On a transcendence type lemma

The purpose of this note is to prove the following lemma:

Lemma. *Let* $K = \mathbb{Q}(x_1, \ldots, x_m, y_1, \ldots, y_n)$ *with*

(1) $\{x_1, \ldots, x_m\}$ *a transcendence basis for* K *over* $\mathbb{Q}$*, and*
(2) $\{y_1, \ldots, y_n\}$ *a (vector space) basis for* K *over* $\mathbb{Q}(x_1, \ldots, x_m)$*.*

Then the transcendence type of K *is at least* $m + 1$*.*

The result is ostensibly by the pigeonhole principle, but there is a little more work that that statement suggests. The lemma actually results from the following three lemmata.

Lemma 1. *Let* $u_{i,j}$ *be real numbers for* $1 \leqslant i \leqslant \nu$*, and* $1 \leqslant j \leqslant \mu$*. Let* $U \in \mathbb{R}$ *satisfy*

$$U \geqslant \max_{1 \leqslant j \leqslant \mu} \sum_{i=1}^{\nu} |u_{i,j}|,$$

and let X *and* ℓ *be two positive integers such that*

$$\ell^{\mu} < (X+1)^{\nu}.$$

Then there exist $\xi_1, \ldots, \xi_\nu \in \mathbb{Z}$ *not all zero such that*

$$\max_{1 \leqslant i \leqslant \nu} |\xi_i| \leqslant X$$

and

$$\max_{1 \leqslant j \leqslant \mu} \left| \sum_{i=1}^{\nu} u_{i,j} \xi_i \right| \leqslant \frac{UX}{\ell}.$$

Proof. The result is reminiscent of Siegel's lemma, and like that result it uses the pigeonhole principle. Let

$$\mathbb{N}(\nu, X) := \{(\xi_1, \ldots, \xi_\nu) \in \mathbb{Z}^\nu \mid 0 \leqslant \xi_i \leqslant X \text{ for } 1 \leqslant i \leqslant \nu\}.$$

Consider the map $\varphi : \mathbb{N}(\nu, X) \to \mathbb{R}^\mu$ that takes $(\xi_1, \ldots, \xi_\nu)$ to $(\eta_1, \ldots, \eta_\mu)$ where

$$\eta_j = \sum_{i=1}^{\nu} u_{i,j} \xi_i \qquad (1 \leqslant j \leqslant \mu).$$

For $1 \leqslant j \leqslant \mu$ we denote by $-V_j$ (and, respectively, W_j) the sum of the negative (respectively positive) elements of the set

$$u_{1,j}, u_{2,j}, \ldots, u_{\nu,j}.$$

Therefore we have by hypothesis

$$V_j + W_j \leqslant U \qquad \text{for all } 1 \leqslant j \leqslant \mu.$$

We may note that if $(\xi_1, \ldots, \xi_\nu) \in \mathbb{N}(\nu, X)$ then $(\eta_1, \ldots, \eta_\mu) = \varphi(\xi_1, \ldots, \xi_\nu)$ is in the set

$$E = \{(\eta_1, \ldots, \eta_\mu) \in \mathbb{R}^\mu \mid -V_j X \leqslant \eta_j \leqslant W_j X\}.$$

We partition each of the intervals $[-V_jX, W_jX]$ into ℓ intervals, each of length $\leqslant UX/\ell$ (since $W_jX - (-V_jX) \leqslant UX$). This partitions E into ℓ^μ subsets E_k $(1 \leqslant k \leqslant \ell^\mu)$.

The set $\mathbb{N}(\nu, X)$ has $(1+X)^\nu$ elements, and by hypothesis

$$\ell^\mu < (1+x)^\nu.$$

So by the pigeonhole principle there exist two distinct elements ξ^* and ξ^{**} of $\mathbb{N}(\nu, X)$ whose image under φ belong to the same subset E_k. We denote by ξ their difference $\xi^* - \xi^{**}$, and by η the value $\varphi(\xi)$. We have

$$\xi = (\xi_1, \ldots, \xi_\nu) \neq 0$$

since ξ^* and ξ^{**} are distinct, and

$$\max_{1 \leqslant i \leqslant \nu} |\xi_i| \leqslant X$$

by definition of $\mathbb{N}(\nu, X)$. Setting $\eta = (\eta_1, \ldots, \eta_\mu)$, we have

$$\max_{1 \leqslant j \leqslant \mu} |\eta_j| = \max_{1 \leqslant j \leqslant \mu} \left| \sum_{i=1}^{\nu} u_{i,j} \xi_i \right| \leqslant \frac{UX}{\ell}$$

since φ is a linear map and so $\varphi(\eta) = \varphi(\xi^* - \xi^{**}) = \varphi(\xi^*) - \varphi(\xi^{**})$. □

Lemma 2. *Let* $u_0, \ldots, u_m \in \mathbb{C}^\times$ *and let* $H \in \mathbb{N}$. *Then there exist* $\xi_0, \ldots, \xi_m \in \mathbb{Z}$ *not all zero such that*

$$\max_{0 \leqslant i \leqslant m} |\xi_i| \leqslant H$$

and

$$|u_0\xi_0 + \ldots + u_m\xi_m| < \sqrt{2}(|u_0| + \ldots + |u_m|)H^{-(m-1)/2}.$$

Proof. If $m = 0$ we require

$$|u_0\xi_0| < \sqrt{2H}|u_0|.$$

Since $H \geqslant 1$, $\sqrt{2H} \geqslant \sqrt{2}$, so $\xi_0 = 1$ suffices.

For $m = 1$ we require

$$|u_0\xi_0 + u_1\xi_1| < \sqrt{2}(|u_0| + |u_1|).$$

Without loss of generality assume $|u_0| \leqslant |u_1|$, then take $\xi_0 = 1$ and $\xi_1 = 0$. Then

$$|u_0\xi_0 + u_1\xi_1| = |u_0| < \sqrt{2}(|u_0| + |u_1|).$$

And $H \geqslant 1$ so $\max_{0 \leqslant i \leqslant 1} |\xi_i| \leqslant H$.

For $m \geqslant 2$ we apply Lemma 1. For $0 \leqslant i \leqslant m$ define $u_{i,1}$ and $u_{i,2}$ by $u_i = u_{i,1} + u_{i,2}\sqrt{-1}$. Now let

$$U = \sum_{i=0}^{m} |u_i|.$$

We have

$$\max_{1 \leqslant j \leqslant 2} \sum_{i=0}^{m} |u_{i,j}| \leqslant U$$

by the triangle inequality.

Let $\ell = \lfloor H^{(m+1)/2} + 1 \rfloor$. So in particular

$$H^{(m+1)/2} < \ell \leqslant H^{(m+1)/2} + 1.$$

Since for all $x \geqslant 0$ and $n > 2$ we have $(x^{n/2} + 1)^2 < (x+1)^n$, we know that

$$\ell^2 \leqslant (H^{(m+1)/2} + 1)^2 < (H+1)^{m+1}.$$

We may now apply Lemma 1, so there exist integers $\xi_0, \ldots, \xi_m$, not all zero and such that

$$\max_{0 \leqslant i \leqslant m} |\xi_i| \leqslant H$$

and

$$\begin{aligned} \max_{1 \leqslant j \leqslant 2} \left| \sum_{i=0}^{m} u_{i,j} \xi_i \right| &\leqslant \frac{UH}{\ell} \\ &= \frac{(|u_0| + \ldots + |u_m|)H}{\lfloor H^{(m+1)/2} + 1 \rfloor} \\ &< \frac{(|u_0| + \ldots + |u_m|)H}{H^{(m+1)/2}} \\ &= (|u_0| + \ldots + |u_m|)H^{-(m-1)/2}. \end{aligned}$$

And since for $z \in \mathbb{C}$ we have $|z| \leqslant \sqrt{2} \max\{|\Re z|, |\Im z|\}$ the result follows. □

Lemma 3. *Let $x_1, \ldots, x_q \in \mathbb{C}$ and $N_1, \ldots, N_q, H \in \mathbb{N}$. Then there exists a nonzero polynomial $P \in \mathbb{Z}[X_1, \ldots, X_q]$ with $\deg_{X_h} P \leqslant N_h$ for $1 \leqslant h \leqslant q$ and height $\leqslant H$ such that*

$$|P(x_1, \ldots, x_q)| \leqslant \sqrt{2} H^{1-M/2} \exp(c(N_1 + \ldots + N_q))$$

where

$$M = \prod_{k=1}^{q} (1 + N_k)$$

and

$$c = 1 + \log \max(1, |x_1|, \ldots, |x_q|).$$

Proof. Let $P \in \mathbb{Z}[X_1, \ldots, X_q]$ satisfy the hypotheses of the lemma, so $P(x_1, \ldots, x_q)$ is a sum of monomials in $x_1, \ldots, x_q$ with degree $\leqslant N_h$ in x_h. This gives at most $(1+N_1)(1+N_2)\cdots(1+N_q) = M$ terms in total. Denote the M monomials by $m_1, \ldots, m_M$.

By Lemma 2 we can find integers $\xi_1, \ldots, \xi_M$ not all zero such that if P has coefficients ξ_i then

$$|P(x_1, \ldots, x_q)| < \sqrt{2} \rho H^{-(M-2)/2}$$

where

$$\rho = \sum_{i=1}^{M} |m_i(x_1, \ldots, x_q)|.$$

Using the fact that $e^t > 1 + e^t$ for all $t > 0$ we have

$$\begin{aligned} M &= \prod_{k=1}^{q} (1 + N_k) \\ &< \prod_{k=1}^{q} e^{N_k} \\ &= \exp(N_1 + \ldots + N_q). \end{aligned}$$

We now estimate ρ as follows.

$$\begin{aligned} \rho &= \sum_{i=1}^{M} |m_i(x_1, \ldots, x_q)| \\ &\leqslant M \max\{1, |x_1|\}^{N_1} \cdots \max\{1, |x_q|\}^{N_q} \\ &< \exp(N_1 + \ldots + N_q) \max\{1, |x_1|, \ldots, |x_q|\}^{N_1 + \ldots + N_q} \\ &= \exp((N_1 + \ldots + N_q)(1 + \log \max\{1, |x_1|, \ldots, |x_q|\})). \end{aligned}$$

□

We can now prove the original lemma, which is restated below to include the definition of transcendence type.

Lemma. *Let $x_1, \ldots, x_m \in \mathbb{C}$ be a transcendence basis for $K \subseteq \mathbb{C}$. Suppose that for every $\alpha \in \mathbb{Q}(x_1, \ldots, x_m)$ we have*

$$-(\operatorname{size} \alpha)^\tau \ll \log |\alpha|.$$

Then $\tau \geqslant m + 1$.

Proof. Let $N, H \in \mathbb{N}$. Then by Lemma 3 there exists a nonzero polynomial $P \in \mathbb{Z}[X_1, \ldots, X_m]$ such that

$$\begin{aligned} \deg_{X_i} P &\leqslant N, \\ \operatorname{ht} P &\leqslant H, \end{aligned}$$

and

$$|P(x_1, \ldots, x_m)| \leqslant \sqrt{2} H^{1 - M/2} e^{cmN}$$

where

$$M = \prod_{k=1}^{m} (1 + N) < e^{mN}, \qquad c = 1 + \log \max\{1, |x_1|, \ldots, |x_m|\}.$$

Consider $\alpha = P(x_1, \ldots, x_m) \in \mathbb{Q}(x_1, \ldots, x_m)$. Let $mN \geqslant \log H$, then

$$\begin{aligned} \deg \alpha &\leqslant mN \\ \operatorname{ht} \alpha &\leqslant H \\ \operatorname{size} \alpha &= \max\{\deg \alpha, \log \operatorname{ht} \alpha\} \leqslant mN. \end{aligned}$$

So:

$$-(\operatorname{size} \alpha)^\tau \geqslant -(mN)^\tau.$$

Moreover,

$$|\alpha| \leqslant \sqrt{2} H^{1-M/2} e^{cmN},$$

so

$$\begin{aligned} \log|\alpha| &\leqslant \log\sqrt{2} + (1 - M/2)\log H + cmN \\ &= \log\sqrt{2} + \left(1 - \frac{1}{2}(1+N)^m\right)\log H + cmN. \end{aligned}$$

Thus we must have

$$-(mN)^\tau \ll \log\sqrt{2} + \left(1 - \frac{1}{2}(1+N)^m\right)\log H + cmN,$$

i.e.

$$N^\tau \gg N^m \log H.$$

Taking $N = m^{-1}\lceil \log H \rceil$ gives the result. □