I.N. Transcendental extensions

Recall that given L/K and $\alpha \in L$,

(I.N.1) α is *transcendental* over $K \iff \mathrm{ev}_\alpha \colon \underset{x\ \mapsto\ \alpha}{K[x] \to L}$ is injective.

I.N.2. PROPOSITION. *In this case, there exists a unique extension of* ev_α *to* $\widetilde{\mathrm{ev}}_\alpha \colon K(x) \hookrightarrow L$, *by setting* $\widetilde{\mathrm{ev}}_\alpha\left(\frac{f(x)}{g(x)}\right) := \frac{f(\alpha)}{g(\alpha)}$.

PROOF. The isomorphism $K[x] \cong K[\alpha]$ induced by ev_α obviously extends uniquely to an isomorphism of fraction fields, and of course $K(\alpha) \subseteq L$. $\square$

I.N.3. DEFINITION. Given a subset $A = \{\alpha_1, \ldots, \alpha_n\} \subset L$, A is **algebraically independent** over K if

$$\mathrm{ev}_A \colon \underset{x_i\ \mapsto\ \alpha_i}{K[x_1, \ldots, x_n] \to L}$$

is injective. Equivalently, there is *no* nontrivial polynomial relation of the form $\sum_j k_j \alpha_1^{d_{1j}} \cdots \alpha_n^{d_{nj}} = 0$ on the α_j's.

Once more, ev_A extends uniquely to $\widetilde{\mathrm{ev}}_A \colon K(x_1, \ldots, x_n) \hookrightarrow L$, factoring through an isomorphism $K(x_1, \ldots, x_n) \cong K(\alpha_1, \ldots, \alpha_n)$. Another characterization is given by the

I.N.4. PROPOSITION. *A is algebraically independent$/K \iff \alpha_i$ is transcendental over $K_{i-1} := K(\alpha_1, \ldots, \alpha_{i-1})$ $(\forall i)$.*

PROOF. If α_i is algebraic$/K_{i-1}$ for some i, then $f(\alpha_i) = 0$ for some $f \in K_{i-1}[x]$. After clearing denominators, this equation takes the form $0 = \sum_{j=0}^n F_j(\alpha_1, \ldots, \alpha_{i-1})\alpha_i^j$ with $F_j \in K[x_1, \ldots, x_{i-1}]$. But then $\{\alpha_1, \ldots, \alpha_i\}$ (and thus A) is not algebraically independent over K. The converse is left to you. $\square$

An *infinite* set A is considered to be algebraically independent over K when all its finite subsets are.

I.N.5. DEFINITION. Let $\mathscr{S} := \{A \subset L \mid A \text{ is alg. ind.}/K\}$, ordered by inclusion. A **transcendence basis** for L/K is a maximal element $\mathcal{S} \in \mathscr{S}$ in this ordering (if one exists!).

I.N.6. THEOREM. *$\mathcal{S} \subset L$ is a transcendence basis for L/K* $\iff$ (i) *$\mathcal{S}$ is algebraically independent over K and* (ii) *$L/K(\mathcal{S})$ is algebraic.*

PROOF. $\underline{(\implies)}$: Let $\alpha \in L \setminus \mathcal{S}$; then $\{\alpha\} \cup \mathcal{S}$ is *not* algebraically independent. So $f(s_1, \ldots, s_n, \alpha) = 0$ for some $s_1, \ldots, s_n \in \mathcal{S}$ and $f = \sum_{i=0}^m f_i(x_1, \ldots, x_n) y^i \in K[x_1, \ldots, x_n][y]$ (where $f_m \neq 0$). But algebraic independence of $\{s_1, \ldots, s_n\} \implies f_m(s_1, \ldots, s_n) \neq 0 \implies \alpha$ is algebraic over $K(\mathcal{S})$. Conclude that $L/K(\mathcal{S})$ is algebraic.

$\underline{(\impliedby)}$: Again let $\alpha \in L \setminus \mathcal{S}$; then α is algebraic over $K(\mathcal{S})$ by (ii), i.e. $g(\alpha) = 0$ for some $g = \sum_{j=0}^m g_j x^j \in K(\mathcal{S})[x]$. In fact, the g_j belong to $K(s_1, \ldots, s_n)$ (for some finite subset $\{s_1, \ldots, s_n\} \subset \mathcal{S}$); clearing denominators of the g_j's, we see that $\{s_1, \ldots, s_n, \alpha\}$ is not algebraically independent over K. So neither is $\mathcal{S} \cup \{\alpha\}$, and $\mathcal{S}$ is maximal. $\square$

I.N.7. THEOREM. *Any extension L/K has a transcendence basis. In particular, given subsets $C \subset A \subset L$ such that $L/K(A)$ is algebraic and C is algebraically independent over K, there exists a transcendence basis B for L/K with $C \subset B \subset A$.*

PROOF. Let $\mathscr{B} := \{\mathcal{S} \subset A \mid \mathcal{S} \supset C,\ \mathcal{S} \text{ alg. ind.}/K\}$. Each chain in $\mathscr{B}$ has an upper bound given by the union of its elements: any finite subset of elements in the union lies in a member of the chain, and so is algebraically independent. Applying Zorn yields a maximal element $B \in \mathscr{B}$. By the proof of I.N.6, any $\alpha \in A$ is algebraic over $K(B)$. So $K(A)/K(B)$ is algebraic, which makes $L/K(B)$ algebraic, which makes B a transcendence basis by I.N.6. Finally, to get *a* transcendence basis, we can simply take $A = L$ and $C = \emptyset$. $\square$

The upshot of these two results is that we can separate out *any* extension L/K into a "purely transcendental" part[53] $K(\mathcal{S})/K$ and an algebraic part $L/K(\mathcal{S})$.

[53] An extension is *purely transcendental* exactly when it can be written as $K(\mathcal{S})/K$ with $\mathcal{S}$ algebraically independent over K.

I.N.8. EXAMPLES. **(a)** Let $K = \mathbb{C}$, $F(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ be an irreducible polynomial, and L the fraction field of $\mathbb{C}[x_1, \ldots, x_n]/(F)$. Assuming F has positive degree in x_n, we have

$$L = \mathbb{C}(x_1, \ldots, x_{n-1})[x_n]/(F).$$

This is an algebraic extension of $\mathbb{C}(x_1, \ldots, x_{n-1})$, making $x_1, \ldots, x_{n-1}$ our transcendence basis. The subset $X_F \subset \mathbb{C}^n$ defined by $F = 0$ is called an *algebraic variety*, and L is its *function field*.

(b) Consider the case of $L = \mathbb{R}$ over $K = \mathbb{Q}$. For any *countable* subset $\mathcal{S} \subset \mathbb{R}$, $\mathbb{Q}(\mathcal{S})$ is countable. Were $\mathbb{R}$ algebraic over such a subfield, it would be countable too: one could count all elements via their minimal polynomials in $\mathbb{Q}(\mathcal{S})[x]$. So any transcendence basis for $\mathbb{R}/\mathbb{Q}$ is uncountable.

(c) If L is finitely generated over K, then I.N.7 provides a transcendence basis which is a subset of the generators, hence finite.

I.N.9. LEMMA. *Given an extension L of K, together with subsets $C = \{c_1, \ldots, c_r\}$ and $A = \{a_1, \ldots, a_s\}$ (of L), with all c_i's distinct and all a_j's distinct. Suppose that $L/K(A)$ is algebraic, and that C is algebraically independent over K. Then $r \leq s$, and there exists a subset $D \subset L$ with $C \subset D \subset A \cup C$ such that $|D| = s$ and $L/K(D)$ is algebraic.*

PROOF. Induce on r (trivial for $r = 0$, by taking $D = A$). Assuming the result for $r - 1$, independence of $C_0 := \{c_1, \ldots, c_{r-1}\}$ implies the existence of $D_0 \subset A \cup C_0$ containing C_0 with $|D_0| = s \geq r - 1$ and $L/K(D_0)$ algebraic. In particular, c_r is algebraic over $K(D_0)$. Relabeling if necessary, we have $D_0 = \{c_1, \ldots, c_{r-1}, a_r, a_{r+1}, \ldots, a_s\}$; and clearly $E := D_0 \cup \{c_r\}$ is algebraically *dependent*.

Algebraic *independence* of C, on the other hand, means that c_r is transcendental over $K(C_0)$. It follows that D_0 must be strictly larger than C_0, whence $s > r - 1$ (i.e. $s \geq r$).

Now the dependence of $E = \{c_1, \ldots, c_r, a_r, \ldots, a_s\}$ means that for some t (with $r \leq t \leq s$), a_t is algebraic over $K(c_1, \ldots, c_r, a_r, \ldots, a_{t-1})$, hence over $K(D)$ with $D := E \setminus \{a_t\}$. This makes $K(E)/K(D)$ algebraic. But $E \supset D_0 \implies L/K(E)$ algebraic $\implies L/K(D)$ algebraic. This completes the inductive step. $\square$

I.N.10. THEOREM. *Any two transcendence bases for L/K are either both infinite or have the same number of elements.*

PROOF. Suppose both are finite. In the notation of the Lemma, take C to be one basis, and A the other, thereby obtaining $r \leq s$; then reverse their roles.

If one basis is infinite, let C be a finite subset with r elements. Suppose the other basis is finite and call it A. Since r is arbitrary this yields a contradiction. $\square$

I.N.11. DEFINITION. The **transcendence degree** of L/K, written $\mathrm{trdeg}(L/K)$, is the number of elements in a transcendence basis.

I.N.12. EXAMPLE. The transcendence degree of the function field of the algebraic variety $X_F = \{F = 0\} \subset \mathbb{C}^n$ is $n-1$, the same as the dimension of X_F.

Finally, there is a tower law for transcendental extensions:

I.N.13. THEOREM. $\mathrm{trdeg}(M/K) = \mathrm{trdeg}(M/L) + \mathrm{trdeg}(L/K)$.

PROOF. If A and B are transcendence bases for L/K resp. M/L, then $A \cup B$ is clearly algebraically independent by I.N.4 (first adjoin successive elements of A, then of B).

To see that $M/K(A \cup B)$ is algebraic, consider the intermediate field $L(B)$: by assumption $M/L(B)$ is algebraic; the same applies to $L/K(A)$ hence to $K(A \cup B)(L)/K(A \cup B) = L(B)/K(A \cup B)$. $\square$

Transcendental numbers. We want to prove that numbers like e and π are transcendental. A first step is to understand why e is irrational: it is approximated by a sequence of rational numbers "better than it should be," in the sense that the denominators of said numbers grow much more slowly than the error in the approximation decreases. The point is that by Taylor's remainder formula, we have (for the k^{th} remainder)

$$\text{(I.N.14)}\quad e - \frac{\sum_{m=0}^{k} \frac{k!}{m!}}{k!} = \frac{1}{k!}\int_0^1 e^x (1-x)^k dt < \frac{3}{(k+1)!} = \frac{3/(k+1)}{k!}.$$

So if e was of the form A/B (for some $A, B \in \mathbb{Z}_{>0}$) then multiplying through by $k!B$ would give

$$\text{(I.N.15)}\qquad 0 \;<\; k!A - B\sum_{m=0}^{k} \frac{k!}{m!} \;<\; \frac{3B}{k+1},$$

where we know the middle term is positive because the integral was. But the middle term is an integer, and by taking $k \geq 3B$ we obtain a contradiction.

Here is another approach which looks markedly different at first, but is in fact closely related, and generalizes well to prove linear independence over $\mathbb{Q}$ of collections of exponentials. We'll need the following basic calculation: given a polynomial $P(z) \in \mathbb{C}[z]$ of degree d, consider the integral

$$\text{(I.N.16)}\qquad I_P(s) := \int_0^s e^{s-z} P(z) dz$$

along the segment from 0 to s in the complex plane. Integrating by parts, this

$$\begin{aligned} &= -e^{s-z}P(z)\big|_0^s + \int_0^s e^{s-z}P'(z)dz \\ &= e^s P(0) - P(s) + I_{P'}(s) = \cdots \\ &= e^s(P(0) + P'(0)) - (P(s) + P'(s)) + I_{P''}(s), \end{aligned}$$

and continuing along in this vein (since $P^{(d+1)} = 0$) yields

$$\text{(I.N.17)}\qquad I_P(s) = e^s \sum_{m=0}^{d} P^{(m)}(0) - \sum_{m=0}^{d} P^{(m)}(s).$$

Now suppose that $\beta_0 + \beta_1 e = 0$ for some $\beta_i \in \mathbb{Z} \setminus \{0\}$. Pick a prime p larger than the $|\beta_i|$, and let $P(z) := z^{p-1}(z-1)^p$. Then using (I.N.17), we have

$$\begin{aligned} J &:= \beta_0 I_P(0) + \beta_1 I_P(1) \\ &= (\beta_0 + \beta_1 e) \textstyle\sum_{m=0}^{2p-1} P^{(m)}(0) - \sum_{k=0,1} \sum_{m=0}^{2p-1} \beta_k P^{(m)}(k) \\ &= -\textstyle\sum_{k=0,1} \sum_{m=0}^{2p-1} \beta_k P^{(m)}(k), \end{aligned}$$

in which one notices that $P^{(m)}(k)$ is divisible by $p!$ unless $k = 0$ and $m = p - 1$, in which case it is divisible by $(p-1)!$ and *not* by $p!$. So $J \neq 0$ and $(p-1)! \mid J$, whence $|J| \geq (p-1)!$. On the other hand, we would be silly not to notice that $I_P(0) = 0$; and writing $|P|$ for the polynomial with its coefficients replaced by their absolute values,[54]

$$|I_P(1)| = |\textstyle\int_0^1 e^{1-z} P(z) dz| \leq e \int_0^1 |P|(z) dz \leq e|P|(1) = 2^p e$$

yields the bound $|J| < C^p$ for some constant C independent of p. Since p was arbitrary, we must have $(p-1)! < C^p$ for all $p \gg 0$, which is of course a contradiction.

If we take $P(z) := (1-z)^k$ instead, then (writing $\beta_0 = -A$ and $\beta_1 = B$), the calculation of J yields something like the middle term of (I.N.15). Moreover, $J = BI_P(1)$ is, up to a constant, the Taylor remainder for e^{-x} at $x = 1$. So, up to some signs, this recovers the first proof. So now we thoroughly understand why $e \notin \mathbb{Q}$, and we are also prepared for the hardest part of the proof of the

I.N.18. LINDEMANN-WEIERSTRASS THEOREM. *If $u_1, \ldots, u_n \in \bar{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then $e^{u_1}, \ldots, e^{u_n}$ are algebraically independent over $\bar{\mathbb{Q}}$.*

Before proving it let's derive some consequences:

I.N.19. COROLLARY. *e and π are transcendental over $\mathbb{Q}$; equivalently, they do not belong to $\bar{\mathbb{Q}}$.*

PROOF. Since the single-element set $\{1\}$ is linearly independent over $\mathbb{Q}$, the set $\{e^1\}$ is algebraically independent over $\bar{\mathbb{Q}}$; that is, e satisfies no polynomial equation with coefficients in $\bar{\mathbb{Q}}$ (*a fortiori* in $\mathbb{Q}$) and is therefore transcendental over $\mathbb{Q}$.

[54] Of course, here this is just $z^{p-1}(z+1)^p$, but I will use this more generally later.

Suppose we had $\pi \in \bar{\mathbb{Q}}$. Then also $\mathbf{i}\pi \in \bar{\mathbb{Q}}$, and by I.N.18 (arguing as for e^1) we would conclude that $e^{\mathbf{i}\pi}$ is transcendental. Which, you know, contradicts the formula by Euler on my coffee cup. □

BAKER'S PROOF OF I.N.18. We use Galois theory (Steps 1-3) to reduce to a statement that can be checked using the integrals (I.N.16) (Step 4).

Step 1: *It suffices to show that* $\alpha_1, \ldots, \alpha_n \in \bar{\mathbb{Q}}$ *distinct* $\implies$ $e^{\alpha_1}, \ldots, e^{\alpha_n}$ *are linearly independent over* $\bar{\mathbb{Q}}$*.*

Consider distinct vectors $\underline{k}^{(i)} \in \mathbb{N}^n$ $(i = 1, \ldots, r)$. Since the $\{u_i\}$ are LI/$\mathbb{Q}$, the $\{\underline{k}^{(i)} \cdot \underline{u}\}_{i=1}^r \subset \bar{\mathbb{Q}}$ are distinct. By the statement displayed in "Step 1", the $\prod_{j=1}^n (e^{u_j})^{k_j^{(i)}} = e^{\underline{k}^{(i)} \cdot \underline{u}}$ are LI/$\bar{\mathbb{Q}}$. So no nontrivial $\bar{\mathbb{Q}}$-linear combination of *monomials* in the e^{u_j}'s can be zero; that is, the $\{e^{u_j}\}$ are algebraically independent.

Step 2: *It suffices to show that* $\alpha_1, \ldots, \alpha_n \in \bar{\mathbb{Q}}$ *distinct* $\implies$ $e^{\alpha_1}, \ldots, e^{\alpha_n}$ *are linearly independent over* $\mathbb{Q}$*.*

Given a $\bar{\mathbb{Q}}$-linear dependency $0 = \sum a_i e^{\alpha_i}$ (with $a_i \in \bar{\mathbb{Q}}^*$), we take $L/\mathbb{Q}$ a SFE for the product $\prod m_{a_i}$ of minimal polynomials. Write[55]

$$\prod_{\sigma \in \mathrm{Aut}(L/\mathbb{Q})} \Big(\sum_i \sigma(a_i) e^{\alpha_i}\Big) = \sum_\ell b_\ell e^{\beta_\ell}, \tag{I.N.20}$$

where the β_ℓ are distinct, and show the b_ℓ are rational numbers that are not all zero. By assumption, the $\sigma = \mathbf{1}$ factor of LHS(I.N.20) is zero, and so $0 = \sum_\ell b_\ell e^{\beta_\ell}$. This $\mathbb{Q}$-linear dependency contradicts the statement displayed in "Step 2".

To see that the b_ℓ belong to $\mathbb{Q}$, first regard the e^{α_i}'s as indeterminates x_i. Since the product polynomial $\prod_{\sigma \in \mathrm{Aut}(L/\mathbb{Q})} (\sum_i \sigma(a_i) x_i)$ is $\mathrm{Aut}(L/\mathbb{Q})$-invariant, its coefficients lie in $\mathbb{Q}$. Substituting e^{α_i}'s (as in LHS(I.N.20)) and collecting coefficients with equal exponents (different sums of α_i's may be equal) doesn't change this. But how do we know that this last step doesn't make all b_ℓ's zero?

[55]At this stage, we do *not* collect together e^β with $e^{\beta'}$ if $e^\beta = e^{\beta'}$ but $\beta \neq \beta'$. The same goes for the RHS of (I.N.21) below.

To see that this doesn't happen, introduce a fake "order" on $\mathbb{C}$: $A < B$ means $\mathrm{Re}(A) < \mathrm{Re}(B)$ or $\mathrm{Re}(A) = \mathrm{Re}(B)$ and $\mathrm{Im}(A) < \mathrm{Im}(B)$. It is at least respected by addition, and since the α_i are distinct, one of them (say α_1) is the highest in this "order". The term $(\prod_\sigma \sigma(a_1))e^{|\mathrm{Aut}(L/\mathbb{Q})|\alpha_1}$ in the expansion of LHS(I.N.20) therefore does not get "combined" with any other terms, so its (obviously nonzero) coefficient is one of the b_ℓ's.

Step 3: *It suffices to show that $m_{\gamma_1}, \ldots, m_{\gamma_n} \in \mathbb{Q}[x]$ distinct $\implies$ $\sum_{\gamma\in\mathcal{R}_1} e^\gamma, \ldots, \sum_{\gamma\in\mathcal{R}_n} e^\gamma$ are linearly independent over $\mathbb{Q}$.* [Here $\mathcal{R}_i := \mathcal{R}_{m_{\gamma_i}}$ are the roots of each minimal polynomial, which is to say the Galois conjugates of each γ_i; we shall write $\mathcal{R}_i = \{\gamma_{i1}, \ldots, \gamma_{id_i}\}$, where $\gamma_{i1} = \gamma_i$, and $d = \sum_i d_i = \deg(\prod_i m_{\gamma_i})$.]

Suppose we have a relation $\sum_{i=1}^n b_i e^{\alpha_i} = 0$, with $b_i \in \mathbb{Q}^*$. We may assume that all $b_i \in \mathbb{Z} \setminus \{0\}$ by multiplying the relation by an integer. We need, once more, to reach a contradiction.

Denote the Galois conjugates of each α_i ($=: \alpha_{i1}$) by $\{\alpha_{ij}\}_{j=1}^{d_i}$, and let $\mathfrak{S}_d$ ($d = \sum d_i$) act on the 2-tuples ij. Note that the polynomial

$$P(x_{11}, \ldots, x_{nd_n}) := \prod_{\tau\in\mathfrak{S}_d} \left(\sum_{i=1}^n b_i x_{\tau(i1)} \right)$$

vanishes on $(e^{\alpha_{11}}, \ldots, e^{\alpha_{nd_n}})$ since the $\tau = \mathbf{1}$ factor is 0 by assumption. Moreover, since the product is symmetric, the coefficients of (say) $\prod_{i,j} x_{ij}^{h_{ij}}$ and $\prod_{i,j} x_{\eta(ij)}^{h_{ij}}$ (for any given $\eta \in \mathfrak{S}_d$) are the same. So expanding

(I.N.21)
$$0 = P(e^{\alpha_{11}}, \ldots, e^{\alpha_{nd_n}}) = \textstyle\prod_{\tau\in\mathfrak{S}_d} \left(\sum_{i=1}^n b_i e^{\alpha_{\tau(i1)}}\right) = \sum_{\underline{h}} c_{\underline{h}} e^{\sum_{i,j} h_{ij}\alpha_{ij}},$$

the coefficient of $e^{\sum_{i,j} h_{ij}\alpha_{ij}}$ is the same as that of each $e^{\sum_{i,j} h_{ij}\alpha_{\eta(ij)}}$ for η in $\mathfrak{S}_d$ *a fortiori* $G := \mathfrak{S}_{d_1} \times \cdots \times \mathfrak{S}_{d_n}$.

This means that, taking a system of representatives $\{\gamma_I\}_{I=1}^N$ of the G-orbits in the $\sum_{i,j} h_{ij}\alpha_{ij}$'s appearing on RHS(I.N.21), the latter takes the form

$$0 = \textstyle\sum_I C_I \left(\sum_{\gamma\in\mathcal{R}'_I} e^\gamma\right) \tag{I.N.22}$$

where now the $\mathcal{R}'_I$ denote roots of m_{γ_I}. Here we collect terms with equal exponents as in (I.N.20). Again, some C_I is nonzero because in each factor of the product in (I.N.21) we can pick the term with "highest" $\alpha_{\tau(ij)}$ in the "order" on $\mathbb{C}$ described before. The linear dependency (I.N.22) thus contradicts the statement in Step 3.

Step 4: *Verify the statement in Step 3.*

Let a linear dependency

$$0 = \textstyle\sum_{i,j} \beta_i e^{\gamma_{ij}} \tag{I.N.23}$$

be given, with $\beta_i \in \mathbb{Z} \setminus \{0\}$. Pick $N \in \mathbb{N}$ such that $N\gamma_{ij} \in \bar{\mathbb{Z}}$, and a prime p greater than N and the β_i. Define polynomials

$$f_{ij}(z) := N^{dp}(z - \gamma_{ij})^{-1} \textstyle\prod_{i',j'} (z - \gamma_{i'j'})^p,$$

and note that the $f_{ij}^{(m)}(\gamma_{k\ell}) \in \bar{\mathbb{Z}}$ are divisible by $p!$ for $m \geq p$, and otherwise vanish unless $m = p-1$ and $(i,j) = (k,\ell)$, in which case they are divisible by $(p-1)!$.

Next recall from (I.N.17) that

$$\begin{aligned} I_{ij}(s) := I_{f_{ij}}(s) &:= \int_0^s e^{s-z} f_{ij}(z) dz \\ &= e^s \sum_{m=0}^{dp-1} f_{ij}^{(m)}(0) - \sum_{m=0}^{dp-1} f_{ij}^{(m)}(s). \end{aligned}$$

The integral definition gives that $|I_{ij}(\gamma_{k\ell})| \leq |\gamma_{k\ell}| e^{|\gamma_{k\ell}|} |f_{ij}|(|\gamma_{k\ell}|) \leq C_{ijk\ell}^p$ for some constants independent of p. Defining

$$J_{ij} := \sum_{k,\ell} \beta_k I_{ij}(\gamma_{k\ell}) \quad \text{and} \quad J := \textstyle\prod_{i,j} J_{ij},$$

this means that $|J| \leq C^p$ for some constant $C \in \mathbb{N}$ independent of p. On the other hand, the sum formula yields

$$\begin{aligned}
J_{ij} &= \sum_{k,\ell} \beta_k \left(e^{\gamma_{k\ell}} \sum_{m=0}^{dp-1} f_{ij}^{(m)}(0) - \sum_{m=0}^{dp-1} f_{ij}^{(m)}(\gamma_{k\ell}) \right) \\
&= \left(\sum_{m=0}^{dp-1} f_{ij}^{(m)}(0) \right) \cancelto{0}{\left(\sum_{k,\ell} \beta_k e^{\gamma_{k\ell}} \right)} - \sum_{k,\ell} \sum_{m=0}^{dp-1} \beta_k f_{ij}^{(m)}(\gamma_{k\ell}) \\
&= - \sum_{k,\ell} \sum_{m=0}^{dp-1} \beta_k f_{ij}^{(m)}(\gamma_{k\ell}) \ \in \ \bar{\mathbb{Z}},
\end{aligned}$$

where we used (I.N.23). Since $p!$ divides all but one term of this sum, which is divisible only by $(p-1)!$, we get that $(p-1)! \mid J_{ij}$ and $J_{ij} \neq 0$.

Finally, we notice that $\prod_{i',j'}(Nz - N\gamma_{i'j'})^p$ is a polynomial with $\mathbb{Z}$-coefficients, since it belongs *a priori* to $\bar{\mathbb{Z}}[z]$ and is Galois-invariant. Since f is obtained by dividing this by $(z - \gamma_{ij})$, it is an easy exercise (left to you) to show that we may write $f_{ij}^{(m)}(z) = \sum_r g_{rm}(\gamma_{ij}) z^r$ for some polynomials $g_{rm} \in \mathbb{Z}[z]$ independent of i, j. But then

$$\begin{aligned}
\sum_{\ell=1}^{d_k} f_{ij}^{(m)}(\gamma_{k\ell}) &= \sum_{\ell=1}^{d_k} \sum_r g_{rm}(\gamma_{ij}) \gamma_{k\ell}^r = \sum_r \left(\sum_{\ell=1}^{d_k} \gamma_{k\ell}^r \right) g_{rm}(\gamma_{ij}) \\
&= \sum_r M_{rk} g_{rm}(\gamma_{ij})
\end{aligned}$$

with $M_{rk} \in \mathbb{Q}$; and so

$$J_{ij} = - \sum_m \sum_{k=1}^{n} \beta_k M_{rk} g_{rm}(\gamma_{ij}) =: G(\gamma_{ij})$$

takes the form of some fixed $G \in \mathbb{Q}[z]$ (independent of i, j) evaluated at γ_{ij}. So the product $J = \prod_{i,j} G(\gamma_{ij})$ is Galois-invariant and must belong to $\mathbb{Q}$. But it also belongs to $\bar{\mathbb{Z}}$ (because the J_{ij} do), and so in fact $J \in \mathbb{Z}$. Moreover, since $(p-1)! \mid J_{ij}$, we have $(p-1)!)^d \mid J$; hence $|J| \geq ((p-1)!)^d$. We reach a contradiction now since $((p-1)!)^d \leq C^p$ cannot hold for all $p \gg 0$. $\square$

Another transcendence result is the *Gel'fand-Schneider Theorem*, which states that if $\alpha \in \bar{\mathbb{Q}} \setminus \{0, 1\}$ and $\beta \in \bar{\mathbb{Q}} \setminus \mathbb{Q}$, then $\alpha^\beta \notin \bar{\mathbb{Q}}$. This is generalized by *Baker's theorem*, which states that if $e^{\alpha_1}, \ldots, e^{\alpha_n} \in \bar{\mathbb{Q}}$ and $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$, then $1, \alpha_1, \ldots, \alpha_n$ are linearly independent over $\bar{\mathbb{Q}}$. An extremely important conjecture in algebraic and arithmetic geometry is Grothendieck's *transcendence conjecture*, which is about transcendence of *periods* (integrals of algebraic differential forms on real semialgebraic sets) and is largely open; for instance, it is expected that $\zeta(3) = \sum_{m>0} \frac{1}{m^3}$ is transcendental, but it is only known that it is irrational. For (say) $\zeta(5)$, we don't even know irrationality.