Chapter 4

Transcendence results

We start with some generalities.

Let $K \supset k$ be a field extension. Recall that $\alpha \in K$ is called transcendental over k if there is no non-zero polynomial $f \in k[X]$ with $f(\alpha) = 0$.

A set of elements $\alpha_1, \ldots, \alpha_r$ is said to be *algebraically independent* over k if there is no non-zero polynomial $f \in k[X_1, \ldots, X_r]$ with $f(\alpha_1, \ldots, \alpha_r) = 0$.

Let S be a subset of K. We say that S has *transcendence degree* r over k, notation $\mathrm{trdeg}_k(S) = r$, if S has r elements which are algebraically independent over k but no $r+1$ elements which are algebraically independent over k.

When speaking about transcendence, algebraic (in)dependence, transcendence degree without specifying a field k, we assume that $k = \mathbb{Q}$.

Lemma 4.1. *Let $K \supset k$ be a field extension, and $\alpha_1, \ldots, \alpha_r \in K$. Further, let L be the algebraic closure of k in K.*
(i) $\alpha_1, \ldots, \alpha_r$ are algebraically independent over k if and only if $\alpha_1, \ldots, \alpha_{r-1}$ are algebraically independent over k and α_r is algebraic over $k(\alpha_1, \ldots, \alpha_{r-1})$.
(ii) $\alpha_1, \ldots, \alpha_r$ are algebraically independent over L if and only if they are algebraically independent over k.

Exercise 4.1. *Prove this lemma.*

4.1 The theorems of Hermite and Lindemann-Weierstrass

In all theorems mentioned below, we take $e^z = \sum_{n=0}^{\infty} z^n/n!$ for $z \in \mathbb{C}$. Further, $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \ \alpha \text{ algebraic over } \mathbb{Q}\}$.

Theorem 4.2 (Hermite, 1873)**.** *e is transcendental.*

We assume that e is algebraic. Under this hypothesis, we construct $M \in \mathbb{Z}$ with $M \neq 0$ and $|M| < 1$ and obtain a contradiction. We need some auxiliary results. Of course we have to use somehow some properties of e. We use that $(e^z)' = e^z$.

Let $f \in \mathbb{C}[X]$ be a polynomial. For $z \in \mathbb{C}$ we define

$$F(z) := \int_0^z e^{z-u} f(u) du. \tag{4.1}$$

Here the integration is over the line segment from 0 to z. We may parametrize this line segment by $u = tz$, $0 \leqslant t \leqslant 1$. Thus,

$$F(z) = \int_0^1 e^{z(1-t)} f(zt) z dt.$$

Lemma 4.3. *Suppose f has degree m. Then*

$$F(z) = e^z \left(\sum_{j=0}^{m} f^{(j)}(0) \right) - \sum_{j=0}^{m} f^{(j)}(z).$$

Proof. Induction on m and integration by parts. For $m = 0$ the assertion is obvious. Let $m \geqslant 1$. Then

$$\begin{aligned} F(z) &= -\int_0^1 f(zt) de^{z(1-t)} = -\left[f(zt) e^{z(1-t)} \right]_0^1 + \int_0^1 e^{z(1-t)} f'(zt) dt \\ &= e^z f(0) - f(z) + \int_0^1 e^{z(1-t)} f'(zt) dt. \end{aligned}$$

Apply the induction hypothesis with f' instead of f. □

Lemma 4.4. *For $z \in \mathbb{C}$ we have*

$$|F(z)| \leqslant |z| \cdot e^{|z|} \cdot \sup_{u \in \mathbb{C},\, |u| \leqslant |z|} |f(u)|.$$

Proof. We have

$$\begin{aligned} |F(z)| &\leqslant \int_0^1 |e^{z(1-t)} f(zt) z| dt \leqslant \int_0^1 e^{|z|} |z| \cdot |f(zt)| dt \\ &\leqslant |z| \cdot e^{|z|} \cdot \sup_{u \in \mathbb{C},\, |u| \leqslant |z|} |f(u)|. \end{aligned}$$

□

Assume that e is algebraic of degree n. Let p be a prime number, which is chosen later to be sufficiently large to make all estimates work. We apply the two lemmas above to

$$f(X) = X^{p-1} \{(X-1)(X-2)\cdots(X-n)\}^p. \tag{4.2}$$

Lemma 4.5. *We have*

$$f^{(p-1)}(0) = (p-1)! \{(-1)^n n!\}^p; \tag{4.3}$$

$$f^{(j)}(a) = 0 \quad \textit{for } a = 0, \ldots, n,\ j = 0, \ldots, p-1,\ (a,j) \neq (0, p-1); \tag{4.4}$$

$$f^{(j)}(a) \equiv 0 \,(\mathrm{mod}\, p!) \quad \textit{for } a = 0, \ldots, n,\ j \geqslant p. \tag{4.5}$$

Proof. In general, if g is a polynomial of the shape $(X-a)^r h$ with $a \in \mathbb{C}$, $h \in \mathbb{C}[X]$, then $g^{(m)}(a) = 0$ for $m = 0, \ldots, r-1$ and $g^{(r)}(a) = r! h(a)$. This implies (4.3), (4.4). To prove (4.5), observe that for any $g = c_r X^r + \cdots + c_0 \in \mathbb{C}[X]$ and all $j \geqslant 0$ we have

$$\frac{1}{j!} g^{(j)} = c_r \tbinom{r}{j} X^{r-j} + c_{r-1} \tbinom{r-1}{j} X^{r-j-1} + \cdots + c_j. \tag{4.6}$$

In particular, since $f \in \mathbb{Z}[X]$ and the binomial coefficients are integers, we have $f^{(j)}/j! \in \mathbb{Z}[X]$, and so $f^{(j)}(a)/j! \in \mathbb{Z}$ for $a = 0, \ldots, n$, $j \geqslant p$. This implies at once (4.5). □

Proof of Theorem 4.2. Since e is assumed to be algebraic of degree n, there are $q_0, q_1, \ldots, q_n \in \mathbb{Z}$ with

$$q_0 + q_1 e + \cdots + q_n e^n = 0, \quad q_0 \neq 0.$$

Let p be a prime number and let f be as in (4.2). Further, let F be as in (4.1). Define

$$M := \frac{1}{(p-1)!} \Big(q_0 F(0) + q_1 F(1) + \cdots + q_n F(n) \Big)$$

(so we replace e^a by $F(a)$ and divide by $(p-1)!$). We show that if p is sufficiently large, then $M \in \mathbb{Z}$, $M \neq 0$, and $|M| < 1$.

(i). $M \in \mathbb{Z}$, $M \neq 0$.
By Lemma 4.3, we can rewrite M as

$$\begin{aligned} M &= \frac{1}{(p-1)!}\left\{\sum_{a=0}^{n} q_a\left(e^a\Big(\sum_{j=0}^{np-1} f^{(j)}(0)\Big) - \sum_{j=0}^{np-1} f^{(j)}(a)\right)\right\} \\ &= \frac{1}{(p-1)!}\left\{\left(\sum_{a=0}^{n} q_a e^a\right)\left(\sum_{j=0}^{np-1} f^{(j)}(0)\right) - \sum_{a=0}^{n}\sum_{j=0}^{np-1} f^{(j)}(a)\right\} \\ &= -\frac{1}{(p-1)!}\sum_{a=0}^{n}\sum_{j=0}^{np-1} q_a f^{(j)}(a). \end{aligned}$$

By Lemma 4.5 we have $M \in \mathbb{Z}$ and

$$M \equiv -q_0\left\{(-1)^n n!\right\}^p \pmod{p}.$$

If $p > |nq_0|$ then $M \not\equiv 0 \pmod{p}$, hence $M \neq 0$.

(ii) $|M| < 1$.
By Lemma 4.4,

$$\begin{aligned} |F(a)| &\leqslant |a| \cdot e^{|a|} \cdot \sup_{|u|\leqslant|a|} |u^{p-1}\left\{(u-1)\cdots(u-n)\right\}^p| \\ &\leqslant |a| \cdot e^{|a|} \cdot n^{np-1} \leqslant e^n \cdot n^{np}. \end{aligned}$$

Hence

$$\begin{aligned} |M| &= \frac{1}{(p-1)!}\Big|\sum_{a=0}^{n} q_a F(a)\Big| \\ &\leqslant \frac{1}{(p-1)!}\left(\sum_{a=0}^{n}|q_a|\right) e^n \cdot n^{np} \leqslant \frac{c^p}{(p-1)!}, \end{aligned}$$

where c is a number independent of p. The factorial grows much faster than the exponential, so for p sufficiently large, we indeed obtain $|M| < 1$. □

Our next result is the famous Lindemann-Weierstrass theorem (Lindemann proved in 1883 that e^α is transcendental for algebraic α, and Weierstrass proved the general result in 1884).

Theorem 4.6. *Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$. Suppose that $\alpha_1, \ldots, \alpha_n$ are pairwise distinct, and that $\beta_1, \ldots, \beta_n \neq 0$. Then*

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0.$$

Before proving this theorem, we state some corollaries.

Corollary 4.7. *(i) Let $\alpha \in \overline{\mathbb{Q}}$ be non-zero. Then e^α is transcendental.*
(ii) π is transcendental.

Proof. (i) Suppose that $e^\alpha =: \beta$ is algebraic. Then it follows that $1 \cdot e^\alpha - \beta \cdot e^0 = 0$, contradicting Theorem 4.6.
(ii) Suppose that π is algebraic. Then πi is algebraic. But $e^{\pi i} = -1$ is not transcendental, contradicting (i). □

Corollary 4.8. *(i) Let $\alpha \in \overline{\mathbb{Q}}$ and $\alpha \neq 0$. Then $\sin\alpha$, $\cos\alpha$, and $\tan\alpha$ are transcendental.*
(ii) Let $\alpha \in \overline{\mathbb{Q}}$ and $\alpha \neq 0, 1$. Then $\log\alpha$ is transcendental (for any choice of $\log\alpha$).

Exercise 4.2. *Prove Corollary 4.8.*

Corollary 4.9. *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Then the following two assertions are equivalent:*
(i) $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$;
(ii) $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent.

Exercise 4.3. *Prove Corollary 4.9.*

We start with some preliminary comments on the proof of Theorem 4.6. Let us assume that

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = 0.$$

In the proof of the transcendence of e we assumed that $q_0 + q_1 e + \cdots + q_n e^n = 0$ for certain rational integers $q_0, \ldots, q_n$. We obtained a contradiction by constructing

$$M = \frac{1}{(p-1)!}\Big(q_0 F(0) + \cdots + q_n F(n)\Big) \quad (p \text{ prime})$$

and showing that $M \in \mathbb{Z}$, $M \neq 0$, $|M| < 1$.

This suggests that in the proof of the Lindemann-Weierstrass Theorem we should construct a number of the shape

$$M = \frac{1}{(p-1)!}\Big(\beta_0 F(\alpha_0) + \cdots + \beta_n F(\alpha_n)\Big) \quad (p \text{ prime}).$$

Here M is an algebraic number, not necessarily in $\mathbb{Q}$ or $\mathbb{Z}$. One may determine a positive $a \in \mathbb{Z}$ such that $a^{np}M$ is an algebraic integer. Following the proof of the transcendence of e, we may be able to show that $|a^{np}M| < 1$ and $a^{np}M \neq 0$. This leads to a non-zero algebraic integer of absolute value < 1. However, this is not impossible, for instance $\frac{1}{2}(1-\sqrt{5})$ is an algebraic integer of absolute value < 1. So to get a contradiction, we really have to construct an integer in $\mathbb{Z}$ and not just an algebraic integer outside $\mathbb{Z}$. To this end, we have to take into consideration also the conjugates of the α_i and β_i and construct a number which is invariant under Galois action.

Before proceeding, we observe that there is no loss of generality to assume that $\beta_1, \ldots, \beta_n$ are algebraic integers. Indeed, there is a positive $m \in \mathbb{Z}$ such that $m\beta_1, \ldots, m\beta_n$ are algebraic integers (e.g, we may take for m the product of the denominators of $\beta_1, \ldots, \beta_n$), and clearly, $\sum_{i=1}^n \beta_i e^{\alpha_i} \neq 0$ if and only if $\sum_{i=1}^n (m\beta_i) e^{\alpha_i} \neq 0$.

As it turns out, it suffices to prove the following weaker version of the Lindemann-Weierstrass Theorem.

Theorem 4.10 ("Weak Lindemann-Weierstrass Theorem")**.** *Let L be a normal algebraic number field. Let $\gamma_1, \ldots, \gamma_t$, $\delta_1, \ldots, \delta_t \in L$ such that*

$$\gamma_1, \ldots, \gamma_t \text{ are distinct}, \quad \delta_1 \cdots \delta_t \neq 0, \quad \delta_1, \ldots, \delta_t \in O_L$$

and suppose moreover, that each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ permutes the pairs $(\gamma_1, \delta_1), \ldots, (\gamma_t, \delta_t)$. Then

$$\delta_1 e^{\gamma_1} + \cdots + \delta_t e^{\gamma_t} \neq 0.$$

We say that $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ permutes the pairs $(\gamma_1, \delta_1), \ldots, (\gamma_t, \delta_t)$ if $(\tau(\gamma_1), \tau(\delta_1)), \ldots, (\tau(\gamma_t), \tau(\delta_t))$ is a permutation of $(\gamma_1, \delta_1), \ldots, (\gamma_t, \delta_t)$.

We first prove the implication Theorem 4.10$\Longrightarrow$Theorem 4.6. After that, we prove Theorem 4.10.

Theorem 4.10 $\Longrightarrow$ Theorem 4.6. Assume that Theorem 4.6 is false. This means that there are distinct algebraic numbers $\alpha_1, \ldots, \alpha_n$, and non-zero algebraic integers $\beta_1, \ldots, \beta_n$ from $\mathbb{C}$, such that

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = 0.$$

We derive from this a contradiction to Theorem 4.10.

Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ and let L be a normal algebraic number field containing K. Further, let

$$\mathrm{Gal}(L/\mathbb{Q}) = \{\tau_1 = \mathrm{id}, \tau_2, \ldots, \tau_d\}.$$

Then clearly,

$$\prod_{i=1}^{d} \left(\tau_i(\beta_1) e^{\tau_i(\alpha_1)} + \cdots + \tau_i(\beta_n) e^{\tau_i(\alpha_n)}\right) = 0.$$

By expanding the product, we get

$$\sum_{i_1=0}^{n} \cdots \sum_{i_d=1}^{n} \tau_1(\beta_{i_1}) \cdots \tau_d(\beta_{i_d}) \cdot e^{\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d})} = 0. \tag{4.7}$$

Each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ permutes the pairs $\big(\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d}),\ \tau_1(\beta_{i_1}) \cdots \tau_d(\beta_{i_d})\big)$, since $\tau\tau_1, \ldots, \tau\tau_d$ is a permutation of $\tau_1, \ldots, \tau_d$.

The exponents $\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d})$ need not be distinct. We group together the terms with equal exponents. Let $\gamma_1, \ldots, \gamma_s$ be the distinct values among $\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d})$ $(0 \leqslant i_1, \ldots, i_n \leqslant d)$, and for $k = 1, \ldots, s$, denote by J_k the set of tuples $(i_1, \ldots, i_d)$ such that

$$\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d}) = \gamma_k.$$

Then (4.7) becomes

$$\sum_{k=1}^{s} \delta_k e^{\gamma_k} = 0, \quad \text{where } \delta_k = \sum_{(i_1, \ldots, i_k) \in J_k} \tau_1(\beta_{i_1}) \cdots \tau_d(\beta_{i_d}). \tag{4.8}$$

Notice that each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ permutes the pairs $(\gamma_1, \delta_1), \ldots, (\gamma_s, \delta_s)$. A priori, all coefficients δ_k might be 0. However, we show that there is a tuple $(i_1, \ldots, i_k)$ such that $\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d})$ is different from all the other exponents. Thus, for some k, the set J_k has cardinality 1, and $\delta_k \neq 0$.

Define a total ordering on $\mathbb{C}$ by setting $\theta < \zeta$ if $\operatorname{Re}\theta < \operatorname{Re}\zeta$ or if $\operatorname{Re}\theta = \operatorname{Re}\zeta$ and $\operatorname{Im}\theta < \operatorname{Im}\zeta$. This ordering has the property that if θ_i, ζ_i are complex numbers with $\theta_i < \zeta_i$ for $i = 1, \dots, r$, then $\sum_{j=1}^{r} \theta_j < \sum_{j=1}^{r} \zeta_j$.

Since $\alpha_1, \dots, \alpha_d$ were assumed to be distinct, for each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, the numbers $\tau(\alpha_1), \dots, \tau(\alpha_d)$ are distinct. Hence for each $k \in \{1, \dots, d\}$, there is an index i_k such that $\tau_k(\alpha_{i_k}) > \tau_k(\alpha_j)$ for $j \neq i_k$. This implies

$$\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d}) > \tau_1(\alpha_{j_1}) + \cdots + \tau_d(\alpha_{j_d})$$

for all tuples $(j_1, \dots, j_d) \neq (i_1, \dots, i_d)$, and so $\tau_1(\alpha_{i_1}) + \cdots + \tau_d(\alpha_{i_d})$ is distinct from the other exponents.

Assume without loss of generality that $\delta_1, \dots, \delta_t$ are the non-zero numbers among $\delta_1, \dots, \delta_s$. Then (4.8) becomes

$$\sum_{k=1}^{t} \delta_k e^{\gamma_k} = 0. \tag{4.9}$$

By construction, the numbers $\gamma_1, \dots, \gamma_t$ are distinct algebraic numbers. Further, $\delta_1, \dots, \delta_t$ are non-zero, and in fact they are algebraic integers since they are sums of products of conjugates of algebraic integers. As observed before, each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ permutes the pairs $(\gamma_1, \delta_1), \dots, (\gamma_s, \delta_s)$ from (4.8). But then τ permutes also the pairs with $\delta_k \neq 0$, i.e., τ permutes $(\gamma_1, \delta_1), \dots, (\gamma_t, \delta_t)$. Now Theorem 4.10 implies that (4.9) is false.

Thus, our assumption that Theorem 4.6 is false leads to a contradiction. □

Proof of Theorem 4.10. We follow the transcendence proof of e, with the necessary modifications.

Let $\gamma_1, \dots, \gamma_t$ be distinct algebraic numbers, and $\delta_1, \dots, \delta_t$ non-zero algebraic integers from the normal number field L, such that each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ permutes the pairs $(\gamma_1, \delta_1), \dots, (\gamma_t, \delta_t)$. Assume that

$$\delta_1 e^{\gamma_1} + \cdots + \delta_t e^{\gamma_t} = 0. \tag{4.10}$$

Let again p be a prime number. Further, let l be a positive rational integer such that $l\gamma_1, \dots, l\gamma_t$ are all algebraic integers (e.g, the product of the denominators of

$\gamma_1, \ldots, \gamma_t$. For $k = 1, \ldots, t$, define

$$f_k(X) := l^{tp}(X - \gamma_k)^{p-1} \prod_{j=1}^{t} (X - \gamma_j)^p,$$

$$F_k(z) := \int_0^z e^{z-u} f_k(u) du,$$

$$M_k := \frac{1}{(p-1)!}\Big(\delta_1 F_k(\gamma_1) + \cdots + \delta_t F_k(\gamma_t)\Big),$$

and then,

$$M := M_1 \cdots M_t.$$

We prove that for p sufficiently large, we have $M \in \mathbb{Z}$, $M \neq 0$, and $|M| < 1$.

Lemma 4.11. *let $k \in \{1, \ldots, t\}$. Then*

$$f_k^{(p-1)}(\gamma_k) = (p-1)! \cdot l^{tp} \left\{ \prod_{j=1,\, j\neq k}^{t} (\gamma_k - \gamma_j) \right\}^p, \tag{4.11}$$

$$f_k^{(m)}(\gamma_j) = 0 \quad \textit{for } j = 1, \ldots, t,\ m = 0, \ldots, p-1,\ (j,m) \neq (k, p-1), \tag{4.12}$$

$$f_k^{(m)}(\gamma_j) = p! \cdot (\text{algebraic integer}) \quad \textit{for } j = 1, \ldots, t,\ m \geqslant p. \tag{4.13}$$

Proof. The proofs of (4.11) and (4.12) are completely analogous to those of (4.3) and (4.4) in Lemma 4.5. We prove only (4.13). Let $k, j \in \{1, \ldots, t\}$ and $m \geqslant p$. Define

$$g_k(X) := f_k(X/l) = l(X - l\gamma_k)^{p-1} \prod_{j=1,\, j\neq k}^{t} (X - l\gamma_j)^p.$$

Then g_k has algebraically integral coefficients. Using (4.6), one easily shows that the coefficients of $g_k^{(m)}/m!$ are algebraic integers. Hence $g^{(m)}(l\gamma_j)/m!$ is an algebraic integer, and therefore,

$$\frac{f_k^{(m)}(\gamma_j)}{m!} = \frac{l^m g_k^{(m)}(l\gamma_j)}{m!}$$

is an algebraic integer. This implies at once (4.13). □

Lemma 4.12. *For p sufficiently large we have $M \in \mathbb{Z}$ and $M \neq 0$.*

Proof. By Lemma 4.3 and our assumption $\sum_{j=1}^{t} \delta_j e^{\gamma_j} = 0$ we have

$$\begin{aligned} M_k &= \frac{1}{(p-1)!} \left\{ \sum_{j=1}^{t} \delta_j F_k(\gamma_j) \right\} \\ &= \frac{1}{(p-1)!} \left\{ \sum_{j=1}^{t} \delta_j \left(\sum_{m=0}^{tp-1} e^{\gamma_j} f_k^{(m)}(0) - \sum_{m=0}^{tp-1} f_k^{(m)}(\gamma_j) \right) \right\} \\ &= \frac{1}{(p-1)!} \left\{ \left(\sum_{j=1}^{t} \delta_j e^{\gamma_j} \right) \left(\sum_{m=0}^{tp-1} f_k^{(m)}(0) \right) - \sum_{j=1}^{t} \sum_{m=0}^{tp-1} \delta_j f_k^{(m)}(\gamma_j) \right\} \\ &= -\frac{1}{(p-1)!} \sum_{j=1}^{t} \sum_{m=0}^{tp-1} \delta_j f_k^{(m)}(\gamma_j). \end{aligned}$$

An application of Lemma 4.11 gives

$$M_k = -\delta_k A_k^p + p \cdot (\text{algebraic integer}) \quad \text{with } A_k := l^t \prod_{j=1,\, j \neq k}^{t} (\gamma_k - \gamma_j).$$

Both δ_k, A_k are algebraic integers, hence M_k is an algebraic integer.

We show that $\tau(M) = M$ for $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, which implies that $M \in \mathbb{Z}$. Take $\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Then there is a permutation τ^* of $1, \ldots, t$ such that

$$(\tau(\gamma_k), \tau(\delta_k)) = (\gamma_{\tau^*(k)}, \delta_{\tau^*(k)}) \ \text{ for } k = 1, \ldots, t.$$

By applying τ to the coefficients of f_k, we obtain

$$l^{tp}(X - \tau(\gamma_k))^{p-1} \prod_{j=1}^{t} (X - \tau(\gamma_j))^p = l^{tp}(X - \gamma_{\tau^*(k)}) \prod_{j=1}^{t} (X - \gamma_{\tau^*(j)})^p = f_{\tau^*(k)}.$$

Hence

$$\begin{aligned} \tau(M_k) &= -\frac{1}{(p-1)!} \sum_{j=1}^{t} \sum_{m=0}^{tp-1} \tau(\delta_j) f_{\tau^*(k)}^{(m)}(\tau(\gamma_j)) \\ &= -\frac{1}{(p-1)!} \sum_{j=1}^{t} \sum_{m=0}^{tp-1} \delta_{\tau^*(j)} f_{\tau^*(k)}^{(m)}(\gamma_{\tau^*(j)}) = M_{\tau^*(k)}. \end{aligned}$$

As a consequence, we obtain indeed

$$\tau(M) = \tau(M_1 \cdots M_t) = M_1 \cdots M_t = M.$$

This holds for all $\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Hence $M \in \mathbb{Z}$.

Put $\delta := \delta_1 \cdots \delta_t$, $A := A_1 \cdots A_t$. Since the δ_k, A_k are non-zero algebraic integers, their products δ, A are non-zero algebraic integers. Similarly as above we have $\tau(A_k) = A_{\tau^*(k)}$ for $k = 1, \ldots, t$, implying $\tau(A) = A$ for $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, hence $A \in \mathbb{Z} \setminus \{0\}$. In precisely the same way, it follows that $\delta \in \mathbb{Z} \setminus \{0\}$.

We proved that $M_k = -\delta_k A_k^p + p \cdot (\text{algebraic integer})$ for $k = 1, \ldots, t$. Hence

$$M = \pm \delta A^p + p \cdot (\text{algebraic integer}).$$

But the algebraic integer is a rational number, hence in $\mathbb{Z}$. Thus, we obtain a congruence in $\mathbb{Z}$,

$$M \equiv \pm \delta A^p \,(\mathrm{mod}\, p).$$

Now if $p > |\delta A|$, then $M \not\equiv 0 \,(\mathrm{mod}\, p)$, hence $M \neq 0$. □

Lemma 4.13. *For p sufficiently large we have $|M| < 1$.*

Proof. By Lemma 4.4 we have for $k, j = 1, \ldots, t$,

$$\begin{aligned} |F_k(\gamma_j)| &\leqslant |\gamma_j| \cdot e^{|\gamma_j|} \cdot \sup_{|u| \leqslant |\gamma_j|} |f_k(u)| \\ &\leqslant |\gamma_j| \cdot e^{|\gamma_j|} \cdot \sup_{|u| \leqslant |\gamma_j|} \left(|l^{tp}| \cdot |u - \gamma_k|^{p-1} \cdot \prod_{h=1,\, h \neq k}^{t} |u - \gamma_h|^p \right) \\ &\leqslant \left(\max_{1 \leqslant j \leqslant t} |\gamma_j| \cdot e^{|\gamma_j|} \right) \cdot l^{tp} (|\gamma_1| + \cdots + |\gamma_t|)^{tp-1} \leqslant c^p \end{aligned}$$

for some constant c independent of j, k and p. It follows that for p sufficiently large we have

$$|M_k| \leqslant \frac{1}{(p-1)!} \left(\sum_{j=1}^{t} |\delta_j| \right) \cdot c^p < 1 \quad \text{for } k = 1, \ldots, t.$$

Hence $|M| = \prod_{k=1}^{t} |M_k| < 1$. □

Thus, our assumption that Theorem 4.10 is false implies the existence of a non-zero $M \in \mathbb{Z}$ with $|M| < 1$, which is impossible. This completes our proof of Theorem 4.10. □

4.2 Other transcendence results

We give an overview of some other transcendence results, without proof. Recall that the logarithm on $\mathbb{C}$ is a multi-valued function: the logarithm of a non-zero complex number z is defined by $\log z := \log|z| + i \arg z$, where $\log|z|$ is the usual real logarithm of the positive number $|z|$ and $\arg z$ is any choice for the argument of z. In the theorems below, we fix a real φ_0, and take $\arg z \in [\varphi_0, \varphi_0 + 2\pi)$. Having fixed φ_0, we have fixed the argument, the logarithm, and also $a^b := e^{b \log a}$ for $a, b \in \mathbb{C}$ with $a \neq 0$, where $e^z := \sum_{n=0}^{\infty} z^n/n!$. The theorems hold for any choice of φ_0.

Theorem 4.14 (Gel'fond, Schneider, 1934)**.** *Let $\alpha, \beta \in \overline{\mathbb{Q}}$ with $\alpha \neq 0, 1$, $\beta \notin \mathbb{Q}$. Then α^β is transcendental.*

Corollary 4.15. *Let $\alpha \in \overline{\mathbb{Q}}$ with $\alpha \notin \mathbb{Q}i$. Then $e^{\pi\alpha}$ is transcendental.*

Proof. Choose $\log(-1) = \pi i$. Then $e^{\pi\alpha} = e^{-i\alpha \log(-1)} = (-1)^{-i\alpha}$. □

Corollary 4.16. *Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \overline{\mathbb{Q}}$ be non-zero. Assume that $\log \alpha_1$, $\log \alpha_2$ are linearly independent over $\mathbb{Q}$. Then*

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

Proof. Suppose $\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 = 0$. Put $\gamma := -\beta_2/\beta_1$. Then by assumption, $\gamma \notin \mathbb{Q}$, and

$$\alpha_2 = e^{\log \alpha_2} = e^{\gamma \log \alpha_1} = \alpha_1^\gamma,$$

contradicting Theorem 4.14. □

In 1966, A. Baker proved the following far-reaching generalization.

Theorem 4.17 (A. Baker, 1966)**.** *Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ be non-zero. Assume that*

$$\log \alpha_1, \ldots, \log \alpha_n \text{ are linearly independent over } \mathbb{Q}.$$

Then $\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n$ is transcendental.

Definition. We say that non-zero complex numbers $\alpha_1, \ldots, \alpha_n$ are *multiplicatively dependent* if there are $x_1, \ldots, x_n \in \mathbb{Z}$, not all 0, such that

$$\alpha_1^{x_1} \cdots \alpha_n^{x_n} = 1.$$

Otherwise, $\alpha_1, \ldots, \alpha_n$ are called multiplicatively independent.

Corollary 4.18. *Let $n \geqslant 1$. Let $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_n, \gamma \in \overline{\mathbb{Q}}$ be such that*

$$\alpha_1, \ldots, \alpha_n \neq 0, \quad \alpha_1, \ldots, \alpha_n \text{ are multiplicatively independent,}$$
$$(\beta_1, \ldots, \beta_n) \notin \mathbb{Q}^n.$$

Then $e^\gamma \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ is transcendental.

Proof. Suppose that $\delta := e^\gamma \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ is algebraic. We have

$$e^{\log \delta} = e^{\gamma + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n}$$

and so, for some $k \in \mathbb{Z}$,

$$\log \delta = \gamma + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n + 2k\pi i. \tag{4.14}$$

Note that $\log(-1) = (2l+1)\pi i$ for some $l \in \mathbb{Z}$ depending on the choice of the log. By Theorem 4.17, $\log \delta$, $\log \alpha_1, \ldots, \log \alpha_n$ and $\log(-1)$ are linearly dependent over $\mathbb{Q}$, that is, there are $x_1, \ldots, x_n, x_{n+1}, x_{n+2} \in \mathbb{Z}$, not all 0, such that

$$x_1 \log \alpha_1 + \cdots + x_n \log \alpha_n + x_{n+1} \log(-1) + x_{n+2} \log \delta = 0. \tag{4.15}$$

Eliminating $\log \delta$ from (4.14) and (4.15), we get

$$x_{n+2}\gamma + (x_{n+2}\beta_1 + x_1) \log \alpha_1 + \cdots + (x_{n+2}\beta_n + x_n) \log \alpha_n + (x_{n+2} \cdot \tfrac{2k}{2l+1} + x_{n+1}) \log(-1) = 0.$$

In (4.15), at least one of $x_1, \ldots, x_n, x_{n+2}$ is $\neq 0$, since $\log(-1) \neq 0$. Since $(\beta_1, \ldots, \beta_n) \notin \mathbb{Q}^n$ we have $x_{n+2}\beta_i + x_i \neq 0$ for at least one $i \in \{1, \ldots, n\}$. Applying again Theorem 4.17, we infer that there are $y_1, \ldots, y_{n+1} \in \mathbb{Z}$, not all 0, such that

$$y_1 \log \alpha_1 + \cdots + y_n \log \alpha_n + y_{n+1} \log(-1) = 0.$$

In fact, at least one of $y_1, \ldots, y_n$ must be $\neq 0$. Now we get

$$\alpha_1^{2y_1} \cdots \alpha_n^{2y_n} = e^{2y_1 \log \alpha_1 + \cdots + 2y_n \log \alpha_n} = e^{-2y_{n+1} \log(-1)} = e^{-2y_{n+1}(2l+1)\pi i} = 1,$$

contrary to our assumption. □

In fact, the conditions that the α_i be multiplicatively independent, and the β_i not all in $\mathbb{Q}$ are needed only if $\gamma = 0$. These conditions can be dropped if we assume that $\gamma \neq 0$.

Exercise 4.4. *Let* $\alpha_1, \ldots, \alpha_n,\ \beta_1, \ldots, \beta_n,\ \gamma \in \overline{\mathbb{Q}}$*, and suppose that* $\gamma, \alpha_1, \ldots, \alpha_n \neq 0$*. Using Corollary 4.18, prove that* $e^{\gamma}\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ *is transcendental.*

There is a far reaching conjecture, due to Schanuel, which implies all results mentioned before and much more.

Schanuel's Conjecture. (1960's) *Let* $x_1, \ldots, x_n$ *be any (not necessarily algebraic) complex numbers which are linearly independent over* $\mathbb{Q}$*. Then*

$$\operatorname{trdeg}_{\mathbb{Q}}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}) \geqslant n.$$

We give some examples of known cases.

Examples. 1. Let $x \in \mathbb{C}^*$. Then either x is transcendental, or x is algebraic and then by Lindemann's Theorem, e^x is transcendental. Hence $\operatorname{trdeg}_{\mathbb{Q}}(x, e^x) \geqslant 1$. Schanuel's Conjecture is still open for $n \geqslant 2$.

2. Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ and suppose they are linearly independent over $\mathbb{Q}$. By Corollary 4.9 (a consequence of the Lindemann-Weierstrass Theorem), $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent. Hence $\operatorname{trdeg}_{\mathbb{Q}}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) = n$.

We deduce some consequences of Schanuel's Conjecture which are still open.

Conjecture. *e and π are algebraically independent.*

Proof under assumption of Schanuel's Conjecture. For instance by Lemma **??**, the transcendence degree of a set of numbers does not change if some algebraic numbers are added to or removed from it. Moreover, the transcendence degree of this set does not change if we multiply its elements with non-zero algebraic numbers. So by Schanuel's conjecture,

$$\operatorname{trdeg}_{\mathbb{Q}}(e, \pi) = \operatorname{trdeg}_{\mathbb{Q}}(e, \pi i) = \operatorname{trdeg}_{\mathbb{Q}}(1, \pi i, e, e^{\pi i}) = 2.$$

□

Conjecture. *Let* $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ *such that* $\alpha_1, \ldots, \alpha_n \neq 0$ *and* $\log \alpha_1, \ldots, \log \alpha_n$ *are linearly independent over* $\mathbb{Q}$*. Then* $\log \alpha_1, \ldots, \log \alpha_n$ *are algebraically independent.*

Proof under assumption of Schanuel's Conjecture. We have

$$\mathrm{trdeg}_{\mathbb{Q}}(\log\alpha_1,\ldots,\log\alpha_n) = \mathrm{trdeg}_{\mathbb{Q}}(\log\alpha_1,\ldots,\log\alpha_n,\alpha_1,\ldots,\alpha_n) \geqslant n.$$

□

According to Lemma 4.3, the above conjecture implies that also $\log\alpha_1,\ldots,\log\alpha_n$ are algebraically independent over $\overline{\mathbb{Q}}$, that is, for every non-trivial polynomial $P \in \overline{\mathbb{Q}}[X_1,\ldots,X_n]$ we have $P(\log\alpha_1,\ldots,\log\alpha_n) \neq 0$. Baker's Theorem 4.17 implies that this holds for linear polynomials $P \in \overline{\mathbb{Q}}[X_1,\ldots,X_n]$, but even for quadratic polynomials P this is still open. For instance, the above conjecture implies that $\log 2 \cdot \log 3$ is transcendental, but as yet not even this very special case could be proved.

We mention some other consequences of Schanuel's conjecture, the deduction of which is left as an exercise.

Exercise 4.5. *Deduce the following from Schanuel's conjecture:*
(i) Let $\alpha \in \overline{\mathbb{Q}}$, $\alpha \notin i\mathbb{Q}$. Then π and $e^{\pi\alpha}$ are algebraically independent.
(ii) Let α, $\beta \in \overline{\mathbb{Q}}$ with $\alpha \notin \{0,1\}$ and β of degree $d \geqslant 2$. Then $\alpha^{\beta}, \alpha^{\beta^2}, \ldots, \alpha^{\beta^{d-1}}$ are algebraically independent.
(iii) Define the sequence $\{x_n\}_{n=1}^{\infty}$ by $x_1 = e$ and $x_n = e^{x_{n-1}}$ for $n \geqslant 2$, i.e., $x_2 = e^e$, $x_3 = e^{e^e}$, etc. Then $x_1,\ldots,x_N$ are algebraically independent for every $N \geqslant 1$.
(iv) Let p, q be two distinct prime numbers. Then for every irrational $x \in \mathbb{R}$, at least one of the numbers p^x, q^x is transcendental.

Remark. The following has been proved.

In 1996, Nesterenko proved (among other things), that π, e^{π} and $\Gamma(\frac{1}{4})$ are algebraically independent. Recall that $\Gamma(x) = \int_0^{\infty} t^{x-1}e^{-t}dt$ for $x > 0$, that $\Gamma(n) = (n-1)!$ for every positive integer n, and that $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

For α, β as in (ii), Diaz proved in 1989 that

$$\mathrm{trdeg}_{\mathbb{Q}}(\alpha^{\beta}, \alpha^{\beta^2}, \ldots, \alpha^{\beta^{d-1}}) \geqslant [(d+1)/2]$$

where $[x]$ is the largest integer $\leqslant x$. This settles (ii) for $d = 3$.

In the 1960's, Lang and Ramachandra independently proved (among other things) that if p_1, p_2, p_3 are three distinct primes and x an irrational real, then at least one of the numbers p_1^x, p_2^x, p_3^x is transcendental.