Theorem 5.2.3. Then there exists an explicitly computable number $C > 1$ such that for all choices of $b_1, \ldots, b_n \in \mathbb{Z}$ we have either $\alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_n^{b_n} = 1$ or*

$$|\alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_n^{b_n} - 1| > B^{-C}.$$

Proof. Suppose we have a complex number z such that $|e^z - 1| < \epsilon$ where $\epsilon < 1/2$. Then an elementary consideration shows that there exists an integer k such that $|z - 2\pi i k| < 2\epsilon$. Let Λ be as in Theorem 5.2.3. We need to show that there exists $C > 1$ such that $|e^\Lambda - 1| > B^{-C}$ for all choices of the b_i. Put $|e^\Lambda - 1| = \epsilon$. We can assume that $\epsilon < 1/2$ and so there exists an integer k such that

$$|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n - 2k\pi i| < 2\epsilon.$$

We now apply Theorem 5.2.2 or 5.2.3 to the logarithms $\log \alpha_1, \ldots, \log \alpha_n, \log(-1) = \pi i$ and find $C_1 > 0$ such that

$$|\Lambda - 2k\pi i| > (\max(B, |k|)^{-C_1}.$$

Notice that $k < c_3 B$ for some constant $c_3 > 0$ and so

$$(c_3 B)^{-C_1} < |\Lambda - 2k\pi i| < 2\epsilon.$$

The desired lower bound for ϵ follows.

□

To see the strength of Corollary 5.2.4 we compare it with a lower bound which can be obtained in an elementary way. Before we do so we need an auxiliary Lemma.

Lemma 5.2.5 *Let α be a non-zero algebraic number with minimal polynomial $P(x) = a_0 x^d + \cdots + a_d$ and height $H = H_\infty(\alpha)$. Then*

$$|\alpha| < \frac{2H}{a_0}.$$

Proof When $|\alpha| \leq 1$ we are done. So assume that $|\alpha| > 1$. From $P(\alpha) = 0$ it follows that

$$a_0\alpha = -a_1 - a_2\alpha^{-1} - \cdots - a_d\alpha^{d-1}.$$

Using the triangle inequality,

$$\begin{aligned} a_0|\alpha| &\leq |a_1| + |a_2||\alpha|^{-1} + \cdots + |a_d||\alpha|^{-d+1} \\ &\leq H(1 + |\alpha|^{-1} + \cdots + |\alpha|^{-d+1} \\ &< H/(1 - |\alpha|^{-1}) \end{aligned}$$

After multiplication by $(1 - |\alpha|^{-1})/a_0$ we get

$$|\alpha| - 1 < H/a_0.$$

Hence $|\alpha| < H/a_0 + 1 \leq 2H/a_0$. □

Lemma 5.2.6 *Let notations be as in Theorem 5.2.3 and let* $A = \max_i A_i$. *Then* $|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1|$ *is either zero or bounded below by* $(3A)^{-ndB}$.

Proof. Let K be the number field generated by $\alpha_1, \ldots, \alpha_n$. Denote the leading coefficients of their minimal polynomials by $a_1, \ldots, a_n$. Suppose that $b_i \geq 0$ for all i. Then, for any embedding $\sigma : K \to \mathbb{C}$ we have, according to the previous Lemma,

$$\begin{aligned} a_1^{b_1} \cdots a_n^{b_n} |\sigma(\alpha_1^{b_1}) \cdots \sigma(\alpha_n^{b_n}) - 1| &< (2A_1)^{b_1} \cdots (2A_n)^{b_n} + A_1^{b_1} \cdots A_n^{b_n} \\ &< (3A)^{b_1 + \cdots + b_n} \leq (3A)^{nB}. \end{aligned}$$

The product of these expressions over all conjugates is at least one. This implies that

$$a_1^{b_1} \cdots a_n^{b_n} |\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| > (3A)^{-nB(d-1)}.$$

Since $a_1^{b_1} \cdots a_n^{b_n} \leq A^{nB}$ our lower bound now follows.
If, for example, $b_1 < 0$ we rewrite $\alpha_1^{b_1}$ as $(\alpha_1^{-1})^{|b_1|}$. Since α_1 and α_1^{-1} have the same height we can use the same argument as above, but now with α_1^{-1} instead of α_1. □

Application of Theorem 5.2.2
Fix X and let S be the set of natural numbers whose largest prime factor is $\leq X$. Order them in the following way,

$$n_1 < n_2 < n_3 < \ldots$$

A lower bound for the difference between consecutive terms has always been of interest for number theory. For example, Störmer (1898) showed that $\liminf_{i \to \infty} (n_{+i+1} - n_i) \geq 2$ and Erdös showed that for any $\epsilon > 0$ there exists $N(\epsilon)$ such that $n_{i+1} - n_i > n_i^{1-\epsilon}$ whenever $n_i > N(\epsilon)$. Using linear forms in logarithms one can prove the following statement

Theorem 5.2.7 (Tijdeman, 1973) *Let notation be as above then there exists a positive number* C, *depending only on* X, *such that*

$$n_{i+1} - n_i > \frac{n_i}{(\log n_i)^C}$$

whenever $n_i \geq 10$.

Proof. Let $p_1, \ldots, p_k$ be the primes $\leq X$. When $k = 1$ our result is of course trivial. Therefore assume that $k \geq 2$. Write $n_i = p_1^{a_1} \cdots p_k^{a_k}$ and $n_{i+1} = p_1^{b_1} \cdots p_k^{b_k}$. Notice that

$$\max_j |b_j - a_j| \leq \log(n_{i+1}) / \log 2 \leq (\log n_i)^2$$

since $n_{i+1} \leq 2n_i$ and $n_i \geq 10$. We apply Theorem 5.2.2 with $B < (\log n_i)^2$ to get

$$\begin{aligned} \left| \frac{n_{i+1}}{n_i} - 1 \right| &> \log \frac{n_{i+1}}{n_i} \\ &= |\sum_{j=1}^{k} (b_j - a_j) \log p_j| \\ &\geq (\log n_i)^{-2C} \end{aligned}$$

where C depends on $p_1, \ldots, p_k$. This proves our statement.

□

Remarkably enough there is also an upper bound of the same type.

Theorem 5.2.8 (Tijdeman) *Let notations be as in the previous theorem. Then there exists $c > 0$ depending only on $p_1, \ldots, p_k$ such that*

$$|n_{i+1} - n_i| < \frac{n_i}{(\log n_i)^c}$$

for all i and $n_i > 10$.

The proof doesn't use linear forms in logarithms, but is of a more elementary nature.

5.3 Exercises

Exercise 5.3.1 *In the text we defined the height of an algebraic number $\alpha \neq 0$ of degree d with minimal polynomial P as the sup-norm of the coefficient vector of P. Notation: $H_\infty(\alpha)$. However we can also take the L^1-norm of the coefficient vector of P, which we denote by $H_1(\alpha)$. So, letting $P = a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d$, we define*

$$H_\infty(\alpha) = \max(|a_0|, \ldots, |a_d|), \qquad H_1(\alpha) = |a_0| + \cdots + |a_d|.$$

Show that for any non-zero $\alpha \in \overline{\mathbb{Q}}$,

1. *$H_1(\alpha) \leq (d+1)H_\infty(\alpha)$.*
2. *$|\alpha| \leq H_1(\alpha)/a_0$.*
3. *when $\alpha \neq -1$, we have $H_1(\alpha + 1) \leq 2^d H_1(\alpha)$*

Exercise 5.3.2 *This problem is about sums of the form*

$$\frac{1}{1} - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \cdots \qquad (A)$$

and its variants (do you see the pattern in (A)?). In general, we wonder about the arithmetic nature of sums

$$\sum_{n=1}^{\infty} \frac{f(n)}{n}$$

where f is a function $f : \mathbb{N} \to \overline{\mathbb{Q}}$ which is periodic with period q, say. In other words $f(n+q) = f(n)$ for all $n \in \mathbb{N}$. To determine these sums we use the power series for $-\log(1-z)$, in particular the evaluation

$$\sum_{n=1}^{\infty} \frac{\zeta^n}{n} = -\log(1-\zeta)$$

for any root of unity $\zeta \neq 1$.

1. *Show that there exist algebraic numbers* $\hat{f}(k)$ *for* $k = 0, 1, \ldots, q-1$ *such that*
$$f(n) = \frac{1}{q}\sum_{k=0}^{q-1} \hat{f}(k) e^{2\pi i k n/q}.$$
($\hat{f}$ *is the so-called Fourier transform of* f*).*
2. *Determine the value of the sum (A) above.*
3. *Show that, in general,* $\sum_{n=1}^{\infty} f(n)/n$ *is either zero or transcendental.*
4. *Give an example of a non-trivial periodic function* f *for which the sum equals* 0*.*

Exercise 5.3.3 *This problem is about sums of the form*
$$F(P,Q) = \sum_{n=1}^{\infty} \frac{P(n)}{Q(n)}$$
where $P, Q \in \mathbb{Z}[x]$ *and* $\deg(P) \leq \deg(Q) - 2$*.*

1. *Suppose* Q *has only simple zero in* $\mathbb{Z}_{\leq 0}$*. Show that* $F(P,Q) \in \mathbb{Q}$*.*
2. *Suppose that* Q *has only simple rational zeros, not in* $\mathbb{N}$*. Show that* $F(P,Q)$ *is either rational or transcendental.*

Exercise 5.3.4 *Let* $A, B \in \mathbb{Z}$*. We are given a recurrent sequence* $u_0, u_1, u_2, \ldots \in \mathbb{Z}$ *defined by prescribing* u_0, u_1 *and*
$$u_{n+1} = Au_n + Bu_{n-1}$$
for $n \geq 1$ *(generalisation of the Fibonacci sequence). Let* θ, θ' *be the zeros of the so-called companion polynomial* $X^2 - AX - B$*. Assume that the companion polynomial is irreducible over* $\mathbb{Q}$ *and that* θ/θ' *is not a root of unity.*

1. *Show that there exist* $\alpha, \alpha' \in \mathbb{Q}(\theta)$ *such that*
$$u_n = \alpha\theta^n + \alpha'(\theta')^n$$
for all n*. (Hint: use induction).*
2. *Suppose that* θ *is real. Show that* θ *and* θ' *have different absolute values of which at least one is* > 1*.*
3. *Let assume* $\theta \in \mathbb{R}$ *and* $|\theta| > |\theta'|$*. Show that there exists a positive constant* c *such that* $|u_n| \geq c \cdot |\theta|^n$*.*
4. *Now assume that* $\theta \notin \mathbb{R}$*. Show that there exist positive constants* c, C *such that*
$$|u_n| \geq c \cdot |\theta|^n n^{-C}.$$
5. *Show that, for any* k*, the equation* $u_n = k$ *in* n *has at most finitely many solutions.*
6. *As a side remark we add that the equation* $u_n = -1$ *for the sequence with* $M = -1, N = -2, u_0 = 0, u_1 = 1$ *has four solutions* $n \in \mathbb{N}$*. Determine them.*