THE EXPONENTIAL WORLD

Garth Warner

Professor of Mathematics (Emeritus)

University of Washington

ABSTRACT

In this book there will be found an introduction to transcendental number theory, starting at the beginning and ending at the frontiers. The emphasis is on the conceptual aspects of the subject, thus the effective theory has been more or less completely ignored, as has been the theory of E-functions and G-functions. Still, a fair amount of ground is covered and while I take certain results without proof, this is done primarily so as not to get bogged down in technicalities, otherwise the exposition is detailed and little is left to the reader.

ACKNOWLEDGEMENT

My thanks to Judith Clare for a superb job of difficult technical typing.

CONTENTS

SUPPLEMENT

TRANSCENDENCE OF SERIES

SUPPLEMENT

ZETA FUNCTION VALUES

§1. BERNOULLI NUMBERS

§2. $\zeta(2n)$

§3. $\zeta(2)$

§4. $\zeta(2)$ (bis)

§5. $\zeta(2n)$ (bis)

§6. $\zeta(3)$

§7. CONJUGATE BERNOULLI NUMBERS

§8. $\zeta(2n + 1)$

REFERENCES

1. E. Burger and R. Tubbs, Making Transcendence Transparent, Springer-Verlag, 2004.

2. N. I. Fel'dman and Yu. V. Nesterenko, Transcendental Numbers, Springer-Verlag, 1998.

3. David Masser, Auxiliary Polynomials in Number Theory, Cambridge University Press, 2016.

4. M. Ram Murty and Purusottam Rath, Transcendental Numbers, Springer-Verlag, 2014.

5. Yu. V. Nesterenko, Algebraic Independence, Narosa Publishing House, 2009.

6. Michel Waldschmidt, Nombres Transcendants, Springer-Verlag, 1974.

7. Michel Waldschmidt, Diophantine Approximation on Linear Algebraic Groups, Springer-Verlag, 2000.

CORRECTION #1.

<u>Re: §15, #30</u>: It has been pointed out to me by Michel Waldschmidt that the proof of this result has a mistake in that Step 2 as formulated does not lead to Step 3. The situation is rectified in the lines below via a modification of Step 2, which is then shown to lead to Step 3.

<u>Step 2</u>: Introduce

$$\alpha = \sum_{j=1}^{\infty} \alpha_j \, 2^{-j}, \quad \beta = \sum_{j=1}^{\infty} \beta_j \, 2^{-j},$$

where for $k! \leq j < (k+1)!$,

$$\begin{cases} \alpha_j = m_j \text{ and } \beta_j = 0 & (k = 1,3,5,\ldots) \\ \alpha_j = 0 \text{ and } \beta_j = m_j & (k = 2,4,6,\ldots). \end{cases}$$

Then

$$x = \alpha + \beta.$$

<u>Step 3</u>: Assume that the series defining α is infinite -- then in this case, α is a Liouville number.

[Break up the series

$$\sum_{j=1}^{\infty} \alpha_j \, 2^{-j}$$

as follows:

$$\sum_{1! \leq k < 2!} \alpha_j \, 2^{-j} + \sum_{2! \leq k < 3!} \alpha_j \, 2^{-j} + \sum_{3! \leq k < 4!} \alpha_j \, 2^{-j} + \sum_{4! \leq k < 5!} \alpha_j \, 2^{-j} + \sum_{5! \leq k < 6!} \alpha^j \, 2^{-j} + \cdots$$

$$= \sum_{1! \leq k < 2!} \alpha_j \, 2^{-j} + \sum_{3! \leq k < 4!} \alpha_j \, 2^{-j} + \sum_{5! \leq k < 6!} \alpha_j \, 2^{-j} + \cdots .$$

Consider

$$0 < \alpha - \sum_{j=1}^{(2k)!-1} \alpha_j 2^{-j}$$

$$= \sum_{j \geq (2k)!} \alpha_j 2^{-j}$$

$$= \sum_{(2k)! \leq j < (2k+1)!} \alpha_j 2^{-j} + \sum_{(2k+1)! \leq j < (2k+2)!} \alpha_j 2^{-j} + \sum_{(2k+2)! \leq j < (2k+3)!} \alpha_j 2^{-j} + \cdots$$

$$= 0 + \sum_{(2k+1)! \leq j < (2k+2)!} \alpha_j 2^{-j} + 0 + \cdots$$

$$\leq \sum_{j=(2k+1)!}^{\infty} 2^{-j}$$

$$= \frac{1}{2^{(2k+1)!}} \sum_{j=0}^{\infty} \frac{1}{2^j}$$

$$= \frac{2}{2^{(2k+1)!}}$$

$$= 2^{1-(2k+1)!} .$$

The remainder of the argument goes through without change.]

§0. *THE CANONICAL ESTIMATE*

THEOREM Given a positive constant C,

$$\lim_{n \to \infty} \frac{C^n}{n!} = 0.$$

PROOF Write

$$n! = n^n e^{-n} \sqrt{n}\, \gamma_n \quad \text{(Stirling's formula)}.$$

Here

$$\frac{e}{\sqrt{2}} \leq \gamma_n \leq e \quad (\Rightarrow \frac{\sqrt{2}}{e} \geq \frac{1}{\gamma_n} \geq \frac{1}{e}).$$

Choose $n >> 0 : eC < n$ -- then

$$0 < \frac{C^n}{n!} = \frac{C^n}{n^n e^{-n} \sqrt{n}\, \gamma_n}$$

$$= \frac{(eC)^n}{n^n} \frac{1}{\sqrt{n}\, \gamma_n}$$

$$\leq \left(\frac{eC}{n}\right)^n \frac{\sqrt{2}}{e} \frac{1}{\sqrt{n}}$$

$$< \frac{\sqrt{2}}{e} \frac{1}{\sqrt{n}} \to 0 \quad (n \to \infty).$$

§1. *ORDERED SETS*

Let X be a nonempty set.

<u>1:</u> DEFINITION An <u>order</u> on X is a relation $<$ with the following properties.

- <u>Trichotomy</u> Given $x,y \in X$, then one and only one of the statements

$$x < y, \ x = y, \ y < x$$

is true.

- <u>Transitivity</u> Given $x,y,z \in X$, if $x < y$ and $y < z$, then $x < z$.

<u>2:</u> <u>N.B.</u>

- $y > x$ means $x < y$.
- $x \leq y$ means $x < y$ or $x = y$.

3: DEFINITION An <u>ordered set</u> is a pair $(X,<)$, where X is a nonempty set equipped with an order $<$.

<u>4:</u> EXAMPLE Take $X = \mathbb{Q}$ -- then X is an ordered set if $p < q$ is defined to mean that $q - p$ is positive.

Let X be an ordered set, $S \subset X$ a nonempty subset.

<u>5:</u> NOTATION

$$U(S) = \{x \in X : \forall \ s \in S, \ s \leq x\}.$$

<u>6:</u> DEFINITION S is <u>bounded above</u> if $U(S) \neq \emptyset$, an element of $U(S)$ being called an <u>upper bound</u> of S.

<u>7:</u> <u>N.B.</u> The terms "bounded below" and "lower bound" are to be assigned the obvious interpretations, where now

$$L(S) = \{x \in X: \forall s \in S, x \leq s\}.$$

Let X be an ordered set, $S \subset X$ a nonempty subset such that $U(S) \neq \emptyset$.

<u>8:</u> DEFINITION An element $x \in U(S)$ is a <u>least upper bound</u> of S if $y < x \Rightarrow y \notin U(S)$.

<u>9:</u> LEMMA Least upper bounds are unique (if they exist at all) and one writes

$$x = \text{lub } S \text{ or } x = \sup S \text{ ("supremum").}$$

[Note: The definition of "greatest lower bound" is analogous, such an element being denoted by

$$x = \text{glb } S \text{ or } x = \inf S \text{ ("infimum").]}$$

<u>10:</u> EXAMPLE Take $X = Q$ and let $S = \{\frac{1}{n}: n \in N\}$ -- then $\sup S = 1$ is in S but $\inf S = 0$ is not in S.

Let X be an ordered set.

<u>11:</u> DEFINITION X has the <u>least upper bound</u> property if each nonempty subset $S \subset X$ which is bounded above has a least upper bound.

<u>12:</u> EXAMPLE Take $X = N$ -- then X has the least upper bound property.

<u>13:</u> EXAMPLE Take $X = Q$ -- then X does not have the least upper bound property.

[Assign to each rational $p > 0$ the rational

$$q = p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}$$

and note that

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2} .$$

Introduce

$$\left[\begin{array}{l} A = \{p \in Q : p > 0 \ \& \ p^2 < 2\} \\ \\ B = \{p \in Q : p > 0 \ \& \ p^2 > 2\}. \end{array}\right.$$

Then

$$\left[\begin{array}{l} p \in A \Rightarrow p < q \ \& \ q \in A \\ \\ p \in B \Rightarrow q < p \ \& \ q \in B. \end{array}\right.$$

Therefore

$$\left[\begin{array}{l} \text{A has no largest element} \\ \text{B has no smallest element.} \end{array}\right.$$

But

$$\left[\begin{array}{l} U(A) = B \\ L(B) = A. \end{array}\right.$$

So A does not have a least upper bound and B does not have a greatest lower bound.]

Let X be an ordered set.

14: LEMMA Suppose that X has the least upper bound property. Let $S \subset X$

be nonempty and bounded below — then

$$\sup L(S) = \inf S.$$

PROOF By hypothesis, $L(S) \neq \emptyset$ and

$$s \in S \Rightarrow s \in U(L(S)) \Rightarrow U(L(S)) \neq \emptyset.$$

Therefore sup $L(S)$ exists, call it λ. Given $s \in S$, there are three possibilities:

$$s < \lambda, \ s = \lambda, \ \lambda < s.$$

However $s < \lambda$ is untenable since it implies that

$$s \notin U(L(S)) \Rightarrow s \notin S.$$

Accordingly

$$s \in S \Rightarrow \lambda \leq s \Rightarrow \lambda \in L(S).$$

If now $\lambda < \lambda'$, then $\lambda' \notin L(S)$ (for otherwise $\lambda' \in L(S) \Rightarrow \lambda' \leq \lambda$ by the very definition of λ ...), thus $\lambda = \inf S$.

15: DEFINITION An ordered field is an ordered set X which is also a field subject to the following conditions.

- If $y < z$, then $\forall\, x$, $x + y < x + z$.
- If $x > 0$ & $y > 0$, then $xy > 0$.

16: EXAMPLE Take $X = Q$ — then X is an ordered field.

§2. *REAL NUMBERS*

The following result is the central theorem of existence.

1: THEOREM There exists an ordered field R with the least upper bound property which contains Q as an ordered subfield.

[Note: Here there is an abuse of the language in that "Q" is not necessarily the rationals but rather an isomorphic replica thereof.]

2: DEFINITION The elements of R are called real numbers.

3: N.B. Suppose that R_1 and R_2 are two realizations of R -- then there exists a unique order preserving field isomorphism $\phi:R_1 \to R_2$ such that $\phi(Q_1) = Q_2$.

4: REMARK There are three standard realizations of R.

- The set of infinite decimal expansions.
- The set of equivalence classes of Cauchy sequences of rational numbers.
- The set of Dedekind cuts.

[Note: The fact that these models are actually ordered fields with the least upper bound property is not obvious, the actual verification involving a fair amount of tedious detail.]

5: REMARK If S is a nonempty subset of R which is bounded below, then S has a greatest lower bound (cf. §1, #14).

[In fact,

$$\text{glb } S = - \text{ lub } - S.]$$

6: LEMMA Let S be a nonempty subset of R which is bounded above -- then for each $\varepsilon > 0$, there is an element $s \in S$ such that $s > \sup S - \varepsilon$.

PROOF If the assertion were false, then for some $\varepsilon > 0$ and all $s \in S$,

$$\sup S - \varepsilon \geq s.$$

Accordingly, by definition of supremum,

$$\sup S - \varepsilon \geq \sup S,$$

so $\varepsilon \leq 0$, a contradiction.

7: LEMMA Let S be a nonempty subset of R which is bounded above. Suppose that μ is an upper bound for S with the property that for each $\varepsilon > 0$, there exists an element $s \in S$ such that $\mu - \varepsilon < s$ -- then $\mu = \sup S$.

PROOF If instead $\mu \neq \sup S$, then $\mu > \sup S$, hence $\mu - \sup S > 0$, thus for some $s \in S$,

$$\mu - (\mu - \sup S) = \sup S < s,$$

a contradiction.

8: ARCHIMEDEAN PROPERTY For every positive real x and for every real y, there exists a natural number n such that $nx > y$.

PROOF Suppose to the contrary that there exist real numbers $x > 0$ and y such that $nx \leq y$ for every natural number n. Let $S = \{nx:n \in N\}$ -- then S is bounded above (by y), hence has a supremum μ, say. Because $\mu - x < \mu$ (x is positive), there must be a natural number n with the property that $nx > \mu - x$ (cf. #6), so $(n + 1)x > \mu$. But $(n + 1)x$ belongs to S, thus the inequality $(n + 1)x > \mu$ contradicts the assumption that μ is, in particular, an upper bound for S.

9: COROLLARY For every real number x, there exists a natural number n such that $n > x$.

10: COROLLARY For every real number x, there exists an integer m such that $x > m$.

[Choose a natural number n such that $n > -x$ (cf. #9) -- then $x > -n$, so we can take $m = -n$.]

11: COROLLARY For every positive real number x, there exists a natural number n such that $x > \frac{1}{n}$.

12: EXAMPLE Let $S = \{\frac{n}{n+1}: n \in N\}$ -- then $1 \in U(S)$ and we claim that $1 = \sup S$. Thus let $\mu = \sup S$ and suppose to the contrary that $\mu < 1$. Using #11, choose a natural number $n > 1$ such that $\frac{1}{n} < 1 - \mu$, hence

$$\mu < 1 - \frac{1}{n} = \frac{n-1}{n},$$

which implies that μ is less than an element of S.

13: LEMMA For every real number x, there exists an integer m such that $x - 1 \leq m < x$.

PROOF Owing to #9 and #10, there exist integers a and b such that $a < x < b$. Let m be the largest integer in the finite collection $a, a + 1, \ldots, b$ such that $m < x$ -- then $m + 1 \geq x$, hence $m \geq x - 1$.

14: DEFINITION A nonempty subset S of R is said to be dense in R if it has the following property: Between any two distinct real numbers there is an element of S.

15: THEOREM Q is dense in R.

PROOF Fix $x,y \in R: x < y$ -- then $y - x > 0$, so there exists a natural number n such that $y - x > \frac{1}{n}$ (cf. #11), i.e., such that $x < y - \frac{1}{n}$. On the other hand, there exists an integer m with the property that

$$ny - 1 \leq m < ny \quad \text{(cf. \#13)},$$

hence

$$y - \frac{1}{n} \leq \frac{m}{n} < y$$

from which

$$x < y - \frac{1}{n} \leq \frac{m}{n} < y.$$

16: SCHOLIUM If x and y are real numbers with $x < y$, then there exists an infinite set of rationals q such that $x < q < y$.

The Archimedean Property is essentially "additive" in character; here is its "multiplicative" analog.

17: LEMMA If $x > 1$ and y are real numbers, then there exists a natural number n such that $x^n > y$.

PROOF Proceeding by contradiction, suppose that there exist real numbers $x > 1$ and y such that $x^n \leq y$ for every natural number n. Let $S = \{x^n : n \in N\}$ -- then S is bounded above (by y), hence has a supremum μ, say. Because $x > 1$, μ is less than μx, hence $\mu/x < \mu$, so there must exist an $n \in N$ such that $\mu/x < x^n$. But then $\mu < x^{n+1}$ and, as $x^{n+1} \in S$, we have arrived at a contradiction.

18: EXAMPLE Let $x > 0$ and $0 < r < 1$ be real numbers; let

$$S = \{\frac{x(1 - r^n)}{1 - r} : n \in N\}.$$

Then, in view of the relation

$$\frac{x(1 - r^n)}{1 - r} = \frac{x}{1 - r} - \frac{xr^n}{1 - r} < \frac{x}{1 - r} \quad (n \in N),$$

it is clear that $\frac{x}{1 - r}$ is an upper bound for S and we claim that

$$\frac{x}{1 - r} = \sup S.$$

To prove this, it suffices to show that if ε is any real number such that $0 < \varepsilon < \frac{x}{1 - r}$, then $\varepsilon \notin U(S)$ (cf. §1, #8). So fix such an ε -- then there exists a natural number n such that

$$\frac{1}{r^n} > \frac{x}{x - \varepsilon(1 - r)} \quad \text{(cf. \#17)} \quad (0 < r < 1 \Rightarrow \frac{1}{r} > 1),$$

thus

$$r^n < \frac{x - \varepsilon(1 - r)}{x} = 1 - \varepsilon(\frac{1 - r}{x})$$

or still,

$$\varepsilon < \frac{x(1 - r^n)}{1 - r} \Rightarrow \varepsilon \notin U(S).$$

<u>19:</u> DEFINITION A real number x is <u>irrational</u> if it is not rational.

<u>20:</u> NOTATION P is the subset of R whose elements are the irrational numbers.

<u>21:</u> <u>N.B.</u> Therefore $R = P \cup Q$, where $P \cap Q = \emptyset$.

<u>22:</u> LEMMA Irrational numbers exist.

[In fact, R is not countable, hence P is neither finite nor countable (Q being countable), hence $P \neq \emptyset$.]

23: THEOREM P is dense in R.

PROOF Fix a positive irrational p and fix $x,y \in R: x < y$. Using #15, choose a nonzero rational q such that

$$\frac{x}{p} < q < \frac{y}{p}.$$

Then

$$x < pq < y$$

and $pq \in P$.

24: N.B. For the record, if $p \in P$, then $-p \in P$ and $\frac{1}{p} \in P$. In addition, if $q \in Q$ $(q \neq 0)$, then

$$p + q,\ p - q,\ pq,\ \frac{p}{q}$$

are irrational.

25: DEFINITION An element $x \in R$ is algebraic or transcendental according to whether it is or is not a root of a nonzero polynomial in $Z[X]$.

26: EXAMPLE If $\frac{a}{b}$ $(b \neq 0)$ is rational, then $\frac{a}{b}$ is algebraic.

[Consider the polynomial $bX - a$.]

27: EXAMPLE Let $r,s \in Q$, $r > 0$ -- then r^s is algebraic.

[Write $s = \frac{m}{n}$ $(m,n \in Z,\ n > 0)$ and consider the polynomial $X^n - r^m$.]

[Note: Take $r = 2$, $s = \frac{1}{2}$, hence $n = 2$ and $2^{\frac{1}{2}} = \sqrt{2}$ is algebraic (but irrational (cf. §6, #2)).]

28: N.B. It will be shown in due course that e and π are transcendental. However the status of $e + \pi$, $e - \pi$, $e\pi$, e^e, and π^π is unknown.

[Note: e^π is transcendental but whether this is true of π^e remains an open question.]

29: EXAMPLE Is $e + \pi$ irrational? Is $e\pi$ irrational? Answer: Nobody knows. But at least one of them must be irrational. To see this, consider the polynomial

$$X^2 - (e + \pi)X + e\pi.$$

Its zeros are e and π. So if both $e + \pi$ and $e\pi$ were rational, then e and π would be algebraic which they are not.

30: NOTATION $\bar{Q}$ is the subset of R whose elements are the algebraic numbers and T is the subset of R whose elements are the transcendental numbers.

31: N.B. Q is a subset of $\bar{Q}$ and T is a subset of P.

32: LEMMA The cardinality of $\bar{Q}$ is aleph-0.

33: N.B. Consequently, on purely abstract grounds, transcendental numbers exist. Historically, the first explicit transcendental was constructed by Liouville, viz.

$$\sum_{n=1}^{\infty} 10^{-n!} \quad \text{(cf. §15, #9)}.$$

34: LEMMA $\bar{Q}$ is the algebraic closure of Q in R and

$$[\bar{Q}:Q] = \text{aleph-0}.$$

Being a field, $\bar{Q}$ is closed under addition and multiplication.

35: LEMMA If $x \neq 0$ is algebraic and y is transcendental, then $x + y$ and xy are transcendental.

36: EXAMPLE $\sqrt{2}\, e$ and $\sqrt{2} + \pi$ are transcendental.

37: LEMMA If $x \in R$ is transcendental, then so is x^2.

[If x^2 were algebraic, then there would be a relation of the form

$$a_0 + a_2x^2 + a_4x^4 + \cdots + a_{2n}x^{2n} = 0 \quad (a_{2k} \in Q)$$

or still,

$$a_0 + 0x + a_2x^2 + 0x^3 + a_4x^4 + \cdots + a_{2n}x^{2n} = 0$$

implying thereby that x is algebraic.]

38: EXAMPLE Not both $e\pi$ and $\frac{\pi}{e}$ can be algebraic.

[In fact,

$$(e\pi)\left(\frac{\pi}{e}\right) = \pi^2.]$$

39: N.B. T is not closed under addition and multiplication.

40: CRITERION Let x and y be real numbers. Suppose that $x \leq y + \varepsilon$ for every $\varepsilon > 0$ -- then $x \leq y$.

PROOF Assume that $x > y$ and put $\varepsilon = \frac{1}{2}(x - y)$ -- then $\varepsilon > 0$. However

$$y + \varepsilon = \frac{1}{2}(x + y) < \frac{1}{2}(x + x) = x,$$

contrary to the supposition that $y + \varepsilon \geq x$ for every $\varepsilon > 0$.

§3. *SUPREMA*

We shall record here some technicalities that will be of use in the sequel.

1: LEMMA Let S be a nonempty subset of R, T a nonempty subset of S. Suppose that S is bounded above -- then T is also bounded above and $\sup T \leq \sup S$.

[This is obvious from the definitions.]

2: LEMMA Let S and T be two nonempty subsets of R, each being bounded above. Suppose further that given any $s \in S$ there is a $t \in T$ such that $s \leq t$ and that given any $t \in T$ there is a $s \in S$ such that $t \leq s$ -- then $\sup S = \sup T$.

PROOF It suffices to rule out the other possibilities:

$$\left[\begin{array}{l} \sup S < \sup T \\ \sup T < \sup S. \end{array}\right.$$

If the first of these were true, then $\sup S \notin U(T)$, so there exists a $t \in T$ such that $\sup S < t \leq \sup T$. But, by hypothesis, there is a $s \in S$ such that $t \leq s$, hence $\sup S < s$, a contradiction. The second of these can be eliminated in the same way.

3: NOTATION Given nonempty subsets S, T of R, put

$$S + T = \{s + t : s \in S, t \in T\}.$$

4: LEMMA Let S and T be nonempty subsets of R, each being bounded above -- then $S + T$ is bounded above and

$$\sup(S + T) = \sup S + \sup T.$$

PROOF Let $r \in S + T$ -- then there exist $s \in S$, $t \in T$ such that $r = s + t$ and so $r \leq \sup S + \sup T$. Since r is an arbitrary element of $S + T$, it follows that $\sup S + \sup T$ is an upper bound for $S + T$, hence $\sup(S + T)$ exists and in fact

$$\sup(S + T) \leq \sup S + \sup T.$$

To reverse this, we shall employ §2, #40 and prove that

$$\sup S + \sup T \leq \sup(S + T) + \varepsilon$$

for every $\varepsilon > 0$. Thus fix $\varepsilon > 0$ and choose $s \in S$, $t \in T$ such that

$$s > \sup S - \frac{\varepsilon}{2}, \ t > \sup T - \frac{\varepsilon}{2} \quad \text{(cf. §2, #6)}.$$

Then

$$s + t > \sup S + \sup T - \varepsilon$$

or still,

$$\begin{aligned} \sup S + \sup T &< s + t + \varepsilon \\ &\leq \sup(S + T) + \varepsilon. \end{aligned}$$

<u>5:</u> NOTATION Given nonempty subsets S, T of R, put

$$S \cdot T = \{st : s \in S, \ t \in T\}.$$

<u>6:</u> LEMMA Let S and T be nonempty subsets of $R_{>0}$, each being bounded above -- then $S \cdot T$ is bounded above and

$$\sup(S \cdot T) = (\sup S) \cdot (\sup T).$$

PROOF Note first that

$$\sup S > 0 \text{ and } \sup T > 0.$$

This said, let $r \in S \cdot T$ -- then there exist $s \in S$, $t \in T$ such that $r = st$ and so $r \leq (\sup S) \cdot (\sup T)$. Since r is an arbitrary element of $S \cdot T$, it follows that $(\sup S) \cdot (\sup T)$ is an upper bound for $S \cdot T$, hence $\sup(S \cdot T)$ exists and in fact

$$\sup(S \cdot T) \leq (\sup S) \cdot (\sup T).$$

To reverse this, we shall employ §2, #40 and prove that

$$(\sup S)\cdot(\sup T) \leq \sup(S\cdot T) + \varepsilon$$

for every $\varepsilon > 0$. Thus fix $\varepsilon > 0$ and choose $s \in S$, $t \in T$ such that

$$s > \sup S - \frac{\varepsilon}{\sup S + \sup T}, \quad t > \sup T - \frac{\varepsilon}{\sup S + \sup T} \quad (\text{cf. §2, \#6}).$$

Then

$$\sup S - s < \frac{\varepsilon}{\sup S + \sup T}, \quad \sup T - t < \frac{\varepsilon}{\sup S + \sup T},$$

from which

$$t(\sup S - s) \leq \frac{\varepsilon\cdot\sup T}{\sup S + \sup T}$$

and

$$\sup S(\sup T - t) < \frac{\varepsilon\cdot\sup S}{\sup S + \sup T}.$$

Therefore

$$\begin{aligned}
&(\sup S)\cdot(\sup T) - st \\
&\qquad = \sup S(\sup T - t) + t(\sup S - s) \\
&\qquad < \frac{\varepsilon\cdot\sup S}{\sup S + \sup T} + \frac{\varepsilon\cdot\sup T}{\sup S + \sup T} \\
&\qquad = \varepsilon,
\end{aligned}$$

i.e.,

$$\begin{aligned}
(\sup S)\cdot(\sup T) &\leq st + \varepsilon \\
&\leq \sup(S\cdot T) + \varepsilon.
\end{aligned}$$

<u>7:</u> REMARK The assertion of #6 may be false if we drop the assumption

that S and T are nonempty subsets of $R_{>0}$.

[Take, e.g., $S = - N$, $T = - N$ -- then both S and T are bounded above but $S \cdot T$ is not.]

§4. *EXPONENTS AND ROOTS*

Let $a > 0$ and x be real numbers -- then the primary objective of the present § is to assign a meaning to the symbol a^x.

If a is any real number and if n is a natural number, then the power a^n is defined inductively by the rule

$$a^1 = a, \quad a^{n+1} = a^n \cdot a.$$

When $a \neq 0$, we define a^0 as 1; we do not define 0^0. When $a \neq 0$, we define a^{-n} as $\frac{1}{a^n}$; we do not define 0^{-n}.

1: LAWS OF EXPONENTS FOR INTEGRAL POWERS Let a and b be nonzero real numbers; let m and n be integers.

(1) $a^m \cdot a^n = a^{m+n}$; (2) $(a^m)^n = a^{mn}$; (3) $\frac{a^m}{a^n} = a^{m-n}$;

(4) $(ab)^m = a^m b^m$; (5) $(\frac{a}{b})^m = \frac{a^m}{b^m}$;

(6) (i) If $n > 0$ and $a,b > 0$, then $a < b$ if and only if $a^n < b^n$.

(6) (ii) If $n < 0$ and $a,b > 0$, then $a < b$ if and only if $a^n > b^n$.

(7) (i) If $a > 1$, then $m < n$ if and only if $a^m < a^n$.

(7) (ii) If $0 < a < 1$, then $m < n$ if and only if $a^m > a^n$.

In order to define the symbol a^r for rational r, it is first necessary to establish the existence and uniqueness of "n^{th} roots".

2. THEOREM For every real $a > 0$ and every natural number n, there is one and only one real $x > 0$ such that $x^n = a$.

Uniqueness is immediate. For suppose that $x_1 > 0$, $x_2 > 0$ are such that $x_1^n = a$, $x_2^n = a$ -- then these conditions imply that $x_1 = x_2$ (cf. #1, 6(i)).

Turning to existence, let S be the set of all positive real numbers s such that $s^n < a$.

3: LEMMA S is nonempty and is bounded above.

PROOF To see that S is nonempty, observe that $\frac{a}{1 + a}$ lies between 0 and 1, hence

$$\frac{a^n}{(1 + a)^n} \leq \frac{a}{1 + a} < a \Rightarrow \frac{a}{1 + a} \in S.$$

In addition, $1 + a \in U(S)$. Indeed, if there exists $s \in S$ such that $s > 1 + a$ (> 1), then $s^n > s > 1 + a > a$, a contradiction.

Let $\mu = \sup S$ -- then we claim that $\mu^n = a$. To establish this, it suffices to eliminate the other possibilities:

$$\left[\begin{array}{l} \mu^n < a \\ \\ \mu^n > a. \end{array}\right.$$

$\mu^n < a$: Since

$$\frac{a - \mu^n}{(1 + \mu)^n - \mu^n}$$

is a positive real number, one can choose a real number ν lying between 0 and 1 and such that

$$\nu < \frac{a - \mu^n}{(1 + \mu)^n - \mu^n} \quad \text{(e.g. quote §2, #15).}$$

Then

$$(\mu + \nu)^n = \mu^n + \binom{n}{1}\mu^{n-1}\nu + \binom{n}{2}\mu^{n-2}\nu^2 + \cdots + \binom{n}{n}\nu^n$$

$$\leq \mu^n + \nu[\binom{n}{1}\mu^{n-1} + \binom{n}{2}\mu^{n-2} + \cdots + \binom{n}{n}]$$

$$= \mu^n + \nu[(1 + \mu)^n - \mu^n]$$

$$< \mu^n + (a - \mu^n) = a.$$

Therefore $\mu + \nu \in S$, which contradicts the fact that μ is an upper bound for S.

$\underline{\mu^n > a}$: Choose a real number ν lying between 0 and 1 with the following properties:

$$\nu < \mu \text{ and } \nu < \frac{\mu^n - a}{(1 + \mu)^n - \mu^n}.$$

Then for $s > \mu - \nu$, we have

$$s^n \geq (\mu - \nu)^n = \mu^n - \binom{n}{1}\mu^{n-1}\nu + \binom{n}{2}\mu^{n-2}\nu^2 - \cdots + (-1)^n\binom{n}{n}\nu^n$$

$$= \mu^n - \nu[\binom{n}{1}\mu^{n-1} - \binom{n}{2}\mu^{n-2}\nu + \cdots - (-1)^n\binom{n}{n}\nu^{n-1}]$$

$$\geq \mu^n - \nu[\binom{n}{1}\mu^{n-1} + \binom{n}{2}\mu^{n-2} + \cdots + \binom{n}{n}]$$

$$= \mu^n - \nu[(1 + \mu)^n - \mu^n]$$

$$> \mu^n - (\mu^n - a) = a.$$

Therefore $\mu - \nu$ is an upper bound for S, which contradicts the fact that μ is the supremum for S.

Consequently

$$\mu^n = a,$$

as claimed.

Let $a > 0$ be a positive real number -- then for each natural number n, the preceding theorem guarantees the existence and uniqueness of a real $x > 0$ such that $x^n = a$. We write $\sqrt[n]{a}$ for this x and call $\sqrt[n]{a}$ the n^{th} root of a.

[Note: If $n = 1$, write a for $\sqrt[1]{a}$; if $n = 2$, write $\sqrt{a}$ for $\sqrt[2]{a}$.]

4: EXAMPLE $\sqrt{2}$ exists.

Suppose now that $a < 0$ is a negative real number -- then for each odd natural number n, $\sqrt[n]{a}$ is taken to be the unique real $x < 0$ such that $-x = \sqrt[n]{-a}$ (e.g. $\sqrt[3]{-8} = -2$). Since n is odd,

$$x^n = (-(-x))^n = (-1)^n(-x)^n = -(-a) = a,$$

thereby justifying the definition.

[Note: We do not define $\sqrt[n]{a}$ when $a < 0$ and n is an even natural number.]

5: N.B. Set $\sqrt[n]{0} = 0$ for all $n \in \mathbb{N}$.

Let $a > 0$ be a positive real number. Given a rational number r, let $\frac{m}{n}$ be the representation of r in lowest terms.

6: DEFINITION

$$a^r = (\sqrt[n]{a})^m,$$

the m^{th} power of the n^{th} root of a (if m = 1, then $a^{\frac{1}{n}} = \sqrt[n]{a}$).

[Note: Regardless of the sign of m, it is clear that $a^r > 0$.]

7: LAWS OF EXPONENTS FOR RATIONAL POWERS Let a and b be positive real numbers; let r and s be rational numbers.

(1) $a^r \cdot a^s = a^{r+s}$; (2) $(a^r)^s = a^{rs}$; (3) $\frac{a^r}{a^s} = a^{r-s}$;

(4) $(ab)^r = a^r b^r$; (5) $(\frac{a}{b})^r = \frac{a^r}{b^r}$;

(6) (i) If $r > 0$, then $a < b$ if and only if $a^r < b^r$.

(6) (ii) If $r < 0$, then $a < b$ if and only if $a^r > b^r$.

(7) (i) If $a > 1$, then $r < s$ if and only if $a^r < a^s$.

(7) (ii) If $0 < a < 1$, then $r < s$ if and only if $a^r > a^s$.

8: REMARK If p is a natural number, then

$$(\sqrt[n]{a})^m = (\sqrt[np]{a})^{mp}.$$

Therefore in the definition of the symbol a^r, it is not necessary to require that r be reduced to lowest terms so, for example,

$$a = a^1 = (\sqrt[n]{a})^n \quad (n \in N).$$

9: LEMMA Let $a > 0$, $a \neq 1$ -- then

$$\frac{a^r - 1}{r} < \frac{a^s - 1}{s}$$

for all $r,s \in Q - \{0\}$ with $r < s$.

PROOF Let us admit for the moment that the lemma is true when, in addition, r and s are nonzero integers with $r < s$. Proceeding to the general case, there is no loss of generality in supposing that $r = p/n$, $s = q/n$, where $n \in \mathbb{N}$, p and $q \in \mathbb{Z} - \{0\}$, and $p < q$. It is then a question of proving that

$$\frac{(a^{p/n} - 1)n}{p} < \frac{(a^{q/n} - 1)n}{q},$$

or, equivalently, since $n > 0$, that

$$\frac{a^{p/n} - 1}{p} < \frac{a^{q/n} - 1}{q}.$$

Put $b = \sqrt[n]{a}$ -- then, since we are granting temporarily the truth of the lemma in the integral case, it follows that

$$\frac{b^p - 1}{p} < \frac{b^q - 1}{q},$$

as desired. Turning now to the case when r and s are nonzero integers with $r < s$, it is enough to consider just three possibilities, namely (i) $0 < r < r + 1 = s$; (ii) $r < r + 1 = s < 0$; (iii) $-1 = r < s = 1$. The first of these is the assertion that

$$\frac{a^r - 1}{r} < \frac{a^{r+1} - 1}{r + 1}$$

or still, upon multiplying both sides of the inequality by $r(r + 1)$, that

$$(r + 1)a^r - 1 < ra^{r+1},$$

or still, that

$$a^r - 1 < ra^r (a - 1),$$

or still, upon division by $a - 1 \neq 0$, that

$$\begin{cases} a^{r-1} + a^{r-2} + \cdots + a + 1 < ra^r \text{ if } a > 1 \\ a^{r-1} + a^{r-2} + \cdots + a + 1 > ra^r \text{ if } 0 < a < 1. \end{cases}$$

But these inequalities do in fact obtain (apply #1, 7(i) and 7(ii)). The second case, $r < r + 1 = s < 0$, can be reduced to the first by considering $-s$, $-r$, and a^{-1}. Finally, if $r = -1$ and $s = 1$, then the inequality to be established can be written $1 - a^{-1} < a - 1$ and this is certainly true for $a > 0$, $a \neq 1$.

Fix a real number $a > 1$. Given a rational number x, let

$$S = \{a^r : r \in Q \text{ and } r < x\}.$$

10: SUBLEMMA S is nonempty and has an upper bound M, say, thus S has a supremum.

11: LEMMA $\sup S = a^x$.

PROOF Since $a^x \in U(S)$, it suffices to show that for each $\varepsilon > 0$, there is a rational number $r < x$ such that $a^x - a^r < \varepsilon$ (cf. §2, #7). Without yet committing ourselves, it can be assumed from the beginning that $0 < x - r < 1$, hence

$$\frac{a^{x-r} - 1}{x-r} < a - 1 < a + 1 \quad \text{(cf. \#9)},$$

from which

$$a^x - a^r = a^r \left[\frac{a^{x-r} - 1}{x-r}\right] (x - r)$$

$$< M(a + 1)(x - r),$$

so if $r < x$ is chosen in such a way that

$$0 < x - r < \frac{1}{2} \min \{\frac{\varepsilon}{M(a + 1)}, 1\},$$

then $a^x - a^r < \varepsilon$.

Fix a real number $a > 1$. Given a real number x, let

$$S = \{a^r : r \in Q \text{ and } r < x\}.$$

12: SUBLEMMA S is nonempty and bounded above.

[It is clear that S is nonempty (cf. §2, #10). On the other hand, if n is any natural number $> x$ (cf. §2, #9), then

$$r < x \Rightarrow r < n \Rightarrow a^r < a^n \quad \text{(cf. \#7, 7(i))}$$

$$\Rightarrow a^n \in U(S) \Rightarrow U(S) \neq \emptyset.]$$

13: DEFINITION $a^x = \sup S$.

[Note: If $a = 1$, we define a^x as 1. If $0 < a < 1$, then $1/a > 1$ and we define a^x as $1/(1/a)^x$. In all cases: $a^x > 0$.]

14: N.B. Matters are consistent when restricted to rational x (cf. #11).

15: LAWS OF EXPONENTS FOR REAL POWERS Let a and b be positive real numbers; let x and y be real numbers.

(1) $a^x \cdot a^y = a^{x+y}$; (2) $(a^x)^y = a^{xy}$; (3) $\dfrac{a^x}{a^y} = a^{x-y}$;

(4) $(ab)^x = a^x b^x$; (5) $(\frac{a}{b})^x = \dfrac{a^x}{b^x}$;

(6) (i) If $x > 0$, then $a < b$ if and only if $a^x < b^x$.

(6) (ii) If $x < 0$, then $a < b$ if and only if $a^x > b^x$.

(7) (i) If $a > 1$, then $x < y$ if and only if $a^x < a^y$.

(7) (ii) If $0 < a < 1$, then $x < y$ if and only if $a^x > a^y$.

The proof of this result is spelled out in the lines below.

[Note: We shall omit consideration of trivial, special cases (e.g. $1^x \cdot 1^y = 1^{x+y}$ etc.]

<u>LAW 1:</u>

<u>Case 1:</u> $a > 1$. Let

$$S = \{a^s : s \in Q \text{ and } s < x\}$$

$$T = \{a^t : t \in Q \text{ and } t < y\}$$

$$U = \{a^u : u \in Q \text{ and } u < x + y\},$$

thus $a^x = \sup S$, $a^y = \sup T$, $a^{x+y} = \sup U$. In addition,

$$\begin{aligned} a^x \cdot a^y &= (\sup S)\cdot(\sup T) \\ &= \sup(S\cdot T) \quad (\text{cf. } §3, \#6), \end{aligned}$$

and

$$\begin{aligned} S\cdot T &= \{a^s \cdot a^t : s, t \in Q \text{ and } s < x, t < y\} \\ &= \{a^{s+t} : s, t \in Q \text{ and } s < x, t < y\}. \end{aligned}$$

So, to prove that $a^x \cdot a^y = a^{x+y}$, it will be enough to prove that $\sup(S\cdot T) = \sup U$ and for this purpose, we shall employ §3, #2. Since $S\cdot T$ is a subset of U, it need only be shown that given any element a^u ($u \in Q$ and $u < x + y$) in U, there exist rational numbers s, t with $s < x$, $t < y$ and such that $u < s + t$ (for then $a^u < a^{s+t} \in S\cdot T$). Noting that

$$\frac{u - x + y}{2} < y, \quad \frac{u - y + x}{2} < x,$$

choose rational numbers s and t such that

$$\frac{u-y+x}{2} < s < x, \quad \frac{u-x+y}{2} < t < y \qquad (\text{cf. §2, \#15}).$$

Then

$$u = \frac{u-y+x}{2} + \frac{u-x+y}{2} < s + t.$$

<u>Case 2:</u> $0 < a < 1$: We have

$$a^x \cdot a^y = \frac{1}{(1/a)^x} \cdot \frac{1}{(1/a)^y}$$

$$= \frac{1}{(1/a)^x \cdot (1/a)^y}$$

$$= \frac{1}{(1/a)^{x+y}} = a^{x+y}.$$

A simple but important consequence of LAW 1 is the fact that

$$a^x = \frac{1}{a^{-x}} \quad (a > 0,\ x \in R).$$

Proof:

$$1 = a^0 = a^{x-x} = a^x \cdot a^{-x} \Rightarrow a^x = \frac{1}{a^{-x}}.$$

<u>LAW 2:</u>

<u>Case 1:</u> $y \in Z$. Suppose first that $y \in N$ and argue by induction. The assertion is trivial if $y = 1$. Assuming that the assertion is true for $y = n$, we have

$$(a^x)^{n+1} = (a^x)^n \cdot a^x \quad \text{(by definition)}$$

$$= (a^{xn}) \cdot a^x \quad \text{(by induction hypothesis)}$$

$$= a^{x(n+1)} \quad \text{(by LAW 1)}.$$

It therefore follows that $(a^x)^y = a^{xy}$ for arbitrary $a > 0$, x real, and y a positive integer. The assertion is trivial if $y = 0$ and the reader can supply the details if y is a negative integer.

<u>Case 2:</u> $y \in Q$. Let $\frac{m}{n}$ be the representation of y in lowest terms. By Case 1, $(a^x)^m = a^{xm}$. Therefore

$$\begin{aligned}(a^x)^{\frac{m}{n}} &= ((a^x)^m)^{\frac{1}{n}} \\ &= (a^{xm})^{\frac{1}{n}} \\ &= (a^{x\frac{m}{n} \cdot n})^{\frac{1}{n}} \\ &= ((a^{x\frac{m}{n}})^n)^{\frac{1}{n}} \quad \text{(by Case 1)} \\ &= a^{x\frac{m}{n}}.\end{aligned}$$

<u>Case 3:</u> $a > 1$, $x > 0$, y arbitrary. Let

$$S = \{(a^x)^s : s \in Q \text{ and } s < y\}$$

$$T = \{a^t : t \in Q \text{ and } t < xy\},$$

thus $(a^x)^y = \sup S$, $a^{xy} = \sup T$, the claim being that $\sup S = \sup T$. To this end, we shall utilize §3, #2. In view of Case 2,

$$S = \{a^{xs} : s \in Q \text{ and } s < y\}.$$

Given $a^{xs} \in S$, choose a rational number t such that $xs < t < xy$ -- then $a^{xs} < a^t$ and $a^t \in T$. On the other hand, given $a^t \in T$, choose a rational number s such that $\frac{t}{x} < s < y$ -- then $a^t < a^{xs}$ and $a^{xs} \in S$.

Case 4: $0 < a < 1$, $x > 0$, y arbitrary. Using LAW 4 below (whose proof does not depend on LAW 2), write

$$(a^x)^y = \left(\frac{1}{(1/a)^x}\right)^y = \frac{1}{((1/a)^x)^y} = \frac{1}{(1/a)^{xy}} = a^{xy}.$$

Case 5: $0 < a$, $x < 0$, y arbitrary. If $x < 0$, then $-x > 0$, hence

$$(a^x)^y = \left(\frac{1}{a^{-x}}\right)^y = \frac{1}{(a^{-x})^y} = \frac{1}{a^{-xy}} = a^{xy}.$$

LAW 3: One need only observe that

$$a^x = a^{x-y+y}$$

$$= a^{x-y} \cdot a^y \quad \text{(by LAW 1)},$$

i.e.,

$$\frac{a^x}{a^y} = a^{x-y}.$$

LAW 4:

Case 1: $a > 1$, $b > 1$. Let

$$S = \{a^s : s \in Q \text{ and } s < x\}$$

$$T = \{b^t : t \in Q \text{ and } t < x\}$$

$$U = \{(ab)^u : u \in Q \text{ and } u < x\},$$

thus $a^x = \sup S$, $b^x = \sup T$, $(ab)^x = \sup U$. Meanwhile,

$$a^x b^x = (\sup S) \cdot (\sup T)$$

$$= \sup(S \cdot T) \quad \text{(cf. §3, \#6)}.$$

So, to prove that $(ab)^x = a^x b^x$, it will be enough to prove that $\sup(S \cdot T) = \sup U$ and for this purpose, we shall employ §3, #2. Since U is a subset of $S \cdot T$, it suffices to go the other way. But a generic element of $S \cdot T$ is of the form $a^s b^t$, where $s, t \in Q$ and $s < x$, $t < x$. And, assuming that $s \leq t$, we have

$$a^s b^t \leq a^t b^t = (ab)^t \in U.$$

<u>Case 2:</u> $0 < a < 1$, $0 < b < 1$. Since $0 < ab < 1$, from the definitions,

$$(ab)^x = \frac{1}{(1/ab)^x}.$$

Since $1/a > 1$, $1/b > 1$, it follows from the discussion in Case 1 that

$$\left(\frac{1}{ab}\right)^x = \left(\frac{1}{a}\right)^x \left(\frac{1}{b}\right)^x.$$

Therefore

$$(ab)^x = \frac{1}{(1/ab)^x}$$

$$= \frac{1}{(1/a)^x \cdot (1/b)^x} = a^x b^x.$$

<u>Case 3:</u> $0 < a < 1$, $b > 1$. In this situation $1/a > 1$. Suppose first that $1 < 1/a \leq b$ -- then $ab \geq 1$, so

$$b^x = \left(ab \cdot \frac{1}{a}\right)^x = (ab)^x \left(\frac{1}{a}\right)^x,$$

hence

$$(ab)^x = b^x \frac{1}{(1/a)^x} = \frac{1}{(1/a)^x} b^x = a^x b^x.$$

The other possibility is that $1 < b < 1/a$. Since in this situation both $1/ab$ and b are greater than 1, we have

$$\left(\frac{1}{a}\right)^x = \left(\frac{1}{ab} \cdot b\right)^x = \left(\frac{1}{ab}\right)^x b^x,$$

so

$$(ab)^x = \frac{1}{(1/ab)^x} = \frac{1}{(1/a)^x}\, b^x = a^x b^x.$$

<u>Case 4:</u> $a > 1$, $0 < b < 1$. This is the same as Case 3 with the roles of a and b interchanged.

A simple but important consequence of LAW 4, used already in Case 4 of LAW 2 above, is the fact that

$$\left(\frac{1}{a}\right)^x = \frac{1}{a^x} \quad (a > 0,\ x \in R).$$

Proof:

$$1^x = \left(a \cdot \frac{1}{a}\right)^x = a^x\left(\frac{1}{a}\right)^x \Rightarrow \left(\frac{1}{a}\right)^x = \frac{1}{a^x}.$$

<u>LAW 5:</u> Write

$$\left(\frac{a}{b}\right)^x = \left(a \cdot \frac{1}{b}\right)^x = a^x\left(\frac{1}{b}\right)^x = a^x\,\frac{1}{b^x} = \frac{a^x}{b^x}.$$

<u>LAW 6:</u> We shall consider (i), leaving (ii) for the reader, and of the two parts to (i), only the assertion $0 < a < b \Rightarrow a^x < b^x$ will be dealt with explicitly. Claim: If $c > 1$, $x > 0$, then $c^x > 1$. Granting the claim for the moment, note now that

$$0 < a < b \Rightarrow 1 < \frac{b}{a} \Rightarrow 1 < \left(\frac{b}{a}\right)^x = \frac{b^x}{a^x} \quad \text{(by LAW 5)}$$

$$\Rightarrow a^x < b^x.$$

Going back to the claim, fix a rational number r such that $0 < r < x$ -- then it will be enough to prove that $1 < c^r$. Since $1 < 2 \Rightarrow r < 2r \Rightarrow c^r < c^{2r}$, it follows that

$$1 = c^{r-r} < c^{2r-r} = c^r.$$

<u>LAW 7:</u> We shall consider (i), leaving (ii) for the reader, and of the two parts to (i), only the assertion $x < y \Rightarrow a^x < a^y$ will be dealt with explicitly. Choose $s \in Q: x < s < y$ -- then

$$r \in Q \text{ and } r < x \Rightarrow r < s \Rightarrow a^r < a^s \Rightarrow a^x \leq a^s.$$

Choose $t \in Q: s < t < y$ -- then $a^s < a^t$ and $a^t \leq a^y$, hence $a^x < a^y$.

<u>16:</u> LEMMA Let $a > 0$, $a \neq 1$ -- then

$$\frac{a^x - 1}{x} < \frac{a^y - 1}{y}$$

for all $x,y \in R - \{0\}$ with $x < y$ (cf. #9).

§5. $\exp_a$ AND $\log_a$

Let $a \neq 1$ be a positive real number.

1: DEFINITION The exponential function to base a is the function $\exp_a$ with domain R defined by the rule

$$\exp_a(x) = a^x \quad (x \in R).$$

2: LEMMA $\exp_a : R \to R_{>0}$ is injective (cf. §4, #15, 7(i) and 7(ii)).

3: LEMMA $\exp_a : R \to R_{>0}$ is surjective.

This is not quite immediate and requires some preparation.

4: SUBLEMMA Let $n > 1$ be a natural number and let $a \neq 1$ be a positive real number -- then

$$n(a^{1/n} - 1) < a - 1.$$

PROOF In §4, #9, take $x = \frac{1}{n}$, $y = 1$ -- then $x < y$ and

$$\frac{a^{1/n} - 1}{y_n} < \frac{a - 1}{1},$$

i.e.,

$$n(a^{1/n} - 1) < a - 1.$$

To discuss #3, distinguish two cases: $a > 1$ or $a < 1$. We shall work through the first of these, leaving the second to the reader.

5: SUBLEMMA If $t > 1$ and

$$n > \frac{a - 1}{t - 1},$$

then $a^{1/n} < t$.

PROOF In fact,

$$a - 1 > n(a^{1/n} - 1) > \frac{a - 1}{t - 1}(a^{1/n} - 1)$$

$$\Rightarrow$$

$$1 > \frac{a^{1/n} - 1}{t - 1}$$

$$\Rightarrow t - 1 > a^{1/n} - 1 \Rightarrow t > a^{1/n}.$$

Fix $y > 0$ -- then the claim is that there is a real x such that $a^x = y$ (x then being necessarily unique). So let

$$S = \{w : a^w < y\}$$

and put $x = \sup S$.

- $a^x < y$ is untenable.

[In #5, take $t = \frac{y}{a^x} > 1$ to get

$$a^{1/n} < \frac{y}{a^x}$$

for $n >> 0$, thus

$$a^{x + \frac{1}{n}} < y$$

for $n >> 0$. But then, for any such n,

$$x + \frac{1}{n} \in S$$

which leads to the contradiction $x \geq x + \frac{1}{n}$.]

- $a^x > y$ is untenable.

[In #5, take $t = \frac{a^x}{y} > 1$ to get

$$a^{1/n} < \frac{a^x}{y}$$

for $n >> 0$, thus

$$y < a^{x - \frac{1}{n}}$$

for $n >> 0$. Owing to §2, #6, for each $n >> 0$, there exists $w_n \in S: w_n > x - \frac{1}{n}$, hence

$$\begin{aligned} y > a^{w_n} > a^{x - \frac{1}{n}} \quad &(\text{cf. §4, #15, 7(i)}) \\ > y, \end{aligned}$$

a contradiction.]

Therefore $a^x = y$, as contended.

6: SCHOLIUM $\exp_a: R \to R_{>0}$ is bijective.

7: REMARK There is another way to establish the surjectivity of $\exp_a$ if one is willing to introduce some machinery, the point being that the range of $\exp_a$ is an open subgroup of $R_{>0}$. One may then quote the following generality: A locally compact topological group is connected if and only if it has no proper open subgroups.

Since

$$\exp_a: R \to R_{>0}$$

is bijective, it admits an inverse

$$\exp_a^{-1}: R_{>0} \to R.$$

8: NOTATION Put

$$\log_a = \exp_a^{-1}.$$

9: DEFINITION The logarithm function to a base a is the function $\log_a$ defined by the rule

$$\log_a(a^x) = x \quad (x \in R).$$

10: LEMMA Let u and v be positive real numbers -- then

$$\begin{cases} \log_a(uv) = \log_a(u) + \log_a(v) \\ \log_a(\frac{u}{v}) = \log_a(u) - \log_a(v). \end{cases}$$

11: LEMMA Let y be a positive real number, r a real number -- then

$$\log_a(y^r) = r\log_a(y).$$

PROOF Write $y = a^x$, thus

$$y^r = (a^x)^r = a^{xr} \quad (\text{cf. §4, \#15, (2)})$$
$$= a^{rx}$$

=>

$$\log_a(y^r) = rx = r\log_a(y).$$

12: N.B. Special cases:

$$\log_a(1) = 0, \log_a(a) = 1.$$

13: LEMMA Let $a \neq 1$, $b \neq 1$ be positive real numbers -- then

$$\log_a(b)\ \log_b(a) = 1.$$

PROOF Put

$$x = \log_a(b),\ y = \log_b(a),$$

so that

$$a^x = b,\ b^y = a,$$

hence

$$a = b^y = (a^x)^y = a^{xy} \quad (\text{cf. §4, #15, (2)})$$

from which $xy = 1$.

14: DEFINITION The <u>common logarithm</u> is $\log_{10}$.

15: EXAMPLE $\log_{10} 2$ is irrational.

[Suppose that

$$\log_{10} 2 = \frac{a}{b},$$

where a and b are positive integers -- then

$$2 = 10^{\frac{a}{b}} \Rightarrow 2^b = 10^a = 2^a 5^a.$$

But 2^b is not divisible by 5.]

[Note: It turns out that $\log_{10} 2$ is transcendental, a point that will be dealt with later on.]

There are irrational numbers α, β such that α^β is rational.

16: EXAMPLE Take $\alpha = \sqrt{10}$ (cf. §7, #6), $\beta = 2\log_{10} 2$ -- then

$$(\sqrt{10})^{2\log_{10}2} = (10^{\frac{1}{2}})^{2\log_{10}2}$$

$$= 10^{\log_{10}2} = 2.$$

APPENDIX

Put

$$E(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!} \quad (x \in R).$$

[Note:

$$E(1) \equiv e.]$$

LEMMA $E(x_1 + \cdots + x_n) = E(x_1)\cdots E(x_n)$.

[Note:

$$E(x)E(-x) = E(x - x) = E(0) = 1.]$$

Take $x_1 = 1, \ldots, x_n = 1$ to get

$$E(n) = e^n.$$

If now $r = \frac{m}{n}$ $(m,n \in N)$, then

$$(E(r))^n = E(nr) = E(m) = e^m$$

$$\Rightarrow E(r) = e^{\frac{m}{n}} = e^r.$$

And

$$E(-r) = \frac{1}{E(r)} = \frac{1}{e^r} = e^{-r}.$$

Summary:

$$E(x) = e^x \quad (x \in Q).$$

But now for any real x,

$$e^x = \sup S,$$

where

$$S = \{e^r : r \in Q \text{ and } r < x\} \quad (\text{cf. §4, #13}).$$

THEOREM $\forall\, x \in R$,

$$E(x) = e^x \ (= \exp_e(x)).$$

REMARK It can be shown that

$$e = \sup\{(1 + \frac{1}{n})^n : n \in N\},$$

a fact which is sometimes used as the definition of e.

§6. *IRRATIONALITY OF $\sqrt{2}$*

Recall that P is the subset of R whose elements are irrational and, on abstract grounds, is uncountable, in particular, irrational numbers exist. Still, the problem of deciding whether a specific real number is irrational or not is generally difficult.

<u>1:</u> RAPPEL $\sqrt{2}$ exists (cf. §4, #4).

<u>2:</u> THEOREM $\sqrt{2}$ is irrational.

There are many proofs of this result. In what follows we shall give a representative sampling.

<u>First Proof:</u> Suppose that $\sqrt{2}$ is rational, say $\sqrt{2} = \frac{x}{y}$, where x and y are positive integers and $\gcd(x,y) = 1$ -- then $\frac{x^2}{y^2} = 2$ or still, $x^2 = 2y^2$, thus $2|x^2$ and x^2 is even. But then x must be even (otherwise, x odd forces x^2 odd), so $x = 2n$ for some positive integer n. And:

$$x^2 = 2y^2 \Rightarrow (2n)^2 = 2y^2$$

$$\Rightarrow 2n^2 = y^2 \Rightarrow 2|y^2 \Rightarrow 2|y.$$

Therefore $\gcd(x,y) \neq 1$, a contradiction.

<u>Second Proof:</u> Suppose that $\sqrt{2}$ is rational, say $\sqrt{2} = \frac{x}{y}$, where x and y are positive integers and y is the smallest such -- then $\frac{x^2}{y^2} = 2$ or still, $x^2 = 2y^2$.

Next

$$y^2 < 2y^2 = x^2 = (2y)y < (2y)(2y)$$

$$\Rightarrow y^2 < x^2 < (2y)^2$$

$$\Rightarrow y < x < 2y \quad \text{(cf. §4, \#1, 6(i))}.$$

Put $u = x - y$, a positive integer:

$$y + u = x < 2y = y + y \Rightarrow u < y.$$

Put $v = 2y - x$, a positive integer:

$$\begin{aligned} v^2 - 2u^2 &= (2y - x)^2 - 2(x - y)^2 \\ &= 4y^2 - 4yx + x^2 - 2(x^2 - 2xy + y^2) \\ &= 4y^2 + x^2 - 2x^2 - 2y^2 \\ &= (x^2 - 2y^2) - 2(x^2 - 2y^2) \\ &= (1 - 2)(x^2 - 2y^2) \\ &= (-1)(0) = 0. \end{aligned}$$

$\Rightarrow$

$$\begin{aligned} v^2 = 2u^2 \Rightarrow \frac{v^2}{u^2} = 2 & \\ &\Rightarrow \left(\frac{v^2}{u^2}\right)^{1/2} = 2^{1/2} = \sqrt{2} \\ &\Rightarrow \frac{v^{2(1/2)}}{u^{2(1/2)}} = \sqrt{2} \quad \text{(cf. §4, \#7, 2)} \\ &\Rightarrow \frac{v}{u} = \sqrt{2}. \end{aligned}$$

But now we have reached a contradiction: u is less than y whereas y was the smallest positive integer with the property that $\frac{x}{y} = \sqrt{2}$ for some positive integer x.

<u>Third Proof:</u> Suppose that $\sqrt{2}$ is rational, say $\sqrt{2} = \frac{x}{y}$, where x and y are positive integers. Write

$$\sqrt{2} + 1 = \frac{1}{\sqrt{2} - 1},$$

thus

$$\frac{x}{y} + 1 = \frac{1}{\frac{x}{y} - 1} = \frac{y}{x - y}$$

=>

$$\sqrt{2} = \frac{x}{y} = \frac{y}{x - y} - 1 = \frac{2y - x}{x - y} \equiv \frac{x_1}{y_1}.$$

But

$$1 < \sqrt{2} < 2 \Rightarrow 1 < \frac{x}{y} < 2 \Rightarrow y < x < 2y$$

$$\Rightarrow \begin{bmatrix} x_1 = 2y - x > 0 \\ \\ y_1 = x - y > 0 \end{bmatrix} \Rightarrow \begin{bmatrix} x_1 \in N \\ \\ y_1 \in N. \end{bmatrix}$$

In addition

$$2y < 2x = x + x \Rightarrow 2y - x < x \Rightarrow x_1 < x.$$

Proceeding, there exist positive integers x_2 and y_2 such that

$$\sqrt{2} = \frac{x_1}{y_1} = \frac{2y_1 - x_1}{x_1 - y_1} \equiv \frac{x_2}{y_2}$$

with $x_2 < x_1 < x$. And so on, ad infinitum. The supposition that $\sqrt{2}$ is irrational therefore leads to an infinite descending chain of natural numbers, an impossibility.

Fourth Proof: Suppose that $\sqrt{2}$ is rational, say $\sqrt{2} = \frac{x}{y}$, where x and y are positive integers. Define sequences

$$\left[\begin{array}{l} a_1, a_2, \ldots \\ b_1, b_2, \ldots \end{array}\right.$$

of natural numbers recursively by

$$\left[\begin{array}{ll} a_1 = 1,\ a_2 = 2,\ a_n = 2a_{n-1} + a_{n-2} & (n > 2) \\ b_1 = 1,\ b_2 = 3,\ b_n = 2b_{n-1} + b_{n-2} & (n > 2). \end{array}\right.$$

Put

$$p_n(t) = a_n^2 t^2 - b_n^2 \quad (n \geq 1).$$

Then

$$p_n(\sqrt{2}) = 2a_n^2 - b_n^2$$

is an integer and $|p_n(\sqrt{2})| = 1$ (details below). On the other hand,

$$\begin{aligned} 1 = |p_n(\sqrt{2})| &= |(a_n\sqrt{2} - b_n)(a_n\sqrt{2} + b_n)| \\ &= |(a_n \tfrac{x}{y} - b_n)(a_n \tfrac{x}{y} + b_n)| \\ &= |a_n x - b_n y|\left(\frac{a_n x + b_n y}{y^2}\right) \end{aligned}$$

=>

$$0 < |a_n x - b_n y| = \frac{y^2}{a_n x + b_n y}.$$

Since the sequence $\{a_n x + b_n y\}$ is strictly increasing, from some point on

$$y^2 < a_n x + b_n y.$$

I.e.:

$$n >> 0 \Rightarrow |a_n x - b_n y| < 1.$$

But there are no integers between 0 and 1.

[Inductively we claim that

$$2a_n^2 - b_n^2 = (-1)^{n+1} \text{ and } 2a_{n-1}a_n - b_{n-1}b_n = (-1)^n.$$

These identities are certainly true when $n = 1$ (take $a_0 = 0$, $b_0 = 1$). Assume therefore that they hold at level $n > 1$ -- then at level $n + 1$:

$$2a_{n+1}^2 - b_{n+1}^2 = 2(2a_n + a_{n-1})^2 - (2b_n + b_{n-1})^2$$

$$= 4(2a_n^2 - b_n^2) + 4(2a_{n-1}a_n - b_{n-1}b_n) + (2a_{n-1}^2 - b_{n-1}^2)$$

$$= 4(-1)^{n+1} + 4(-1)^n + (-1)^n$$

$$= (-1)^n = (-1)^{n+2}.$$

And, analogously,

$$2a_n a_{n+1} - b_n b_{n+1} = (-1)^{n+1}.$$

Finally

$$p_n(\sqrt{2}) = 2a_n^2 - b_n^2 = (-1)^{n+1}$$

$$\Rightarrow |p_n(\sqrt{2})| = 1.]$$

Fifth Proof: Let S be the set of positive integers n with the property that $n\sqrt{2}$ is a positive integer. If $\sqrt{2}$ were rational, then S would be nonempty, hence would have a smallest element, call it k. Now, from the definitions,

$$k \in S \Rightarrow (\sqrt{2} - 1)k \in N.$$

But

$$((\sqrt{2} - 1)k)\sqrt{2} = 2k - k\sqrt{2}$$

$$= (2 - \sqrt{2})k$$

is a positive integer, so $(\sqrt{2} - 1)k \in S$. However

$$(\sqrt{2} - 1)k < (2 - 1)k = k,$$

which contradicts the assumption that k is the smallest element of S.

§7. *IRRATIONALITY: THEORY AND EXAMPLES*

For use below:

1: RAPPEL Let a,b,c be integers such that a,b have no prime factors in common and $a|b^n c$ $(n \in \mathbb{N})$ -- then $a|c$.

The following result is the so-called "rational roots test".

2: THEOREM Let

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

be a polynomial with integral coefficients. Suppose that it has a rational root $\frac{p}{q}$: $p,q \in \mathbb{Z}$ and $\gcd(p,q) = 1$ -- then $p|a_0$ and $q|a_n$.

PROOF Take $X = \frac{p}{q}$ to get

$$a_0 + a_1 (\frac{p}{q}) + a_2 (\frac{p}{q})^2 + \cdots + a_n (\frac{p}{q})^n = 0$$

so, after multiplying through by q^n,

$$\begin{aligned} q^n a_0 &= - (a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n) \\ &= - p(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1}) \in \mathbb{Z} \\ &\Rightarrow p|q^n a_0 \Rightarrow p|a_0 \quad (\text{cf. } \#1). \end{aligned}$$

That $q|a_n$ can be established analogously.

3: N.B. When specialized to the case where $a_n = 1$, the conclusion is that if the polynomial

$$a_0 + a_1X + a_2X^2 + \cdots + X^n$$

has a rational root, then this root is an integer (which divides a_0).

[Consider a rational root $\frac{p}{q}$ and take q positive (in the event that q were negative absorb the minus sign into p). From the above, q divides $a_n = 1$, hence $q = 1$, hence $\frac{p}{q} = \frac{p}{1} = p$ (and $p|a_0$).]

4: EXAMPLE If p is a prime, then $\sqrt{p}$ is irrational.

[Consider the polynomial $X^2 - p$, thus $(\sqrt{p})^2 - p = 0$, i.e., $\sqrt{p}$ is a root. Suppose that $\sqrt{p}$ was rational so for some $k \in N$,

$$\sqrt{p} = k \Rightarrow p = k^2.$$

But k^2 has an even number of prime factors, from which it follows that the stated relation is impossible (or quote #1: $a = p$, $b = k$, $n = 2$, $c = 1$, implying that $p|1$).]

Therefore in particular $\sqrt{2}$ and $\sqrt{3}$ are irrational but this does not automatically imply that $\sqrt{2} + \sqrt{3}$ is irrational (the sum of two irrationals may be either rational or irrational).

5: EXAMPLE $\sqrt{2} + \sqrt{3}$ is irrational.

[$\sqrt{2} + \sqrt{3}$ is a zero of the function

$$X^2 - 2X\sqrt{2} - 1,$$

so $\sqrt{2} + \sqrt{3}$ is a root of the polynomial

$$(X^2 + 2X\sqrt{2} - 1)(X^2 - 2X\sqrt{2} - 1) = X^4 - 10X^2 + 1.$$

From the above, the only possible rational roots of this polynomial are integers which divide 1, i.e., ± 1. And $\sqrt{2} + \sqrt{3} \neq \pm 1$, thus $\sqrt{2} + \sqrt{3}$ is not among the possible roots of

$$X^4 - 10X^2 + 1,$$

thus is irrational.]

<u>6:</u> EXAMPLE Let a and n be positive integers -- then $\sqrt[n]{a}$ is either irrational or a positive integer. And if $\sqrt[n]{a}$ is a positive integer, then a is the n^{th} power of a positive integer.

[Consider the polynomial $X^n - a$, hence $(\sqrt[n]{a})^n - a = a - a = 0$. There are now two possibilities, viz. either $\sqrt[n]{a}$ is irrational or else $\sqrt[n]{a}$ is rational in which case $\sqrt[n]{a} \equiv k$ is a positive integer (and $a = k^n$).]

<u>7:</u> REMARK Consequently, if a is a positive integer such that $\sqrt{a}$ is not a positive integer, then $\sqrt{a}$ is irrational (cf. #4).

[Here is another proof. Assume instead that $\sqrt{a}$ is rational, say $\sqrt{a} = \frac{x}{y}$, where x and y are positive integers and y is the smallest such:

$$y\sqrt{a} = x \Rightarrow (y\sqrt{a})\sqrt{a} = x\sqrt{a} \Rightarrow ya = x\sqrt{a}.$$

Choose $n \in \mathbb{N}: n < \sqrt{a} < n + 1$ -- then

$$\sqrt{a} = \frac{x}{y} = \frac{x(\sqrt{a} - n)}{y(\sqrt{a} - n)}$$

$$= \frac{x\sqrt{a} - xn}{y\sqrt{a} - yn} = \frac{ya - xn}{x - yn}.$$

The numerator and denominator of the fraction

$$\frac{ya - xn}{x - yn}$$

are integers that, in fact, are positive:

$$\begin{cases} ya - xn = x\sqrt{a} - xn = x(\sqrt{a} - n) > 0 \\ x - yn = y\sqrt{a} - yn = y(\sqrt{a} - n) > 0. \end{cases}$$

And

$$x - yn = y(\sqrt{a} - n) < y$$

which contradicts the choice of y.]

8: THEOREM Suppose that $a_1, a_2, \ldots, a_n$ are positive integers. Assume:

$$\Sigma \equiv \sqrt{a_1} + \sqrt{a_2} + \cdots + \sqrt{a_n}$$

is rational -- then $\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}$ are rational.

9: APPLICATION If for some k $(1 \le k \le n)$, $\sqrt{a_k}$ is irrational, then

$$\sqrt{a_1} + \sqrt{a_2} + \cdots + \sqrt{a_n}$$

is irrational.

10: EXAMPLE $\sqrt{2} + \sqrt{3}$ is irrational (cf. #5).

11: EXAMPLE $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is irrational.

Passing to the proof of #8, it will be enough to show that $\sqrt{a_1}$ is rational. For this purpose, introduce

$$F(X;a_1) = \Pi(X - \sqrt{a_1} \pm \sqrt{a_2} \pm \cdots \pm \sqrt{a_n}),$$

where the product ranges over all combinations of plus and minus signs, thus

$$F(\Sigma;a_1) = 0.$$

Next multiply out the expression defining $F(X;a_1)$ -- then $\sqrt{a_1}$ appears to both even and odd powers but $\sqrt{a_2},\ldots,\sqrt{a_n}$ appear only to even powers. Assemble the even powered terms in $\sqrt{a_1}$, call the result $G(X;a_1)$, and assemble the odd powered terms in $\sqrt{a_1}$, call the result $-\sqrt{a_1}\,H(X;a_1)$ -- then

$$F(X;a_1) = G(X;a_1) - \sqrt{a_1}\,H(X;a_1)$$

and $G(X;a_1)$, $H(X;a_1)$ are polynomials with integral coefficients.

E.g.: When $n = 2$,

$$F(X) = (X - \sqrt{a_1} + \sqrt{a_2})\ (X - \sqrt{a_1} - \sqrt{a_2})$$

$$= (X - \sqrt{a_1})^2 - (\sqrt{a_2})^2$$

$$= (X^2 + (\sqrt{a_1})^2 - (\sqrt{a_2})^2) - \sqrt{a_1}\ (2X).$$

Now evaluate the data at $X = \Sigma$:

$$0 = F(\Sigma;a_1) = G(\Sigma;a_1) - \sqrt{a_1}\,H(\Sigma;a_1)$$

$$\Rightarrow$$

$$\sqrt{a_1} = \frac{G(\Sigma;a_1)}{H(\Sigma;a_1)} \in Q$$

provided $H(\Sigma;a_1) \neq 0$. To check that this is so, write

$$F(\Sigma;a_1) - F(\Sigma;-a_1)$$

$$= 0 - F(\Sigma;-a_1)$$

$$= (G(\Sigma;a_1) - \sqrt{a_1}\, H(\Sigma;a_1)) - (G(\Sigma;a_1) + \sqrt{a_1}\, H(\Sigma;a_1))$$

$$= -\, 2\sqrt{a_1}\, H(\Sigma;a_1)$$

$\Rightarrow$

$$H(\Sigma;a_1) = \frac{1}{2\sqrt{a_1}} F(\Sigma;-a_1)$$

$$= \frac{1}{2\sqrt{a_1}} \Pi(\Sigma + \sqrt{a_1} \pm \sqrt{a_2} \pm \cdots \pm \sqrt{a_n})$$

$$= \frac{1}{2\sqrt{a_1}} \Pi(2\sqrt{a_1} + (\sqrt{a_2} \pm \sqrt{a_2}) + \cdots + (\sqrt{a_n} \pm \sqrt{a_n})$$

$$= \frac{1}{2\sqrt{a_1}} \prod_{S \subset \{\sqrt{a_2},\ldots,\sqrt{a_n}\}} (2\sqrt{a_1} + 2 \sum_{a_i \in S} \sqrt{a_i})$$

$$= \frac{1}{\sqrt{a_1}} \prod_{S \subset \{\sqrt{a_2},\ldots,\sqrt{a_n}\}} (\sqrt{a_1} + \sum_{a_i \in S} \sqrt{a_i}).$$

But

$$\sqrt{a_1} + \sum_{a_i \in S} \sqrt{a_i}$$

is never zero.

<u>12:</u> THEOREM Given $x \in R$, there are infinitely many coprime solutions p,q $(q > 0)$ to

$$|x - \frac{p}{q}| \leq \frac{1}{q} .$$

One can say more if x is irrational.

<u>13:</u> THEOREM Given $x \in P$, there are infinitely many coprime solutions p,q $(q > 0)$ to

$$|x - \frac{p}{q}| \leq \frac{1}{q^2}.$$

[Note: This estimate can be sharpened to

$$|x - \frac{p}{q}| \leq \frac{1}{\sqrt{5}\, q^2}$$

but $\frac{1}{\sqrt{5}}$ cannot be replaced by a smaller real number unless some restriction is placed on x. To see this, take

$$x = \frac{\sqrt{5} - 1}{2}.$$

Then it can be shown that there is a coprime sequence $\frac{p_n}{q_n}$ $(q_n > 0)$ with the property that if $0 < C < \frac{1}{\sqrt{5}}$, then

$$|x - \frac{p_n}{q_n}| > \frac{C}{q_n^2} \quad \forall\ n >> 0.]$$

<u>14:</u> NOTATION For any real number r, write

$$\{r\} = r - [r],$$

the <u>fractional part</u> of r.

[Note: $0 \leq \{r\} < 1$.]

<u>15:</u> BOX PRINCIPLE If $n + 1$ objects are placed in n boxes, then some box contains at least 2 objects.

<u>16:</u> CONSTRUCTION Let $n > 1$ be a positive integer and divide the interval

$[0,1]$ into n subintervals $[\frac{j}{n}, \frac{j+1}{n}]$ $(j = 0,1,\ldots,n-1)$. Assuming that x is irrational, the n + 1 numbers 0, $\{x\},\ldots, \{nx\}$ are distinct elements of $[0,1]$, hence by the Box Principle at least 2 of them must be in one of the subintervals $[\frac{j}{n}, \frac{j+1}{n}]$ $(j = 0,1,\ldots,n-1)$. Arrange matters in such a way that $\{j_1x\}$ and $\{j_2x\}$ $(j_2 > j_1)$ are contained in one subinterval of width $\frac{1}{n}$. Set

$$p = [j_2x] - [j_1x],\ q = j_2 - j_1 \geq 1 \quad (q < n).$$

Then

$$|\{j_2x\} - \{j_1x\}| < \frac{1}{n}$$

$$\Rightarrow$$

$$|(j_2 - j_1)x - ([j_2x] - [j_1x])| < \frac{1}{n}$$

$$\Rightarrow$$

$$|qx - p| < \frac{1}{n}$$

$$\Rightarrow$$

$$|x - \frac{p}{q}| < \frac{1}{nq} < \frac{1}{q^2}.$$

Existence per #13 is thereby established. To conclude, it has to be ruled out that there is just a finite number of coprime solutions to

$$|x - \frac{p}{q}| \leq \frac{1}{q^2},$$

say

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}.$$

Since x is irrational, there exists a positive integer $m > 1$ such that

$$|x - \frac{p_i}{q_i}| > \frac{1}{m} \quad (i = 1,2,\ldots,k).$$

In #16, replace n by m^2 and $\frac{p}{q}$ by $\frac{a}{b}$, thus

$$|x - \frac{a}{b}| < \frac{1}{m^2 b} < \frac{1}{b^2}.$$

On the other hand,

$$\frac{1}{m^2 b} < \frac{1}{m} \quad (b \geq 1),$$

so

$$|x - \frac{a}{b}| < \frac{1}{m}.$$

But

$$\frac{a}{b} = \frac{p_i}{q_i} \quad (\exists\ i)$$

which implies that

$$|x - \frac{a}{b}| > \frac{1}{m}.$$

Contradiction.

<u>17:</u> THEOREM Given $x = \frac{a}{b} \in Q$ ($a,b \in Z$, $b > 0$, $\gcd(a,b) = 1$), for any coprime pair (p,q) $(q > 0)$ with

$$\frac{a}{b} \neq \frac{p}{q}$$

there follows

$$\left|\frac{a}{b} - \frac{p}{q}\right| \geq \frac{1}{bq}.$$

PROOF

$$\frac{a}{b} \neq \frac{p}{q} \Rightarrow aq - bp \neq 0$$

$$\Rightarrow |aq - bp| \geq 1$$

$\Rightarrow$

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq - bp}{bq}\right|$$

$$= \frac{|aq - bp|}{|bq|}$$

$$= \frac{|aq - bp|}{bq}$$

$$\geq \frac{1}{bq}.$$

18: CRITERION Let $x \in R$. Assume: There exists a coprime sequence p_n, q_n ($q_n > 0$) such that $x \neq \frac{p_n}{q_n}$ for all n and $q_n x - p_n \not\to 0$ as $n \to \infty$ -- then x is irrational.

[Suppose instead that x is rational, say $x = \frac{a}{b}$ ($b > 0$, $\gcd(a,b) = 1$), thus

$$\frac{|q_n x - p_n|}{q_n} = \left|x - \frac{p_n}{q_n}\right|$$

$$= \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \geq \frac{1}{bq_n}$$

$\Rightarrow$

$$|q_n x - p_n| \geq \frac{1}{b} > 0.$$

But this is a contradiction since $q_n x - p_n \to 0$ by hypothesis.

<u>19:</u> CRITERION Let $x \in R$. Fix positive constants C and δ. Assume: There are infinitely many coprime solutions p,q $(q > 0)$ to

$$|x - \frac{p}{q}| < \frac{C}{q^{1+\delta}} .$$

Then x is irrational.

[The contrapositive is the assertion that for a rational x there are but finitely many coprime p,q $(q > 0)$ satisfying the stated inequality. Take x as $\frac{a}{b}$ per #17, hence

$$\frac{C}{q^{1+\delta}} > |x - \frac{p}{q}|$$

$$= \left|\frac{a}{b} - \frac{p}{q}\right|$$

$$\geq \frac{1}{bq}$$

=>

$$\frac{C}{q^{\delta}} > \frac{1}{b} \Rightarrow (Cb)^{1/\delta} > q.$$

Accordingly, there are but finitely many possibilities for q. The same is true of p. To see this, fix p and q subject to

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{C}{q^{1+\delta}}$$

and consider fractions of the form

$$\frac{p+r}{q} \quad (r \in Z).,$$

where

$$\left|\frac{a}{b} - \frac{p+r}{q}\right| < \frac{C}{q^{1+\delta}}.$$

Then

$$\frac{|r|}{q} = \left|\frac{r}{q} + \frac{p}{q} - \frac{a}{b} - \frac{p}{q} + \frac{a}{b}\right|$$

$$\leq \left|\frac{p+r}{q} - \frac{a}{b}\right| + \left|\frac{p}{q} - \frac{a}{b}\right|$$

$$< \frac{2C}{q^{1+\delta}}$$

=>

$$|r| < \frac{2C}{q^{\delta}} \leq 2C.$$

Our contention is therefore manifest.]

20: APPLICATION Let $x \in R$. Assume: There is a $\delta > 0$ and a sequence $\frac{p_n}{q_n}$ $(q_n > 0) \neq x$ of rational numbers such that

$$\left|x - \frac{p_n}{q_n}\right| = O\,(q_n^{-(1+\delta)}).$$

Then x is irrational.

APPENDIX

IRRATIONALITY CRITERIA Let x be a real number -- then the following conditions are equivalent.

(i) x is irrational.

(ii) $\forall\ \varepsilon > 0,\ \exists\ \frac{p}{q} \in Q$ such that

$$0 < \left|x - \frac{p}{q}\right| < \frac{\varepsilon}{q} .$$

(iii) $\forall$ real number $Q > 1$, $\exists$ an integer q in the range $1 \leq q < Q$ and a rational integer p such that

$$0 < \left|x - \frac{p}{q}\right| < \frac{1}{qQ} .$$

(iv) $\exists$ infinitely many $\frac{p}{q} \in \mathbb{Q}$ such that

$$\left|x - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\, q^2} .$$

§8. IRRATIONALITY OF e

Recall that e can be defined as

$$\sup\{\sum_{k=0}^{n} \frac{1}{k!}:n \in N\}$$

or, equivalently, as

$$\sup\{(1 + \frac{1}{n})^n:n \in N\}.$$

1: N.B.

$$\sum_{k=0}^{n} \frac{1}{k!} < \sum_{k=0}^{n+1} \frac{1}{k!} \text{ and } (1 + \frac{1}{n})^n < (1 + \frac{1}{n + 1})^{n+1}.$$

2: SUBLEMMA Let $0 < r < 1$ -- then

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1 - r},$$

so

$$\sum_{n=1}^{\infty} r^n = \frac{r}{1 - r}.$$

3: THEOREM e is irrational.

PROOF Suppose that e is rational, say $e = \frac{x}{y}$, where x and y are positive integers and $\gcd(x,y) = 1$. Since $2 < e < 3$, y is > 1. Write

$$e = (1 + \frac{1}{1!} + \cdots + \frac{1}{y!}) + \cdots .$$

Then

$$y!e = y! \frac{x}{y}$$

$$= (y - 1)!x$$

$$= (y! + \frac{y!}{1!} + \cdots + \frac{y!}{y!}) + R.$$

Here

$$R = y! \left(\frac{1}{(y + 1)!} + \frac{1}{(y + 2)!} + \cdots\right)$$

is a positive integer. Continuing,

$$y! \left(\frac{1}{(y + 1)!} + \frac{1}{(y + 2)!} + \cdots\right)$$

$$= \frac{1}{y + 1} + \frac{1}{(y + 1)(y + 2)} + \cdots$$

$$< \frac{1}{y + 1} + \frac{1}{(y + 1)^2} + \cdots$$

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

$$= \frac{\frac{1}{y + 1}}{1 - \frac{1}{y + 1}} = \frac{1}{y} < 1.$$

But this implies that R is less than 1, a contradiction.

[Note: The preceding is actually an instance of §7, #18. Thus take $q_n = n!$,

$p_n = q_n \sum_{k=0}^{n} \frac{1}{k!}$ -- then

$$q_n e - p_n = q_n \left(e - \sum_{k=0}^{n} \frac{1}{k!}\right)$$

$$= n! \left(\sum_{k=n+1}^{\infty} \frac{1}{k!}\right)$$

$$= \frac{1}{n+1} + \frac{1}{(n+1)(n+2)}$$

$$< \frac{1}{n} \text{ (cf. supra)}$$

$$\to 0 \ (n \to \infty).]$$

The foregoing argument can be extended to establish the irrationality of e^2. Thus start as before by assuming that $e^2 = \frac{x}{y}$, where x and y are positive integers and $\gcd(x,y) = 1$ $(y > 1)$, hence

$$ye = \frac{x}{e}$$

=>

$$y\left(\sum_{k=0}^{\infty} \frac{1}{k!}\right) = x\left(\sum_{k=0}^{\infty} (-1)^k \frac{1}{k!}\right)$$

=> $(\forall\, n \in \mathbb{N})$

$$y\left(\sum_{k=0}^{n} \frac{1}{k!} + \sum_{k>n} \frac{1}{k!}\right)$$

$$= x\left(\sum_{k=0}^{n} (-1)^k \frac{1}{k!} + \sum_{k>n} (-1)^k \frac{1}{k!}\right)$$

$$\equiv y\left(A_n + \sum_{k>n} \frac{1}{k!}\right) + x\left(B_n + \sum_{k>n} (-1)^k \frac{1}{k!}\right).$$

Now multiply both sides of the last relation by n! to get

$$y\left(C_n + n! \sum_{k>n} \frac{1}{k!}\right) = x\left(D_n + n! \sum_{k>n} (-1)^k \frac{1}{k!}\right),$$

$$\left[\begin{array}{l} C_n = n!A_n \\ D_n = n!B_n \end{array}\right.$$

being integers. Moving on,

$$yC_n + y\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right)$$

$$= xD_n + x(-1)^{n+1}\left(\frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \cdots\right)$$

or still,

$$yC_n - xD_n$$

$$= x(-1)^{n+1}\left(\frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \cdots\right)$$

$$- y\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right).$$

Therefore

$$|yC_n - xD_n|$$

$$\leq x\left|\frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \cdots\right|$$

$$+ y\left|\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right|$$

$$\leq x\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right)$$

$$+ y\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right)$$

$$< x\,\frac{1}{n} + y\,\frac{1}{n}$$

$$= \frac{x+y}{n}\,.$$

Finally, for all $n >> 0$,

$$\frac{x+y}{n} < 1.$$

I.e.: For an infinite set of n,

$$|yC_n - xD_n| = 0,$$

or still, for an infinite set of n,

$$yC_n = xD_n,$$

an impossibility.

4: DEFINITION An irrational number r is a quadratic irrational if there exist integers A, B, C not all zero such that

$$Ar^2 + Br + C = 0.$$

[Note: A quadratic irrational is necessarily algebraic.]

5: EXAMPLE $\sqrt{2}$ is a quadratic irrational.

6: THEOREM e is not a quadratic irrational.

The proof is detailed in the lines below.

To arrive at a contradiction, suppose that there are integers A, B, C not all zero such that

$$Ae^2 + Be + C = 0.$$

7: N.B. If $A = 0$, matters are clear. If $A \neq 0$ and if $B = 0$, matters are clear. If $A \neq 0$ and if $B \neq 0$ and if $C = 0$, matters are clear. One can accordingly assume from the beginning that $A \neq 0$, $B \neq 0$, $C \neq 0$. Moreover, we shall work instead with the equation

$$Ae + B + \frac{C}{e} = 0.$$

8: SUBLEMMA Given $n \in \mathbb{N}$, there is an integer I_n such that

$$n!e = I_n + \frac{1}{n + \alpha_n},$$

where $0 < \alpha_n < 1$.

PROOF Write

$$n!e = \sum_{k=0}^{n} \frac{n!}{k!} + \sum_{k=n+1}^{\infty} \frac{n!}{k!}.$$

- $$\sum_{k=n+1}^{\infty} \frac{n!}{k!} = \frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \cdots$$

$$> \frac{n!}{(n+1)!} = \frac{1}{n+1}.$$

- $$\sum_{k=n+1}^{\infty} \frac{n!}{k!} = \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots$$

$$< \frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots$$

$$= \frac{1}{n}.$$

Therefore

$$\frac{1}{n+1} < \sum_{k=n+1}^{\infty} \frac{n!}{k!} < \frac{1}{n},$$

from which

$$\sum_{k=n+1}^{\infty} \frac{n!}{k!} = \frac{1}{n + \alpha_n} \quad (0 < \alpha_n < 1).$$

To conclude, it remains only to set

$$I_n = \sum_{k=0}^{n} \frac{n!}{k!}.$$

<u>9:</u> SUBLEMMA Given $n \in \mathbb{N}$, there is an integer J_n such that

$$\frac{n!}{e} = J_n + \frac{(-1)^{n+1}}{n+1+\beta_n},$$

where $0 < \beta_n < 1$.

PROOF Write

$$\frac{n!}{e} = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} + \sum_{k=n+1}^{\infty} (-1)^k \frac{n!}{k!}.$$

- $$\sum_{k=n+1}^{\infty} (-1)^k \frac{n!}{k!} = \sum_{\ell=0}^{\infty} (-1)^{\ell + (n+1)} \frac{n!}{(\ell + (n+1))!}$$

$$= (-1)^{n+1} \sum_{\ell=0}^{\infty} (-1)^{\ell} \frac{n!}{(\ell + (n+1))!} \equiv (-1)^{n+1} S.$$

Put

$$S_N = \sum_{\ell=0}^{N} (-1)^{\ell} \frac{n!}{(\ell + (n+1))!}.$$

Then

$$S_N < S < S_{N+1}.$$

In particular ($N = 1$):

$$\frac{1}{n+1} - \frac{1}{(n+1)(n+2)} < S < \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)}.$$

- $$\frac{1}{n+1} - \frac{1}{(n+1)(n+2)}$$

$$= \frac{1}{n+1}\left(1 - \frac{1}{n+2}\right) = \frac{1}{n+2}$$

and

$$\frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)}$$

$$= \frac{1}{n+1} \left(1 - \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} \right)$$

$$= \frac{1}{n+1} \left(1 + \frac{1}{n+2} \left(- 1 + \frac{1}{n+3}\right)\right)$$

$$= \frac{1}{n+1} \left(1 + \frac{1}{n+2} \left(\frac{- n - 3 + 1}{n+3}\right)\right)$$

$$= \frac{1}{n+1} \left(1 + \frac{1}{n+2} \left(\frac{- n - 2}{n+3}\right)\right)$$

$$= \frac{1}{n+1} \left(1 - \frac{1}{n+3}\right) < \frac{1}{n+1} .$$

Therefore

$$\frac{1}{n+2} < S < \frac{1}{n+1} \Rightarrow S = \frac{1}{n+1+\beta_n} \quad (0 < \beta_n < 1).$$

And then

$$\sum_{k=n+1}^{\infty} (-1)^k \frac{n!}{k!} = (-1)^{n+1} S = \frac{(-1)^{n+1}}{n+1+\beta_n} .$$

To conclude, let

$$J_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} .$$

Summary:

$$\left[\begin{array}{l} n!e - I_n = o\left(\frac{1}{n}\right) \\ \\ \frac{n!}{e} - J_n = o\left(\frac{1}{n}\right). \end{array}\right.$$

Return now to the equation

$$Ae + B + \frac{C}{e} = 0$$

and consider

$$A(n!e - I_n) + C(\frac{n!}{e} - J_n)$$

$$= n!(Ae + B + \frac{C}{e}) - (AI_n + Bn! + CJ_n)$$

$$= -(AI_n + Bn! + CJ_n)$$

$$\equiv - K_n.$$

Then K_n is an integer. But

$$K_n = O(\frac{1}{n}).$$

Therefore

$$K_n = 0 \quad (n >> 0).$$

10: SUBLEMMA

$$K_{n+2} - (n + 1)(K_n + K_{n+1}) = 2A.$$

[Use the relations

$$\begin{cases} I_{n+1} = 1 + (n + 1)I_n \\ J_{n+1} = (-1)^{n+1} + (n + 1)J_n.] \end{cases}$$

Since $A \neq 0$, the relation figuring in #10 is impossible for $n >> 0$. And this contradiction closes out the proof of #6.

11: SCHOLIUM $1, e, e^2$ are linearly independent over Q.

APPENDIX

EXAMPLE 1 Suppose that r is a nonzero rational -- then the number

$$\sum_{k=0}^{\infty} \frac{r^k}{2^{k(k-1)/2}} = 1 + r + \frac{1}{2} r^2 + \frac{1}{8} r^3 + \cdots$$

is irrational.

EXAMPLE 2 Suppose that r is a nonzero rational subject to $0 < |r| < 1$ -- then the number

$$\sum_{k=0}^{\infty} r^{2^k} = r + r^2 + r^4 + r^8 + \cdots$$

is irrational.

EXAMPLE 3 Suppose that M is an integer ≥ 2 -- then the number

$$\sum_{k=1}^{\infty} \frac{1}{M^{k^2}}$$

is irrational.

§9. *IRRATIONALITY OF* $e^{a/b}$

Let a/b be a nonzero rational number.

1: THEOREM $e^{a/b}$ is irrational.

[Note: Special cases, namely e and e^2 are irrational, as has been shown in §8.]

2: LEMMA If e^r is irrational for all integers $r \geq 1$, then $e^{a/b}$ is irrational for all nonzero rationals a/b.

PROOF Take $a \in N$ and suppose that $e^{a/b}$ is rational, say $e^{a/b} = q \in Q$ -- then

$$e^a = (e^{a/b})^b = q^b \in Q.$$

Working toward a contradiction, assume that for some $r \in N$, e^r is rational and choose a positive integer m with the property that $me^r \in N$.

The data in place, we shall now introduce the machinery that will be utilized to arrive at our objective.

3: NOTATION Given $n \in N$, let

$$T_n(X) = \prod_{j=n+1}^{2n} (X - j),$$

an element of $Z[X]$.

4: RAPPEL

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Put

$$\delta = x\frac{d}{dx} .$$

5: SUBLEMMA

$$T_n(\delta)x^k = T_n(k)x^k.$$

6: LEMMA

$$T_n(\delta)e^x = Q_n(x)e^x = (x^n + \cdots)e^x$$

$$= P_n(x) + R_n(x),$$

where

$$P_n(x) = \sum_{k=0}^{n} T_n(k) \frac{x^k}{k!} = (-1)^n \sum_{k=0}^{n} \frac{(2n-k)!}{n!} \binom{n}{k} x^k$$

and

$$R_n(x) = \sum_{k=n+1}^{\infty} T_n(k) \frac{x^k}{k!}$$

$$= \sum_{k=2n+1}^{\infty} T_n(k) \frac{x^k}{k!} = \sum_{k=2n+1}^{\infty} \frac{(k-n-1)!}{(k-2n-k)!} \frac{x^k}{k!} .$$

7: N.B.

$$\left[\begin{array}{l} Q_n(x) \in Z[x] \\ \\ P_n(x) \in Z[x]. \end{array}\right.$$

Accordingly, at an $r \in N$,

$$\left[\begin{array}{l} Q_n(r) \in Z \\ \\ P_n(r) \in Z. \end{array}\right.$$

8: REMAINDER ESTIMATE

$$|R_n(x)| \le \frac{n!}{(2n+1)!} \sum_{k=2n+1}^{\infty} \frac{|x|^k}{(k-2n-1)!}$$

$$= \frac{n!\,|x|^{2n+1}}{(2n+1)!} e^{|x|}.$$

Returning to the situation above, we claim that for sufficiently large n,

$$0 < mR_n(r) < 1.$$

To see this, consider

$$\frac{n!r^{2n+1}}{(2n+1)!} e^r = \frac{n!}{(2n+1)!} r^{2n}(re^r).$$

Then

$$\frac{n!}{(2n+1)!} r^{2n} = \frac{n!}{n!} \cdot \frac{r^2}{n+1} \cdot \frac{r^2}{n+2} \cdots \frac{r^2}{n+n} \cdot \frac{1}{2n+1}$$

$$= \frac{r^2}{n+1} \cdot \frac{r^2}{n+2} \cdots \frac{r^2}{n+n} \cdot \frac{1}{2n+1}.$$

Choose $n >> 0$:

$$\frac{r^2}{n+1} < 1,$$

thus

$$\frac{n!}{(2n+1)!} r^{2n} < \frac{1}{2n+1},$$

from which the claim is immediate.

On the other hand,

$$mR_n(r) = \underline{\underline{m}}(Q_n(r)e^r - P_n(r))$$

$$= (me^r)Q_n(r) - mP_n(r)$$

$$\in \mathbb{Z}.$$

But there are no integers between 0 and 1.

9: REMARK It will be shown in due course that if $x \neq 0$ is algebraic, then e^x is irrational, so, e.g., $e^{\sqrt{2}}$ is irrational.

APPENDIX

$0 \leq k \leq n$: Here

$$(-1)^n \frac{(2n-k)!}{n!} \binom{n}{k}$$

$$= (-1)^n \frac{(2n-k)!}{n!} \frac{n!}{k!(n-k)!}$$

$$= (-1)^n \frac{(2n-k)!}{(n-k)!} \frac{1}{k!}$$

and the claim is that

$$T_n(k) = (-1)^n \frac{(2n-k)!}{(n-k)!}.$$

[• $k = 0$:

$$T_n(0) = \prod_{j=n+1}^{2n} (0-j)$$

$$= -(n+1)(-(n+2)) \cdots (-(2n))$$

$$= (-1)^n (n+1)(n+2) \cdots (2n)$$

$$= (-1)^n \frac{2n!}{n!}.$$

- $k = 1$:

$$T_n(1) = \prod_{j=n+1}^{2n} (1 - j)$$

$$= (1 - (n + 1))\ (1 - (n + 2))\ \cdots\ (1 - (2n))$$

$$= (-n).(-n - 1)\ \cdots\ (-(2n - 1))$$

$$= (-1)^n\ (n)\,(n + 1)\ \cdots\ (2n - 1)$$

$$= (-1)^n \frac{(2n - 1)!}{(n - 1)!}$$

. . . .

- $k = n$:

$$T_n(n) = \prod_{j=n+1}^{2n} (n - j)$$

$$= (n - (n + 1))\,(n - (n + 2))\ \cdots\ (n - (2n))$$

$$= (-1)\,(-2)\ \cdots\ (-n)$$

$$= (-1)^n\ n!$$

$$= (-1)^n \frac{(2n - n)!}{(n - n)!}\ .]$$

<u>$2n + 1 \leq k < \infty$:</u> In this situation, the claim is that

$$T_n(k) = \frac{(k - n - 1)!}{(k - 2n - 1)!}\ .$$

[• $k = 2n + 1$:

$$T_n(2n + 1) = \prod_{j=n+1}^{2n} (2n + 1 - j)$$

$$= (2n + 1 - (n + 1))(2n + 1 - (n + 2))(2n + 1 - 2n)$$

$$= (n)(n - 1) \cdots (1)$$

$$= n!$$

$$= \frac{(2n + 1 - n - 1)!}{(2n + 1 - 2n - 1)!}\,.$$

• $k = 2n + 2$:

$$T_n(2n + 2) = \prod_{j=n+1}^{2n} (2n + 2 - j)$$

$$= (2n + 2 - (n + 1))(2n + 2 - (n + 2))\cdots(2n + 2 - 2n)$$

$$= (n + 1)(n) \cdots (2)$$

$$= (n + 1)!$$

$$= \frac{(2n + 2 - n - 1)!}{(2n + 2 - 2n - 1)!}$$

. . . .

To prove the remainder estimate, one has to show that

$$\frac{(k - n - 1)!}{k!} \leq \frac{n!}{(2n + 1)!} \quad (k \geq 2n + 1).$$

Let $k = 2n + r$ $(r = 1,2,\ldots)$ and take $r > 1$ -- then

$$\frac{(k - n - 1)!}{k!} = \frac{(2n + r - n - 1)!}{(2n + r)!}$$

$$= \frac{(n + r - 1)!}{(2n + r)!}$$

$$= \frac{(n + r - 1)!}{(2n + 1)!(2n + 2)\cdots(2n + r)} .$$

Cancelling the

$$\frac{1}{(2n + 1)!} ,$$

there remains the claim that

$$\frac{(n + r - 1)!}{(2n + 2)\cdots(2n + r)} \leq n! .$$

Write

$$(n + r - 1)!$$

$$= 1 \cdot 2 \cdots (n - 1)(n + 1 - 1)(n + 2 - 1) \cdots (n + r - 1)$$

$$= (n - 1)!(n + 1 - 1)(n + 2 - 1) \cdots (n + r - 1).$$

Cancelling the $(n - 1)!$, matters thus reduce to

$$\frac{(n + 1 - 1)(n + 2 - 1) \cdots (n + r - 1)}{(2n + 2) \cdots (2n + r)} \leq n$$

or still,

$$\frac{(n + 2 - 1) \cdots (n + r - 1)}{(2n + 2) \cdots (2n + r)} \leq 1,$$

which is obvious.

§10. *IRRATIONALITY OF* $e^{a/b}$ (bis)

There is another way to prove that $e^{a/b}$ is irrational (a/b a nonzero rational number). Thus, proceeding as in §9, suppose that for some $r \in \mathbb{N}$, e^r is rational, say $e^r = \frac{u}{v}$ ($u,v \in \mathbb{Z}$, $v > 0$).

Let
$$f(x) = \frac{x^n(1-x)^n}{n!}.$$
Then
$$0 < x < 1 \Rightarrow 0 < f(x) < \frac{1}{n!}.$$

<u>1:</u> LEMMA

$$f^{(j)}(0) \in \mathbb{Z} \quad (j = 1,2,\ldots).$$

<u>2:</u> <u>N.B.</u>

$$f^{(j)}(1) \in \mathbb{Z} \quad (j = 1,2,\ldots).$$

[This is because
$$f(1-x) = f(x).]$$

Given $n \in \mathbb{N}$, put
$$F(x) = r^{2n} f(x) - r^{2n-1} f'(x) + r^{2n-2} f''(x) - \cdots - rf^{(2n-1)}(x) + f^{(2n)}(x),$$
and note that
$$F(0),\ F(1) \in \mathbb{Z}.$$

Obviously
$$\frac{d}{dx}(e^{rx}F(x)) = e^{rx}(rF(x) + F'(x)) = r^{2n+1} e^{rx} f(x)$$

=>

$$vr^{2n+1} \int_0^1 e^{rx} f(x)\,dx = r(e^{rx}F(x)\Big|_0^1$$

$$= v(e^r F(1)) - vF(0)$$

$$= uF(1) - vF(0),$$

an integer. On the other hand,

$$0 < vr^{2n+1} \int_0^1 e^{rx} f(x)\,dx$$

$$< \frac{vr^{2n+1}\ e^r}{n!}$$

$$= vre^r \frac{(r^2)^n}{n!} < 1$$

for $n >> 0$ (cf. §0), giving a contradiction.

This is a good place to insert an application.

<u>3:</u> DEFINITION The <u>natural logarithm</u> is $\log_e$.

<u>4:</u> NOTATION Write ℓn in place of $\log_e$.

<u>5:</u> THEOREM If $q \neq 1$ is rational and positive, then $\ell n(q)$ is irrational.

PROOF Suppose that $\ell n(q)$ is rational -- then $e^{\ell n(q)}$ is irrational. Meanwhile

$$q = e^{\ell n(q)}.$$

<u>6:</u> SCHOLIUM If $x \neq 1$ is a positive real number and if $\ell n(x)$ is rational, then x is irrational.

APPENDIX

Let $a \neq 1$, $b \neq 1$ be positive real numbers -- then

$$\log_a(b)\ell n(a) = \ell n(a^{\log_a(b)})$$

$$= \ell n(b),$$

so

$$\log_a(b) = \frac{\ell n(b)}{\ell n(a)}.$$

EXAMPLE

$$\log_3 9 = \frac{\ell n(9)}{\ell n(3)} = \frac{\ell n(3^2)}{\ell n(3)} = 2\,\frac{\ell n(3)}{\ell n(3)} = 2.$$

§11. IRRATIONALITY OF π

There are many ways to introduce the number π.

1: DEFINITION Geometrically, π is the length of a semicircle of radius one, i.e., analytically,

$$\pi = \int_{-1}^{1} \frac{dx}{\sqrt{1 - x^2}} .$$

2: THEOREM Consider the complex exponential function

$$\exp : \mathbf{C} \to \mathbf{C}.$$

Then π is the unique positive real number with the property that

$$\operatorname{Ker}(\exp) = 2\pi \sqrt{-1}\, \mathbf{Z}.$$

3: THEOREM π is the unique positive real number such that $\cos \frac{\pi}{2} = 0$ and $\cos x \neq 0$ for $0 \leq x < \frac{\pi}{2}$.

4: THEOREM π is irrational.

We shall give four proofs of this result.

First Proof: Suppose that $\pi = \frac{a}{b}$, where a and b are positive integers. Introduce

$$f(x) = \frac{x^n (a - bx)^n}{n!}$$

and

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x),$$

$n \in \mathbb{N}$ to be determined momentarily. Note that $f^{(j)}(0) \in \mathbb{Z}$ $(j = 1,2,\ldots)$, hence $f^{(j)}(\pi) \in \mathbb{Z}$ $(j = 1,2,\ldots)$ (since $f(x) = f(\frac{a}{b} - x) = f(\pi - x)$). Next

$$\frac{d}{dx}(F'(x)\sin x - F(x)\cos x)$$

$$= F''(x)\sin x + F(x)\sin x$$

$$= f(x)\sin x \quad (\text{since } F(x) + F''(x) = f(x)).$$

Therefore

$$\int_0^\pi f(x)\sin x\,dx = (F'(x)\sin x - F(x)\cos x\,\Big|_0^\pi$$

$$= F(\pi) + F(0).$$

But $F(\pi) + F(0)$ is an integer. On the other hand,

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!} \quad (0 \leq x \leq \pi),$$

so

$$\int_0^\pi f(x)\sin x\,dx < \pi\,\frac{\pi^n a^n}{n!}$$

is positive and tends to zero as $n \to \infty$ (cf. §0).

<u>Second Proof:</u> This proof is a slightly more complicated variant of the preceding proof and has the merit that it establishes the stronger result that π^2 is irrational. Proceeding to the details, suppose that $\pi^2 = \frac{a}{b}$, where a and b are positive integers but this time introduce

$$f(x) = \frac{x^n(1 - x)^n}{n!},$$

a polynomial encountered earlier (cf. §10). Put

$$F(x) = b^n\{\pi^{2n} f(x) - \pi^{2n-2} f^{(2)}(x) + \pi^{2n-4} f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x)\}$$

and note that

$$F(0),\ F(1) \in \mathbb{Z}.$$

Moreover

$$\frac{d}{dx}\{F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\}$$

$$= (F^{(2)}(x) + \pi^2 F(x))\sin(\pi x)$$

$$= b^n \pi^{2n+2} f(x)\sin(\pi x)$$

$$= \pi^2 a^n f(x)\sin(\pi x).$$

Therefore

$$\pi a^n \int_0^1 f(x)\sin(\pi x)\,dx$$

$$= \left(\frac{F'(x)\sin(\pi x)}{\pi} - F(x)\cos(\pi x)\right\rvert_0^1$$

$$= F(1) + F(0),$$

an integer. On the other hand,

$$0 < \pi a^n \int_0^1 f(x)\sin(\pi x)\,dx < \frac{\pi a^n}{n!} < 1$$

if $n >> 0$, from which the usual contradiction.

Third Proof: Let

$$I_n = \int_{-1}^1 (1 - x^2)^n \cos\left(\frac{\pi x}{2}\right)dx \quad (n = 0,1,2,\ldots).$$

Then for $-1 < x < 1$,

$$0 < (1 - x^2)^n \cos(\frac{\pi x}{2}) < 1$$

$$\Rightarrow 0 < I_n < 2.$$

In addition, there is a recurrence relation, viz.

$$\frac{\pi^2}{4} I_n = 2n(2n - 1)I_{n-1} - 4n(n-1)I_{n-2} \quad (n \geq 2),$$

as can be seen by integration by parts (twice). Using this, it follows via induction that

$$(\frac{\pi}{2})^{2n+1} I_n = n!P_n,$$

where P_n is a polynomial in $\frac{\pi^2}{4}$ with integral coefficients of degree $[\frac{n}{2}]$:

$$(\frac{\pi}{2})^{2n+3} I_{n+1}$$

$$= (\frac{\pi}{2})^{2n+3} (\frac{2}{\pi})^2 \{2(n + 1)(2n + 1)I_n - 4(n + 1)n\ I_{n-1}\}$$

$$= (\frac{\pi}{2})^{2n+1} \{2(n + 1)(2n + 1)I_n - 4(n + 1)n\ I_{n-1}\}$$

$$= 2(n + 1)(2n + 1)(\frac{\pi}{2})^{2n+1} I_n - 4(n + 1)n(\frac{\pi}{2})^2 (\frac{\pi}{2})^{2n-1} I_{n-1}$$

$$= 2(n + 1)(2n + 1)n!P_n - 4(n + 1)n(\frac{\pi^2}{4})(n - 1)!\ P_{n-1},$$

the degree being that of the second term, i.e.,

$$1 + \left[\frac{n - 1}{2}\right] = \left[1 + \frac{(n - 1)}{2}\right] = \left[\frac{n + 1}{2}\right].$$

Suppose now that $\frac{\pi^2}{4} = \frac{a}{b}$, where a and b are positive integers -- then

$$(\frac{\pi^2}{4})^{2n+1} I_n^2 = (n!)^2 (P_n)^2$$

=>

$$(\frac{a}{b})^{2n+1} I_n^2 = (n!)^2 (P_n)^2$$

=>

$$\frac{a^{2n+1}}{(n!)^2} I_n^2 = b^{2n+1} (P_n)^2.$$

But P_n is a polynomial in $\frac{a}{b}$ with integral coefficients of degree $\left[\frac{n}{2}\right]$, hence the degree of $(P_n)^2$ is $2\left[\frac{n}{2}\right] < 2n + 1$, hence $b^{2n+1}(P_n)^2$ is an integer. To get the contradiction, simply note that

$$0 < \frac{a^{2n+1}}{(n!)^2} I_n^2 < 4a \frac{(a^2)^n}{n!} \rightarrow 0 \quad (n \rightarrow \infty) \quad (\text{cf. §0}).$$

<u>Fourth Proof:</u> The machinery employed in §9 can also be used to establish that π is irrational. So assume once again that $\pi = \frac{a}{b}$, where a and b are positive integers, and let $z_0 = \pi b \sqrt{-1} = a \sqrt{-1}$ -- then

$$\begin{aligned} R_n(z_0) &= Q_n(a \sqrt{-1}) e^{\pi b \sqrt{-1}} - P_n(a \sqrt{-1}) \qquad (\text{cf. §9, \#6}) \\ &= Q_n(a \sqrt{-1}) (e^{\pi\sqrt{-1}})^b - P_n(a \sqrt{-1}) \\ &= Q_n(a \sqrt{-1}) (-1)^b - P_n(a \sqrt{-1}), \end{aligned}$$

an element of $Z[\sqrt{-1}]$. Replacing x by z_0 in §9, #8 (a formal maneuver), it follows that

$$R_n(z_0) = 0 \quad (n >> 0).$$

Next

$$\Delta(x) \equiv Q_n(x)R_{n+1}(x) - Q_{n+1}(x)R_n(x)$$

$$= Q_n(x)\,(Q_{n+1}(x)e^x - P_{n+1}(x))$$

$$- Q_{n+1}(x)\,(Q_n(x)e^x - P_n(x))$$

$$= - Q_n(x)P_{n+1}(x) + Q_{n+1}(x)P_n(x)$$

$$= 2(-1)^n x^{2n+1}.$$

Therefore $\Delta(z_0) \neq 0$. Meanwhile

$$R_n(z_0) = R_{n+1}(z_0) = 0 \quad (n >> 0).$$

§12. *IRRATIONALITY OF* cos(x)

Let x be a nonzero rational number.

1: THEOREM cos(x) is irrational.

2: APPLICATION π is irrational.

[Suppose that π is rational -- then $\cos(\pi)$ is irrational. But $\cos(\pi) = -1\ldots$.]

3: LEMMA Let $g(X) \in Z[X]$ and put

$$f(X) = \frac{X^n}{n!} g(X) \quad (n \in N).$$

Then $\forall\, j \in N$,

$$f^{(j)}(0) \in Z,$$

and in addition,

$$(n + 1) \mid f^{(j)}(0)$$

except perhaps for $j = n$ $(f^{(n)}(0) = g(0))$.

Let $a,b \in N$ $(\gcd(a,b) = 1)$ and let $p > a$ be an odd prime.

Put

$$f(X) = \frac{X^{p-1}}{(p - 1)!} g(X),$$

where

$$g(X) = (a - bX)^{2p}(2a - bX)^{p-1}.$$

Then #3 is applicable (take $n = p - 1$), hence $\forall\, j \in N$,

$$f^{(j)}(0) \in Z,$$

and in addition,

$$p \mid f^{(j)}(0)$$

except perhaps for $j = p - 1$.

FACT

$$f^{(p-1)}(0) = g(0) = a^{2p}(2a)^{p-1} = 2^{p-1}a^{3p-1}$$

$$\Rightarrow$$

$$p \nmid f^{(p-1)}(0).$$

<u>4:</u> LEMMA Given a real number r, suppose that $\phi(X) \in Z[(r - X)^2]$, i.e.,

$$\phi(X) = a_{2n}(r - X)^{2n} + a_{2n-2}(r - X)^{2n-2}$$

$$+ \cdots + a_2(r - X)^2 + a_0.$$

Then for any positive odd integer k, $f^{(k)}(r) = 0$.

To ensure the applicability of #4, take $r = \frac{a}{b}$ and note that

$$f(X) = \frac{(r - X)^{2p}(r^2 - (r - X)^2)^{p-1}}{(p - 1)!} b^{3p-1}$$

$$\in Z[(r - X)^2].$$

Turning now to the proof of #1, it suffices to establish that $\cos(x)$ $(x > 0)$ is irrational. This said, assume that $x = \frac{a}{b}$, where $a,b \in N$ $(\gcd(a,b) = 1)$. Working with $f(X)$ per supra ($p > a$ an odd prime), introduce

$$F(X) = f(X) - f^{(2)}(X) + f^{(4)}(X) - \cdots - f^{(4p-2)}(X).$$

Then

$$F^{(2)}(X) + F(X) = f(X).$$

Moreover

$$\frac{d}{dX}(F'(X)\sin(X) - F(X)\cos(X))$$

$$= F^{(2)}(X)\sin(X) + F(X)\sin(X)$$

$$= f(X)\sin(X)$$

$\Rightarrow$

$$\int_0^x f(X)\sin(X)dX = F'(x)\sin(x) - F(x)\cos(x) + F(0).$$

From here, the procedure is to investigate the three terms on the right and see how the supposition that $\cos(x)$ is rational leads to a contradiction.

- $f^{(2j+1)}(x) = 0 \Rightarrow F'(x) = 0.$
- $f^{(j)}(0) \in Z \Rightarrow F(0) \in Z.$
- $p|f^{(j)}(0) \quad (j \neq p - 1).$
- $p \nmid f^{(p-1)}(0).$
- $F(0) = q \quad (\gcd(p,q) = 1).$

So far then

$$\int_0^x f(X)\sin(X)dX = - F(x)\cos(x) + q.$$

Observe next that $f(X)$ can be viewed as a function of the variable $y = x - X$:

$$f(X) = h(Y)$$

$$= \frac{Y^{2p}(x^2 - Y^2)^{p-1}}{(p - 1)!} b^{3p-1}$$

$$= \frac{Y^{p-1}Y^{p+1}(x^2 - Y^2)^{p-1}}{(p - 1)!} b^{3p-1}$$

$$= \frac{Y^{p-1}}{(p - 1)!} (Y^{p+1}(x^2 - Y^2)^{p-1}) b^{3p-1}.$$

FACT $\forall j \in N$,

$$f^{(j)}(x) = h^{(j)}(0).$$

In view of #3, the $h^{(j)}(0)$ are divisible by p with the possible exception of $h^{(p-1)}(0)$. But here

$$h^{(p-1)}(0) = (Y^{p+1}(x^2 - Y^2)^{p-1}) \Big|_{Y = 0} b^{3p-1}$$

$$= 0.$$

Therefore

$$F(x) = mp$$

for some $m \in Z$.

Assume henceforth that

$$\cos(x) = \frac{c}{d} \quad (c,d \in Z,\ d > 0).$$

Then

$$\int_0^x f(X)\sin(X)dX = - mp(\tfrac{c}{d}) + q$$

or still,

$$d\int_0^x f(X)\sin(X)dX = - mpc + dq.$$

However for $0 < X < x$,

$$0 < f(X) < \frac{x^{2p}(x^2)^{p-1}}{(p - 1)!} b^{3p-1}$$

$$= \frac{x^{4p-2}}{(p-1)!} b^{3p-1}$$

=>

$$\left| d \int_0^x f(X) \sin(X) dX \right|$$

$$= d \left| \int_0^x f(X) \sin(X) dX \right|$$

$$\leq d \int_0^x |f(X)| \, |\sin(X)| dX$$

$$= d \int_0^x f(X) \, |\sin(X)| dX$$

$$\leq d \int_0^x f(X) dX$$

$$< dx \frac{x^{4p-2}}{(p-1)!} b^{3p-1}$$

$$= dx^3 b^2 \frac{(x^4 b^3)^{p-1}}{(p-1)!}$$

$$= \frac{K_1 K_2^{p-1}}{(p-1)!},$$

where

$$K_1 = dx^3 b^2 \text{ and } K_2 = x^4 b^3.$$

Since

$$\lim_{p \to \infty} \frac{K_2^{p-1}}{(p-1)!} = 0 \quad (\text{cf. } \S 0),$$

it follows that

$$\lim_{p \to \infty} d \int_0^x f(X) \sin(X) dX = 0.$$

To arrive at a contradiction, choose $p >> 0$:

$$-mpc + dq \in \mathbb{Z} - \{0\}$$

while simultaneously

$$\left|d\int_0^x f(X)\sin(X)dX\right| < 1.$$

<u>5:</u> APPLICATION The values of the trigonometric functions are irrational at any nonzero rational value of the argument.

[E.g.: If $\sin(x) \in \mathbb{Q}$ for some $0 \neq x \in \mathbb{Q}$, then

$$\cos(2x) = 1 - 2\sin^2(x) \in \mathbb{Q}$$

$$\ldots .]$$

<u>6:</u> <u>N.B.</u> The squares of these numbers are irrational.

[E.g.:

$$\cos^2(x) = \frac{1 + \cos(2x)}{2} .]$$

§13. *IRRATIONALITY OF* cosh(x).

Let x be a nonzero rational number.

1: THEOREM cosh(x) is irrational.

The proof is similar to that in the trigonometric case. Thus, as there, assume that $x = \frac{a}{b}$, where $a,b \in \mathbb{N}$ $(\gcd(a,b) = 1)$ and define $f(X)$ as before. But this time let

$$F(X) = f(X) + f^{2}(X) + f^{4}(X) + \cdots + f^{(4p-2)}(X).$$

Then

$$F(X) - F^{(2)}(X) = f(X).$$

Moreover

$$\frac{d}{dX}(F(X)\cosh(X) - F'(X)\sinh(X))$$

$$= F(X)\sinh(X) - F^{(2)}(X)\sinh(X)$$

$$= f(X)\sinh(X)$$

$\Rightarrow$

$$\int_0^x f(X)\sinh(X)dX = F(x)\cosh(x) - F'(x)\sinh(x) - F(0).$$

Note that for $0 < X < x$,

$$f(X) > 0 \text{ and } \sinh(X) > 0,$$

thus the integral on the left hand side is positive, a point that serves to simplify matters.

Proceeding,

$$F'(x) = 0,\ F(x) \in \mathbb{Z},\ \text{and } F(0) \in \mathbb{Z}.$$

Assume henceforth that

$$\cosh(x) = \frac{c}{d} \ (c,d \in Z,\ d > 0).$$

Then

$$\int_0^x f(X)\sinh(X)dX = F(x)\ \frac{c}{d} - F(0)$$

or still,

$$d\int_0^x f(X)\sinh(X)dX = cF(X) - dF(0).$$

The RHS is an integer while the LHS admits the estimate

$$0 < d\int_0^x f(X)\sinh(X)dX$$

$$< dx\ \frac{x^{4p-2}b^{3p-1}}{(p-1)!} \cdot \frac{e^x - e^{-x}}{2}$$

$$= \frac{dx^3b^2(e^x - e^{-x})}{2} \cdot \frac{(x^4b^3)^{p-1}}{(p-1)!}$$

which is < 1 if p > > 0 (for this, p could have been any positive integer). Contradiction.

<u>2:</u> APPLICATION The values of the hyperbolic functions are irrational at any nonzero rational value of the argument.

[Use the identities

$$\cosh(2X) = 1 + 2\sinh^2(X)$$

$$= \frac{1 + \tanh^2(X)}{1 - \tanh^2(X)}\ .]$$

§14. ALGEBRAIC AND TRANSCENDENTAL NUMBERS

1: DEFINITION A complex number x is said to be an algebraic number if it is the zero of a nonzero polynomial $P(X)$ in $Z[X]$.

2: EXAMPLE $\sqrt{-1}$ is algebraic (consider $P(X) = X^2 + 1$).

3: N.B. If x is algebraic, then so is its complex conjugate $\bar{x}$ and its absolute value $|x|$.

4: N.B. If $x = a + \sqrt{-1}\, b$ $(a,b \in R)$, then x is algebraic iff both a and b are algebraic.

5: NOTATION $\bar{Q}$ is the algebraic closure of Q in C.

6: LEMMA $\bar{Q}$ is a countable subfield of C.

7: LEMMA Suppose that x is an algebraic number — then there is a unique nonzero polynomial $f_x \in Z[X]$ such that $f_x(x) = 0$, f_x is irreducible in $Q[X]$, the leading coefficient of f_x is positive, and the coefficients of f_x have greatest common divisor 1.

[Note: Spelled out,

$$f_x(X) = a_0 + a_1 X + \cdots + a_n X^n \quad (a_n > 0)$$

with

$$\gcd(a_0, a_1, \ldots, a_n) = 1.]$$

8: DEFINITION The polynomial f_x is called the minimal polynomial of x.

Its degree is the <u>degree $d(x)$</u> of x, hence

$$d(x) = [Q(x):Q].$$

[Note: The set of real algebraic numbers of fixed degree n (≥ 2) is dense in R.]

<u>9:</u> DEFINITION The zeros of f_x are called the <u>conjugates</u> of x.

[Note: They too are, of course, algebraic.]

<u>10:</u> EXAMPLE Take x rational, say $x = \frac{a}{b}$ $(a,b \in Z,\ b > 0,\ \gcd(a,b) = 1)$ -- then

$$f_x(X) = bX - a.$$

<u>11:</u> DEFINITION An algebraic number x is said to be an <u>algebraic integer</u> if its minimal polynomial f_x has leading coefficient 1.

<u>12:</u> EXAMPLE $\sqrt{5}$ is an algebraic integer (consider $X^2 - 5$) but $\sqrt{5}/2$ is not an algebraic integer (consider $4X^2 - 5$).

<u>13:</u> EXAMPLE The integers Z are algebraic integers and if x is a rational number which is also an algebraic integer then $x \in Z$.

[Note: Accordingly, a rational number which is not an integer is not an algebraic integer.]

<u>14:</u> LEMMA Under the usual operations, the set of algebraic integers forms a ring.

<u>15:</u> LEMMA If x is an algebraic number, then $a_n x$ is an algebraic integer.

PROOF In fact,

$$f_x(x) = 0$$

=>

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

=>

$$1(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_n^{n-2} a_1 (a_n x) + a_n^{n-1} a_0 = 0.$$

Given an algebraic number $x \in \bar{Q}$, let D_x be the set of integers $n \in Z$ such that nx is an algebraic integer -- then D_x is a nonzero ideal of Z.

16: N.B. That D_x is nonzero is implied by #15.

17: DEFINITION A positive element of D_x is called a denominator of x.

18: DEFINITION The positive generator d_x of D_x is called the denominator of x.

19: N.B. The a_n of #15 needn't be d_x (consider $4X^2 + 2X + 1$).

20: DEFINITION A complex number x is said to be a transcendental number if it is not an algebraic number.

Therefore the set of transcendental numbers is the complement of the field $\bar{Q}$ in the field C.

21: N.B. In general, the sum or product of two transcendental numbers is not transcendental. However the sum of a transcendental number and an algebraic number is a transcendental number and the product of a transcendental number and a nonzero algebraic number is again a transcendental number.

22: EXAMPLE e is transcendental (cf. §17, #1) and π is transcendental (cf. §19, #1) but it is unknown whether $e + \pi$ and $e\pi$ is transcendental (cf. §2, #29).

APPENDIX

Given an algebraic number $x \neq 0$, let $x_1 = x, x_2, \ldots, x_n$ $(n = d(x))$ be the conjugates of x (cf. #9) and put

$$H(x) = \max_{1 \leq j \leq n} |x_j|,$$

the house of x.

LEMMA Let $T \in D_x$ $(T > 0)$ -- then

$$|x| \geq \frac{1}{T^n H(x)^{n-1}}.$$

§15. LIOUVILLE THEORY

1: RAPPEL (cf. §7, #17) Given $x = \frac{a}{b} \in \mathbb{Q}$ $(a,b \in \mathbb{Z},\ b > 0,\ \gcd(a,b) = 1,$ for any coprime pair (p,q) $(q > 0)$ with

$$\frac{a}{b} \neq \frac{p}{q}$$

there follows

$$\left| \frac{a}{b} - \frac{p}{q} \right| \geq \frac{1}{bq}.$$

2: THEOREM If x is real and algebraic of degree $d(x) = n$ (cf. §14, #8), then there is a constant $C = C(x) > 0$ such that for any coprime pair (p,q) $(q > 0)$,

$$\left| x - \frac{p}{q} \right| > \frac{C}{q^n}.$$

PROOF The case $d(x) = 1$ is #1 above (choose $C = C(x) < \frac{1}{b}$), so take $d(x) \geq 2$ and recall that

$$f_x(X) = a_0 + a_1 X + \cdots + a_n X^n$$

is the minimal polynomial of x. Let M be the maximum value of $|f_x'(X)|$ on $[x - 1, x + 1]$, let $\{y_1,\ldots,y_m\}$ $(m \leq n)$ be the distinct zeros of f_x which are different from x, and then choose C:

$$0 < C < \min\,\{1, \frac{1}{M}, |x - y_1|, \ldots, |x - y_m|\}.$$

To arrive at a contradiction, suppose that for some coprime pair (p,q) $(q > 0)$

$$\left| x - \frac{p}{q} \right| \leq \frac{C}{q^n}$$

or still,

$$\leq C < \min\{1, |x - y_1|, \ldots, |x - y_m|\}.$$

Of course,

$$\left| x - \frac{p}{q} \right| > 0,$$

x being irrational. And

$$\left| x - \frac{p}{q} \right| = \left| \frac{p}{q} - x \right| < 1 \Rightarrow x - 1 < \frac{p}{q} < x + 1.$$

In addition

$$0 < \left| x - \frac{p}{q} \right| < |x - y_1|, \ldots, |x - y_m|$$

$$\Rightarrow \frac{p}{q} \neq y_k \quad (k = 1, \ldots, m)$$

$$\Rightarrow f_x\left(\frac{p}{q}\right) \neq 0.$$

Owing to the mean value theorem, there is an x_0 between $\frac{p}{q}$ and x such that

$$\left|f_x(x) - f_x\left(\frac{p}{q}\right)\right| = \left|x - \frac{p}{q}\right| \, |f_x'(x_0)|,$$

i.e.,

$$\left|f_x\left(\frac{p}{q}\right)\right| = \left|x - \frac{p}{q}\right| \, |f_x'(x_0)|$$

$$\Rightarrow |f_x'(x_0)| \neq 0$$

$$\Rightarrow$$

$$\left|x - \frac{p}{q}\right| = \frac{\left|f_x\left(\frac{p}{q}\right)\right|}{|f_x'(x_0)|}$$

$$\geq \frac{\left|f_x\left(\frac{p}{q}\right)\right|}{M} \quad .$$

But

$$0 < |f_x(\tfrac{p}{q})| = |\sum_{j=0}^{n} a_j(\tfrac{p}{q})^j|$$

$$= |\sum_{j=0}^{n} a_j p^j q^{n-j}| / q^n.$$

Since the numerator of this fraction is a positive integer, it follows that

$$|\sum_{j=0}^{n} a_j p^j q^{n-j}| \geq 1,$$

thus

$$|f_x(\tfrac{p}{q})| \geq \frac{1}{q^n}.$$

Finally

$$|x - \tfrac{p}{q}| \geq \frac{|f_x(\tfrac{p}{q})|}{M}$$

$$\geq \frac{1}{Mq^n}$$

$$> \frac{C}{q^n} \geq |x - \tfrac{p}{q}|$$

from which $1 < 1$, contradiction.

<u>3:</u> REMARK The preceding proof goes through if $f(X) \in Z[X]$ has degree $n > 1$ and x is an irrational root of $f(X)$.

<u>4:</u> DEFINITION A real number x is a <u>Liouville number</u> if for every positive integer k there exist $p,q \in Z$ $(q > 1, \gcd(p,q) = 1)$ such that

$$0 < |x - \tfrac{p}{q}| < \frac{1}{q^k}.$$

<u>5:</u> NOTATION L is the subset of R whose elements are the Liouville numbers.

<u>6:</u> LEMMA Every Liouville number is irrational.

PROOF Suppose instead that $x = \frac{a}{b}$ $(a,b \in Z,\ b > 0,\ \gcd(a,b) = 1)$. Let k be a positive integer: $2^{k-1} > b$ and take $p,q: \frac{a}{b} \neq \frac{p}{q}$ -- then

$$|x - \frac{p}{q}| = |\frac{a}{b} - \frac{p}{q}|$$

$$= \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$$

$$> \frac{1}{2^{k-1}q}$$

$$\geq \frac{1}{q^{k-1}q} \quad (q \geq 2)$$

$$= \frac{1}{q^k}.$$

So x is not a Liouville number.

Therefore

$$L \subset P.$$

<u>7:</u> THEOREM Every Liouville number is transcendental.

PROOF Assume that x is an algebraic irrational number with $d(x) = n$, hence per #2, for any coprime pair (p,q) $(q > 0)$,

$$|x - \frac{p}{q}| > \frac{c}{q^n}.$$

Choose a positive integer $r: 2^r \geq \frac{1}{C}$ and then, using the definition of Liouville number, choose p,q:

$$0 < |x - \frac{p}{q}| < \frac{1}{q^{n+r}} \quad (k \equiv n + r).$$

But

$$\frac{1}{q^{n+r}} \leq \frac{1}{2^r q^n} \leq \frac{C}{q^n}$$

=>

$$|x - \frac{p}{q}| < \frac{C}{q^n}.$$

On the other hand,

$$|x - \frac{p}{q}| \not< \frac{C}{q^n} \quad \text{(cf. \#2)}.$$

Contradiction.

Therefore

$$\mathbb{L} \subset \mathbb{T} \subset \mathbb{P}.$$

8: REMARK Not every transcendental number is a Liouville number, e.g., e and π are transcendental but not in $\mathbb{L}$.

9: EXAMPLE Let a be a positive integer ≥ 2. Put

$$x = \sum_{j=1}^{\infty} \frac{1}{a^{j!}}.$$

Then x is a Liouville number.

[Define a sequence of rationals $\frac{p_k}{q_k}$ (k = 1,2,...) by the prescription

$$\frac{p_k}{q_k} = \sum_{j=1}^{k} \frac{1}{a^{j!}}, \quad q_k = a^{k!}.$$

Then

$$|x - \frac{p_k}{q_k}| = \sum_{j=k+1}^{\infty} \frac{1}{a^{j!}}.$$

But

$$\sum_{j=k+1}^{\infty} \frac{1}{a^{j!}} < \sum_{j=(k+1)!}^{\infty} \frac{1}{a^{j}}$$

$$= \frac{1}{a^{(k+1)!}} \sum_{j=0}^{\infty} \frac{1}{a^{j}}$$

$$= \frac{1}{a^{(k+1)!}} \cdot \frac{a}{a-1}$$

$$= \frac{1}{q_k^{k+1}} \cdot \frac{a}{a-1}$$

$$\leq \frac{2}{q_k q_k^{k}}$$

$$\leq \frac{1}{q_k^{k}} \quad (q_k \geq 2).$$

So, $\forall\ k \in N$,

$$0 < |x - \frac{p_k}{q_k}| < \frac{1}{q_k^{k}}.$$

Therefore x is in L (cf. #4).]

<u>10:</u> <u>N.B.</u> The preceding discussion can be generalized. Thus fix an integer

$n \geq 2$ and a sequence of integers $m_j \in \{0,1,2,\ldots,n-1\}$ $(j = 1,2,\ldots)$ such that $m_j \neq 0$ for infinitely many j. Put

$$x = \sum_{j=1}^{\infty} \frac{m_j}{n^{j!}}.$$

Then x is a Liouville number.

[Define a sequence of rationals $\frac{p_k}{q_k}$ $(k = 1,2,\ldots)$ by the prescription

$$\frac{p_k}{q_k} = \sum_{j=1}^{k} \frac{m_j}{n^{j!}}, \quad q_k = n^{k!}.$$

Then

$$\left| x - \frac{p_k}{q_k} \right| = \sum_{j=k+1}^{\infty} \frac{m_j}{n^{j!}}.$$

But as above

$$\sum_{j=k+1}^{\infty} \frac{m_j}{n^{j!}} \leq \sum_{j=k+1}^{\infty} \frac{n-1}{n^{j!}}$$

$$< \sum_{j=(k+1)!}^{\infty} \frac{n-1}{n^{j}}$$

$$= \frac{n-1}{n^{(k+1)!}} \sum_{j=0}^{\infty} \frac{1}{n^{j}}$$

$$= \frac{n-1}{n^{(k+1)!}} \cdot \frac{n}{n-1}$$

$$= \frac{n}{n^{(k+1)!}}$$

$$\leq \frac{n^{k!}}{n^{(k+1)!}}$$

$$= n^{k!-(k+1)!}$$

$$= (n^{-k!})^k$$

$$= (q_k^{-1})^k = (\frac{1}{q^k})^k = \frac{1}{q_k^k}.$$

So, $\forall\, k \in \mathbb{N}$,

$$0 < \left| x - \frac{p_k}{q_k} \right| < \frac{1}{q_k^k}.$$

Therefore x is in L (cf. #4).]

11: EXAMPLE Put

$$x = \sum_{j=1}^{\infty} \frac{1}{2^{2^j}}.$$

Then x is a Liouville number.

In #10, it is traditional to take $n = 10$, hence $m_j \in \{0,1,2,\ldots,9\}$ $(j = 1,2,\ldots)$.

12: LEMMA Put

$$x = \sum_{j=1}^{\infty} m_j\, 10^{-j!},\ y = \sum_{j=1}^{\infty} n_j\, 10^{-j!}.$$

Assume: $m_j \neq n_j$ for some j and let k be the least index j such that $m_j \neq n_j$ -- then $x \neq y$.

PROOF

$$|x - y| = \left| (m_k - n_k) 10^{-k!} + \sum_{j=k+1}^{\infty} (m_j - n_j) 10^{-j!} \right|$$

$$\geq |m_k - n_k| 10^{-k!} - \left| \sum_{j=k+1}^{\infty} (m_j - n_j) 10^{-j!} \right|$$

$$\geq |m_k - n_k| 10^{-k!} - \sum_{j=k+1}^{\infty} |m_j - n_j| 10^{-j!}$$

$$\geq 10^{-k!} - \sum_{j=k+1}^{\infty} (8) 10^{-j!}$$

$$> 10^{-k!} - \sum_{j=(k+1)!}^{\infty} (8) 10^{-j}$$

$$= 10^{-k!} - (80/9) 10^{-(k+1)!}$$

$$> 0.$$

13: SCHOLIUM The set of Liouville numbers is uncountable.

[The Liouville numbers of the form

$$\sum_{j=1}^{\infty} m_j \, 10^{-j!}$$

constitute an uncountable set (use a Cantor diagonalization argument).]

14: THEOREM Suppose that $f(X) \in \mathbb{Z}[X]$ has degree ≥ 1 and let $x \in \mathbb{L}$ -- then $f(x) \in \mathbb{L}$.

To begin with:

15: LEMMA If the degree of $f(X) \in \mathbb{R}[X]$ is ≥ 1 and if $a \in \mathbb{R}$, then there is a polynomial $g(X) \in \mathbb{R}[X]$ such that

$$f(X) - f(a) = (X - a) g(X).$$

PROOF Write

$$f(X) = \sum_{j=0}^{r} c_j X^j.$$

Then for $j \geq 1$,

$$X^j - a^j$$

$$= (X - a)(X^{j-1} + aX^{j-2} + a^2X^{j-3} + \cdots + a^{j-2}X + a^{j-1})$$

$$= (X - a)g_j(X).$$

Therefore

$$f(X) - f(a)$$

$$= C_0 + \sum_{j=1}^{r} C_jX^j - C_0 - \sum_{j=1}^{r} C_ja^j$$

$$= \sum_{j=1}^{r} C_j(X^j - a^j)$$

$$= \sum_{j=1}^{r} C_j(X - a)g_j(X)$$

$$= (X - a) \sum_{j=1}^{r} C_jg_j(X)$$

$$\equiv (X - a)g(X).$$

To set up the particulars for #14, note first that $\{X:X \neq x \ \& \ f(X) = f(x)\}$ is a finite set (the degree of $f(X)$ being by assumption ≥ 1). Fix $\delta > 0$ subject to

$$0 < \delta < \min\{|X - x|:X \neq x \ \& \ f(X) = f(x)\}$$

and put

$$M = \max\{|g(X)|:|X - x| \leq \delta\}.$$

Bearing in mind the definition figuring in #4, let k be a positive integer and choose a natural number $m > kr$ (r the degree of f) such that

$$1 < \delta 2^m \text{ and } M2^{kr} < 2^m.$$

Next, determine $p,q \in Z$ ($q > 1$, $\gcd(p,q) = 1$):

$$0 < \left|x - \frac{p}{q}\right| < \frac{1}{q^m}.$$

Step 1:

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^m} \leq \frac{1}{2^m} < \delta$$

=>

$$\left|g(\tfrac{p}{q})\right| \leq M \text{ and } f(\tfrac{p}{q}) \neq f(x).$$

Step 2:

$$M2^{kr} < 2^m \Rightarrow M < 2^{m-kr}$$

=>

$$\left|g(\tfrac{p}{q})\right| \leq M < 2^{m-kr} \leq q^{m-kr}.$$

Step 3:

$$\begin{aligned} 0 < \left|f(x) - f(\tfrac{p}{q})\right| &= \left|x - \tfrac{p}{q}\right|\left|g(\tfrac{p}{q})\right| \\ &< \frac{1}{q^m}\, q^{m-kr} \\ &= \left(\frac{1}{q^r}\right)^k. \end{aligned}$$

Step 4: Write

$$f(X) = \sum_{j=0}^{r} C_j X^j \quad (C_j \in Z).$$

Then

$$f\left(\frac{p}{q}\right) = \sum_{j=0}^{r} c_j \left(\frac{p}{q}\right)^j$$

$$= \left(\sum_{j=0}^{r} c_j p^j q^{r-j}\right)/q^r$$

$$= \frac{C}{q^r},$$

where $C \in Z$.

Step 5:

$$0 < \left| f(x) - f\left(\frac{p}{q}\right) \right|$$

$$= \left| f(x) - \frac{C}{q^r} \right| < \left(\frac{1}{q^r}\right)^k.$$

To fulfill the requirements of #4, it remains only to take

$$\begin{cases} \text{"}p\text{"} = C \\ \text{"}q\text{"} = q^r. \end{cases}$$

16: APPLICATION If $a \neq 0$, $b \neq 0$ are integers and if $x \in L$, then

$$a + bx \in L.$$

[Consider

$$f(X) = a + bX.]$$

17: APPLICATION If $x \in L$, then $\forall\, n \in N$, $x^n \in L$.

[Consider

$$f(X) = X^n.]$$

18: LEMMA If x is a Liouville number and if $r \in Q$ is nonzero, then $rx \in L$.

PROOF Write $r = \frac{a}{b}$ $(a,b \in Z,\ b > 0)$. Given a natural number k, choose a natural number $m > k$:

$$|a|\, b^{k-1} < 2^{m-k}.$$

Next, per the definition of L (cf. #4), there exist $p,q \in Z$ $(q > 1,\ \gcd(p,q) = 1)$:

$$0 < \left|x - \frac{p}{q}\right| < \frac{1}{q^m}.$$

Therefore

$$\begin{aligned}
0 < \left| rx - \frac{ap}{bq} \right| & \\
& < \frac{|r|}{q^m} \\
& < \frac{|a|}{bq^m} \\
& < \frac{2^{m-k}}{b^{k-1}} \cdot \frac{1}{bq^m} \\
& \leq \frac{q^{m-k}}{b^{k-1}} \cdot \frac{1}{bq^m} \\
& = \frac{1}{(bq)^k}.
\end{aligned}$$

[Note: The assertion may be false if r is merely algebraic. For example, consider

$$\sqrt{3/2} \sum_{j=1}^{\infty} \frac{1}{10^{j!}}.]$$

19: APPLICATION Every interval $]a,b[$ $(a < b)$ contains a Liouville number.

[Take a positive Liouville number x and consider

$$]\frac{a}{x}, \frac{b}{x}[.$$

Fix a nonzero rational number r:

$$\frac{a}{x} < r < \frac{b}{x} \quad (\text{cf. } \S 2, \#15).$$

Then

$$a < rx < b.]$$

20: SCHOLIUM $\mathbb{L}$ is a dense subset of $\mathbb{R}$ (cf. §2, #14).

21: THEOREM Let $f(X) \in \mathbb{Q}[X]$ be nonconstant and suppose that $x \in \mathbb{L}$ -- then $f(x) \in \mathbb{L}$.

PROOF Choose $n \in \mathbb{N}$:

$$(nf)(X) \in \mathbb{Z}[X].$$

Then

$$(nf)(x) \in \mathbb{L} \ (\text{cf. } \#14) \Rightarrow \frac{1}{n}(nf)(x) \in \mathbb{L} \ (\text{cf. } \#18),$$

i.e., $f(x) \in \mathbb{L}$.

[In particular, the sum of a rational number $\frac{a}{b}$ and a Liouville number x is again a Liouville number:

$$\frac{a}{b} + x = \frac{1}{b}(a + bx).]$$

22: THEOREM The set of Liouville numbers in $[0,1]$ is a set of measure 0.

PROOF Fix $\varepsilon > 0$. Let k be a positive integer such that

$$4 \sum_{q=2}^{\infty} \frac{1}{q^{k-1}} < \varepsilon.$$

That such a choice is possible can be seen by noting that

$$4 \sum_{q=2}^{\infty} \frac{1}{q^{k-1}} = 4 \left(\frac{1}{2^{k-1}} + \frac{1}{3^{k-1}} + \cdots\right)$$

$$= 4 \cdot \frac{1}{2^{k-3}} \left(\frac{1}{2^2} + \frac{1}{3^2} + \cdots\right).$$

This said, let x be a Liouville number in [0,1] and per #4, write

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^k}$$

or still,

$$\frac{p}{q} - \frac{1}{q^k} < x < \frac{p}{q} + \frac{1}{q^k} .$$

Put

$$I_{p/q} = \left] \frac{p}{q} - \frac{1}{q^k} , \frac{p}{q} + \frac{1}{q^k} \right[,$$

an open interval of length

$$\frac{p}{q} + \frac{1}{q^k} - \frac{p}{q} + \frac{1}{q^k} = \frac{2}{q^k} .$$

Since $x \in [0,1]$ and $\frac{1}{q^k} \leq \frac{1}{2}$, it follows that

$$\frac{p}{q} \in \left] -\frac{1}{2}, \frac{3}{2} \right[,$$

i.e.,

$$-\frac{1}{2} < \frac{p}{q} < \frac{3}{2} \Rightarrow -\frac{q}{2} < p < \frac{3q}{2} .$$

Therefore the total number of $I_{p/q}$ is $\leq 2q$.

Put

$$I(q) = \bigcup_{p/q} I_{p/q},$$

a set of measure

$$\leq \sum_{p/q} \frac{2}{q^k} = \frac{2}{q^k} \sum_{p/q} 1$$

$$\leq \frac{2}{q^k} \cdot 2q$$

$$= \frac{4q}{q^k}.$$

The set of Liouville numbers in [0,1] is contained in

$$\bigcup_{q>1} I(q),$$

a set of measure

$$\leq \sum_{q=2}^{\infty} \frac{4q}{q^k} = 4 \sum_{q=2}^{\infty} \frac{1}{q^{k-1}} < \varepsilon,$$

from which the assertion.

23: APPLICATION There are transcendental numbers that are not Liouville numbers.

[Let S be the set of algebraic numbers in [0,1] and let T be the set of transcendental numbers in [0,1] -- then

$$[0,1] = S \cup T, \ S \cap T = \emptyset.$$

Since S is countable, it is of measure 0, hence T is of measure 1.]

[Note: Almost all transcendental numbers in [0,1] are non-Liouville.]

Working within $\mathbf{R}$, it follows that $\mathbf{L}$ is a set of measure 0.

24: NOTATION Given $k \in \mathbf{N}$, put

$$U_k = \bigcup_{q\geq 2} \bigcup_{p\in \mathbf{Z}} \left]\frac{p}{q} - \frac{1}{q^k}, \frac{p}{q} + \frac{1}{q^k}\right[- \left\{\frac{p}{q}\right\}$$

or still,

$$U_k = \bigcup_{q\geq 2} \bigcup_{p\in \mathbf{Z}} \left\{x \in \mathbf{R}: 0 < \left|x - \frac{p}{q}\right| < \frac{1}{q^k}\right\}.$$

25: LEMMA U_k is an open dense subset of $\mathbf{R}$.

[Each $\frac{p}{q} \in \mathbf{Q}$ belongs to the closure of U_k.]

26: LEMMA

$$\mathbf{L} = \bigcap_{k=1}^{\infty} U_k.$$

27: RAPPEL A G_δ-subset of a topological space X is the countable intersection of open dense subsets of X.

Therefore $\mathbf{L}$ is a G_δ-subset of $\mathbf{R}$.

28: RAPPEL If X is a complete metric space and if $\{G_n\}$ is a sequence of open dense subsets of X. then

$$\bigcap_{n=1}^{\infty} G_n$$

is not empty and, in fact, is dense in X.

Therefore $\mathbf{L}$ is a dense subset of $\mathbf{R}$ (cf. #20).

29: RAPPEL If X is a complete metric space without isolated points and if S is a G_δ-subset of X, then S is uncountable.

Therefore L is an uncountable subset of R (cf. #13).

30: THEOREM Every real number x is the sum of two Liouville numbers:

$$x = \alpha + \beta \ (\alpha, \beta \in L).$$

31: THEOREM Every nonzero real number x is the product of two Liouville numbers:

$$x = \alpha\beta \ (\alpha, \beta \in L).$$

It will be enough to sketch the proof of #30.

Step 1: Put

$$\alpha = \sum_{j=1}^{\infty} 10^{-j!}.$$

Then

$$0 = \alpha + (-1)\alpha, \ 1 = \alpha + (1 + (-1)\alpha).$$

Recalling #21, these representations take care of the cases when $x = 0$, $x = 1$. But then matters follow if x is any rational.

Step 2: Take x irrational and without loss of generality, suppose further that $0 < x < 1$ — then x admits a dyadic expansion:

$$x = \sum_{j=1}^{\infty} m_j 2^{-j} \quad (m_j \in \{0,1\}).$$

Define

$$\alpha_j = \begin{cases} m_j \text{ if } j \text{ is odd} \\ \\ 0 \text{ if } j \text{ is even} \end{cases}$$

and put $\beta_j = m_j - \alpha_j$. Introduce

$$\alpha = \sum_{j=1}^{\infty} \alpha_j 2^{-j} \text{ and } \beta = \sum_{j=1}^{\infty} \beta_j 2^{-j}.$$

Then

$$x = \alpha + \beta.$$

Step 3: Assume that the series defining α is infinite -- then in this case, α is a Liouville number.

[For $k \geq 1$,

$$0 < \alpha - \sum_{j=1}^{(2k)!-1} \alpha_j 2^{-j}$$

$$= \sum_{j \geq (2k)!} \alpha_j 2^{-j} < 2^{1-(2k+1)!}.$$

Define a sequence of rationals $\frac{p_k}{q_k}$ $(k = 1,2,\ldots)$ by the prescription

$$\frac{p_k}{q_k} = \sum_{j=1}^{(2k)!-1} \alpha_j 2^{-j}, \quad q_k = 2^{(2k)!-1}.$$

Then p_k and q_k are integers, $q_k > 1$, and

$$0 < \alpha - \frac{p_k}{q_k} < \frac{1}{q_k^k}.$$

Therefore α is a Liouville number.]

[Note: Tacitly

$$2^{1-(2k+1)!} < 2^{k-k(2k)!}.$$

In fact,

$$1 - (2k + 1)! + k(2k)!$$

$$= 1 - (2k)!(2k + 1) + k(2k)!$$

$$= 1 - (k + k)(2k)! - (2k)! + k(2k)!$$

$$= 1 - k(2k)! - k(2k)! - (2k)! + k(2k)!$$

$$= 1 - k(2k)! - (2k)! < k.]$$

Step 4: Assume that the series defining β is infinite -- then in this case, β is a Liouville number.

Step 5: So if the series defining α and the series defining β are infinite, we are done.

Step 6: If the series defining α is finite, then α is rational. If the series defining β is infinite, then β is a Liouville number, thus $x = \alpha + \beta$ is a Liouville number, thence $\frac{x}{2}$ is a Liouville number and

$$x = \frac{x}{2} + \frac{x}{2}.$$

Step 7: Reverse the roles of α and β in the previous step.

Step 8: The case when both defining series are finite cannot occur (for then α and β are rational, contradicting the assumption that $x = \alpha + \beta$ is irrational).

32: THEOREM If x is a Liouville number, then for any algebraic number $\alpha > 0$ $(\alpha \neq 1)$, the power α^x is transcendental.

It is a question of showing that $\alpha^x \neq \alpha'$ for every algebraic $\alpha' > 0$, i.e., that $\ell n(\alpha^x) \neq \ell n(\alpha')$, i.e., that $x\ell n(\alpha) \neq \ell n(\alpha')$, or still, that

$$|x\ell n(\alpha) - \ell n(\alpha')| > 0.$$

If

$$\frac{\ell n(\alpha')}{\ell n(\alpha)}$$

were rational and if

$$|x\ell n(\alpha) - \ell n(\alpha')| = 0,$$

then it would follow that

$$x = \frac{\ell n(\alpha')}{\ell n(\alpha)},$$

which is impossible (x, being Liouville, is transcendental (cf. #7)). So assume that

$$\frac{\ell n(\alpha')}{\ell n(\alpha)}$$

is irrational and write

$$|x\ell n(\alpha) - \ell n(\alpha')|$$

$$= |x\ell n(\alpha) - \frac{p}{q}\ell n(\alpha) + \frac{p}{q}\ell n(\alpha) - \ell n(\alpha')|$$

$$= |(x - \frac{p}{q})\ell n(\alpha) + \frac{p}{q}\ell n(\alpha) - \ell n(\alpha')|$$

$$= |\frac{p}{q}\ell n(\alpha) - \ell n(\alpha') - - (x - \frac{p}{q})\ell n(\alpha)|$$

$$\geq |\frac{p}{q}\ell n(\alpha) - \ell n(\alpha')| - |-(x - \frac{p}{q})\ell n(\alpha)|$$

$$= |\frac{p}{q}\ell n(\alpha) - \ell n(\alpha')| - |(x - \frac{p}{q})\ell n(\alpha)|$$

$$= |\frac{p}{q}\ell n(\alpha) - \ell n(\alpha')| - |x - \frac{p}{q}|\,|\ell n(\alpha)|$$

$$> |\frac{p}{q}\ell n(\alpha) - \ell n(\alpha')| - \frac{|\ell n(\alpha)|}{q^k}$$

$$= \frac{|p\ell n(\alpha) - q\ell n(\alpha')|}{q} - \frac{|\ell n(\alpha)|}{q^k}$$

$$= \frac{1}{q}(|p\ell n(\alpha) - q\ell n(\alpha')| - \frac{|\ell n(\alpha)|}{q^{k-1}})$$

thereby reducing matters to the positivity of

$$|p\ell n(\alpha) - q\ell n(\alpha')| - \frac{|\ell n(\alpha)|}{q^{k-1}} .$$

In any event,

$$|p\ell n(\alpha) - q\ell n(\alpha')|$$

is positive since otherwise

$$\frac{p}{q} = \frac{\ell n(\alpha')}{\ell n(\alpha)}$$

contradicting the supposition that

$$\frac{\ell n(\alpha')}{\ell n(\alpha)}$$

is irrational.

33: LEMMA

$$|p\ell n(\alpha) - q\ell n(\alpha')| \geq \frac{1}{\max\{|p|,q\}^c} ,$$

where $c > 0$ depends only on $\ell n(\alpha)$ and $\ell n(\alpha')$.

[This estimate will be established later on (cf. §32 , #4).]

Assume that $x \in [0,1]$, choose $k >> 0$:

$$\frac{|\ln(\alpha)|}{q^{k-1-c}} < \frac{1}{2} \min \{(\tfrac{2}{3})^c, \tfrac{1}{2}\},$$

and take $|p| \neq 0$, hence

$$-\frac{q}{2} < p < \frac{3q}{2} \quad \text{(cf. \#22)}$$

$$\Rightarrow 0 < |p| < \frac{3q}{2} \Rightarrow \frac{1}{|p|} > \frac{2}{3q}.$$

There are now two possibilities:

$$|p\ln(\alpha) - q\ln(\alpha')| \geq \begin{bmatrix} \dfrac{1}{q^c} \\ \\ \dfrac{1}{|p|^c} \end{bmatrix}.$$

- Work with $\frac{1}{q^c}$ -- then the issue is the positivity of

$$\frac{1}{q^c} - \frac{|\ln(\alpha)|}{q^{k-1}}$$

or still, the positivity of

$$1 - \frac{|\ln(\alpha)|}{q^{k-1-c}} > 1 - \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} > 0.$$

- Work with $\frac{1}{|p|^c}$ -- then the issue is the positivity of

$$\frac{1}{|p|^c} - \frac{|\ln(\alpha)|}{q^{k-1}}$$

or still, the positivity of

$$\left(\frac{2}{3q}\right)^c - \frac{|\ell n(\alpha)|}{q^{k-1}}$$

$$= \left(\frac{2}{3}\right)^c \frac{1}{q^c} - \frac{|\ell n(\alpha)|}{q^{k-1}}$$

or still, the positivity of

$$\left(\frac{2}{3}\right)^c - \frac{|\ell n(\alpha)|}{q^{k-1-c}} > \left(\frac{2}{3}\right)^c - \frac{1}{2}\left(\frac{2}{3}\right)^c = \frac{1}{2}\left(\frac{2}{3}\right)^c > 0.$$

33: REMARK Take α as above and assume that x is positive -- then

$$\ell n(x\alpha) \text{ and } x\ell n(\alpha)$$

are transcendental.

§16. *THE MAHLER CLASSIFICATION*

What follows is a proofless summary of the relevant facts.

<u>1:</u> DEFINITION Let $P(X) \in C[X]$, say

$$P(X) = a_0 + a_1X + \cdots + a_nX^n.$$

Then the <u>height</u> of PX, denoted $H(P)$, is

$$\max\{|a_0|, |a_1|, \ldots, |a_n|\}.$$

<u>2:</u> NOTATION Given a real number x, $w_n(x)$ $(n \in N)$ is the supremum of the real numbers w such that

$$0 < |P(x)| \leq H(P)^{-w}$$

has infinitely many solutions $P(X) \in Z[X]$ of degree at most n.

<u>3:</u> LEMMA For any nonzero rational number $\frac{a}{b}$,

$$w_n(x) = \begin{cases} w_n(x + \frac{a}{b}) \\ \\ w_n(\frac{a}{b}x). \end{cases}$$

<u>4:</u> LEMMA For any positive integer n,

$$0 \leq w_n(x) \leq \infty.$$

<u>5:</u> <u>N.B.</u> The sequence $\{w_n(x)\}$ is increasing: $w_1(x) \leq w_2 < \ldots$ and $w_n(x) \geq n$.

<u>6:</u> MAIN PROBLEM Suppose that $\{w_n\}$ is an increasing sequence of real numbers with $w_n \geq n \ \forall \ n \in \mathbb{N}$. Does there exist a real number x such that for all n, $w_n(x) = w_n$?

<u>7:</u> NOTATION Put

$$w(x) = \lim_{n \to \infty} \sup \frac{w_n(x)}{n}.$$

Therefore

$$0 \leq w(x) \leq \infty.$$

[Note: Real numbers with $0 < w(x) < 1$ do not exist.]

<u>8:</u> DEFINITION A real number x is an

- <u>A-number</u> if $w(x) = 0$;
- <u>S-number</u> if $0 < w(x) < \infty$;
- <u>T-number</u> if $w(x) = \infty$ & $\forall \ n \geq 1$, $w_n(x) < \infty$;
- <u>U-number</u> if $w(x) = \infty$ & $\forall \ n >> 1$, $w_n(x) = \infty$.

Write A, S, T, U for the corresponding sets (termed <u>Mahler classes</u>) -- then

$$\mathbb{R} = A \cup S \cup T \cup U,$$

a disjoint union.

[Note: The transcendentals $\mathbb{T}$ decompose as

$$S \cup T \cup U.]$$

9: THEOREM The A-numbers are exactly the real algebraic numbers.

10: THEOREM The Mahler classes S, T, U are not empty.

11: REMARK A(= $\bar{Q}$) is a set of measure 0 (being countable). It can be shown that T and U are also sets of measure 0, hence almost all real numbers are S-numbers.

12: EXAMPLE Suppose that α is a nonzero algebraic number -- then e^α is an S-number, thus in particular, e is an S-number.

13: EXAMPLE For any positive integer d,

$$\sum_{j=1}^{\infty} 2^{-(d+1)j}$$

is an S-number.

14: EXAMPLE π is not a U-number, so, being transcendental, is either an S-number or a T-number but no one knows which one.

15: N.B. Exhibiting explicit T-numbers is complicated business.

16: DEFINITION A U-number x is a U_n-number if n is the smallest positive integer such that $w_n(x) = \infty$.

Write U_n for the set of such.

17: THEOREM Each U_n is nonempty and

$$U = \bigcup_{n=1}^{\infty} U_n,$$

a disjoint union.

18: EXAMPLE $\forall\, n \in N$,

$$\sqrt[n]{3/2} \cdot \sum_{j=1}^{\infty} 10^{-j!}$$

is a U_n-number.

19: EXAMPLE Let $m_j \in \{2,4\}$ $(j = 1,2,\ldots)$. Put

$$x = (3 + \sum_{j=1}^{\infty} m_j\, 10^{-j!})/4.$$

Then for all $n \geq 1$, the positive real n^{th} root of x is a U_n-number.

20: SCHOLIUM $\forall\, n \geq 1$, U_n is uncountable.

21: N.B. $U_1 = L$.

22: DEFINITION Two real numbers x and y are algebraically dependent if there is a nonzero polynomial $P(X,Y) \in Z[X,Y]$ such that $P(x,y) = 0$ (cf. §20, #1).

[Note: The denial is algebraically independent.]

23: THEOREM Algebraically dependent real numbers belong to the same Mahler class.

24: EXAMPLE If x is a U-number and y is not a U-number, then x and y are algebraically independent. So, e.g., $\sum_{j=1}^{\infty} 10^{-j!}$ and π are algebraically independent.

[Note: $x + y$ is transcendental: Given

$$\sum_{j=0}^{n} a_j (x + y)^j = 0,$$

consider

$$P(X,Y) = \sum_{j=0}^{n} a_j (X + Y)^j.]$$

25: REMARK In general, if x and y are transcendental numbers, then at least one of x + y and xy must be transcendental (cf. §2, #29).

[To see this, consider the polynomial

$$X^2 - (x + y)X + xy.$$

Its zeros are x and y. So if both x + y and xy were algebraic, then x and y would be algebraic which they are not.]

26: EXAMPLE It can be shown that the numbers π and e^π are algebraically independent but it is not known whether e^π is or is not a U-number (recall that π is not a U-number (cf. #14)).

§17. *TRANSCENDENCE OF* e

We have seen that e is irrational (cf. §8, #3) but more is true.

1: THEOREM e is transcendental.

2: SCHOLIUM $\forall\, n \in \mathbb{N}$, $1, e, e^2, \ldots, e^n$ are linearly independent over $\mathbb{Q}$ (cf. §8, #11).

3: LEMMA Given $f \in \mathbb{R}[X]$ of degree M,

$$e^x \int_0^x f(t)e^{-t}dt = F(0)e^x - F(x),$$

where

$$F(x) = \sum_{\ell=0}^{M} f^{(\ell)}(x).$$

PROOF Integrate by parts to get

$$\int_0^x f(t)e^{-t}dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t}dt.$$

Then interate this.

[Note: If f has integer coefficients, then the same is true of F.]

Consider now a relation of the form

$$a_0 + a_1e + a_2e^2 + \cdots + a_me^m = 0,$$

where $a_0 > 0$, $a_m \neq 0$ ($a_k \in \mathbb{Z}$) -- then from #3,

$$F(0)e^k - F(k) = e^k \int_0^k f(t)e^{-t}dt \quad (k = 0,1,\ldots,m),$$

so

$$F(0)\sum_{k=0}^{m} a_k e^k - \sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt$$

or still,

$$-\sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt,$$

i.e.,

$$-a_0F(0) - \sum_{k=1}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt.$$

The polynomial f is at our disposal and the trick is to choose it appropriately in order to reach a contradiction. One choice is to put

$$g(X) = X^{n-1}(X-1)^n \cdots (X-m)^n$$

and let

$$f(X) = \frac{g(X)}{(n-1)!},$$

$n \in \mathbb{N}$ to be determined in due course.

FACTS

$$\deg f = (m+1)n - 1 \equiv M$$

$$f^{(\ell)}(0) = 0 \qquad (0 \leq \ell \leq n-2),$$

$$f^{(n-1)}(0) = (-1)^{mn}(m!)^n,$$

$$n \mid f^{(\ell)}(0) \qquad (\forall\, \ell \neq n-1).$$

[Write

$$f(X) = \frac{g(X)}{(n-1)!} = \frac{X^{n-1}}{(n-1)!}(b_0 + b_1X + \cdots + b_{mn}X^{mn})$$

$$= \frac{1}{(n-1)!} (b_0 X^{n-1} + b_1 X^n + \cdots + b_{mn} X^{(m+1)n-1})$$

$$= \frac{1}{(n-1)!} \sum_{\ell=n-1}^{M} c_\ell X^\ell \quad (c_{n-1} = b_0,\ c_n = b_1, \ldots).$$

Then

$$\ell < n - 1 \Rightarrow f^{(\ell)}(0) = 0.$$

And

$$\ell \geq n - 1 \Rightarrow \frac{f^{(\ell)}(0)}{\ell!} = \frac{c_\ell}{(n-1)!}$$

$$\Rightarrow f^{(\ell)}(0) = \ell! \frac{c_\ell}{(n-1)!} \in Z.$$

Therefore

$$\ell \geq n \Rightarrow n | f^{(\ell)}(0)$$

but

$$\ell = n - 1 \Rightarrow f^{(n-1)}(0) = c_{n-1}$$

$$= b_0 = (-1)^{mn} (m!)^n.]$$

Consequently

$$F(0) = \sum_{\ell=0}^{M} f^{(\ell)}(0)$$

$$= \sum_{\ell=n-1}^{M} f^{(\ell)}(0)$$

$$= f^{(n-1)}(0) + f^{(n)}(0) + \cdots + f^{((m+1)n-1)}(0)$$

$$= (-1)^{mn}(m!)^n + nC,$$

C an integer.

The next step is to get a handle on the $F(k)$ $(1 \leq k \leq m)$. To this end, let

$$g_k(X) = \frac{g(X)}{(X-k)^n}$$

$$= X^{n-1} \prod_{\substack{\ell=1 \\ \ell \neq k}}^{m} (X-\ell)^m,$$

a polynomial with integral coefficients. Using now the formula for differentiating a product,

$$g^{(j)}(X) = \sum_{i=0}^{j} \binom{j}{i} ((X-k)^n)^{(i)} (g_k(X))^{(j-i)}.$$

Due to the presence of the factor $X - k$, it follows that

$$g^{(j)}(k) = 0 \quad (j < n).$$

On the other hand, if $j \geq n$, then

$$g^{(j)}(k) = \binom{j}{n} n!\, g_k^{(j-n)}(k).$$

So, for all j, $g^{(j)}(k)$ is an integer divisible by $n!$, say

$$g^{(j)}(k) = n!\, n_j(k).$$

And then

$$F(k) = \sum_{\ell=0}^{M} f^{(\ell)}(k)$$

$$= \sum_{\ell=n}^{M} f^{(\ell)}(k)$$

$$= \sum_{\ell=n}^{M} \frac{g^{(\ell)}(k)}{(n-1)!}$$

$$= \sum_{\ell=n}^{M} \frac{n!n_\ell(k)}{(n-1)!}$$

$$= n \sum_{\ell=n}^{M} n_\ell(k)$$

$$= nn_k \quad (n_k \in Z).$$

Take $n >> 0$ (n prime):

$$n > a_0 \text{ and } \gcd(n,m!) = 1,$$

hence

$$n \not| \; a_0 F(0) \qquad (\text{cf. §7, \#1}).$$

And this implies that

$$- a_0F(0) - \sum_{k=1}^{m} a_kF(k)$$

$$= - a_0F(0) - \sum_{k=1}^{m} a_k(nn_k)$$

$$= - a_0F(0) - n \left(\sum_{k=1}^{m} a_kn_k\right)$$

$$\neq 0.$$

To recapitulate:

$$- a_0F(0) - \sum_{k=1}^{m} a_kF(k)$$

is a nonzero integer, thus

$$\left| \sum_{k=0}^{m} a_kF(k) \right| \geq 1.$$

Return now to

$$\sum_{k=0}^{m} a_ke^k \int_0^k f(t)e^{-t}dt,$$

an entity that depends on n and which can be made arbitrarily small (leading thereby to the sought for contradiction).

To see this, note that

$$|f(x)| \le \frac{M}{(n-1)!} \quad (0 \le x \le m)\ (M = (m+1)n-1),$$

so

$$\left| \sum_{k=0}^{m} a_k e^k \int_0^k f(t) e^{-t} dt \right|$$

$$\le \frac{M}{(n-1)!} \sum_{k=0}^{m} |a_k| \int_0^k e^{k-t} dt$$

$$\le \frac{m^{(m+1)n}}{(n-1)!} \sum_{k=0}^{m} |a_k| (e^k - 1)$$

$$\le \frac{m^{(m+1)n}}{(n-1)!} \sum_{k=0}^{m} |a_k| e^k$$

$$\le \frac{m^{(m+1)n}}{(n-1)!} e^m \sum_{k=0}^{m} |a_k|$$

$$= \frac{C^n}{(n-1)!} e^m \sum_{k=0}^{m} |a_k|,$$

where

$$C = m^{m+1}.$$

But

$$\frac{C^n}{(n-1)!} = C \cdot \frac{C^{n-1}}{(n-1)!}$$

$$\rightarrow 0 \quad (n \rightarrow \infty) \quad (\text{cf. } \S 0).$$

Here is an application of #1.

4: SCHOLIUM Let q be a nonzero rational number -- then e^q is transcendental (cf. §9, #1).

[Take $q > 0$ and suppose that e^q is algebraic. Write $q = \frac{a}{b}$ $(a,b > 0)$ -- then $(e^{\frac{a}{b}})^b = e^a$ is algebraic, which implies that e is algebraic (cf. §2, #37), a contradiction.]

APPENDIX

Consider the transcendence status of the three examples figuring in the Appendix to §8.

- Is the number

$$\sum_{k=0}^{\infty} \frac{r^k}{2^{k(k-1)/2}}$$

transcendental? Ans: Unknown.

- Is the number

$$\sum_{k=0}^{\infty} r^{2^k}$$

transcendental? Ans: Yes.

- Is the number

$$\sum_{k=1}^{\infty} \frac{1}{M^{k^2}}$$

transcendental? Ans: Yes.

§18. SYMMETRIC ALGEBRA

1: RAPPEL Let A be a commutative ring with unit -- then a polynomial

$$P(X_1,\ldots,X_n) \in A[X_1,\ldots,X_n]$$

is symmetric if for any permutation σ of $\{1,\ldots,n\}$,

$$P(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = P(X_1,\ldots,X_n).$$

2: DEFINITION The elementary symmetric polynomials $s_1,s_2,\ldots,s_n$ in n variables $x_1,x_2,\ldots,x_n$ appear as coefficients in the monic polynomial of degree n and roots $x_1,x_2,\ldots,x_n$:

$$(X - x_1)(X - x_2)\cdots(X - x_n) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n.$$

Explicated:

$$s_1 = x_1 + x_2 + \cdots + x_n$$

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n$$

$$\vdots$$

$$s_n = x_1x_2 \cdots x_n.$$

3: THEOREM Every symmetric polynomial can be written as a polynomial in the elementary symmetric polynomials: If $P \in A[X_1,\ldots,X_n]$ is symmetric, then there exists a polynomial $F \in A[s_1,\ldots,s_n]$ such that

$$P = F(s_1,\ldots,s_n).$$

E.g.:

$$\begin{aligned} P(X_1,X_2) &= 3(X_1X_2)^3 - ((X_1 + X_2)^2 - 2X_1X_2) \\ &= 3s_2^2 - s_1^2 - 2s_2 \\ &\equiv F(s_1,s_2). \end{aligned}$$

<u>4:</u> LEMMA Let α be an algebraic number, let $d = \deg \alpha$ ($\equiv d(\alpha)$), let $\alpha_1,\ldots,\alpha_d$ ($\alpha = \alpha_1$) be the zeros of f_α (cf. §14, #7), and let

$$F = F(X;\alpha_1,\ldots,\alpha_d) \in Q[X;\alpha_1,\ldots,\alpha_d].$$

Assume: As a polynomial in $\alpha_1,\ldots,\alpha_d$ with coefficients in $Q[X]$, F is symmetric -- then

$$F = F(X) \in Q[X].$$

PROOF Write

$$\begin{aligned} f_\alpha(z) &= a_0 + a_1z + \cdots + a_dz^d \quad (a_0,a_1,\ldots,a_d \in Z) \\ &= a_d(z - \alpha_1)(z - \alpha_2)\cdots(z - \alpha_d) \\ &= a_d(z^d - (\alpha_1 + \alpha_2 + \cdots + \alpha_d)z^{d-1} \\ &\quad + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{d-1}\alpha_d)z^{d-2} \\ &\quad + \cdots + (-1)^d(\alpha_1\alpha_2\cdots\alpha_d)), \end{aligned}$$

from which

$$s_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_d = -\frac{a_{d-1}}{a_d}$$

$$s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{d-1}\alpha_d = \frac{a_{d-2}}{a_d}$$

$$\vdots$$

$$s_d = \alpha_1\alpha_2 \cdots \alpha_d = (-1)^d \frac{a_0}{a_d},$$

implying thereby that the elementary symmetric polynomials in the $\alpha_1,\alpha_2,\ldots,\alpha_d$ are rational numbers. Turning now to F, being a symmetric polynomial in $\alpha_1,\alpha_2,\ldots,\alpha_d$, it can be written as a polynomial in the elementary symmetric polynomials $s_1,s_2,\ldots,s_d$ with coefficients in $Q[X]$. But $s_1,s_2,\ldots,s_d \in Q$, hence

$$F = F(X) \in Q[X].$$

5: N.B. Suppose that α is an algebraic integer and let

$$F = F(X;\alpha_1,\ldots,\alpha_d) \in Z[X;\alpha_1,\ldots,\alpha_d].$$

Assume: As a polynomial in $\alpha_1,\ldots,\alpha_d$ with coefficients in $Z[X]$, F is symmetric -- then

$$F = F(X) \in Z[X].$$

§19. *TRANSCENDENCE OF* π

Here is the objective:

<u>1:</u> THEOREM π is transcendental.

Suppose that π is algebraic -- then $\alpha \equiv \pi\sqrt{-1}$ is algebraic. Agreeing to use the notation of §18, #4, in view of the relation $e^{\pi\sqrt{-1}} + 1 = 0$, it follows that

$$(1 + e^{\alpha_1})(1 + e^{\alpha_2}) \cdots (1 + e^{\alpha_d}) = 0$$

or still, upon expanding the product,

$$\sum_{\varepsilon_1=0}^{1} \sum_{\varepsilon_2=0}^{1} \cdots \sum_{\varepsilon_d=0}^{1} e^{\varepsilon_1\alpha_1 + \varepsilon_2\alpha_2 + \cdots + \varepsilon_d\alpha_d} = 0.$$

<u>2:</u> EXAMPLE Take $\varepsilon_1 = 1$, $\varepsilon_2 = \cdots = \varepsilon_d = 0$ -- then

$$\varepsilon_1\alpha_1 + \varepsilon_2\alpha_2 + \cdots + \varepsilon_d\alpha_d \neq 0.$$

Take $\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_d = 0$ -- then

$$\varepsilon_1\alpha_1 + \varepsilon_2\alpha_2 + \cdots + \varepsilon_d\alpha_d = 0.$$

Denoting the exponents by β_k, rewrite matters in the form

$$1 + \sum_{k=1}^{2^d-1} e^{\beta_k} = 0,$$

where things have been arranged so that the nonzero β_k are placed first:

$$\beta_1 \neq 0,\ \beta_2 \neq 0, \ldots,\ \beta_r \neq 0,\ 0, \ldots, 0.$$

Put

$$A = 1 + (2^d - 1) - r.$$

Then $A \geq 1$ and

$$1 + \sum_{k=1}^{2^d-1} e^{\beta_k}$$

$$= A + e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_r} = 0.$$

3: LEMMA The nonzero numbers $\beta_1, \ldots, \beta_r$ are the set of roots of a polynomial $\varphi(X) \in Z[X]$ of degree r (hence are algebraic).

PROOF Let

$$\psi(X) = \prod_{\varepsilon_1=0}^{1} \prod_{\varepsilon_2=0}^{1} \cdots \prod_{\varepsilon_d=1}^{1} (X - (\varepsilon_1\alpha_1 + \varepsilon_2\alpha_2 + \cdots + \varepsilon_d\alpha_d)).$$

Viewed as a polynomial in $\alpha_1, \alpha_2, \ldots, \alpha_d$ with coefficients in $Q[X]$, it is symmetric. Therefore $\psi(X)$ is in $Q[X]$ (cf. §18, #4). On the other hand, the roots of $\psi(X)$ are the β_k $(1 \leq k \leq r)$ and 0 with multiplicity $A(r + A = r + 2^d - r = 2^d$, the degree of $\psi(X))$, thus the roots of the polynomial

$$X^{-A}\psi(X)$$

are $\beta_1, \ldots, \beta_r$. Denoting by m the least common denominator of the coefficients of this polynomial, take

$$\varphi(X) = mX^{-A}\psi(X)$$

$$= C_rX^r + \cdots + C_1X + C_0$$

$$\in Z[X] \quad (C_r > 0,\ C_0 \neq 0).$$

4: RAPPEL Given $f \in R[X]$ of degree M,

$$e^x \int_0^x f(t)e^{-t}dt = F(0)e^x - F(x) \quad \text{(cf. §17, #3)}.$$

[Note: Complex x are admitted in which case the integral $\int_0^x$ is calculated along the line segment joining 0 and x.]

Feed into this relation $x = \beta_1, \ldots, x = \beta_r$ to get:

$$\begin{cases} e^{\beta_1} \int_0^{\beta_1} f(t)e^{-t}dt = F(0)e^{\beta_1} - F(\beta_1) \\ \vdots \\ e^{\beta_r} \int_0^{\beta_r} f(t)e^{-t}dt = F(0)e^{\beta_r} - F(\beta_r). \end{cases}$$

But

$$A + e^{\beta_1} + \cdots + e^{\beta_r} = 0.$$

Therefore

$$- AF(0) - \sum_{k=1}^{r} F(\beta_k) = \sum_{k=1}^{r} e^{\beta_k} \int_0^{\beta_k} f(t)e^{-t}dt.$$

Just as in the proof of the transcendence of e, the modus operandi at this juncture is to choose f judiciously so as to bring about a contradiction. To this end, let

$$f(X) = \frac{1}{(n-1)!} (C_r)^{nr-1} X^{n-1}(\varphi(X))^n$$

or still,

$$f(X) = \frac{1}{(n-1)!} (C_r)^{nr-1} X^{n-1}(C_r(X - \beta_1)\cdots(X - \beta_r))^n$$

$$= \frac{1}{(n-1)!} (C_r)^{n(r+1)-1} X^{n-1}(X - \beta_1)^n \cdots (X - \beta_r)^n,$$

$n \in \mathbb{N}$ a "large" natural number to be held in abeyance for the moment.

FACTS

$$\deg f = n(r+1) - 1 \equiv M,$$

$$f^{(\ell)}(0) = 0 \quad (0 \leq \ell \leq n-2),$$

$$f^{(n-1)}(0) = (C_r)^{nr-1} C_0^n,$$

$$n \mid f^{(\ell)}(0) \quad (\forall\, \ell \neq n-1).$$

Consequently

$$\begin{aligned} F(0) &= \sum_{\ell=0}^{M} f^{(\ell)}(0) \\ &= \sum_{\ell=n-1}^{M} f^{(\ell)}(0) \\ &= f^{(n-1)}(0) + f^{(n)}(0) + \cdots + f^{(n(r+1)-1)}(0) \\ &= (C_r)^{nr-1} C_0^n + nC, \end{aligned}$$

C an integer.

Moving on, from the definitions,

$$F(\beta_k) = \sum_{\ell=0}^{M} f^{(\ell)}(\beta_k).$$

And β_k is a root of $f(X)$ of multiplicity n, thus

$$f^{(\ell)}(\beta_k) = 0 \quad (0 \leq \ell \leq n-1,\ 1 \leq k \leq r),$$

leaving

$$F(\beta_k) = \sum_{\ell=n}^{M} f^{(\ell)}(\beta_k).$$

<u>5:</u> LEMMA If $p(X) \in Z[X]$, then $\forall\, \ell \in N$, all the coefficients of the ℓ^{th} derivative $p^{(\ell)}(X)$ are divisible by $\ell!$.

PROOF Since differentiation is a linear operation, it suffices to check this on the powers X^k, restricting ourselves to when $1 \leq \ell \leq k$, in which case the ℓ^{th} derivative of X^k is equal to

$$\ell!\binom{k}{\ell}X^{k-\ell}$$

and the binomial coefficient $\binom{k}{\ell}$ is a positive integer.

It therefore follows that for $\ell \geq n$, the coefficients of $f^{(\ell)}(X)$ are integers divisible by $n(C_r)^{nr-1}$.

[In detail, the polynomial

$$X^{n-1}(\varphi(X))^n \in Z[X] \quad \text{(cf. \#3)}$$

and its ℓ^{th} derivative has all coefficients divisible by $\ell!$, so for $\ell \geq n$, its ℓ^{th} derivative has all coefficients divisible by $n!$ $(\ell! = n!\,(n+1)\ldots\ell)$. If $\ell \geq n$ and if generically, $n!W$ $(W \in Z)$ is a coefficient of

$$(X^{n-1}(\varphi(X))^n)^{(\ell)},$$

then

$$\frac{1}{(n-1)!}(C_r)^{nr-1}n!W = n(C_r)^{nr-1}W$$

is a coefficient of $f^{(\ell)}(X)$.]

<u>6:</u> LEMMA Let $P(X_1,\ldots,X_r)$ be a polynomial with integer coefficients of degree $s \leq t$ symmetric in the X_k -- then

$$C_r^t P(\beta_1,\ldots,\beta_r)$$

is an integer.

PROOF The algebraic numbers $C_r\beta_1,\ldots,C_r\beta_r$ are the roots of the monic polynomial

$$(C_r)^{r-1}\varphi(\frac{X}{C_r})$$

$$= X^r + C_{r-1}X^{r-1} + C_rC_{r-2}X^{r-2} + \cdots + C_r^{r-1}C_0,$$

thus the elementary symmetric polynomials per $C_r\beta_1,\ldots,C_r\beta_r$ are integers, since

$$s_1 = -\frac{C_{r-1}}{1}\ ,\ s_2 = \frac{C_rC_{r-2}}{1}\ ,\ \ldots,\ s_r = \frac{C_r^{r-1}C_0}{1}\ .$$

If $p(X_1,\ldots,X_r)$ is a homogeneous symmetric polynomial of degree $s \leq t$ with integer coefficients, then

$$C_r^s p(\beta_1,\ldots,\beta_r) = p(C_r\beta_1,\ldots,C_r\beta_r).$$

But the right hand side can be written as a polynomial with integer coefficients in the elementary symmetric polynomials per $C_r\beta_1,\ldots,C_r\beta_r$, hence

$$C_r^s p(\beta_1,\ldots,\beta_r)$$

is an integer, hence a fortiori

$$C_r^t p(\beta_1,\ldots,\beta_r)$$

is an integer. To treat the general case, simply separate the polynomial P into a sum of homogeneous polynomials p.

Fix $\ell : n \leq \ell \leq M$ and pass to

$$\sum_{k=1}^{r} f^{(\ell)}(\beta_k)$$

or still, in suggestive notation,

$$n(C_r)^{nr-1} \sum_{k=1}^{r} g_\ell(\beta_k).$$

<u>7:</u> <u>N.B.</u> The degree of $f^{(n)}$ is

$$M - n = (n(r + 1) - 1) - n = nr - 1,$$

so the degree of $f^{(\ell)}$ $(n \le \ell \le M)$ is $\le nr - 1$.

Applying #6 to

$$(C_r)^{nr-1} \sum_{k=1}^{r} g_\ell(\beta_k),$$

legal since the sum is symmetric in the β_k, we conclude that

$$\sum_{k=1}^{r} f^{(\ell)}(\beta_k) = nN_\ell,$$

N_ℓ an integer.

Therefore

$$\begin{aligned}\sum_{k=1}^{r} F(\beta_k) &= \sum_{k=1}^{r} \sum_{\ell=n}^{M} f^{(\ell)}(\beta_k) \\ &= \sum_{\ell=n}^{M} \sum_{k=1}^{r} f^{(\ell)}(\beta_k) \\ &= n \sum_{\ell=n}^{M} N_\ell \equiv nB.\end{aligned}$$

Now assemble what has been established thus far:

$$AF(0) + \sum_{k=1}^{r} F(\beta_k)$$

$$= A((C_r)^{nr-1} C_0^n + nC) + nB$$

$$= A(C_r)^{nr-1} C_0^n + n(AC + B).$$

Choose $n >> 0$ (n prime):

$$n > A \ \& \ \gcd(n, C_r C_0) = 1.$$

Then

$$A(C_r)^{nr-1} C_0^n + n(AC + B)$$

is an integer not divisible by n, hence in particular is nonzero, hence

$$|AF(0) + \sum_{k=1}^{r} F(\beta_k)| \geq 1.$$

It remains to estimate

$$\sum_{k=1}^{r} e^{\beta_k} \int_0^{\beta_k} f(t) e^{-t} dt.$$

Suppose that

$$|\beta_k| \leq R \quad (k = 1, \ldots, r)$$

and put

$$T = \max_{|z| \leq R} |(C_r)^r \varphi(z)| \quad (C_r \geq 1 \Rightarrow \frac{1}{C_r} \leq 1).$$

Then

$$\max_{|z| \leq R} |f(z)|$$

$$\leq \max_{|z| \leq R} \frac{1}{(n-1)!} |(C_r)^{nr-1} z^{n-1} (\varphi(z))^n|$$

$$\leq \max_{|z|\leq R} \frac{1}{(n-1)!} |z|^{n-1} \frac{1}{C_r} |(C_r^r)^n (\varphi(z))^n|$$

$$\leq \frac{R^{n-1}}{(n-1)!} \max_{|z|\leq R} |(C_r^r)^n (\varphi(z))^n|$$

$$\leq \frac{R^{n-1}T^n}{(n-1)!} .$$

Consequently, for all n per supra

$$\left|\sum_{k=1}^{r} e^{\beta_k} \int_0^{\beta_k} f(t)e^{-t}dt\right|$$

$$\leq \sum_{k=1}^{r} \left|e^{\beta_k} \int_0^{\beta_k} f(t)e^{-t}dt\right|$$

$$\leq \sum_{k=1}^{r} \left|\int_0^{\beta_k} |f(t)|\ |e^{(\beta_k-t)}|\ dt\right|$$

$$\leq \frac{R^{n-1}T^n}{(n-1)!} \sum_{k=1}^{r} \left|\int_0^{\beta_k} |e^{(\beta_k-t)}|\ dt\right|$$

$$\leq \frac{R^{n-1}T^n}{(n-1)!}\ e^R \sum_{k=1}^{r} \left|\int_0^{\beta_k} dt\right|$$

$$\leq \frac{R^{n-1}T^n}{(n-1)!}\ e^R(rR)$$

$$= re^R \frac{(RT)^n}{(n-1)!} = re^R(RT)\ \frac{(RT)^{n-1}}{(n-1)!} ,$$

which leads to a contradiction in the usual way (cf. §0).

§20. ALGEBRAIC (IN)DEPENDENCE

1: TERMINOLOGY Let L be a field, $K \subset L$ a subfield.

- A finite subset $S = \{\alpha_1,\ldots,\alpha_n\} \subset L$ is algebraically dependent over K if there is a nonzero polynomial $P \in K[X_1,\ldots,X_n]$ such that

$$P(\alpha_1,\ldots,\alpha_n) = 0.$$

- A finite subset $S = \{\alpha_1,\ldots,\alpha_n\} \subset L$ is algebraically independent over K if there is no nonzero polynomial $P \in K[X_1,\ldots,X_n]$ such that

$$P(\alpha_1,\ldots,\alpha_n) = 0.$$

2: N.B. Take $S = \{\alpha\}$, a one element set -- then by definition, α is algebraic over K if S is algebraically dependent over K and α is transcendental over K if S is algebraically independent over K, i.e., $\alpha \in S$ is algebraic or transcendental over K according to whether it is or is not a root of a polynomial in K[X] (cf. §2, #25).

3: LEMMA Suppose that S is algebraically independent over K -- then the elements of S are transcendental over K.

The setup for us is when

$$L = \mathbf{C} \text{ and } K = \mathbf{Q},$$

in which case one can work either with polynomials P in $\mathbf{Q}[X_1,\ldots,X_n]$ or in $\mathbf{Z}[X_1,\ldots,X_n]$.

[Note: Here, of course, "algebraic" means algebraic over Q and "transcendental" means transcendental over Q and to say that the complex numbers $x_1,\ldots,x_n$ are algebraically dependent or algebraically independent means that the set $\{x_1,\ldots,x_n\}$ is algebraically dependent over Q or algebraically independent over Q.]

4: REMARK A complex number x is transcendental iff the numbers $1, x, x^2,\ldots$ are linearly independent over Q. And, in general, the complex numbers $x_1,\ldots,x_n$ are algebraically independent over Q iff the powers

$$x_1^{k_1} \cdots x_n^{k_n} \quad (k_i \in Z, k_i \geq 0)$$

are linearly independent over Q.

5: LEMMA Suppose that $S \subset C$ is algebraically independent over Q -- then the elements of S are transcendental over Q (cf. #3).

[Note: If any of the elements in S are algebraic over Q, then S is algebraically dependent over Q.]

6: REMARK It can happen that all the elements of S are transcendental over Q, yet S is not algebraically independent over Q.

[The real numbers $\sqrt{\pi}$ and $2\pi + 1$ are transcendental but $\{\sqrt{\pi}, 2\pi + 1\}$ is not algebraically independent over Q. Thus consider

$$P(X,Y) = 2X^2 - Y + 1.$$

Then

$$P(\sqrt{\pi}, 2\pi + 1) = 0.]$$

7: LEMMA If $\{x_1,\ldots,x_n\}$ is algebraically independent over Q, then $\{x_1,\ldots,x_n\}$ is algebraically independent over $\bar{Q}$ and for any nonconstant polynomial

$P \in \bar{Q}[X_1,\ldots,X_n]$, the number

$$P(x_1,\ldots,x_n)$$

is transcendental.

8: EXAMPLE The numbers $e^{\sqrt{2}}$, $e^{3\sqrt{2}}$ are algebraically dependent.

[Consider

$$P(X_1,X_2) = X_1^3 - X_2.$$

Then

$$P(e^{\sqrt{2}}, e^{3\sqrt{2}}) = (e^{\sqrt{2}})^3 - e^{3\sqrt{2}}$$

$$= e^{3\sqrt{2}} - e^{3\sqrt{2}} = 0.]$$

9: EXAMPLE Let a and b be relatively prime natural numbers ≥ 1 -- then the Liouville numbers (cf. §15, #9)

$$x = \sum_{j=1}^{\infty} \frac{1}{a^{j!}} \text{ and } y = \sum_{j=1}^{\infty} \frac{1}{b^{j!}}$$

are algebraically independent over Q.

10: EXAMPLE Nesterenko proved in 1996 that the numbers π, e^{π} are algebraically independent over Q.

11: REMARK The question of whether the numbers e,π are algebraically dependent over Q or algebraically independent over Q is open.

Instead of numbers, one must also deal with functions.

12: DEFINITION A function f(z) of a complex variable z is algebraic if there is a nonzero polynomial $P \in \mathbb{C}[X,Y]$ such that $\forall z$,

$$P(z,f(z)) = 0.$$

13: THEOREM An entire function is algebraic iff it is a polynomial.

14: DEFINITION An entire function which is not algebraic is said to be transcendental.

15: EXAMPLE e^z, $\cos z$, $\sin z$ are transcendental, as is the function $z \to \int_0^z e^{-t^2}\,dt$.

16: DEFINITION A collection of entire functions $f_1,\ldots,f_n$ is said to be algebraically dependent over $\mathbb{C}$ if there is a nonzero polynomial $P \in \mathbb{C}[X_1,\ldots,X_n]$ such that $P(f_1,\ldots,f_n)$ is the zero function.

17: DEFINITION A collection of entire functions $f_1,\ldots,f_n$ is said to be algebraically independent over $\mathbb{C}$ if for any nonzero polynomial $P \in \mathbb{C}[X_1,\ldots,X_n]$, the function $P(f_1,\ldots,f_n)$ is not the zero function.

18: EXAMPLE Let $I(z) = z$ be the identity function -- then an entire function f is algebraic (transcendental) iff I and f are algebraically dependent (independent) over $\mathbb{C}$.

19: EXAMPLE $\sin z$ and $\cos z$ are algebraically dependent over $\mathbb{C}$.

[Consider

$$P(X,Y) = X^2 + Y^2 - 1.$$

Then

$$P(\sin z, \cos z) = (\sin z)^2 + (\cos z)^2 - 1 = 1 - 1 = 0.]$$

20: EXAMPLE Take

$$f_1(z) = e^z,\ f_2(z) = e^{\frac{1}{2}z}.$$

Then thé functions f_1, f_2 are algebraically dependent over $\mathbb{C}$.

[Consider

$$P(X_1,X_2) = X_2^6 - X_1X_2^4 + X_1^2X_2^2 - X_1^3.$$

Then

$$\begin{aligned} P(e^z, e^{\frac{1}{2}z}) &= e^{3z} - e^{3z} + e^{3z} - e^{3z} \\ &= 0.] \end{aligned}$$

21: EXAMPLE Take

$$f_1(z) = e^z,\ f_2(z) = e^{\sqrt{-1}\,z}.$$

Then the functions f_1, f_2 are algebraically independent over $\mathbb{C}$ (cf. #26 infra).

[Fix a nonzero $P \in \mathbb{C}[X_1,X_2]$ and choose z_0 such that the polynomial $P(e^z, e^{\sqrt{-1}\,z_0})$ in z is not identically zero. Use the periodicity of e^z to infer that if $P(e^z, e^{\sqrt{-1}\,z})$ is identically zero, then the polynomial $P(x, e^{\sqrt{-1}\,z_0})$ in x has infinitely many zeros, namely $\forall\ k \in \mathbb{Z}$,

$$\begin{aligned} &P(e^{z_0 + 2\pi\sqrt{-1}\,k}, e^{\sqrt{-1}\,z_0}) \\ &\quad = P(e^{z_0}, e^{\sqrt{-1}\,z_0}) = 0.] \end{aligned}$$

<u>22:</u> EXAMPLE The functions $1, z, z^2, \ldots, z^n$ are linearly independent over $\mathbb{C}$ and the functions $z, e^z, e^{z^2}, \ldots, e^{z^n}$ are algebraically independent over $\mathbb{C}$.

<u>23:</u> LEMMA Let $\lambda_1, \ldots, \lambda_n$ be distinct complex numbers -- then the entire functions

$$e^{\lambda_1 z}, \ldots, e^{\lambda_n z}$$

are linearly independent over $\mathbb{C}(z)$.

PROOF The case $n = 1$ is trivial. Proceed from here by induction, assuming that the statement is true at level $n - 1$ $(n > 1)$ and consider the dependence relation

$$F_1 e^{\lambda_1 z} + \cdots + F_n e^{\lambda_n z} = 0,$$

where $F_1, \ldots, F_n$ are nonzero elements of $\mathbb{C}(z)$, the objective being to derive a contradiction from this. Divide by F_n:

$$\frac{F_1}{F_n} e^{\lambda_1 z} + \cdots + \frac{F_n}{F_n} e^{\lambda_n z} \equiv G_1 e^{\lambda_1 z} + \cdots + 1\, e^{\lambda_n z} \quad (G_n = 1)$$

$$= 0$$

or still,

$$e^{\lambda_n z}(G_1 e^{(\lambda_1 - \lambda_n) z} + \cdots + 1\, e^{0z}) = 0$$

or still,

$$G_1 e^{(\lambda_1 - \lambda_n) z} + \cdots + 1\, e^{0z} = 0$$

or still,

$$G_1^{\sigma_1 z} + \cdots + 1\, e^{\sigma_n z} = 0,$$

where

$$\sigma_1 = \lambda_2 - \lambda_n \neq 0, \ldots, \sigma_n = 0.$$

Now differentiate:

$$(G_1' + \sigma_1 G_1)e^{\sigma_1 z} + \cdots + (G_{n-1}' + \sigma_{n-1} G_{n-1})e^{\sigma_{n-1} z} = 0,$$

thereby leading to a dependence relation at level n - 1 with distinct exponents $\sigma_1, \ldots, \sigma_{n-1}$, so

$$G_1' + \sigma_1 G_1 = 0, \ldots, G_{n-1}' + \sigma_{n-1} G_{n-1} = 0.$$

But each of these coefficients is nonzero, hence the purported dependence relation

$$F_1 e^{\lambda_1 z} + \cdots + F_n e^{\lambda_n z} = 0$$

has led to a contradiction.

<u>24:</u> APPLICATION Let $\lambda_1, \ldots, \lambda_n$ be distinct complex numbers -- then the entire function

$$c_1 e^{\lambda_1 z} + \cdots + c_n e^{\lambda_n z} \quad (c_1, \ldots, c_n \in \mathbb{C})$$

is not identically zero if the c_i are not all zero.

<u>25:</u> LEMMA Let $\lambda_1, \ldots, \lambda_n$ be distinct complex numbers which are linearly independent over $\mathbb{Q}$ -- then the entire functions

$$e^{\lambda_1 z}, \ldots, e^{\lambda_n z}$$

are algebraically independent over $\mathbb{C}$.

PROOF Let

$$P(X_1, \ldots, X_n) \in \mathbb{C}[X_1, \ldots, X_n]$$

be a nonzero polynomial -- then the claim is that

$$f(z) = P(e^{\lambda_1 z},\ldots,e^{\lambda_n z})$$

is not identically zero. To this end, write

$$P(X_1,\ldots,X_n) = \sum_{(k_1,\ldots,k_n)} a_{k_1,\ldots,k_n} X_1^{k_1}\cdots X_n^{k_n},$$

where the $a_{k_1,\ldots,k_n} \in \mathbf{C}$ and not all of them are zero, thus

$$f(z) = \sum_{(k_1,\ldots,k_n)} a_{k_1,\ldots,k_n} \exp((k_1\lambda_1 + \cdots k_n\lambda_n)z).$$

But, due to our assumption on $\lambda_1,\ldots,\lambda_n$, the complex numbers

$$k_1\lambda_1 + \cdots + k_n\lambda_n$$

are distinct:

$$k_1\lambda_1 + \cdots + k_n\lambda_n = \ell_1\lambda_1 + \cdots + \ell_n\lambda_n$$

$\Rightarrow$

$$(k_1 - \ell_1)\lambda_1 + \cdots + (k_n - \ell_n)\lambda_n = 0$$

$\Rightarrow$

$$(k_1 - \ell_1) = 0,\ldots,(k_n - \ell_n) = 0.$$

To conclude that $f(z)$ is not identically zero, it remains only to quote #24.

<u>26:</u> EXAMPLE Take $\lambda_1 = 1$, $\lambda_2 = \beta \notin \mathbf{Q}$ -- then e^z, $e^{\beta z}$ are algebraically independent over $\mathbf{C}$ (take $\beta = \sqrt{-1}$ to recover #21).

§21. *THE LINDEMANN-WEIERSTRASS THEOREM*

This is the following statement.

1: THEOREM Let $\alpha_0, \alpha_1, \ldots, \alpha_t$ be distinct algebraic numbers -- then e^{α_0}, $e^{\alpha_1}, \ldots, e^{\alpha_t}$ are linearly independent over $\bar{Q}$, i.e., if $b_0, b_1, \ldots, b_t$ are algebraic numbers not all zero, then

$$b_0 e^{\alpha_0} + b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} \neq 0.$$

[Note:

$$b_0 e^{\alpha_0} + b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t}$$

is a transcendental number. For suppose it was algebraic, say

$$b_0 e^{\alpha_0} + b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} = c(\in \bar{Q}) = ce^0.$$

Then

$$b_0 e^{\alpha_0} + b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} - ce^0 = 0.$$

There are now two possibilities:

- $\alpha_i \neq 0 \ \forall \ i = 0,1,\ldots,t$, so $\alpha_0, \alpha_1, \ldots, \alpha_t, 0$ are distinct, from which the obvious contradiction.

- $\exists \ i:\alpha_i = 0$, say $i = 0$, hence

$$(b_0 - c)e^0 + b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} = 0,$$

where $0, \alpha_1, \ldots, \alpha_t$ are distinct, a contradiction once again.]

2: N.B. We are working here in the complex domain, hence $\sqrt{-1}$ is algebraic (consider $X^2 + 1 = 0$) and $\bar{Q}$, computed in C, is a field.

3: LEMMA Suppose that a and b are real -- then $a + \sqrt{-1}\, b$ is algebraic iff a and b are algebraic (cf. §14, #4).

PROOF If a and b are algebraic, then the combination $a + \sqrt{-1}\, b$ is algebraic ($\bar{Q}$ being a field). Conversely, if $a + \sqrt{-1}\, b$ is algebraic, then $p(a + \sqrt{-1}\, b) = 0$, where $p(X)$ is a polynomial with rational coefficients, thus also $p(a - \sqrt{-1}\, b) = 0$. Therefore

$$\left[\begin{array}{l} (a + \sqrt{-1}\, b) + (a - \sqrt{-1}\, b) = 2a \in \bar{Q} \\ \\ (a + \sqrt{-1}\, b) - (a - \sqrt{-1}\, b) = 2\sqrt{-1}\, b \in \bar{Q} \end{array}\right. \Rightarrow \left[\begin{array}{l} \frac{1}{2}(2a) = a \in \bar{Q} \\ \\ -\frac{\sqrt{-1}}{2}(2\sqrt{-1}\, b) = b \in \bar{Q}, \end{array}\right.$$

i.e., a and b are algebraic.]

Before tackling the proof of the theorem, we shall consider some applications and examples.

4: LEMMA If α is a nonzero algebraic number, then e^α is transcendental (Hermite-Lindemann).

[A nontrivial relation of the form

$$q_0 + q_1 e^\alpha + \cdots + q_n e^{n\alpha} = 0 \quad (q_k \in Q)$$

is impossible, or, alternatively, consider the formula

$$(1^0)e^\alpha - (e^\alpha)e^0 = 0$$

which, if e^α were algebraic, would be impossible.]

[Note: Consequently, if a is a nonzero complex number, then at least one of the numbers a or e^a is transcendental.]

In particular: e is transcendental (cf. §17, #1). And if $a,b \in \mathbb{N}$, then $e^a \neq b$.

<u>5:</u> EXAMPLE $e^{\sqrt{2}}$ is transcendental.

<u>6:</u> EXAMPLE π is transcendental (cf. §19, #1).

[For if π were algebraic, then $\pi\sqrt{-1}$ would be algebraic, hence $e^{\pi\sqrt{-1}}$ would be transcendental (cf. #4), contrary to the fact that $1 + e^{\pi\sqrt{-1}} = 0$.]

<u>7:</u> EXAMPLE Let α be a real nonzero algebraic number -- then $\cos(\alpha)$ is transcendental (cf. §12, #1).

[Suppose instead that $\cos(\alpha) \equiv \beta$ was algebraic. Write

$$\cos(\alpha) = \frac{e^{\alpha\sqrt{-1}} + e^{-\alpha\sqrt{-1}}}{2\sqrt{-1}} = \frac{e^{\alpha\sqrt{-1}}}{2\sqrt{-1}} + \frac{e^{-\alpha\sqrt{-1}}}{2\sqrt{-1}}$$

or still,

$$\left(-\frac{\sqrt{-1}}{2}\right) e^{\sqrt{-1}\alpha} + \left(-\frac{\sqrt{-1}}{2}\right) e^{-\sqrt{-1}\alpha} + (-\beta)e^{0} = 0,$$

a contradiction (cf. #1) ($\sqrt{-1}\alpha$ and $-\sqrt{-1}\alpha$ are obviously distinct).]

[Note: Consider the unique real fixed point of the cosine function, thus $\cos(x) = x = 0.739085\ldots$ -- then x is transcendental. For suppose that x is algebraic -- then $\cos(x)$ would be transcendental. But $\cos(x) = x$.]

The story for $\sin(\alpha)$ is analogous, as are the stories for

$$\left[\begin{array}{l} \cosh(\alpha) \\ \sinh(\alpha). \end{array}\right.$$

8: EXAMPLE Let α be a real nonzero algebraic number -- then $\tan(\alpha)$ is transcendental.

[Assuming the opposite, write

$$\tan(\alpha) = \frac{e^{\alpha\sqrt{-1}} - e^{-\alpha\sqrt{-1}}}{\sqrt{-1}(e^{\alpha\sqrt{-1}} + e^{-\alpha\sqrt{-1}})} \equiv \beta$$

$$\Rightarrow$$

$$(1 - \beta\sqrt{-1})e^{\alpha\sqrt{-1}} - (1 + \beta\sqrt{-1})e^{-\alpha\sqrt{-1}} = 0$$

and note that $1 - \beta\sqrt{-1}$ and $1 + \beta\sqrt{-1}$ cannot simultaneously be zero.]

9: EXAMPLE Let $\alpha \neq 1$ be a positive algebraic number -- then $\ell n(\alpha)$ is transcendental.

[If $\ell n(\alpha)$ were algebraic, then $e^{\ell n(\alpha)}$ would be transcendental (cf. #4). But $e^{\ell n(\alpha)} = \alpha \ldots$.]

10: LEMMA Let α be a nonreal algebraic number -- then

$$\left[\begin{matrix} \operatorname{Re}(e^{\alpha}) \\ \\ \operatorname{Im}(e^{\alpha}) \end{matrix}\right.$$

are transcendental.

PROOF Write $\alpha = a + \sqrt{-1}\, b$ $(b \neq 0)$ -- then a and b are algebraic (cf. #3). Moreover, by definition,

$$e^{\alpha} = e^{a + \sqrt{-1}b} = e^{a}(\cos b + \sqrt{-1} \sin b)$$

and the claim is that

$$\left[\begin{matrix} e^{a} \cos b \\ \\ e^{a} \sin b \end{matrix}\right.$$

are transcendental. To deal with the first of these, proceed by contradiction and assume that $e^a \cos b \equiv \beta$ is algebraic, thus $\beta \neq 0$ (the zeros of the cosine are transcendental). Next

$$e^{a + \sqrt{-1}\, b} + e^{a - \sqrt{-1}\, b}$$

$$= e^a(e^{\sqrt{-1}\, b} + e^{-\sqrt{-1}\, b})$$

$$= e^a(\cos b + \sqrt{-1} \sin b + \cos(-b) + \sqrt{-1} \sin(-b))$$

$$= 2e^a \cos b = 2\beta,$$

$\Rightarrow$

$$2\beta e^0 - e^{a + \sqrt{-1}\, b} - e^{a - \sqrt{-1}\, b} = 0.$$

Owing to #1, the algebraic numbers 0, $a + \sqrt{-1}\, b$, $a - \sqrt{-1}\, b$ are not distinct, hence $b = 0$. On the other hand, α is not real, so $b \neq 0$.

11: N.B. If in #10, α was real, then matters are covered by #4.

12: THEOREM Suppose that $\beta_1, \ldots, \beta_r$ are nonzero algebraic numbers which are linearly independent over Q -- then the transcendental numbers $e^{\beta_1}, \ldots, e^{\beta_r}$ are algebraically independent over Q.

PROOF Assume instead that for some nonzero polynomial

$$P(X_1, \ldots, X_r) \in Q\,[X_1, \ldots, X_r],$$

say

$$P(X_1, \ldots, X_r) = \sum_{(k_1, \ldots, k_r)} a_{k_1, \ldots, k_r} X_1^{k_1} \cdots X_r^{k_r},$$

we have

$$P(e^{\beta_1},\ldots,e^{\beta_r}) = 0$$

or still,

$$\sum_{(k_1,\ldots,k_r)} a_{k_1,\ldots,k_r} e^{k_1\beta_1 + \cdots + k_r\beta_r} = 0,$$

where the $a_{k_1,\ldots,k_r} \in Q$ and not all of them are zero. To settle the issue and arrive at a contradiction, it suffices to check that the exponents

$$k_1\beta_1 + \cdots + k_r\beta_r$$

are distinct (since then one can quote #1). So suppose that

$$(k_1,\ldots,k_r) \neq (\ell_1,\ldots,\ell_r)$$

with

$$k_1\beta_1 + \cdots + k_r\beta_r = \ell_1\beta_1 + \cdots + \ell_r\beta_r,$$

thus

$$(k_1 - \ell_1)\beta_1 + \cdots + (k_r - \ell_r)\beta_r = 0,$$

a nontrivial dependence relation over Q.

13: EXAMPLE The transcendental numbers e, $e^{\sqrt{2}}$ are algebraically independent over Q.

[For it is clear that the algebraic numbers 1, $\sqrt{2}$ are linearly independent over Q.]

14: THEOREM Suppose that $\beta_1,\ldots,\beta_r$ are nonzero algebraic numbers for which the transcendental numbers $e^{\beta_1},\ldots,e^{\beta_r}$ are algebraically independent over Q — then $\beta_1,\ldots,\beta_r$ are linearly independent over Q.

PROOF Consider a nontrivial dependence relation over Q:

$$b_1\beta_1 + \cdots + b_r\beta_r = 0.$$

Clear the denominators and take the b_k integral -- then not all of them are zero and

$$1 = e^0 = e^{b_1\beta_1 + \cdots + b_r\beta_r}.$$

Define

$$P(X_1,\ldots,X_r) \in Q[X_1,\ldots,X_r]$$

by the prescription

$$P(X_1,\ldots,X_r) = X_1^{b_1} \cdots X_r^{b_r} - 1.$$

Then

$$P(e^{\beta_1},\ldots,e^{\beta_r}) = e^{b_1\beta_1} \cdots e^{b_r\beta_r} - 1$$

$$= e^{b_1\beta_1 + \cdots + b_r\beta_r} - 1 = 1 - 1 = 0.$$

But $e^{\beta_1},\ldots,e^{\beta_r}$ are algebraically independent over Q. Therefore

$$P(X_1,\ldots,X_r) \equiv 0 \Rightarrow b_1 = 0,\ldots,b_r = 0,$$

a contradiction.

<u>15:</u> SCHOLIUM Nonzero algebraic numbers $\beta_1,\ldots,\beta_r$ are linearly independent over Q iff the transcendental numbers $e^{\beta_1},\ldots,e^{\beta_r}$ are algebraically independent over Q.

<u>16:</u> LEMMA Let α be an algebraic number whose real and imaginary parts are both nonzero -- then the transcendental numbers $\mathrm{Re}(e^\alpha)$, $\mathrm{Im}(e^\alpha)$ are algebraically independent over Q (cf. #10).

We need a preliminary.

<u>17:</u> SUBLEMMA Let x and y be nonzero real numbers -- then x and y are algebraically dependent over Q iff $x + \sqrt{-1}\, y$ and $x - \sqrt{-1}\, y$ are algebraically dependent over Q.

PROOF To deal with one direction, assume that there exists a nonzero polynomial

$$P(X,Y) = \sum_{m,n} a_{mn} X^m Y^n \in Q[X,Y]$$

such that

$$P(x,y) = 0.$$

Let

$$\left[\begin{array}{l} \alpha = x + \sqrt{-1}\, y \\ \\ \bar{\alpha} = x - \sqrt{-1}\, y \end{array}\right. \Rightarrow \left[\begin{array}{l} x = \dfrac{\alpha + \bar{\alpha}}{2} \\ \\ y = \dfrac{\alpha - \bar{\alpha}}{2\sqrt{-1}} \end{array}\right. .$$

Then

$$\sum_{m,n} a_{mn} \left(\frac{1}{2}\right)^{m+n} (-\sqrt{-1})^n (\alpha + \bar{\alpha})^m (\alpha - \bar{\alpha})^n = 0.$$

Introduce

$$Q(X,Y) = \sum_{m,n} a_{mn} \left(\frac{1}{2}\right)^{m+n} (-\sqrt{-1})^n X^m Y^n$$

$$\bar{Q}(X,Y) = \sum_{m,n} a_{mn} \left(\frac{1}{2}\right)^{m+n} (\sqrt{-1})^n X^m Y^n.$$

Thus

$$Q, \bar{Q} \in C[X,Y]$$

but

$$Q\bar{Q} \in \mathbb{Q}[X,Y].$$

Put now

$$P^+(X,Y) = Q(X + Y, X - Y)\bar{Q}(X + Y, X - Y).$$

Then

$$Q(\alpha + \bar{\alpha}, \alpha - \bar{\alpha}) = 0,$$

so

$$P^+(\alpha,\bar{\alpha}) = 0,$$

thereby establishing that α and $\bar{\alpha}$ are algebraically dependent over $\mathbb{Q}$.

Passing to the proof of #16, write $\alpha = a + \sqrt{-1}\, b$ (thus $a \neq 0$, $b \neq 0$ are algebraic (cf. #3)) -- then $e^a \cos b$ and $e^a \sin b$ are algebraically dependent over $\mathbb{Q}$ iff

$$e^{\alpha} = e^a \cos b + \sqrt{-1}\, e^a \sin b \text{ and } e^{\bar{\alpha}} = e^a \cos b - \sqrt{-1}\, e^a \sin b$$

are algebraically dependent over $\mathbb{Q}$ (cf. #17), i.e., iff α and $\bar{\alpha}$ are linearly dependent over $\mathbb{Q}$ (cf. #15), i.e., iff $a = 0$ or $b = 0$, which cannot be.

We shall conclude this § with an indication of the steps leading up to a proof of #1. So let as there $b_0, b_1, \ldots, b_t$ be algebraic numbers not all zero but with

$$b_0 e^{\alpha_0} + b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} = 0.$$

<u>Step 1</u>: By discarding terms whose coefficients are zero and rearranging the notation, it can be assumed that no coefficient is zero and

$$b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} = 0.$$

Consider the Taylor series expansion

$$b_1 e^{\alpha_1 z} + \cdots + b_t e^{\alpha_t z} = \sum_{n=0}^{\infty} \frac{u_n}{n!} z^n.$$

<u>Step 2:</u> $\forall\, n = 0,1,\ldots,$

$$u_n = \sum_{i=1}^{t} b_i \alpha_i^n.$$

Define $a_1,\ldots,a_t$ by writing

$$(X - \alpha_1)\cdots(X - \alpha_t) = X^t - a_1 X^{t-1} - \cdots - a_t.$$

<u>Step 3:</u> $\forall\, n = 0,1,\ldots,$

$$\alpha_i^{t+n} = a_1 \alpha_i^{t+n-1} + \cdots + a_t \alpha_i^n \quad (i = 1,\ldots,t).$$

<u>Step 4:</u> $\forall\, n = 0,1,\ldots,$

$$u_{n+t} = a_1 u_{n+t-1} + \cdots + a_t u_n.$$

<u>Step 5:</u> It suffices to treat the case in which the $u_n \in Q$ $(n = 0,1,\ldots)$ and the $a_i \in Q$ $(i = 1,\ldots,t)$.

[Consider the product

$$\prod_{\sigma} (\sigma(b_1) e^{\sigma(\alpha_1) z} + \cdots + \sigma(b_t) e^{\sigma(\alpha_t) z}),$$

where

$$\sigma \in \mathrm{Gal}(Q(b_1,\ldots,b_t,\ \alpha_1,\ldots,\alpha_t)/Q).$$

This expression is still 0 (one of its factors is zero) and upon expanding has the form

$$\sum_i b_i' e^{\alpha_i' z}.$$

Since the sets $\{b_i'\}$, $\{\alpha_i'\}$ are Galois stable, the numbers u_n' and a_i' are rational.]

Step 6: Upon clearing denominators if necessary, it can be assumed that $u_0, \ldots, u_{t-1} \in Z$, thus using Step 4 recursively, $\forall\, n \geq 0$,

$$d^n u_n \in Z,$$

where d is a common denominator of the a_i $(i = 1, \ldots, t)$.

[So, if $d = 1$, then the u_n are integers.]

Step 7: Put

$$A = \max\{1, |\alpha_1|, \ldots, |\alpha_t|\}.$$

Then there exists a positive constant C such that $\forall\, n \geq 0$,

$$|u_n| \leq CA^n \quad \text{(use Step 2)}.$$

Recall now that the assumption is that

$$b_1 e^{\alpha_1} + \cdots + b_t e^{\alpha_t} = 0,$$

hence

$$\sum_{n=0}^{\infty} \frac{u_n}{n!} = 0.$$

Given $k \in N$, put

$$v_k = k! \sum_{n=0}^{k} \frac{u_n}{n!} \; (v_0 \equiv u_0).$$

<u>Step 8:</u> $\forall\, k ; A < k + 1$,

$$|v_k| = k! \; \Big| \sum_{n=0}^{k} \frac{u_n}{n!} \Big|$$

$$= k! \; \Big| \sum_{n=k+1}^{\infty} \frac{u_n}{n!} \Big|$$

$$\le k! \sum_{n=k+1}^{\infty} \frac{|u_n|}{n!}$$

$$\le Ck! \sum_{n=k+1}^{\infty} \frac{A^n}{n!}$$

$$= Ck! \; \left(\frac{A^{k+1}}{(k+1)!} + \frac{A^{k+2}}{(k+2)!} + \cdots \right)$$

$$= C \; \left(\frac{A^{k+1}}{k+1} + \frac{A^{k+2}}{(k+1)(k+2)} + \cdots \right)$$

$$\le C \; \left(\frac{A^{k+1}}{k+1} + \frac{A^{k+2}}{(k+1)^2} + \cdots \right)$$

$$= CA^k \; \left(\frac{A}{k+1} + \frac{A^2}{(k+1)^2} + \cdots \right)$$

$$= CA^k \; \left(\frac{\frac{A}{k+1}}{1 - \frac{A}{k+1}}\right) \quad \left(\frac{A}{k+1} < 1\right) \quad (\text{cf. } \S 8, \#2)$$

$$= CA^k \; \left(\frac{A}{k+1-A}\right)$$

$$= C \, \frac{A^{k+1}}{k+1-A} \, .$$

<u>Step 9:</u> $\forall\, k : 2A < k + 1$,

$$0 < k + 1 - 2A$$

=>

$$k + 1 < 2(k + 1) - 2A$$

=>

$$\frac{1}{k + 1 - A} < \frac{2}{k + 1}.$$

To recapitulate: $\forall\ k: 2A < k + 1$,

$$|v_k| \leq C \frac{A^{k+1}}{k + 1 - A}$$

$$< 2C \frac{A^{k+1}}{k + 1}.$$

[Note: If $d = 1$, then the $v_k \in Z$ (cf. Step 6) and if in addition, $A = 1$, then $\forall\ k >> 0$, $v_k = 0$ (thus $\sum_{k=0}^{\infty} v_k X^k$ is a polynomial) and we would have a contradiction but, of course, in general $d > 1$ and $A > 1$.]

Step 10: Define $v_k(n)$ by the stipulation

$$\sum_{k=0}^{\infty} v_k(n) X^k = (1 - a_1 X - \cdots - a_t X^t)^n \sum_{k=0}^{\infty} v_k X^k.$$

Then $\forall\ n \geq 0$,

$$v_k(n+1) = v_k(n) - a_1 v_{k-1}(n) - \cdots - a_t v_{k-t}(n) \quad (k \geq t).$$

Step 11: Let

$$T = 1 + |a_1| + \cdots + |a_t|.$$

Then $\forall\ k \geq nt$,

$$|v_k(n)| \leq (2C)A^k T^n.$$

Moreover

$$d^k v_k(n) \in Z$$

and

$$n! \text{ divides } d^k v_k(n).$$

Step 12: If $k \geq nt$ and if $v_k(n) \neq 0$, then

$$\begin{aligned} n! &\leq |d^k v_k(n)| \\ &= d^k |v_k(n)| \\ &\leq d^k (2C) A^k T^n \\ &= (2C)(dA)^k T^n. \end{aligned}$$

So, if

$$n! > (2C)(dA)^k T^n$$

and if $k \geq nt$, then $v_k(n) = 0$.

Step 13: Choose n_0 so large that $\forall\, n \geq n_0$,

$$n! > (2C)(dA)^{10nt} T^n.$$

Step 14:

$$v_k(n) = 0 \;\forall\, n \geq n_0,\ nt \leq k \leq 10nt.$$

In particular:

$$v_k(n_0) = 0 \text{ if } n_0 t \leq k \leq 10 n_0 t.$$

Step 15:

$$v_k(n) = 0 \text{ if } n_0 \leq n \leq k/10t,$$

thus

$$v_k(n_0) = 0 \text{ if } 10n_0t \leq k.$$

Step 16: $\forall\ k \geq n_0 t$,

$$v_k(n_0) = 0.$$

Recall now the definition of $v_k(n)$, viz.

$$\sum_{k=0}^{\infty} v_k(n)X^k = (1 - a_1X - \cdots - a_tX^t)^n \sum_{k=0}^{\infty} v_kX^k.$$

Take $n = n_0$ -- then in view of Step 16,

$$\sum_{k=0}^{\infty} v_k(n_0)X^k \in Q[X].$$

Therefore

$$\sum_{k=0}^{\infty} v_kX^k \in Q(X),$$

i.e.,

$$\sum_{k=0}^{\infty} v_kX^k$$

is a rational function.

To finish this sketch, let

$$v(X) = \sum_{k=0}^{\infty} v_kX^k.$$

Then from the definitions

$$\frac{v_k}{k!} - \frac{v_{k-1}}{(k-1)!} = \frac{u_k}{k!}$$

$$\Rightarrow \quad v_k - kv_{k-1} = u_k$$

$\Rightarrow$

$$\sum_{k=0}^{\infty} (v_k - kv_{k-1})X^k = \sum_{k=0}^{\infty} u_k X^k$$

$$= \sum_{n=0}^{\infty} u_n X^n$$

$$= \sum_{n=0}^{\infty} \left(\sum_{i=1}^{t} b_i \alpha_i^n\right) X^n \qquad \text{(cf. Step 2)}$$

$$= \sum_{i=1}^{t} b_i \left(\sum_{n=0}^{\infty} \alpha_i^n X^n\right)$$

$$= \sum_{i=1}^{t} \frac{b_i}{1 - \alpha_i X}.$$

On the other hand,

$$\sum_{k=0}^{\infty} (v_k - kv_{k-1})X^k$$

$$= v(X) - X \frac{d}{dX} (Xv(X))$$

$$= (1 - X)v(X) - X^2 \frac{d}{dX} v(X).$$

Accordingly, if

$$L \equiv - X^2 \frac{d}{dX} + (1 - X),$$

then $v(X)$ satisfies the differential equation

$$Lv(X) = \sum_{i=1}^{t} \frac{b_i}{1 - \alpha_i X}.$$

And $v(X)$ is a rational function, thus the order of the nonzero poles of $Lv(X)$ is at least 2. But the poles of the rational function

$$\sum_{i=1}^{t} \frac{b_i}{1 - \alpha_i X}$$

are at the $\frac{1}{\alpha_i}$ and are simple. Contradiction.

§22. *EXCEPTIONAL SETS*

Is it true that "in general" a transcendental function takes transcendental values at algebraic points?

<u>1:</u> DEFINITION The <u>exceptional set</u> E_f of an entire function f is the set of algebraic numbers α such that $f(\alpha)$ is algebraic:

$$E_f = \{\alpha \in \bar{Q}: f(\alpha) \in \bar{Q}\}.$$

<u>2:</u> EXAMPLE Take $f(z) = e^z$ -- then $E_f = \{0\}$ (cf. §21, #4).

<u>3:</u> DEFINITION A subset S of $\bar{Q}$ is <u>exceptional</u> if there exists a transcendental function f such that $E_f = S$.

<u>4:</u> EXAMPLE An arbitrary finite subset

$$\{\alpha_1, \ldots, \alpha_n\} \subset \bar{Q}$$

is exceptional.

[Consider

$$f(z) = e^{(z-\alpha_1)\cdots(z-\alpha_n)}.$$

If $\alpha \in \bar{Q}$ and if $\alpha \neq \alpha_i$ $(i = 1, \ldots, n)$, then

$$(\alpha - \alpha_1) \ldots (\alpha - \alpha_n) \in \bar{Q}$$

is nonzero, hence $f(\alpha)$ is transcendental (cf. §21, #4).]

5: EXAMPLE Take

$$f(z) = e^z + e^{z+1}.$$

Then $E_f = \emptyset$.

[First, $f(0) = 1 + e$ is not algebraic (since e is transcendental) (cf. §17, #1). Suppose therefore that α is a nonzero algebraic number. In §21, #1, take

$$\alpha_0 = \alpha,\ \alpha_1 = \alpha + 1,\ b_0 = 1,\ b_1 = 1,$$

thus

$$e^\alpha + e^{\alpha+1}$$

is transcendental.]

6: THEOREM Given any subset $S \subset \bar{Q}$, there exists a transcendental function f such that $E_f = S$.

7: N.B. It was proved in 1895 by Stäckel that there exists a transcendental function f such that $E_f = \bar{Q}$.

8: DEFINITION The exceptional set $E_f(\text{mul})$ with multiplicities of an entire function f is the subset of $\bar{Q} \times Z_{\geq 0}$ consisting of those points (α,n) such that $f^{(n)}(\alpha) \in \bar{Q}$.

[Note: Here $f^{(n)}$ is the n^{th} derivative of f.]

9: THEOREM Given any subset $S \subset \bar{Q} \times Z_{\geq 0}$, there exists a transcendental function f such that $E_f(\text{mul}) = S$.

§23. COMPLEX LOGARITHMS AND COMPLEX POWERS

1: DEFINITION Given a complex number $z \neq 0$, a logarithm of z is a complex number w such that $e^w = z$, denoted $\log z$.

[Note: $\log 0$ is left undefined (there is no complex number w such that $e^w = 0$).]

Therefore

$$\log z = \ln(|z|) + \sqrt{-1} \arg z,$$

where $\ln(|z|)$ is the natural logarithm of $|z|$ (cf. §10, #3 & #4) and $\arg z$ is given all admissible values. Since the latter differ by multiples of 2π, it follows that the various determinations of $\log z$ differ by multiples of $2\pi\sqrt{-1}$.

2: DEFINITION The principal determination of the logarithm corresponds to the choice

$$-\pi < \operatorname{Arg} z \leq \pi,$$

so

$$-\pi < \operatorname{Im}(\log z) \leq \pi$$

and one signifies this by writing $\operatorname{Log} z$, thus $\operatorname{Log}|R_{>0} = \ln$.

3: EXAMPLE

$$\operatorname{Log}(-3\sqrt{-1}) = \ln(3) - \frac{\pi\sqrt{-1}}{2}.$$

4: N.B. The restriction of the exponential function to the horizontal strip S consisting of all complex numbers $x + \sqrt{-1}\, y$ $(-\pi < y \leq \pi)$ has an inverse: $\exp|S$ maps S bijectively to $C^\times = C - \{0\}$ and the inverse of this restriction is

$\text{Log}: \mathbf{C}^{\times} \to S$, hence

$$\left[\begin{array}{l} \text{Log} \circ \exp|S = \text{id}_S \\ \\ \exp \circ \text{Log} = \text{id}_{\mathbf{C}^{\times}}. \end{array}\right.$$

[Note: Log is discontinuous at each negative real number but is continuous everywhere else on $\mathbf{C}^{\times}$.]

5: REMARK It is always true that

$$\text{Log}(z_1 z_2) \equiv \text{Log}\, z_1 + \text{Log}\, z_2 \pmod{2\pi\sqrt{-1}}$$

but the relation

$$\text{Log}(z_1 z_2) = \text{Log}\, z_1 + \text{Log}\, z_2$$

can fail. E.g.:

$$\begin{aligned} \text{Log}((-1)\sqrt{-1}) &= \text{Log}(-\sqrt{-1}) \\ &= \ln|-\sqrt{-1}| - \frac{\pi\sqrt{-1}}{2} \\ &= \ln(1) - \frac{\pi\sqrt{-1}}{2} \\ &= -\frac{\pi\sqrt{-1}}{2} \end{aligned}$$

while

$$\begin{aligned} &\text{Log}(-1) + \text{Log}(\sqrt{-1}) \\ &\quad = (\ln(1) + \pi\sqrt{-1}) + (\ln(1) + \frac{\pi\sqrt{-1}}{2}) \\ &\quad = \frac{3\pi\sqrt{-1}}{2} \neq -\frac{\pi\sqrt{-1}}{2}. \end{aligned}$$]

6: LEMMA

$$\text{Log } z = \int_1^z \frac{dt}{t} \quad (|\arg z| < \pi),$$

the integral being taken along the line segment $[1,z]$.

7: LEMMA

$$\text{Log } z = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (z - 1)^n \quad (|z - 1| < 1).$$

8: DEFINITION Let D be an open simply connected region in the complex plane that does not contain 0 -- then a branch of log z is a continuous function L with domain D such that L(z) is a logarithm of z for each z in D:

$$e^{L(z)} = z.$$

9: EXAMPLE Take $D = \mathbb{C} - \mathbb{R}_{\leq 0}$ -- then the restriction of Log to D is a branch of log z.

10: CONSTRUCTION A branch of log z with domain D can be obtained by first fixing a point a in D, then choosing a logarithm b of a, and then defining L by the prescription

$$L(z) = b + \int_a^z \frac{dw}{w}.$$

Here the integration is along any path in D that connects a and z.

11: LEMMA L(z) is holomorphic in D, its derivative being $\frac{1}{z}$.

[Note: Different choices of b will in general lead to different functions.]

12: RAPPEL If α is a nonzero algebraic number, then e^α is transcendental (cf. §21, #4) (Hermite-Lindemann).

13: EXAMPLE (cf. §21, #9) Let α be a nonzero algebraic number -- then $\text{Log}\ \alpha$ is transcendental.

[The point is that $e^{\text{Log}\ \alpha} = \alpha$.

Let a be a complex number with $a \neq 0, \neq e$.

14: DEFINITION The principal power of a is the holomorphic function

$$z \to a^z = e^{z\ \text{Log}\ a}.$$

15: DEFINITION The k^{th} associate of a^z $(k \in \mathbb{Z})$ is the holomorphic function

$$\begin{aligned} z \to\ & e^{z(\text{Log}\ a\ +\ 2k\pi\sqrt{-1})} \\ & = a^z(e^{2k\pi\sqrt{-1}\ z}). \end{aligned}$$

16: N.B. The reason for excluding e is that we want e^z to remain single valued and to mean the power series

$$\sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

17: EXAMPLE

$$1^z = e^{z\ \text{Log}\ 1} = e^{z(\ell n(1)\ +\ \sqrt{-1}\ 0)} = 1^0 = 1$$

and its k^{th} associate is

$$e^{z(\text{Log}\ 1\ +\ 2k\pi\sqrt{-1})} = e^{2k\pi\sqrt{-1}\ z}.$$

18: EXAMPLE Take $a = \sqrt{-1}$ and take $z = -\ 2\sqrt{-1}$ -- then with this data,

$$\sqrt{-1}^{-\ 2\sqrt{-1}} = e^{-\ 2\sqrt{-1}\ \text{Log}(\sqrt{-1})}$$

$$= e^{-2\sqrt{-1}(\sqrt{-1}\,\frac{\pi}{2})}.$$

Therefore the associates of $\sqrt{-1}^{\,-2\sqrt{-1}}$ are the

$$e^{-2\sqrt{-1}(\sqrt{-1}\,\frac{\pi}{2} + 2k\pi\sqrt{-1})} = e^{\pi(4k+1)} \quad (k \in Z).$$

<u>19:</u> EXAMPLE Let n be a positive integer and write

$$a = |a|e^{\sqrt{-1}\,\theta}(-\pi < \theta \leq \pi).$$

Then

$$a^{\frac{1}{n}} = e^{\frac{1}{n}\operatorname{Log} a}$$

$$= e^{\frac{1}{n}(\ell n(|a|) + \sqrt{-1}\,\theta)}$$

$$= e^{\frac{1}{n}\ell n(|a|)}\, e^{\frac{1}{n}\sqrt{-1}\,\theta}$$

$$= e^{\ell n(|a|^{\frac{1}{n}})}\, e^{\frac{1}{n}\sqrt{-1}\,\theta}$$

$$= |a|^{\frac{1}{n}}\, e^{\frac{1}{n}\sqrt{-1}\,\theta}.$$

Therefore the associates of $a^{\frac{1}{n}}$ are the

$$|a|^{\frac{1}{n}}\, e^{\frac{1}{n}\sqrt{-1}(\theta + 2k\pi)} \quad (k \in Z).$$

And there are only n different values for

$$\exp(\frac{1}{n}\, 2k\pi\sqrt{-1}).$$

The laws of exponents spelled out in §4 over R do not hold without qualification over C.

- In general, $(a^b)^c$ has more values than a^{bc}.
- In general, $a^b a^c$ has more values than a^{b+c}.

§24. THE GELFOND-SCHNEIDER THEOREM

This is the following statement.

1: THEOREM If $\alpha \neq 0, 1$ is algebraic and if $\beta \notin Q$ is algebraic, then α^β is transcendental.

[Note: Here α^β is the principal power (cf. §23, #14):

$$\alpha^\beta = e^{\beta \operatorname{Log} \alpha}.$$

Nevertheless it can be shown that the Gelfond-Schneider theorem goes through if the principal power α^β is replaced by any of its associates (cf. §31, #16).]

Special Cases:

2: EXAMPLE $2^{\sqrt{2}}$ is transcendental.

3: EXAMPLE $\sqrt{3}^{\sqrt{2}}$ is transcendental.

4: EXAMPLE $\sqrt{-1}^{\sqrt{-1}}$ is transcendental.

5: EXAMPLE e^π is transcendental.

[Starting from the fact that

$$e^{\pi\frac{\sqrt{-1}}{2}} = \sqrt{-1}$$

and using the principal determination of the logarithm:

$$\begin{aligned} \operatorname{Log} \sqrt{-1} &= \ell n(|\sqrt{-1}|) + \sqrt{-1} \operatorname{Arg} \sqrt{-1} \\ &= \ell n(1) + \sqrt{-1}\,\frac{\pi}{2} \\ &= \sqrt{-1}\,\frac{\pi}{2} \end{aligned}$$

=>

$$\pi = -2\sqrt{-1}\ \mathrm{Log}\ \sqrt{-1}$$

=>

$$e^{\pi} = e^{-2\sqrt{-1}\ \mathrm{Log}\ \sqrt{-1}} = \sqrt{-1}^{-2\sqrt{-1}} \quad \text{(cf. §23, #18)}$$

and the entity on the right is transcendental.]

6: EXAMPLE Take $f(z) = 2^z$, thus $2^z = e^{z\ \mathrm{Log}\ 2} = e^{z\ \ell n(2)}$.

If $\alpha = 2$ in Gelfond-Schneider and if $z \notin Q$ is algebraic, then 2^z is transcendental. On the other hand, the $2^{1/n}$ $(n \in N)$ are algebraic, as are the $(2^{1/n})^m$ $(m \in Z)$. Therefore the exceptional set E_f of f is equal to Q.

[Note: $f'(z) = 2^z\ \ell n(2)$, so

$$E_f \cap E_{f'} = \emptyset$$

since $\ell n(2)$ is transcendental (cf. §21, #9).]

7: EXAMPLE Take $f(z) = e^{\pi\sqrt{-1}\ z}$ -- then

$$e^{\pi\sqrt{-1}\ z} = (-1)^z,$$

principal power. In fact,

$$\begin{aligned}(-1)^z &= e^{z\ \mathrm{Log}\ -1} \\ &= e^{z(\ell n(|-1|) + \pi\sqrt{-1})} \\ &= e^{\pi\sqrt{-1}\ z}.\end{aligned}$$

So, if $\alpha = -1$ in Gelfond-Schneider and if $z \notin Q$ is algebraic, then $e^{\pi\sqrt{-1}\ z}$ is transcendental. As for what happens if $z \in Q$, write

$$e^{\pi\sqrt{-1}\, z} = \cos(\pi z) + \sqrt{-1}\,\sin(\pi z)$$

and quote the wellknown fact that the trigonometric functions cos and sin are algebraic numbers at arguments that are rational multiples of π. Therefore the exceptional set E_f of f is equal to Q.

<u>8:</u> THEOREM Given nonzero complex numbers a and b with $a \notin Q$, then at least one of a, e^b, e^{ab} is transcendental.

<u>9:</u> <u>N.B.</u> #8 <=> #1.

[To see that #8 => #1, take $a = \beta$, $b = \operatorname{Log} \alpha$ -- then at least one of the following numbers is transcendental: β, $e^{\operatorname{Log} \alpha} = \alpha$, or $e^{\beta \operatorname{Log} \alpha} = \alpha^\beta$. But the first two of these are algebraic, hence α^β must be transcendental. That #1 => #8 is analogous.]

<u>10:</u> EXAMPLE Let α, β be algebraic numbers not equal to 0 or 1. Suppose that

$$\frac{\operatorname{Log} \beta}{\operatorname{Log} \alpha} \notin Q.$$

Then

$$\frac{\operatorname{Log} \beta}{\operatorname{Log} \alpha}$$

is transcendental.

[In #8, take

$$a = \frac{\operatorname{Log} \beta}{\operatorname{Log} \alpha} \text{ and } b = \operatorname{Log} \alpha.$$

Then at least one of the following numbers is transcendental:

$$\frac{\mathrm{Log}\ \beta}{\mathrm{Log}\ \alpha},\ e^{\mathrm{Log}\ \alpha} = \alpha,\ e^{\frac{\mathrm{Log}\ \beta}{\mathrm{Log}\ \alpha}\mathrm{Log}\ \alpha} = e^{\mathrm{Log}\ \beta} = \beta.]$$

[Note: If Log α and Log β are linearly independent over Q, then

$$\frac{\mathrm{Log}\ \beta}{\mathrm{Log}\ \alpha} \notin Q,$$

as can be seen by putting

$$\gamma = \frac{\mathrm{Log}\ \beta}{\mathrm{Log}\ \alpha}$$

and considering the dependence relation

$$\gamma\ \mathrm{Log}\ \alpha - \mathrm{Log}\ \beta = 0.$$

Consequently

$$\frac{\mathrm{Log}\ \beta}{\mathrm{Log}\ \alpha}$$

is transcendental, thus for any nonzero algebraic numbers μ and ν,

$$\mu\ \mathrm{Log}\ \alpha + \nu\ \mathrm{Log}\ \beta \neq 0,$$

i.e., Log α and Log β are linearly independent over $\bar{Q}$.]

<u>11:</u> EXAMPLE Let r be a positive rational number. Write (see the Appendix to §10)

$$\log_{10}(r) = \frac{\ell n(r)}{\ell n(10)}.$$

Therefore, if $\log_{10}(r)$ is not rational, then by the above it must be transcendental (cf. §5, #15).

Question: For what pairs (β, t) ($\beta \in \bar{Q}$, $\beta \neq 0$) and $t \in R^\times$) is $e^{t\beta}$ algebraic?

12: EXAMPLE Take $\beta \in \bar{Q} \cap R$ ($\beta \neq 0$) and

$$t = \frac{\ln(2)}{\beta}.$$

Then

$$e^{t\beta} = e^{\ln(2)} = 2.$$

13: EXAMPLE Take $\beta \in \bar{Q} \cap \sqrt{-1}\, R$ ($\beta \neq 0$) and

$$t = \frac{\sqrt{-1}\,\pi}{\beta}.$$

Then

$$e^{t\beta} = e^{\sqrt{-1}\,\pi} = -1.$$

14: THEOREM Let $\beta \in \bar{Q}$ ($\beta \neq 0$) and $t \in R^\times$. Assume: $\beta \notin R \cup \sqrt{-1}\, R$ -- then $e^{t\beta}$ is transcendental.

PROOF Put $\alpha = e^{t\beta}$ -- then the complex conjugate $\bar{\alpha}$ of α is $e^{t\bar{\beta}} = \alpha^{\bar{\beta}/\beta}$. The algebraic number $\bar{\beta}/\beta$ is not real (for $|\bar{\beta}/\beta| = 1$ but $\bar{\beta}/\beta \neq \pm 1$), hence is not rational. In #8, take

$$a = \bar{\beta}/\beta,\ b = t\beta,$$

leading thereby to

$$\bar{\beta}/\beta,\ e^{t\beta} = \alpha,\ e^{t\bar{\beta}} = \bar{\alpha}.$$

Since $\bar{\beta}/\beta$ is algebraic, either α or $\bar{\alpha}$ must be transcendental. But α is transcendental iff $\bar{\alpha}$ is transcendental.

It remains to give a proof of Gelfond-Schneider, a task that requires some preliminaries.

§25. *INTERPOLATION DETERMINANTS*

<u>1.</u> NOTATION Given $w \in \mathbf{C}$, $R \in \mathbf{R}_{\geq 0}$, let

$$\begin{cases} D(R,w) = \{z \in \mathbf{C}: |z - w| < R\} \\ \bar{D}(R,w = \{z \in \mathbf{C}: |z - w| \leq R\}. \end{cases}$$

[Note: Write

$$\begin{cases} D(R) \\ \bar{D}(R) \end{cases}$$

if $w = 0$.]

<u>2:</u> NOTATION Let $|f|_R$ stand for the maximum value of $|f(z)|$ when $|z| = R$.

<u>3:</u> RAPPEL If $f(z)$ is a function holomorphic in $D(R)$ and continuous in $\bar{D}(R)$, then

$$|f(z)| \leq |f|_R$$

for every $z \in \bar{D}(R)$.

<u>4:</u> LEMMA Let T be a nonnegative integer, let r and R be positive real numbers subject to $0 < r \leq R$, and let $F(z)$ be a function of one complex variable holomorphic in $D(R)$ and continuous in $\bar{D}(R)$. Assume: F has a zero of multiplicity at least T at 0 -- then

$$|F|_r \leq (\frac{R}{r})^{-T} |F|_R.$$

PROOF Put

$$G(z) = z^{-T} F(z).$$

Then

$$|G|_r \leq |G|_R$$

or still,

$$r^{-T}|F|_r \leq R^{-T}|F|_R$$

or still,

$$|F|_r \leq (\frac{R}{r})^{-T}|F|_R.$$

5: THEOREM Let r and R be positive real numbers subject to $0 < r \leq R$, let $f_1(z),\ldots,f_L(z)$ be functions of one complex variable which are holomorphic in $D(R)$ and continuous in $\bar{D}(R)$, and let $\zeta_1,\ldots,\zeta_L$ belong to the disc $|z| \leq r$. Put

$$\Delta = \det \begin{bmatrix} f_1(\zeta_1) & \cdots\cdots & f_L(\zeta_1) \\ \vdots & & \vdots \\ f_1(\zeta_L) & \cdots\cdots & f_L(\zeta_L) \end{bmatrix}.$$

Then

$$|\Delta| \leq (\frac{R}{r})^{-L(L-1)/2}\, L! \prod_{j=1}^{L} |f_j|_R.$$

PROOF Let $F(z)$ be the determinant of the $L \times L$ matrix

$$(f_j(\zeta_i z))_{1 \leq j,i \leq L} \ (\Rightarrow F(1) = \Delta).$$

Since the ζ_i satisfy $|\zeta_i| \leq r$, the functions $f_j(\zeta_i z)$ are holomorphic in $D(R/r)$ and continuous in $\bar{D}(R/r)$. And since the determinant is a sum of products of the

$f_j(\zeta_i z)$, the determinant $F(z)$ itself is holomorphic in $D(R/r)$ and continuous in $\bar{D}(R/r)$. The claim then is that $F(z)$ vanishes at 0 with multiplicity at least $L(L-1)/2$. To see this, put

$$K = L(L-1)/2$$

and consider the expansion

$$f_j(\zeta_i z) = \sum_{k=0}^{K-1} a_k(j)\zeta_i^k z^k + z^K g_{ij}(z),$$

where $a_k(j) \in \mathbb{C}$ and $g_{ij}(z)$ is holomorphic in $D(R/r)$ and continuous in $\bar{D}(R/r)$. Since the determinant is linear in its columns, one can view $F(z)$ as z^K times a function holomorphic in $D(R/r)$ plus terms involving the factor

$$z^{n_1+n_2+\cdots+n_L}\det(\zeta_i^{n_j}),$$

i.e.,

$$z^{n_1+n_2+\cdots+n_L}\det\begin{bmatrix} \zeta_1^{n_1} & \cdots\cdots & \zeta_1^{n_L} \\ \vdots & & \vdots \\ \zeta_L^{n_1} & \cdots\cdots & \zeta_L^{n_L} \end{bmatrix},$$

where $n_1, n_2, \ldots, n_L \in \mathbb{Z}_{\geq 0}$ and $n_j \in \{0,1,\ldots,K-1\}$. The determinant vanishes if two of the n_j are identical, so the nonzero terms satisfy

$$n_1 + n_2 + \cdots + n_L \geq 0 + 1 + \cdots + (L-1) = \frac{L(L-1)}{2}.$$

Take now in #4

$$T = L(L - 1)/2$$

and replace r by 1 and R by R/r, hence

$$|\Delta| = |F(1)|$$

$$\leq |F|_1 \leq (\frac{R}{r})^{-L(L-1)/2} |F|_{R/r}.$$

It remains to bound $|F|_{R/r}$. From its very definition, the determinant of a L × L matrix is the sum of L! products, where each product consists of L entries such that for each row and column only one entry is a part of a product. Since $|z| = R/r \Rightarrow |\zeta_i z| \leq R$, for each column index j,

$$|f_j(\zeta_i z)| \leq |f_j|_R \quad (i = 1,2,\ldots,L).$$

Therefore

$$|F|_{R/r} \leq L! \prod_{j=1}^{L} |f_j|_R.$$

So finally

$$|\Delta| \leq (\frac{R}{r})^{-L(L-1)/2} L! \prod_{j=1}^{L} |f_j|_R.$$

6: REMARK The derivatives of F(z) can be calculated via an application of the product rule, viz:

$$(\frac{d}{dz})^k F(z)$$

$$= \sum_{\kappa_1 + \cdots + \kappa_L = k} \frac{k!}{\kappa_1! \cdots \kappa_L!} \det((\frac{d}{dz})^{\kappa_i} f_j(\zeta_i z))_{1 \leq j,\, i \leq L}.$$

The foregoing can be generalized by incorporating derivatives.

7: THEOREM Let r and R be positive real numbers subject to $0 < r \leq R$, let $\sigma_1,\ldots,\sigma_L$ be nonnegative integers, let $f_1,\ldots,f_L$ be entire functions, and let $\zeta_1,\ldots,\zeta_L$ belong to the disc $|z| \leq r$. Put

$$\Delta = \det\left(\left(\frac{d}{dz}\right)^{\sigma_i} f_j(\zeta_i)\right)_{1 \leq j,\, i \leq L}.$$

Then

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-L(L-1)/2 + \sigma_1 + \cdots + \sigma_L} L! \prod_{j=1}^{L} \max_{1 \leq i \leq L} \sup_{|z| = R} \left|\left(\frac{d}{dz}\right)^{\sigma_i} f_j(z)\right|.$$

APPENDIX

Suppose that $1 \leq j \leq p_k$ $(\in N)$, $1 \leq k \leq \ell$, $1 \leq i \leq n$ -- then

$$\frac{d^{i-1}}{dz^{i-1}} (z^{j-1} e^{w_k z}) \Big|_{z=0} = \frac{d^{j-1}}{dz^{j-1}} (z^{i-1}) \Big|_{z=w_k},$$

their common value being

$$\begin{cases} \dfrac{(i-1)!}{(i-j)!} w_k^{i-j} & \text{if } i \geq j \\ 0 & \text{if } i < j. \end{cases}$$

§26. *ZERO ESTIMATES*

1: LEMMA Let $P_1,\ldots,P_n$ be nonzero polynomials in R[X] of degrees $\leq$ $d_1,\ldots,d_n$ and let $w_1,\ldots,w_n$ be distinct real numbers -- then

$$F(x) = \sum_{j=1}^{n} P_j(x)e^{w_j x}$$

has at most

$$d_1 + \cdots + d_n + n - 1$$

real zeros counting multiplicities.

To begin with:

2: SUBLEMMA If a continuously differentiable function F of a real variable x has at least N real zeros counting multiplicities (N a positive integer), then its derivative F' has at least N - 1 real zeros counting multiplicities.

PROOF Let $x_1,\ldots,x_k$ $(k \geq 1)$ be distinct real zeros of F arranged in increasing order: $x_1 < \cdots < x_k$ with n_1 the multiplicity of $x_1,\ldots,$ n_k the multiplicity of x_k and $n_1 + \cdots + n_k \geq N$ -- then x_i is a zero of F' of multiplicity $\geq n_i - 1$ $(1 \leq i \leq k)$. Owing to Rolle's theorem, F' has at least one zero in the open interval $]x_i,x_{i+1}[$ $(1 \leq i \leq k)$, so all told, F' has at least

$$\begin{aligned}(n_1 - 1) + \cdots + (n_k - 1) + (k - 1)\\ \geq N - k + (k - 1) = N - 1\end{aligned}$$

real zeros counting multiplicities.

Passing to the proof of #1, upon multiplying through by $e^{-w_n x}$, it can be assumed that $w_n = 0$ and $w_j \neq 0$ for $j = 1,\ldots,n-1$. Put

$$D = d_1 + \cdots + d_n + n$$

and proceed from here by induction on D, matters being clear if $D = 1$ (since $n = 1$ and $d_1 = 0$) so in this case there are at most $D - 1 = 0$ real zeros. Suppose now that the lemma holds if $k = 2,\ldots,D - 1$ and consider the situation at level $k = D$. Take the first derivative of $F(x)$:

$$F'(x) = \sum_{j=1}^{n-1} (w_j P_j(x) + \frac{d}{dx} P_j(x)) + \frac{d}{dx} P_n(x).$$

Then

$$w_j P_j(x) + \frac{d}{dx} P_j(x)$$

is a polynomial of degree d_j whereas $\frac{d}{dx} P_n(x)$ is a polynomial of degree $d_n - 1$. It therefore follows from the induction hypothesis that $F'(x)$ has at most

$$\begin{aligned} d_1 + \cdots + d_{n-1} + d_n - 1 + n - 1 \\ = d_1 + \cdots + d_n + n - 2 \end{aligned}$$

real zeros counting multiplicities. Let N be a positive integer such that F has at least N real zeros counting multiplicities, hence by #2,

$$N - 1 \leq d_1 + \cdots + d_n + n - 2$$

$$\Rightarrow$$

$$N \leq d_1 + \cdots d_n + n - 1.$$

<u>3:</u> REMARK Let $d_1,\ldots,d_n$ be nonnegative integers and let $w_1,\ldots,w_n$ be distinct real numbers. Fix distinct real numbers $x_1,\ldots,x_N$, where

$$N = d_1 + \cdots + d_n + n - 1.$$

Then there are polynomials $P_1,\ldots,P_n$ in $\mathbb{R}[X]$ of degrees $d_1,\ldots,d_n$ such that the function

$$F(x) = \sum_{j=1}^{n} P_j(x)e^{w_j x}$$

has a simple zero at each point $x_1,\ldots,x_N$ and no other zeros.

[Note: This can be generalized by dropping the requirement that the $x_1,\ldots,x_N$ be distinct and incorporating multiplicities.]

4: N.B. The upper bound in #1 is thus the best possible.

There is also an estimate in the complex domain.

5: LEMMA Let $P_1,\ldots,P_n$ be nonzero polynomials in $\mathbb{C}[X]$ of degrees $d_1,\ldots,d_n$ and let $w_1,\ldots,w_n$ be distinct complex numbers. Put

$$\Omega = \max\{|w_1|,\ldots,|w_n|\}.$$

Then the number of zeros counting multiplicities of

$$F(z) = \sum_{j=1}^{n} P_j(z)e^{w_j z}$$

in the disc $|z| \leq R$ is at most

$$3(d_1 + \cdots + d_n + n - 1) + 4R\Omega.$$

6: NOTATION If $f(z)$ is a function holomorphic in $D(R,w)$ and continuous in $\bar{D}(R,w)$, put

$$M(R,w,f) = \max_{z\in\bar{D}(R,w)} |f(z)|.$$

[Note: Write

$$M(R,f)$$

if $w = 0$.]

7: NOTATION If $f(z)$ is a function holomorphic in $D(R,w)$ and continuous in $\bar{D}(R,w)$, denote by

$$N(r,w,f)$$

the number of zeros counting multiplicities of $f(z)$ in $\bar{D}(R,w)$.

[Note: Write

$$N(R,f)$$

if $w = 0$.]

8: RAPPEL (Jensen) Let $R > 0$, $s > 1$ -- then

$$\int_0^{sR} \frac{N(r,w,f)}{r}\, dr = \frac{1}{2\pi} \int_0^{2\pi} \ell n(|f(w + sRe^{\sqrt{-1}\,\theta})|)d\theta - \ell n(|f(w)|).$$

9: SUBLEMMA Let $R,s,t \in \mathbb{R}_{>0}$, $s > 1$, and let $f \not\equiv 0$ be holomorphic in $D((st + s + t)R)$ and continuous in $\bar{D}((st + s + t)R)$ -- then

$$N(R,f) \leq \frac{1}{\ell n(s)} \ell n(\frac{M((st + s + t)R,f)}{M(tR,f)}).$$

PROOF Choose $w \in \bar{D}(tR): |f(w)| = M(tR,f)$ (cf. §25, #3) -- then $|w| = tR$. So

$$z \in \bar{D}(R)$$

$$\Rightarrow |z - w| \leq |z| + |w|$$

$$\leq R + tR = (1 + t)R$$

$$\Rightarrow$$

$$\bullet \quad \bar{D}(R) \subset \bar{D}((1 + t)R,w)$$

and

$$z \in \bar{D}((st + s)R,w)$$

$$\Rightarrow$$

$$\begin{aligned} |z| &= |z - w + w| \\ &\leq |z - w| + |w| \\ &\leq (st + s)R + tR = (st + s + t)R \end{aligned}$$

$$\Rightarrow$$

$$\bullet \quad \bar{D}((st + s)R,w) \subset \bar{D}((st + s + t)R).$$

Next

$$\begin{aligned} N(R,w,f) &= \frac{1}{\ell n(s)} \int_R^{sR} \frac{N(R,w,f)}{r}\, dr \\ &\leq \frac{1}{\ell n(s)} \int_0^{sR} \frac{N(r,w,f)}{r}\, dr \end{aligned}$$

$$= \frac{1}{\ell n(s)} \left[\frac{1}{2\pi} \int_0^{2\pi} \ell n(|f(w + sRe^{\sqrt{-1}\,\theta})|)d\theta - \ell n(|f(w)|)\right]$$

$$= \frac{1}{\ell n(s)} \left[\frac{1}{2\pi} \int_0^{2\pi} \ell n(|f(w + sRe^{\sqrt{-1}\,\theta})|)d\theta - \frac{1}{2\pi} \int_0^{2\pi} \ell n(|f(w)|)d\theta\right]$$

$$= \frac{1}{\ell n(s)} \left[\frac{1}{2\pi} \int_0^{2\pi} \ell n\left(\frac{|f(w + sRe^{\sqrt{-1}\,\theta})|}{|f(w)|}\right)d\theta\right] \quad .$$

Take

$$z = w + sRe^{\sqrt{-1}\,\theta}.$$

Then

$$|z - w| = |w + sRe^{\sqrt{-1}\,\theta} - w|$$

$$= |sRe^{\sqrt{-1}\,\theta}| = sR.$$

Therefore

$$N(R,w,f) \leq \frac{1}{\ell n(s)} M(sR,w,\ell n(\frac{|f|}{|f(w)|})).$$

Spelled out

$$N(R,w,f) = |N(R,w,f)|$$

$$= \frac{1}{\ell n(s)} \frac{1}{2\pi} |\int_0^{2\pi} \ell n(\frac{|f(w + sRe^{\sqrt{-1}\,\theta})|}{|f(w)|}) d\theta|$$

$$\leq \frac{1}{\ell n(s)} \frac{1}{2\pi} \int_0^{2\pi} |\ell n(\frac{|f(w) + sRe^{\sqrt{-1}\,\theta})|}{|f(w)|}) |d\theta$$

$$\leq \frac{1}{\ell n(s)} \frac{1}{2\pi} \int_0^{2\pi} M(sR,w,\ell n(\frac{|f|}{|f(w)|})) d\theta$$

$$= \frac{1}{\ell n(s)} M(sR,w,\ell n(\frac{|f|}{|f(w)|})).$$

Finally

$$N(R,f) \leq N((1 + t)R,w,f)$$

since

$$\bar{D}(R) \subset \bar{D}((1 + t)R,w).$$

And working in the above with $(1 + t)R$ rather than just R, it follows that

$$N((1 + t)R,w,f)$$

is majorized by

$$\frac{1}{\ell n(s)} M(s(1 + t)R,w,\ell n(\frac{|f|}{|f(w)|}))$$

or still, by

$$\frac{1}{\ln(s)} M((st + s)R,\ w,\ \ln(\frac{|f|}{M(tR,f)}))$$

which in turn is

$$\leq \frac{1}{\ln(s)} M((st + s + t)R,\ \ln(\frac{|f|}{M(tR,f)}))$$

because

$$\bar{D}((st + s)R,w) \subset \bar{D}((st + s + t)R).$$

Accordingly

$$N(R,f) \leq \frac{1}{\ln(s)} M((st + s + t)R,\ \ln(\frac{|f|}{M(tR,f)}$$

$$\leq \frac{1}{\ln(s)} \ln(\frac{M((st + s + t)R,f)}{M(tR,f)}).$$

Keep to the notation and assumptions of #5 and set for simplicity

$$D = \sum_{j=1}^{n} d_j + n.$$

FACT Let $R,\gamma \in R_{>0}$, $\gamma > 1$ -- then

$$M(\gamma R,F) \leq \frac{\gamma^D - 1}{\gamma - 1} e^{R\Omega(\gamma+1)} M(R,F).$$

[This technicality is dispensed with in the Appendix to this §].

With this preparation, let us take up the proof of #5. In the preceding, work with tR rather than R, hence

$$M(\gamma tR,F) \leq \frac{\gamma^D - 1}{\gamma - 1} e^{tR\Omega(\gamma+1)} M(tR,F).$$

Now specialize and take

$$\gamma = (st + s + t)/t.$$

Then

$$\frac{\gamma^D - 1}{\gamma - 1} \leq \frac{1}{\gamma - 1}\gamma^D$$

$$= \frac{t}{st + s}\gamma^D$$

$$= \frac{t}{s(t+1)}\left(\frac{st + s + t}{t}\right)^D$$

$$= \frac{t}{s(t+1)}\left(\frac{st + s + t}{t}\right)^{D-1}\left(\frac{st + s + t}{t}\right)$$

$$= \frac{1}{s(t+1)}\left(\frac{st + s + t}{t}\right)^{D-1}(s(t+1) + t)$$

$$= \left(1 + \frac{t}{s(t+1)}\right)\left(\frac{st + s + t}{t}\right)^{D-1}$$

$$\leq \left(1 + \frac{1}{s}\right)\left(\frac{st + s + t}{t}\right)^{D-1}.$$

Therefore

$$M((st + s + t)R,F)$$

$$\leq \left(1 + \frac{1}{s}\right)\left(\frac{st + s + t}{t}\right)^{D-1} e^{(st + s + 2t)R\Omega}\, M(tR,F)$$

$\Rightarrow$

$$\frac{M((st + s + t)R,F)}{M(tR,F)}$$

$$\leq \left(1 + \frac{1}{s}\right)\left(\frac{st + s + t}{t}\right)^{D-1} e^{(st + s + 2t)R\Omega}$$

=>

$$N(R,F) \le \frac{1}{\ln(s)} \ln\left(\frac{M((st+s+t)R,F)}{M(tR,F)}\right) \qquad \text{(cf. \#9)}$$

=>

$$N(r,F) \le \frac{1}{\ln(s)} \left[\ln\left(1+\frac{1}{s}\right) + (D-1)\ln\left(\frac{st+s+t}{t}\right) + (st+s+2t)R\Omega\right]$$

$$\le \frac{1}{\ln(s)} \left[\frac{1}{s} + (D-1)\ln\left(\frac{st+s+t}{t}\right) + (st+s+2t)R\Omega\right].$$

Into this relation insert $s = 5$ and $t = \frac{1}{5}$. Toss the "$\frac{1}{s}$" and note that

$$\frac{\ln(31)}{\ln(5)} < 2.2 \text{ and } \frac{32}{5\ln(5)} < 3.9$$

giving

$$N(R,F) \le 3(D-1) + 4R\Omega,$$

the assertion of #5.

<u>10:</u> <u>N.B.</u> One can replace the origin by any complex number w and, upon consideration of $F(z - w)$, conclude that still

$$N(R,w,F) \le 3(D-1) + 4R\Omega.$$

APPENDIX

Recall the setup of #5. Thus, as there, let $P_1,\ldots,P_n$ be nonzero polynomials in $C[X]$ of degrees $d_1,\ldots,d_n$ and let $w_1,\ldots,w_n$ be distinct complex numbers. Put

$$\Omega = \max\{|w_1|,\ldots,|w_n|\}, \; D = \sum_{j=1}^{n} d_j + n,$$

and form

$$F(z) = \sum_{j=1}^{n} P_j(z)e^{w_j z}.$$

PREFACT Fix a point $z_0 \in C$ -- then

$$|F(z_0)| \leq e^{(|z_0| + 1)\Omega} \left(\sum_{k=0}^{D-1} |z_0|^k\right) \max_{j=1,\ldots,D} \left| \frac{F^{(j-1)}(0)}{(j-1)!} \right| .$$

FACT Let $R,\gamma \in R_{>0}$, $\gamma > 1$ -- then

$$M(\gamma R,F) \leq \frac{\gamma^D - 1}{\gamma - 1} e^{R\Omega(\gamma + 1)} M(R,F).$$

PROOF Choose $z_0(|z_0| = \gamma)$:

$$|F(z_0 R)| = \max_{|z| \leq \gamma R} |F(z)|.$$

Consider

$$G(z) = F(zR) = \sum_{j=1}^{n} P_j(zR)e^{w_j Rz}.$$

Then by the above applied to G (hence now it is a question of $w_j R$ rather than w_j and it is also a question of $R\Omega$ rather than Ω) we have

$$|G(z_0)| < e^{(\gamma + 1)R\Omega} \left(\sum_{k=0}^{D-1} \gamma^k\right) \max_{j=1,\ldots,D} \left| \frac{R^{j-1} F^{(j-1)}(0)}{(j-1)!} \right| .$$

But

$$\sum_{k=0}^{D-1} \gamma^k = \frac{\gamma^D - 1}{\gamma - 1}$$

and, thanks to Cauchy's inequality,

$$\max_{j=1,\ldots,D} \left| \frac{R^{j-1}F^{(j-1)}(0)}{(j-1)!} \right| \leq \max_{|z|\leq R} |F(z)|.$$

Therefore

$$\begin{aligned} M(\gamma R,F) &= \max_{|z|\leq\gamma R} |F(z)| \\ &= |F(z_0 R)| \\ &= |G(z_0)| \\ &\leq \frac{\gamma^D - 1}{\gamma - 1} e^{R\Omega(\gamma + 1)} \max_{|z|\leq R} |F(z)| \\ &= \frac{\gamma^D - 1}{\gamma - 1} e^{R\Omega(\gamma + 1)} M(R,F). \end{aligned}$$

REMARK The estimate figuring in #5 can be sharpened to

$$N(R,F) \leq 2(D - 1) + \frac{4}{\pi} R\Omega.$$

§27. *GELFOND-SCHNEIDER: SETTING THE STAGE*

Recall the claim:

1: THEOREM If $\alpha \neq 0,1$ is algebraic and if $\beta \notin Q$ is algebraic, then α^β is transcendental.

[Note: Here α^β is the principal power (cf. §23, #14):

$$\alpha^\beta = e^{\beta \text{Log } \alpha}.]$$

Methodology: Assume that $\alpha \neq 0,1$ is algebraic, that β is algebraic, and that α^β is algebraic -- then the theorem will follow if it can be shown that $\beta \in Q$.

2: NOTATION Given a positive odd integer $N >> 0$, put

$$L = N^8, \quad S = \frac{1}{2}(N^4 - 1),$$

and

$$\begin{cases} L_0 = N^6 - 1 \\ L_1 = N^2 - 1. \end{cases}$$

[Note: Restricting N to be odd guarantees that S is an integer.]

3: LEMMA

$$L = (L_0 + 1)(L_1 + 1) = (2S + 1)^2.$$

PROOF

$$\begin{cases} L_0 + 1 = N^6 \\ L_1 + 1 = N^2 \end{cases} \Rightarrow (L_0 + 1)(L_1 + 1) = N^8.$$

And

$$(2S + 1)^2 = (N^4 - 1 + 1)^2 = N^8.$$

During the ensuing analysis, there will emerge a positive absolute constant C.

<u>4:</u> LEMMA Given $C \in R_{>0}$, $\exists\, N_0(C) >> 0 : \forall\, N > N_0(C)$,

$$CL_0 \ln(S) \leq L \text{ and } CL_1 S \leq L.$$

<u>5:</u> <u>N.B.</u> Therefore

$$CL(L_0 \ln(S) + L_1 S)$$

$$= L(CL_0 \ln(S) + CL_1 S)$$

$$\leq L(L) + L(L) = 2L^2.$$

- Choose an ordering of the integral pairs (s_1,s_2) with $|s_1| \leq S$ and $|s_2| \leq S$, i.e., $(s_1,s_2) \in Z^2$ and $-S \leq s_1,s_2 \leq S$.

[Note: There are $S + (S + 1)$ choices for s_1 and $S + (S + 1)$ choices for s_2, hence there are all told

$$(2S + 1) \times (2S + 1) = (2S + 1)^2 = L$$

integral pairs (s_1,s_2).]

- Choose an ordering of the integral pairs

$$(u,v) \in \{0,\ldots,L_0\} \times \{0,\ldots,L_1\}.$$

[Note: There are $L_0 + 1$ choices for u and $L_1 + 1$ choices for v, hence there are all told

$$(L_0 + 1)(L_1 + 1) = L \ (= (2S + 1)^2)$$

choices for (u,v).]

6: NOTATION Introduce a $L \times L$ matrix $\mathcal{M}$ via the prescription

$$\mathcal{M} = ((s_1(i) + s_2(i)\beta)^{u(j)} (\alpha^{s_1(i) + s_2(i)\beta})^{v(j)})$$

and let

$$\Delta = \det(\mathcal{M}).$$

[Note: j is the column index and i is the row index.]

7: N.B. The orderings for the columns and rows has not been explicated but a change in these orderings simply changes matters by a factor ± 1, which has no effect on the absolute value $|\Delta|$ of Δ.

Define a function of one complex variable z by

$$f_j(z) = z^{u(j)} \alpha^{v(j)z} \quad (1 \leq j \leq L)$$

and put

$$\zeta_i = s_1(i) + s_2(i)\beta \quad (1 \leq i \leq L).$$

8: SUBLEMMA $\forall$ complex numbers z_1, z_2,

$$|e^{z_1 z_2}| = e^{\operatorname{Re}(z_1 z_2)} \leq e^{|z_1 z_2|} = e^{|z_1|} e^{|z_2|}.$$

9: LEMMA $\forall\ R \in \mathbb{R}_{>0}$,

$$M(R, f_j) \leq R^{u(j)} e^{v(j) R |\operatorname{Log} \alpha|}.$$

PROOF For by definition,

$$\alpha^{v(j)z} = \exp(v(j) z \operatorname{Log} \alpha).$$

choices for (u,v).]

6: NOTATION Introduce a $L \times L$ matrix M via the prescription

$$M = ((s_1(i) + s_2(i)\beta)^{u(j)}(\alpha^{s_1(i) + s_2(i)\beta})^{v(j)})$$

and let

$$\Delta = \det(M).$$

[Note: j is the column index and i is the row index.]

7: N.B. The orderings for the columns and rows has not been explicated but a change in these orderings simply changes matters by a factor ± 1, which has no effect on the absolute value $|\Delta|$ of Δ.

Define a function of one complex variable z by

$$f_j(z) = z^{u(j)}\alpha^{v(j)z} \quad (1 \leq j \leq L)$$

and put

$$\zeta_i = s_1(i) + s_2(i)\beta \quad (1 \leq i \leq L).$$

8: SUBLEMMA $\forall$ complex numbers z_1, z_2,

$$|e^{z_1 z_2}| = e^{\mathrm{Re}(z_1 z_2)} \leq e^{|z_1 z_2|} = e^{|z_1|}e^{|z_2|}.$$

9: LEMMA $\forall\, R \in \mathbb{R}_{>0}$,

$$M(R,f_j) \leq R^{u(j)}e^{v(j)R|\mathrm{Log}\ \alpha|}.$$

PROOF For by definition,

$$\alpha^{v(j)z} = \exp(v(j)z\ \mathrm{Log}\ \alpha).$$

Therefore

$$\ell n(M(R,f_j)) \leq u(j)\ell n(R) + v(j)R|\text{Log } \alpha|$$

$$\leq L_0 \ell n(R) + L_1 R|\text{Log } \alpha|.$$

10: RAPPEL In the notation of §25, #5,

$$|\Delta| \leq (\frac{R}{r})^{-L(L-1)/2} L! \prod_{j=1}^{L} |f_j|_R.$$

[Note: The symbols $|f_j|_R$ and $M(R,f_j)$ mean one and the same thing.]

In the case at hand,

$$\Delta = \det(f_j(\zeta_i)),$$

thus the foregoing generality is applicable.

- Take $r = S(1 + |\beta|)$ and note that

$$|\zeta_i| = |s_1(i) + s_2(i)\beta|$$

$$\leq |s_1(i)| + |s_2(i)\beta|$$

$$\leq S + S|\beta| = S(1 + |\beta|).$$

- Take $R = e^2 r$ and note that

$$(\frac{R}{r})^{-L(L-1)/2} = (\frac{e^2 r}{r})^{-L(L-1)/2}$$

$$= e^{-L(L-1)}.$$

11: LEMMA

$$|\Delta| \leq e^{-L(L-1)} L! \prod_{j=1}^{L} M(R,f_j),$$

where

$$R = e^2 S(1 + |\beta|).$$

12: LEMMA

$$\ell n(|\Delta|) \leq -\frac{L^2}{2}.$$

PROOF Starting with #11,

$$\ell n(|\Delta|) \leq -L(L-1) + \ell n(L!) + \sum_{j=1}^{L} \ell n(M(R,f_j))$$

$$\leq -L^2 + L + L\ell n(L) + L \max_{1 \leq j \leq L} \ell n(M(R,f_j))$$

$$\leq -L^2 + L(1 + \ell n(L) + L_0 \ell n(R) + L_1 R|\mathrm{Log}\ \alpha|).$$

- $LL_0 \ell n(R)$

$$= LL_0 \ell n(e^2 S(L + |\beta|))$$

$$= LL_0(\ell n(e^2) + \ell n(S) + \ell n(1 + |\beta|))$$

$$= LL_0 \ell n(e^2) + LL_0 \ell n(1 + |\beta|) + LL_0 \ell n(S)$$

$$\leq C_1 LL_0 \ell n(S).$$

- $LL_1 R|\mathrm{Log}\ \alpha|$

$$= LL_1 e^2 S(1 + |\beta|)\ |\mathrm{Log}\ \alpha|$$

$$= e^2(1 + |\beta|)\ |\mathrm{Log}\ \alpha| LL_1 S$$

$$\leq C_2 LL_1 S.$$

Therefore

$$
\begin{aligned}
- L^2 &+ L(1 + \ell n(L) + L_0 \ell n(R) + L_1 R|\mathrm{Log}\ \alpha|) \\
&\leq - L^2 + L(1 + \ell n(L)) + C_1 L L_0 \ell n(S) + C_2 L L_1 S \\
&\leq - L^2 + C_3 (L L_0 \ell n(S) + L L_1 S) \\
&\qquad + C_1 L L_0 \ell n(S) + C_2 L L_1 S \\
&\leq - L^2 + C_4 (L L_0 \ell n(S) + L L_1 S),
\end{aligned}
$$

the positive absolute constant C_4 being independent of $N >> 0$. Take now $C \geq 4C_4$ and unravel the data:

$$
\begin{aligned}
\ell n(|\Delta|) &\leq - L^2 + C_4 (L L_0 \ell n(S) + L L_1 S) \\
&\leq - L^2 + \frac{C}{4} (L L_0 \ell n(S) + L L_1 S) \\
&= - L^2 + \frac{1}{4} CL (L_0 \ell n(S) + L_1 S) \\
&\leq - L^2 + \frac{1}{4} (2L^2) \qquad \text{(cf. \#5)} \\
&= - L^2 + \frac{L^2}{2} = - \frac{L^2}{2},
\end{aligned}
$$

thereby completing the proof.

<u>13:</u> LEMMA

$$\ell n(|\Delta|) \geq - \frac{L^2}{3}$$

if $\Delta \neq 0$.

14: N.B. Granted this, we have a contradiction: $\frac{1}{3} \geq \frac{1}{2}$. Thus the conclusion is that

$$\Delta = \det(\mathcal{M}) = 0.$$

Bearing in mind that for #13, $\Delta \neq 0$, fix $T \in \mathbb{N}$ such that $T\alpha$, $T\beta$, and $T\alpha^{\beta}$ are algebraic integers (recall that $\forall\, x \in \bar{\mathbb{Q}}$, D_x is a nonzero ideal of $\mathbb{Z}$ (cf. §14)) -- then $T^{L_0 + 2L_1S}$ times any element of the matrix $\mathcal{M}$ is an algebraic integer. Moreover the algebraic integer

$$T^{L(L_0 + 2L_1S)}\Delta$$

is a zero of a monic polynomial of degree d, where d is at most the product of the degrees of the minimal polynomials of α, β, and α^{β}.

15: SUBLEMMA

$$\overline{|\Delta|} \leq L!\, S^{L_0L}(1 + \overline{|\beta|})^{L_0L}(1 + \overline{|\alpha|})^{L_1LS}(1 + \overline{|\alpha^{\beta}|})^{L_1LS}.$$

[Note: The house of an algebraic number $x \neq 0$ is, by definition, the maximum of the absolute values of x and its conjugates (see the Appendix to §14, in particular the result formulated there, to be used infra).]

On the other hand,

$$\Delta \neq 0 \text{ and } T^{L(L_0 + 2L_1S)} \in D_{\Delta},$$

hence

$$|\Delta| \geq T^{-dL(L_0 + 2L_1S)}\,\overline{|\Delta|}^{\,1 - d}$$

$$\geq T^{-dL(L_0 + 2L_1S)} H(\Delta)^{-d}$$

=>

$$|\Delta| \geq T^{-dL(L_0 + 2L_1S)} (L!)^{-d} S^{-dL_0L}$$

$$\times\ (1 + H(\beta))^{-dL_0L} (1 + H(\alpha))^{-dL_1LS} (1 + H(\alpha^\beta))^{-dL_1LS}$$

=>

$$\ln(|\Delta|) \geq - dL(L_0 + 2L_1S)\ln(T) - dL\ln(L) - dL_0L\ln(S)$$

$$- dL_0L\ln(1 + H(\beta)) - dL_1LS\ln(1 + H(\alpha)) - dL_1LS\ln(1 + H(\alpha^\beta))$$

=>

$$\ln(|\Delta|) \geq - K_1L(L_0 + \ln(L) + L_0\ln(S) + L_1S)$$

=>

$$\ln(|\Delta|) \geq - K_2L(L_0\ln(S) + L_1S),$$

the positive absolute constant K_2 being independent of $N >> 0$. Take now $C \geq 6K_2$ -- then

$$\begin{aligned} \ln(|\Delta|) &\geq - \frac{C}{6} L(L_0\ln(S) + L_1S) \\ &= \frac{1}{6} (- CL(L_0\ln(S) + L_1S)) \\ &\geq \frac{1}{6} (- 2L^2) \quad \text{(cf. \#5)} \\ &= - \frac{L^2}{3}, \end{aligned}$$

the assertion of #13.

§28. GELFOND-SCHNEIDER: EXECUTION

Under the assumption that $\alpha \neq 0,1$ is algebraic, that β is algebraic, and that α^β is algebraic, the central conclusion of §27 is that

$$\Delta = \det(f_j(\zeta_i)) = 0,$$

the goal being to show that $\beta \in \mathbb{Q}$.

Proceeding, assume momentarily that $\alpha,\beta,\alpha^\beta \in \bar{\mathbb{Q}} \cap \mathbb{R}$ $(\alpha > 0)$, hence all data is real and the columns of the matrix $(f_j(\zeta_i))$ are linearly dependent over $\mathbb{R}$, thus there exist real numbers $b_1,\ldots,b_L$ not all zero such that

$$\sum_{j=1}^{L} b_j f_j(\zeta_i) = 0 \quad (1 \leq i \leq L).$$

But

$$f_j(\zeta_i) = \zeta_i^{u(j)}\alpha^{v(j)\zeta_i},$$

so

$$\sum_{j=1}^{L} b_j \zeta_i^{u(j)}\alpha^{v(j)\zeta_i} = 0 \quad (1 \leq i \leq L)$$

or still,

$$\sum_{v=0}^{L_1} \Big(\sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}\zeta_i^u\Big)\alpha^{v\zeta_i} = 0.$$

Introduce

$$a_v(t) = \sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}t^u,$$

where $t \in \mathbb{R}$, and consider

$$\sum_{v=0}^{L_1} a_v(t)e^{w_v t} \quad (w_v = v \operatorname{Log} \alpha).$$

Since

$$0 = \sum_{v=0}^{L_1} a_v(\zeta_i)e^{w_v\zeta_i} \quad (\zeta_i = s_1(i) + s_2(i)\beta),$$

it follows that each of the L values of ζ_i is a zero of

$$A(t) \equiv \sum_{v=0}^{L_1} a_v(t)e^{w_v t}.$$

At this point, #1 of §26 is applicable:

- The degree of $a_v(t)$ is $\leq L_0$.
- The w_v are distinct real numbers.
- The sum defining $A(t)$ consists of $L_1 + 1$ polynomials.

Accordingly $A(t)$ has at most

$$L_0(L_1 + 1) + (L_1 + 1) - 1$$

real zeros counting multiplicities. And:

$$\begin{aligned} & L_0(L_1 + 1) + (L_1 + 1) - 1 \\ & = L_0L_1 + L_0 + L_1 + 1 - 1 \\ & = (L_0 + 1)(L_1 + 1) - 1 \\ & = L - 1 \quad (\text{cf. §27, \#3}) \\ & < L. \end{aligned}$$

Consequently two of the ζ_i must be the same, so

$$s_1(i) + s_2(i)\beta = s_1(i') + s_2(i')\beta$$

for some i,i' with $1 \leq i < i' \leq L$. However, since the pairs $(s_1(i),s_2(i))$ and

$(s_1(i'),s_2(i'))$ are distinct, either

$$\beta = \frac{s_1(i) - s_1(i')}{s_2(i') - s_2(i)} \quad \text{if } s_2(i') \neq s_2(i)$$

or

$$\frac{1}{\beta} = \frac{s_2(i') - s_2(i)}{s_1(i) - s_1(i')} \quad \text{if } s_1(i) \neq s_1(i').$$

In any event, β is rational... .

To discuss the general case, it is necessary to elaborate on what has been said in §27.

Step 1: Redefine S and replace $\frac{1}{2}(N^4 - 1)$ by $2N^4$ -- then

$$\frac{S}{2} = N^4 \Rightarrow \frac{S^2}{4} = N^8 = L.$$

And

$$\begin{aligned}(2S + 1)^2 &= 4S^2 + 4S + 1 \\ &= 16N^8 + 8N^4 + 1 \\ &> 16N^8 = 16L > L.\end{aligned}$$

Step 2: Define the $(2S + 1)^2 \times L$ matrix M as in §27 and note that all the $L \times L$ submatrices of M have determinant zero, as can be gleaned from the argumentation used there.

Step 3: The columns of the matrix M are linearly dependent over $\mathbf{C}$, thus there exist complex numbers $b_1,\ldots,b_L$ not all zero such that

$$\sum_{j=1}^{L} b_j f_j(\zeta_i) = 0 \quad (i \in \{1,\ldots,(2S + 1)^2\}).$$

<u>Step 4</u>: Introduce as before

$$A(t) \equiv \sum_{v=0}^{L_1} a_v(t)e^{w_v t}$$

and observe that

$$A(\zeta_i) = 0 \quad (i \in \{1,\ldots,(2S+1)^2\}).$$

Owing to §26, #5,

$$N(R,A) \leq 3(D-1) + 4R\Omega$$

or better, its improvement

$$N(R,A) \leq 2(D-1) + \frac{4}{\pi}R\Omega,$$

as noted in the Appendix to §26. Here

$$D \leq L_0(L_1+1) + (L_1+1) = L.$$

And

$$\zeta_i = s_1(i) + s_2(i)\beta,$$

where a priori β is complex and $|s_1|,|s_2| \leq S$, the choice

$$R = S(1+|\beta|)$$

ensures that the disc of radius R centered at the origin contains all the points ζ_i. In addition

$$\Omega = \max_{v=0,\ldots,L_1} |w_v| = \max_{v=0,\ldots,L_1} |v\mathrm{Log}\,\alpha|$$

$$= L_1\,|\mathrm{Log}\,\alpha|.$$

Therefore

$$N(R,A) \leq 2(L-1) + \frac{4}{\pi}S(1+|\beta|)L_1\,|\mathrm{Log}\,\alpha|$$

or still,

$$N(R,A) \leq 2(L-1) + KSL_1,$$

where

$$K = \frac{4}{\pi}(1 + |\beta|)\ |\mathrm{Log}\ \alpha|.$$

But:

- $2(L-1) < 2L = 2(\frac{S^2}{4}) = \frac{S^2}{2}$

- $KSL_1 = K(2N^4)(N^2 - 1)$

$$< 2KN^6$$

$$< N^8 \quad (N >> 0)$$

$$= \frac{S^2}{4}$$

=>

$$N(R,A) < \frac{S^2}{2} + \frac{S^2}{4}$$

$$= \frac{3}{4}S^2 < (2S+1)^2.$$

Since A admits $(2S + 1)^2$ zeros ζ_i, two of them must be the same, forcing in the end the rationality of β.

§29. THE SCHNEIDER-LANG CRITERION

Fix an algebraic number field K.

[Note: Therefore K is a subfield of C which, when considered as a vector space over Q, is finite dimensional, denoted [K:Q] and called the <u>degree</u> of K over Q.]

<u>1:</u> THEOREM Let f_1, f_2 be entire functions of finite strict orders $\leq \rho_1, \leq \rho_2$. Assume: f_1, f_2 are algebraically independent over C and that the derivatives $\frac{d}{dz} f_1, \frac{d}{dz} f_2$ belong to the ring $K[f_1, f_2]$ (i.e., can be written as polynomials in f_1, f_2) -- then the set

$$S = \{w \in C: f_1(w), f_2(w) \in K\}$$

is finite.

There are two "canonical" examples that illustrate this criterion.

<u>2:</u> APPLICATION Schneider-Lang => Hermite-Lindemann

I.e.: If α is a nonzero algebraic number, then e^α is transcendental (cf. §21, #4).

[Suppose instead that e^α is algebraic, let $K = Q(\alpha, e^\alpha)$, and take $f_1(z) = z(\rho_1 = 0)$, $f_2(z) = e^z(\rho_2 = 1)$ (which are algebraically independent over C (cf. §20, #18)). Since it is clear that

$$\frac{d}{dz} z, \frac{d}{dz} e^z \in K[f_1(z), f_2(z)],$$

the assumptions of #1 are satisfied. On the other hand, $\forall\, n \in \mathbb{N}$,

$$f_1(n\alpha) = n\alpha \in K,\ f_2(n\alpha) = e^{n\alpha} \in K,$$

an infinite set of conditions, from which a contradiction.]

<u>3:</u> APPLICATION Schneider-Lang => Gelfond-Schneider

I.e.: If $\alpha \neq 0,1$ is algebraic and if $\beta \in \mathbb{Q}$ is algebraic, then α^β is transcendental (cf. §24, #1).

[Suppose instead that α^β is algebraic, let $K = \mathbb{Q}(\alpha,\beta,\alpha^\beta)$, and take $f_1(z) = e^z$ $(\rho_1 = 1)$, $f_2(z) = e^{\beta z}$ $(\rho_2 = 1)$ -- then $f_1(z), f_2(z)$ are algebraically independent over $\mathbb{C}$ $(\beta \notin \mathbb{Q})$ (cf. §20, #26). Moreover

$$\frac{d}{dz} f_1 = f_1,\ \frac{d}{dz} f_2 = \beta f_2,$$

so $K[f_1(z), f_2(z)]$ is closed under differentiation, thus in view of #1 there are but finitely many points $w \in \mathbb{C}$ such that $f_1(w) \in K$ and $f_2(w) \in K$. But for all $k = 1,2,\ldots,$

$$f_1(k\operatorname{Log}\alpha) = \alpha^k \in K \text{ and } f_2(k\operatorname{Log}\alpha) = (\alpha^\beta)^k \in K,$$

an infinite set of conditions, from which a contradiction.]

<u>4:</u> REMARK The objective is to show that the set S figuring in #1 is finite. In fact, it will turn out that the cardinality of S is bounded by

$$(\rho_1 + \rho_2)[K:\mathbb{Q}].$$

As for the proof, we shall not provide all the details but will say enough to render the whole affair believable.

Let $N >> 0$ be a positive integer.

5: NOTATION Put

$$R_1 (= R_1(N)) = [N^{\frac{\rho_2}{\rho_1 + \rho_2}} (\ell n(N))^{1/2}]$$

and

$$R_2 (= R_2(N)) = [N^{\frac{\rho_1}{\rho_1 + \rho_2}} (\ell n(N))^{1/2}].$$

6: N.B.

$$\begin{aligned} R_1 R_2 &\leq N^{\frac{\rho_2}{\rho_1 + \rho_2}} (\ell n(N))^{1/2} N^{\frac{\rho_1}{\rho_1 + \rho_2}} (\ell n(N))^{1/2} \\ &= N \ell n(N). \end{aligned}$$

Therefore

$$(R_1 + 1)(R_2 + 1) \geq N\ell n(N).$$

[Note: If $C \in R_{>0}$, then

$$N\ell n(N) + CN \leq 2N\ell n(N)$$

provided N is large enough:

$$N >> 0 \Rightarrow \frac{N}{N\ell n(N)} < \frac{1}{C}.]$$

Let $w_1, \ldots, w_r$ be elements of S.

7: SUBLEMMA There exists a nonzero polynomial $P_N \in Z[X_1, X_2]$ whose degree w.r.t X_1 is $\leq R_1$ and whose degree w.r.t. X_2 is $\leq R_2$ such that the function

$$F_N = P_N(f_1, f_2)$$

has the property that

$$\frac{d^n}{dz^n} F_N(w_j) = 0 \qquad (n = 0,\ldots,N-1;\ j = 1,\ldots,r).$$

[Note: Explicated, there are integers

$$C_{\lambda_1,\lambda_2} : \left[\begin{array}{l} 0 \leq \lambda_1 \leq R_1 \\ \\ 0 \leq \lambda_2 \leq R_2 \end{array}\right.$$

with

$$F_N = \sum_{\lambda_1=0}^{R_1} \sum_{\lambda_2=0}^{R_2} C_{\lambda_1,\lambda_2} f_1^{\lambda_1} f_2^{\lambda_2}.$$

Moreover

$$0 < \max_{\lambda_1,\lambda_2} |C_{\lambda_1,\lambda_2}| < e^{3[K:\mathbb{Q}]rN}.]$$

Bearing in mind that, by assumption, $f_1(z), f_2(z)$ are algebraically independent over $\mathbb{C}$, let M be the smallest positive integer with the property that for some $j_0: 1 \leq j_0 \leq r$,

$$\gamma_N \equiv \frac{d^M}{dz^M} F_N(w_{j_0}) \neq 0.$$

<u>8:</u> <u>N.B.</u> $\gamma_N \in K$ is an algebraic number. In addition

$$\frac{d^m}{dz^m} F_N(w_j) = 0 : \left[\begin{array}{l} 1 \leq j \leq r \\ \\ 0 \leq m \leq M - 1, \end{array}\right.$$

hence $N \leq M$.

<u>9:</u> NOTATION Put

$$R = M^{\frac{1}{\rho_1 + \rho_2}} .$$

Ultimately, all relevant data depends on $N >> 0$. This said, choose $N >> 0$ so as to force $M >> 0$:

$$|w_j| < \frac{R}{2} \ (j = 1, \ldots, r).$$

<u>10:</u> LEMMA If $|z| = R$, then $\forall\, j = 1, \ldots, r$,

$$\frac{1}{|z - w_j|} \leq \frac{2}{R} .$$

PROOF

$$|z - w_j| \geq ||z| - |w_j||$$

$\Rightarrow$

$$\frac{1}{|z - w_j|} \leq \frac{1}{||z| - |w_j||}$$

$$= \frac{1}{|R - |w_j||} .$$

But

$$|w_j| < \frac{R}{2} \Rightarrow - |w_j| > - \frac{R}{2}$$

$$\Rightarrow R - |w_j| > R - \frac{R}{2} = \frac{R}{2}$$

$$\Rightarrow \frac{1}{|R - |w_j||} < \frac{2}{R} \, .$$

The function

$$G_N(z) = F_N(z) \prod_{j=1}^{r} (z - w_j)^{-M}$$

is entire and

$$\gamma_N = M! \; G_N(w_{j_0}) \prod_{j \neq j_0} |(w_{j_0} - w_j)^M .$$

To estimate $|\gamma_N|$, write

$$|\gamma_N| \leq M! \prod_{j \neq j_0} |w_{j_0} - w_j|^M \cdot \sup_{|z|=R} \prod_{j=1}^{r} |z - w_j|^{-M} \cdot |F_N|_R$$

- $M! \leq M^M$
- $\prod_{j \neq j_0} |w_{j_0} - w_j|^M \equiv C^M \quad (C \in R_{>0})$
- $\frac{1}{|z - w_j|^M} \leq (\frac{2}{R})^M$

$\Rightarrow$

$$\sup_{|z| = R} \prod_{j=1}^{r} |z - w_j|^{-M} \leq (\frac{2}{R})^{rM}$$

-

$$|F_N|_R = \left| \sum_{\lambda_1=0}^{R_1} \sum_{\lambda_2=0}^{R_2} C_{\lambda_1,\lambda_2} f_1^{\lambda_1} f_2^{\lambda_2} \right|_R$$

$$\leq \sum_{\lambda_1=0}^{R_1} \sum_{\lambda_2=0}^{R_2} |C_{\lambda_1,\lambda_2}| \, |f_1^{\lambda_1} f_2^{\lambda_2}|_R$$

$$\leq (R_1 + 1)(R_2 + 1) \max_{\lambda_1,\lambda_2} |C_{\lambda_1,\lambda_2}| \, |f_1^{\lambda_1} f_2^{\lambda_2}|_R$$

$$\leq (R_1 + 1)(R_2 + 1) \, e^{3[K:Q]rN}(|f_1|_R + 1)^{R_1}(|f_2|_R + 1)^{R_2}$$

- $|z| \leq R \Rightarrow \begin{cases} |f_1(z)| \leq K_1 R^{\rho_1} \\ |f_2(z)| \leq K_2 R^{\rho_2} \end{cases} \quad (\exists\, K_1, K_2 \in R_{>0})$

$\Rightarrow$

$$(|f_1|_R + 1)^{R_1} (|f_2|_R + 1)^{R_2}$$

$$\leq (K_1 R^{\rho_1} + 1)^{R_1} (K_2 R^{\rho_2} + 1)^{R_2}$$

$$\leq K(R_1 R^{\rho_1} + R_2 R^{\rho_2}).$$

The next step is to use these majorants and derive an estimate for $\ln(|\gamma_N|)$.

FACT For $N >> 0$,

$$\ln(|\gamma_N|) \leq \left(1 - \frac{r}{\rho_1 + \rho_2}\right) M \ln(M) + M(\ln(M))^{3/4}.$$

<u>11:</u> LEMMA Let $x \in K$ be a nonzero algebraic number -- then

$$\ln(|x|) + [K:Q]\ln(d_x) + ([K:Q] - 1)\ln(H(x)) \geq 0.$$

[Here d_x is the denominator of x and H(x) is the house of x (cf. §14).]

Take $x = \gamma_N$ in #11.

FACT $\ell n(d_{\gamma_N}) \leq M(\ell n(M))^{1/2}$.

FACT $\ell n(H(\gamma_N)) \leq M\ell n(M) + M(\ell n(M))^{1/2}$.

Therefore

$$\ell n(|\gamma_N|) + [K:Q]M(\ell n(M))^{1/2}$$

$$+ ([K:Q] - 1)(M\ell n(M) + M(\ell n(M))^{1/2})$$

$$\geq 0$$

or still,

$$(1 - \frac{r}{\rho_1 + \rho_2})M\ell n(M) + M(\ell n(M))^{3/4}$$

$$+ [K:Q]M(\ell n(M))^{1/2}$$

$$+ ([K:Q] - 1)(M\ell n(M) + M(\ell n(M)^{1/2})$$

$$\geq 0$$

or still,

$$([K:Q] - \frac{r}{\rho_1 + \rho_2})M\ell n(M) + M(\ell n(M))^{3/4}$$

$$+ [K:Q]M(\ell n(M))^{1/2}$$

$$+ [K:Q]M(\ell n(M)^{1/2}) - M(\ell n(M)^{1/2})$$

$$\geq 0$$

or still,

$$([K:Q] - \frac{r}{\rho_1 + \rho_2})M\ell n(M) + M(\ell n(M))^{3/4}$$

$$+ (2[K:Q] - 1)M(\ell n(M))^{1/2}$$

$$\geq 0$$

or still,

$$([K:Q] - \frac{r}{\rho_1 + \rho_2})M\ell n(M)$$

$$\geq - M(\ell n(M)^{3/4} - (2[K:Q] - 1)M(\ell n(M))^{1/2}$$

or still,

$$(\frac{r}{\rho_1 + \rho_2} - [K:Q])M\ell n(M)$$

$$\leq M(\ell n(M))^{3/4} + (2[K:Q] - 1)M(\ell n(M))^{1/2}$$

or still,

$$(\frac{r}{\rho_1 + \rho_2} - [K:Q])\ell n(M)$$

$$\leq (\ell n(M))^{3/4} + (2[K:Q] - 1)(\ell n(M))^{1/2}$$

or still,

$$(\frac{r}{\rho_1 + \rho_2} - [K:Q]) \leq (\ell n(M))^{-1/4} + (2[K:Q] - 1)(\ell n(M))^{-1/2}.$$

But $N \to \infty \Rightarrow M > \infty$, hence

$$\frac{r}{\rho_1 + \rho_2} - [K:Q] \leq 0$$

$$\Rightarrow$$

$$\frac{r}{\rho_1 + \rho_2} \leq [K:Q]$$

$$\Rightarrow$$

$$r \leq (\rho_1 + \rho_2)[K:Q],$$

from which the claimed bound on S (cf. #4).

12: EXAMPLE Take $K = Q$, $f_1(z) = z$, $f_2(z) = e^z$ -- then

$$S = \{w \in C: w, e^w \in Q\}.$$

But

$$w \in Q \ (w \neq 0) \Rightarrow e^w \in P \quad (\text{cf. §9, \#1}),$$

so $S = \{0\}$, a set of cardinality 1. On the other hand,

$$\rho_1 = 0,\ \rho_1 = 1 \Rightarrow \rho_1 + \rho_2 = 1,$$

thus in this case, the estimate

$$(\rho_1 + \rho_2)[K:Q]$$

is the best possible.

APPENDIX

We shall indicate the derivation of the estimate

$$\ell n(|\gamma_N|) \leq (1 - \frac{r}{\rho_1 + \rho_2})M\ell n(M) + M(\ell n(M))^{3/4}.$$

First of all, the term

$$M(\ell n(M))^{3/4}$$

results from the discussion of $|F_N|_R$, hence can be set aside. As for

$$(1 - \frac{r}{\rho_1 + \rho_2})M\ell n(M),$$

note that

- $\ell n(M!) \leq M\ell n(M)$
- $\ell n(C^M) \leq M\ell n(C)$
- $\ell n(\frac{2}{R})^{rM}$

$$= \ell n(2^{rM}) - \ell n(M^{\frac{rM}{\rho_1 + \rho_2}})$$

$$= Mr\ell n(2) - \frac{r}{\rho_1 + \rho_2} M\ell n(M).$$

One must then add these terms. But since $N >> 0 \Rightarrow M >> 0$, one can ignore

$$M\ell n(C) \text{ and } Mr\ell n(2),$$

leaving

$$M\ell n(M) - \frac{r}{\rho_1 + \rho_2} M\ell n(M)$$

$$= (1 - \frac{r}{\rho_1 + \rho_2})M\ell n(M).$$

§30. SCHNEIDER-LANG CRITERIA

There are extensions and variants of the Schneider-Lang criterion (cf. §29, #1), e.g., work with meromorphic functions (i.e., quotients of two entire functions) or raise the variables from 1 to n (i.e., replace $\mathbb{C}$ by $\mathbb{C}^n$).

Fix an algebraic number field K.

1: RAPPEL A meromorphic function is said to be of finite strict order $\leq \rho$ if it is the quotient of two entire functions each of finite strict order $\leq \rho$.

2: THEOREM Let $f_1, f_2, \ldots, f_n$ $(n \geq 2)$ be meromorphic functions such that f_1, f_2 are of finite strict orders $\leq \rho_1$, $\leq \rho_2$. Assume: f_1, f_2 are algebraically independent over $\mathbb{C}$ and that the derivative $\frac{d}{dz}$ maps the ring $K[f_1, f_2, \ldots, f_n]$ into itself -- then the set S of $w \in \mathbb{C}$ which are not among the singularities of $f_1, f_2, \ldots, f_n$ but such that

$$f_i(w) \in K \quad (1 \leq i \leq n)$$

is finite and in fact the cardinality of S is bounded by

$$(\rho_1 + \rho_2)[K:\mathbb{Q}].$$

[The argument is a straight forward extension of that used to establish the Schneider-Lang criterion. Thus let $w_1, \ldots, w_r$ be elements of S which are not among the singularities of $f_1, f_2, \ldots, f_n$ but such that

$$f_i(w_j) \in K \quad (1 \leq i \leq n;\ 1 \leq j \leq r).$$

Choose entire functions g_1, g_2 of finite strict orders $\leq \rho_1$, $\leq \rho_2$ with the property that g_1f_1, g_2f_2 are entire and

$$\begin{cases} g_1(w_j) \neq 0 & (1 \leq j \leq r) \\ g_2(w_j) \neq 0 & (1 \leq j \leq r). \end{cases}$$

Define F_N as in §29, #7 and form

$$g_1^{R_1} g_2^{R_2} F_N,$$

an entire function admitting $w_1,\ldots,w_r$ as zeros of order at least equal to M. Put

$$G_N(z) = g_1(z)^{R_1} g_2(z)^{R_2} F_N(z) \prod_{j=1}^{r} (z - w_j)^{-M},$$

take R as in §29, #9, and note that

$$\gamma_N = M!\ G_N(w_{j_0})g_1(w_{j_0})^{-R_1} g_2(w_{j_0})^{-R_2} \prod_{j \neq j_0} (w_{j_0} - w_j)^M.$$

Proceed from this point as before.]

There are also versions of Schneider-Lang where $\mathbf{C}$ is replaced by $\mathbf{C}^n$.

To set matters up, fix an algebraic number field K and suppose that $f_1,\ldots,f_m$ are entire functions of the complex variables $z_1,\ldots,z_n$ with $m \geq n + 1$. Assume: $f_1,\ldots,f_{n+1}$ are algebraically independent over $\mathbf{C}$ of finite strict orders $\leq \rho_1,\ldots,$ $\leq \rho_{n+1}$ and that the partial derivatives $\frac{\partial}{\partial z_i}$ $(1 \leq i \leq n)$ map the ring $K[f_1,\ldots,f_m]$ into itself. Denote by S the set of $w \in \mathbf{C}^n$ such that

$$f_k(w) \in K \quad (1 \leq k \leq m).$$

3: REMARK It can be shown that S is contained in an algebraic hypersurface of degree at most

$$n(\rho_1 + \cdots + \rho_{n+1})[K:\mathbb{Q}].$$

[Note: This means that S is the set of zeros of a nonzero polynomial in $\mathbb{C}[X_1,\ldots,X_n]$, its degree being the minimum of the degrees of the nonzero polynomials which annihilate S.]

4: THEOREM Let $e_1,\ldots,e_n$ be a basis for $\mathbb{C}^n$ over $\mathbb{C}$ and let $S_1,\ldots,S_n$ be subsets of $\mathbb{C}$. Suppose further that

$$S \supset \{s_1e_1 + \cdots + s_ne_n : (s_1,\ldots,s_n) \in S_1 \times \cdots \times S_n\}.$$

I.e.: $\forall\ (s_1,\ldots,s_n) \in S_1 \times \cdots \times S_n$:

$$f_k(s_1e_1 + \cdots + s_ne_n) \in K \quad (1 \leq k \leq m).$$

Then

$$\min_{1\leq i\leq n} \text{card } S_i \leq n(\rho_1 + \cdots + \rho_{n+1})[K:\mathbb{Q}].$$

[Note: Take $n = 1$ to recover the Schneider-Lang criterion.]

5: N.B. Therefore the set S cannot contain a product $S_1 \times \cdots \times S_n$, where each S_i is infinite.

Let Γ be an additive subgroup of $\mathbb{C}^n$ which contains a basis for $\mathbb{C}^n$ over $\mathbb{C}$ -- then the points of Γ are linearly independent over the complex numbers and this allows one to change coordinates so as to render Γ a product:

$$\Gamma \approx S_1 \times \cdots \times S_n.$$

Consider the values

$$f_k(\zeta_1,\ldots,\zeta_n) \quad (1 \le k \le m),$$

where

$$(\zeta_1,\ldots,\zeta_n) \in \Gamma.$$

Then the set S cannot contain Γ (cf. #5).

<u>6:</u> EXAMPLE It is shown in §31, #13 that

$$\int_0^1 \frac{1}{1+x^3}\,dx = \frac{1}{3}\left(\ln(2) + \frac{\pi}{\sqrt{3}}\right)$$

is transcendental. Here is another approach. Suppose that

$$\frac{1}{3}\left(\ln(2) + \frac{\pi}{\sqrt{3}}\right)$$

is algebraic -- then

$$\alpha \equiv 3\sqrt{3}\,\sqrt{-1}\cdot\frac{1}{3}\left(\ln(2) + \frac{\pi}{\sqrt{3}}\right)$$

$$= \sqrt{3}\,\sqrt{-1}\,\ln(2) + 3\sqrt{-1}\,\pi$$

is algebraic. Work in C^2 with the functions

$$f_1(z_1,z_2) = \exp(z_1),\ f_2(z_1,z_2) = \exp(z_2),\ f_3(z_1,z_2) = z_1 + \sqrt{3}\,\sqrt{-1}\,z_2$$

and let $K = Q(\sqrt{3}\,\sqrt{-1},\alpha)$. Denote by Γ the additive subgroup of C^2 generated by the points

$$u = (3\pi\sqrt{-1},\ \ln(2)),\ v = (-3\ln(2),\ 3\pi\sqrt{-1})$$

$$\Rightarrow \Gamma = Zu + Zv.$$

Then these points are linearly independent over $\mathbf{C}$ since their determinant

$$\begin{vmatrix} 3\pi\sqrt{-1} & \ln(2) \\ -3\ln(2) & 3\pi\sqrt{-1} \end{vmatrix} = -9\pi^2 + 3(\ln(2))^2 \neq 0.$$

The claim now is that $S \subset \Gamma$, a contradiction. It is trivial that

$$f_1(\Gamma) \subset K,\ f_2(\Gamma) \subset K.$$

As for f_3, we have

$$\begin{aligned} f_3(3\pi\sqrt{-1}, \ln(2)) &= 3\pi\sqrt{-1} + \sqrt{3}\sqrt{-1}\ln(2) \\ &= \sqrt{3}\sqrt{-1}\ln(2) + 3\sqrt{-1}\pi \\ &= \alpha \end{aligned}$$

and

$$\begin{aligned} f_3(-3\ln(2), 3\pi\sqrt{-1}) &= -3\ln(2) + \sqrt{3}\sqrt{-1}\,3\pi\sqrt{-1} \\ &= -3\ln(2) - 3\sqrt{3}\pi. \end{aligned}$$

By construction, $\sqrt{3}\sqrt{-1} \in K$. With this in mind, consider

$$\begin{aligned} &\sqrt{3}\sqrt{-1}\,(-3\ln(2) - 3\sqrt{3}\pi) \\ &\quad = -3(\sqrt{3}\sqrt{-1}\ln(2) + 3\sqrt{-1}\pi) \\ &\quad = -3\alpha \end{aligned}$$

or still,

$$\begin{aligned} -3\ln(2) - 3\sqrt{3}\pi &= \frac{-3}{\sqrt{3}\sqrt{-1}}\alpha \\ &\in K. \end{aligned}$$

7: NOTATION Given

$$\left[\begin{array}{l} \underline{z} = (z_1,\ldots,z_n) \\ \\ \underline{w} = (w_1,\ldots,w_n) \end{array}\right.$$

in $\mathbf{C}^n$, write

$$\underline{zw} = z_1w_1 + \cdots + z_nw_n.$$

Let d_0, d_1, and n be integers with

$$0 \leq d_0 \leq n < d_0 + d_1.$$

8: N.B. The role of m above is played at this juncture by

$$d \equiv d_0 + d_1 > n \Rightarrow n + 1 \leq d.$$

Let $\underline{x}_1,\ldots,\underline{x}_{d_1}$ be $\mathbf{Q}$-linearly independent elements of $\overline{\mathbf{Q}}^n$ and let $\underline{y}_1,\ldots,\underline{y}_n$ be a basis for $\mathbf{C}^n$ over $\mathbf{C}$. Write

$$\underline{y}_j = (y_{1j},\ldots,y_{nj}) \quad (1 \leq j \leq n)$$

and call Γ the additive subgroup of $\mathbf{C}^n$ generated by the $\underline{y}_j$.

9: THEOREM At least one of the following numbers

$$y_{hj}\,(1 \leq h \leq d_0),\ e^{\underline{x}_i\underline{y}_j} \quad (1 \leq i \leq d_1,\ 1 \leq j \leq n)$$

is transcendental.

PROOF Consider the functions

$$f_h(\underline{z}) = z_h \quad (1 \leq h \leq d_0),\ f_{d_0+i}(\underline{z}) = e^{\underline{x}_i\underline{z}} \quad (1 \leq i \leq d_1).$$

The condition on the "finite strict orders" is certainly satisfied and since $\underline{x}_1,\ldots,\underline{x}_{d_1}$ are linearly independent over Q, the functions $f_1,\ldots,f_d$ are algebraically independent over the field $Q(z_1,\ldots,z_n)$. Moreover

$$\frac{\partial}{\partial z_j} f_h = \delta_{hj} = \begin{cases} 0 \text{ if } h \neq j \\ \\ 1 \text{ if } h = j \end{cases} \quad (1 \leq h \leq d_0)$$

and

$$\frac{\partial}{\partial z_j} f_{d_0+i} = x_{ji}\, f_{d_0+i} \quad (1 \leq i \leq d_1),$$

where $\underline{x}_i = (x_{1i},\ldots,x_{ni})$ $(1 \leq i \leq d_1)$. Therefore the partial derivative requirement is satisfied. Now let K be the field generated over Q by the $(d_0 + 2d_1)n$ numbers

$$x_{ji},\ f_h(\underline{y}_j) = y_{hj},\ f_{d_0+i}\ (\underline{y}_j) = e^{\underline{x}_i \underline{y}_j},$$

the range of the parameters being

$$1 \leq h \leq d_0,\ 1 \leq i \leq d_1,\ 1 \leq j \leq n.$$

To arrive at a contradiction, assume that these numbers are algebraic, hence that K is an algebraic number field. Take a typical point

$$Y \equiv s_1\underline{y}_1 + \cdots + s_n\underline{y}_n \quad (\underline{s} = (s_1,\ldots,s_n) \in Z^n)$$

on Γ -- then

$$f_1(Y) \in K,\ldots,f_d(Y) \in K.$$

I.e.: $\Gamma \subset S$, an impossibility (cf. supra). Accordingly the supposition that K is an algebraic number field is false. Since the x_{ji} are algebraic (by hypothesis), it follows that at least one of the following numbers

$$y_{hj} (1 \le h \le d_0),\ e^{\underline{x}_i \underline{y}_j} \ (1 \le i \le d_1,\ 1 \le j \le n)$$

is transcendental.

<u>10:</u> APPLICATION Take $d_0 = 0$, so $d = d_1 > n$ (formally, this just means to ignore in the above anything involving d_0), hence y_{hj} is no longer part of the theory and the conclusion is that at least one of the

$$e^{\underline{x}_i \underline{y}_j} \ (1 \le i \le d,\ 1 \le j \le n)$$

is transcendental, hence at least one of the

$$\underline{x}_i \underline{y}_j \quad (1 \le i \le d,\ 1 \le j \le n)$$

does not belong to L.

[Note: It suffices for the analysis that the set $\{\underline{y}_1, \ldots, \underline{y}_d\}$ contain a basis for $\mathbb{C}^n$ over $\mathbb{C}$.]

<u>11:</u> EXAMPLE Let $\lambda_1, \lambda_2, \lambda_3$ be elements of L and assume that

$$\lambda_1 + \sqrt[3]{2}\, \lambda_2 + \sqrt[3]{4}\, \lambda_3 = 0.$$

Then

$$1,\ \sqrt[3]{2},\ \sqrt[3]{4}$$

belong to $\overline{\mathbb{Q}}$ and we claim that

$$\lambda_1 = 0,\ \lambda_2 = 0,\ \lambda_3 = 0.$$

To see this, start by multiplying the given relation by $\sqrt[3]{2}$ and $\sqrt[3]{4}$:

$$2\lambda_3 + \sqrt[3]{2}\,\lambda_1 + \sqrt[3]{4}\,\lambda_2 = 0 \text{ and } 2\lambda_2 + 2\sqrt[3]{2}\,\lambda_3 + \sqrt[3]{4}\,\lambda_1 = 0.$$

Put

$$\begin{bmatrix} \underline{x}_1 = (1,0),\ \underline{x}_2 = (0,1),\ \underline{x}_3 \doteq (\sqrt[3]{2}\,,\sqrt[3]{4}) \\ \\ \underline{y}_1 = (\lambda_2,\lambda_3),\ \underline{y}_2 = (\lambda_1,\lambda_2),\ \underline{y}_3 = (2\lambda_3,\lambda_1). \end{bmatrix}$$

Here d = 3, n = 2 and

$$\begin{array}{lll} \underline{x}_1\underline{y}_1 = \lambda_2, & \underline{x}_1\underline{y}_2 = \lambda_1, & \underline{x}_1\underline{y}_3 = 2\lambda_3, \\ \underline{x}_2\underline{y}_1 = \lambda_3, & \underline{x}_2\underline{y}_2 = \lambda_2, & \underline{x}_2\underline{y}_3 = \lambda_1, \\ \underline{x}_3\underline{y}_1 = -\lambda_1, & \underline{x}_3\underline{y}_2 = -2\lambda_3, & \underline{x}_3\underline{y}_3 = -2\lambda_2. \end{array}$$

Moreover if $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, $\lambda_3 \neq 0$, then the matrix

$$\begin{bmatrix} \lambda_2 & \lambda_1 & 2\lambda_3 \\ \lambda_3 & \lambda_2 & \lambda_1 \end{bmatrix}$$

has rank 2, thus $\{\underline{y}_1,\underline{y}_2,\underline{y}_3\}$ contains a basis for C^2 over C. Therefore this data realizes the setup of #10, hence at least one of the

$$\underline{x}_i\underline{y}_j \quad (1 \leq i \leq 3,\ 1 \leq j \leq 3)$$

does not belong to L, an impossibility. Since the supposition that $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, $\lambda_3 \neq 0$ has led to a contradiction, at least one of $\lambda_1,\lambda_2,\lambda_3$ is 0, say $\lambda_1 = 0$, leaving λ_2 and λ_3:

$$\sqrt[3]{2}\,\lambda_2 + \sqrt[3]{4}\,\lambda_3 = 0.$$

Obviously

$$\left[\begin{array}{l} \lambda_2 = 0 \Rightarrow \lambda_3 = 0 \\ \\ \lambda_3 = 0 \Rightarrow \lambda_2 = 0. \end{array}\right.$$

If now both λ_2 and λ_3 are nonzero, then on general grounds (cf. §24, #10), the ratio λ_2/λ_3 is either rational or transcendental. But λ_2/λ_3 is not rational but is algebraic... .

<u>12:</u> APPLICATION Take $d_0 = 1$, $d_1 = n$ ($\Rightarrow d = 1 + n$). Work this time with $\underline{x}_1,\ldots,\underline{x}_n$ Q-linearly independent elements of $\overline{\mathbb{Q}}^n$ and $\underline{y}_1,\ldots,\underline{y}_n$ a basis for $\mathbb{C}^n$ over $\mathbb{C}$. Write

$$\underline{y}_j = (y_{1j},\ldots,y_{nj}) \quad (1 \leq j \leq n)$$

and assume that the numbers

$$y_{1j} (1 \leq j \leq n) \quad (h = 1)$$

are algebraic -- then the conclusion is that at least one of the

$$e^{\underline{x}_i \underline{y}_j} \quad (1 \leq i \leq n,\ 1 \leq j \leq n)$$

is transcendental, hence at least one of the

$$\underline{x}_i \underline{y}_j \quad (1 \leq i \leq n,\ 1 \leq j \leq n)$$

does not belong to L.

[Note: This is a literal transcription of #9 to the current setting. For later use, observe that the symbol d does not appear in any of the formulas. Because of this, one can replace n by d thru out, so now at least one of the

$$\underline{x}_i \underline{y}_j \quad (1 \leq i \leq d,\ 1 \leq j \leq d)$$

does not belong to L.]

§31. BAKER: STATEMENT

1: NOTATION Put

$$L = \{\lambda \in \mathbf{C} : e^{\lambda} \in \bar{\mathbf{Q}}^{\times}\}$$

or still,

$$L = \exp^{-1}(\bar{\mathbf{Q}}^{\times}).$$

2: LEMMA L is a $\mathbf{Q}$-vector space.

3: LEMMA $\bar{\mathbf{Q}} \cap L = \{0\}$ (cf. §21, #4).

4: N.B. Therefore every nonzero element of L is transcendental.

5: THEOREM The following assertions are equivalent.

- If α is a nonzero algebraic number, then e^{α} is transcendental (Hermite-Lindemann).
- If $\lambda \in L$ is nonzero, then $1, \lambda$ are $\bar{\mathbf{Q}}$-linearly independent.
- If a is a nonzero complex number, then at least one of the two numbers a, e^{a} is transcendental.

6: THEOREM The following assertions are equivalent.

- If $\alpha \neq 0,1$ is algebraic and if $\beta \notin \mathbf{Q}$ is algebraic, then α^{β} is transcendental (Gelfond-Schneider).
- If $\lambda_1 \in L$, $\lambda_2 \in L$ are nonzero and $\mathbf{Q}$-linearly independent, then λ_1, λ_2 are $\bar{\mathbf{Q}}$-linearly independent.
- If a,b are nonzero complex numbers with $a \notin \mathbf{Q}$, then at least one of the three numbers a, e^{b}, e^{ab} is transcendental.

7: REMARK L is not a $\bar{Q}$-vector space.

Items 5 and 6 serve to motivate the central result which is due to Baker.

8: THEOREM If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and Q-linearly independent, then $1, \lambda_1, \ldots, \lambda_n$ are $\bar{Q}$-linearly independent.

9: N.B. This is the so-called "inhomogeneous case". Dropping the "1" gives the "homogeneous case". I.e.: If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and Q-linearly independent, then $\lambda_1, \ldots, \lambda_n$ are $\bar{Q}$-linearly independent.

We shall postpone the proof of #8 until §33 and simply assume its validity for the remainder of this §.

10: SCHOLIUM If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and Q-linearly independent, then

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n \neq 0$$

for every tuple $(\beta_0, \beta_1, \ldots, \beta_n)$ of algebraic numbers different from $(0,0,\ldots,0)$.

11: LEMMA Every nonzero linear combination

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n \quad (\lambda_1 \in L, \ldots, \lambda_n \in L)$$

with algebraic coefficients is transcendental.

PROOF Argue by induction on n, starting with n = 1, the validity in this case being ensured by #4. Proceeding, suppose first that $\lambda_1, \ldots, \lambda_n$ are nonzero and Q-linearly independent and suppose that

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n \equiv - \beta_0$$

is algebraic, hence

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n = 0$$

$$\Rightarrow$$

$$\beta_1 = 0, \ldots, \beta_n = 0,$$

contradicting the assumption that

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n \neq 0.$$

If now instead there exist rationals $q_1, \ldots, q_n$ such that

$$q_1\lambda_1 + \cdots + q_n\lambda_n = 0$$

with $q_n \neq 0$, then

$$\begin{aligned}
&q_n(\beta_1\lambda_1 + \cdots + \beta_n\lambda_n) \\
&= q_n\beta_1\lambda_1 + \cdots + q_n\beta_n\lambda_n \\
&= q_n\beta_1\lambda_1 + \cdots + q_n\beta_n\lambda_n - \beta_n(q_1\lambda_1 + \cdots + q_n\lambda_n) \\
&= (q_n\beta_1 - q_1\beta_n)\lambda_1 + \cdots + (q_n\beta_n - q_n\beta_n)\lambda_n \\
&= (q_n\beta_1 - q_1\beta_n)\lambda_1 + \cdots + (q_n\beta_{n-1} - q_{n-1}\beta_n)\lambda_{n-1},
\end{aligned}$$

a number which, by the induction hypothesis, is transcendental.

12: APPLICATION If α, β are nonzero algebraic numbers, then

$$\beta\pi + \operatorname{Log}\alpha$$

is transcendental.

[In #11, take

$$\left[\begin{array}{l}
\lambda_1 = 2\pi\sqrt{-1} \quad (e^{\lambda_1} = 1),\ \lambda_2 = \operatorname{Log}\alpha \\
\beta_1 = \sqrt{-1}\,\beta,\ \beta_2 = -2.
\end{array}\right.$$

Then

$$\sqrt{-1}\ \beta(2\pi\sqrt{-1}) + (-2)\text{Log}\ \bar{\alpha}$$

is transcendental, i.e.,

$$-\beta 2\pi + (-2)\text{Log}\ \alpha$$

is transcendental, i.e.,

$$-\frac{1}{2}(-\beta 2\pi + (-2)\text{Log}\ \alpha)$$

is transcendental, i.e.,

$$\beta\pi + \text{Log}\ \alpha$$

is transcendental.

[Note: Take $\alpha = 1$, $\beta = 1$ and conclude that π is transcendental (cf. §19, #1). On the other hand, if $\alpha \neq 1$, then Log α is transcendental (cf. #4).]

13: EXAMPLE Put

$$I = \int_0^1 \frac{1}{1 + x^3}\,dx.$$

Then

$$I = \frac{1}{3}\left(\ell n(2) + \frac{\pi}{\sqrt{3}}\right)$$

is transcendental.

14: LEMMA If $\alpha_1,\ldots,\alpha_n$ and $\beta_0,\beta_1,\ldots,\beta_n$ are nonzero algebraic numbers, then

$$e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n} \quad \text{(principal powers)}$$

is transcendental.

PROOF Suppose that

$$\alpha_{n+1} \equiv e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$$

were algebraic. Take Log's -- then for some $k \in Z$,

$$\text{Log}\ \alpha_{n+1} = \text{Log}(e^{\beta_0}\ \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n})$$

$$= \beta_0 + \beta_1 \text{ Log } \alpha_1 + \cdots + \beta_n \text{ Log } \alpha_n + 2\pi \sqrt{-1}\, k \quad (\text{cf. §23, \#5}).$$

But

$$\text{Log } {-1} = \ell n(\,|-1|\,) + \pi\sqrt{-1}$$

$$= \pi \sqrt{-1}.$$

Therefore

$$\text{Log}\ \alpha_{n+1} = \beta_0 + \beta_1 \text{ Log } \alpha_1 + \cdots + \beta_n \text{ Log } \alpha_n + 2k \text{ Log } {-1}.$$

or still,

$$\beta_1 \text{ Log } \alpha_1 + \cdots + \beta_n \text{ Log } \alpha_n + 2k \text{ Log } {-1} - \text{Log}\ \alpha_{n+1} = -\beta_0.$$

But the RHS is algebraic and nonzero, thus so is the LHS, which contradicts #11.

15: EXAMPLE $e^{\sqrt{2}}\ 2^{\sqrt{3}}$ is transcendental.

16: EXAMPLE Consider

$$e^{\pi\alpha + \beta} \quad (\alpha, \beta \in \bar{\mathbb{Q}},\ \alpha \neq 0,\ \beta \neq 0).$$

Then

$$e^{\pi\alpha} = (-1)^{-\sqrt{-1}\,\alpha} = e^{-\sqrt{-1}\,\alpha \text{ Log } {-1}}.$$

In the preceding, take

$$\alpha_1 = -1,\ \beta_0 = \beta,\ \beta_1 = -\sqrt{-1}\,\alpha.$$

Then

$$e^{\beta_0}\ \alpha_1^{\beta_1} = e^{\beta}\ (-1)^{-\sqrt{-1}\,\alpha} = e^{\beta}e^{\pi\alpha} = e^{\pi\alpha+\beta}$$

is transcendental.

[Note: Take $\alpha = 2\sqrt{-1}$ and conclude that e^{β} is transcendental (cf. §21, #4).]

<u>17:</u> LEMMA If $\alpha_1 \neq 0,1,\ldots,\alpha_n \neq 0,1$ are algebraic numbers and if $\beta_1,\ldots,\beta_n$ are algebraic numbers with $1,\beta_1,\ldots,\beta_n$ Q-linearly independent, then

$$\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n} \quad \text{(principal powers)}$$

is transcendental.

PROOF Suppose that

$$\alpha_{n+1} \equiv \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$$

were algebraic. Write

$$\begin{aligned} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n} &= e^{\beta_1 \operatorname{Log} \alpha_1} \cdots e^{\beta_n \operatorname{Log} \alpha_n} \\ &= e^{\beta_1 \operatorname{Log} \alpha_1 + \cdots + \beta_n \operatorname{Log} \alpha_n} \\ &= e^{\Lambda} \end{aligned}$$

if

$$\Lambda = \beta_1 \operatorname{Log} \alpha_1 + \cdots + \beta_n \operatorname{Log} \alpha_n.$$

Then

$$e^{\Lambda} = \alpha_{n+1} \Rightarrow \Lambda \in L.$$

Put

$$\lambda_1 = \operatorname{Log} \alpha_1,\ldots,\lambda_n = \operatorname{Log} \alpha_n, \lambda_{n+1} = \Lambda$$

to get

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n + 1(-\lambda_{n+1}) = 0.$$

On the other hand, thanks to the assumption that $1, \beta_1, \ldots, \beta_n$ are Q-linearly independent, the entity

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n + 1(-\lambda_{n+1})$$

is nonzero (cf. §32, #3 (ii)). Contradiction.

18: REMARK Consider Gelfond-Schneider (cf. #6). Here $\alpha^\beta = e^{\beta \operatorname{Log} \alpha}$ is the principal power. Pass to its k^{th} associate:

$$\alpha^\beta(e^{2k\pi\sqrt{-1}\,\beta}) \quad (k \in \mathbb{Z}) \quad (\text{cf. §23, #15})$$

and write

$$\begin{aligned} e^{2k\pi\sqrt{-1}\,\beta} &= e^{\pi(2k\sqrt{-1}\,\beta)} \\ &= (-1)^{-\sqrt{-1}(2k\sqrt{-1}\,\beta)} \quad (\text{cf. #16}) \\ &= (-1)^{2k\beta}. \end{aligned}$$

Therefore

$$\alpha^\beta(e^{2k\pi\sqrt{-1}\,\beta}) = \alpha^\beta(-1)^{2k\beta}$$

is transcendental.

APPENDIX

For the record,

$$e^{\operatorname{Log} z} = z$$

but

$$\operatorname{Log} e^z \equiv z \pmod{2\pi\sqrt{-1}}.$$

EXAMPLE Consider α^β -- then $\exists\, k \in \mathbb{Z}$:

$$\begin{aligned}\operatorname{Log} \alpha^{\beta} &= \operatorname{Log} e^{\beta \operatorname{Log} \alpha} \\ &= \beta \operatorname{Log} \alpha + 2\pi \sqrt{-1}\, k\end{aligned}$$

and

$$\begin{aligned}e^{\beta \operatorname{Log} \alpha + 2\pi \sqrt{-1}\, k} &= e^{\beta \operatorname{Log} \alpha}\, e^{2\pi \sqrt{-1}\, k} \\ &= \alpha^{\beta} \cdot 1 = \alpha^{\beta}.\end{aligned}$$

§32. *EQUIVALENCES*

In this §, we shall formulate various statements that are equivalent to inhomogeneous Baker or homogeneous Baker.

<u>1:</u> THEOREM The following assertions are equivalent.

(i) If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and Q-linearly independent, then $1, \lambda_1, \ldots, \lambda_n$ are $\bar{Q}$-linearly independent (inhomogeneous Baker).

(ii) If $\lambda_1 \in L, \ldots, \lambda_{n-1} \in L$ are nonzero and Q-linearly independent and if $\beta_0, \beta_1, \ldots, \beta_{n-1}$ are algebraic numbers such that

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1}$$

is an element of L, then $\beta_0 = 0$ and $\beta_1, \ldots, \beta_{n-1}$ are rational.

(iii) If $\lambda_1 \in L, \ldots, \lambda_{n-1} \in L$ are nonzero and Q-linearly independent and if $\beta_0, \beta_1, \ldots, \beta_{n-1}$ are algebraic numbers such that

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1}$$

is an element of L, then $\beta_0 = 0$ and $\beta_1, \ldots, \beta_{n-1}$ are Q-linearly dependent.

The proof proceeds according to the scheme:

(ii) => (iii), (i) => (ii), (iii) => (i).

(ii) => (iii): Obvious.

(i) => (ii): Fix the data per the assumption:

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1} \in L.$$

Then there exists $\lambda_n \in L$:

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1} - \lambda_n = 0.$$

Therefore $1, \lambda_1, \ldots, \lambda_n$ are $\bar{Q}$-linearly dependent. But $\lambda_1, \ldots, \lambda_{n-1}$ are Q-linearly independent, so by (i), there are rational numbers $q_1, \ldots, q_{n-1}$ not all zero such that

$$\lambda_n = q_1\lambda_1 + \cdots + q_{n-1}\lambda_{n-1},$$

hence

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1} - (q_1\lambda_1 + \cdots + q_{n-1}\lambda_{n-1}) = 0$$

or still,

$$\beta_0 + (\beta_1 - q_1)\lambda_1 + \cdots + (\beta_{n-1} - q_{n-1})\lambda_{n-1} = 0.$$

Finally, appealing to (i) once again, it follows that $\beta_0 = 0$ and $\beta_i = q_i$ $(1 \leq i \leq n-1)$, thus $\beta_1, \ldots, \beta_{n-1}$ are rational.

(iii) => (i): Denote by $\mathcal{P}(L)$ the set of finite nonempty subsets S of L subject to:

1. The elements of S are Q-linearly independent.
2. The elements of $S \cup \{1\}$ are $\bar{Q}$-linearly dependent.

Then the claim is that $\mathcal{P}(L) = \emptyset$, which will do it. Suppose instead that $\mathcal{P}(L) \neq \emptyset$ -- then

$$n \equiv \inf\{\text{card } S : S \in \mathcal{P}(L)\}$$

is ≥ 1. Fix an element $S = \{\lambda_1, \ldots, \lambda_n\} \in \mathcal{P}(L)$ at which the inf is attained -- then the λ_i $(1 \leq i \leq n)$ are Q-linearly independent and by definition of $\mathcal{P}(L)$ there exist algebraic numbers $\beta_0, \beta_1, \ldots, \beta_n$ with $\beta_1, \ldots, \beta_n$ not all zero:

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n = 0.$$

Assume now without loss of generality that $\beta_n \neq 0$, so

$$\frac{\beta_0}{-\beta_n} + \frac{\beta_1}{-\beta_n}\lambda_1 + \cdots + \frac{\beta_n}{-\beta_n}\lambda_n = 0.$$

Adjusting the notation, one can suppose from the beginning that $\beta_n = -1$ and work with

$$\beta_0 + \beta_1\lambda_1 + \cdots + (-1)\lambda_n = 0,$$

hence

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{n-1}\lambda_{n-1} = \lambda_n \in L.$$

Therefore $\beta_0 = 0$ and $\beta_1,\ldots,\beta_{n-1}$ are Q-linearly dependent (cf. (iii)), thus there exist rational numbers $q_1,\ldots,q_{n-1}$ not all zero such that

$$q_1\beta_1 + \cdots + q_{n-1}\beta_{n-1} = 0.$$

Choose

$$q_k \in \{q_1,\ldots,q_{n-1}\} : q_k \neq 0$$

$\Rightarrow$

$$\beta_k = \sum_{i\neq k} \left(-\frac{q_i}{q_k}\right)\beta_i$$

implying thereby that not all the β_i $(i \neq k)$ are zero. Meanwhile, since $\beta_0 = 0$,

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n = 0 \quad (\beta_n = -1)$$

$\Rightarrow$

$$0 = \sum_{i\neq k} \lambda_i\beta_i + \lambda_k\beta_k$$

$$= \sum_{i \neq k} \lambda_i \beta_i - \lambda_k \sum_{i \neq k} \frac{q_i}{q_k} \beta_i$$

$$= \sum_{i \neq k} (\lambda_i - \lambda_k \frac{q_i}{q_k}) \beta_i.$$

Put

$$\gamma_i = \lambda_i - \lambda_k \frac{q_i}{q_k} \quad (i \neq k).$$

Then the $\gamma_i \in L$ $(i \neq k)$ are Q-linearly independent (see infra) and

$$\sum_{i \neq k} \gamma_i \beta_i = 0.$$

Because the β_i $(i \neq k)$ are not all zero, we have reached a contradiction to the minimality of n.

[Note: To check that the γ_i $(i \neq k)$ are Q-linearly independent, consider a dependence relation

$$\sum_{i \neq k} C_i \gamma_i = 0 \quad (C_i \in Q).$$

Then

$$\sum_{i \neq k} C_i (\lambda_i - \lambda_k \frac{q_i}{q_k}) = 0$$

=>

$$\sum_{i \neq k} C_i \lambda_i - \sum_{i \neq k} \lambda_k \frac{q_i}{q_k} = 0$$

=>

$$\sum_{i \neq k} C_i \lambda_i - C\lambda_k = 0,$$

where

$$C = \sum_{i \neq k} \frac{q_i}{q_k} \in Q.$$

But the λ_i $(1 \leq i \leq n)$ are $\mathbb{Q}$-linearly independent (by hypothesis), so $C_i = 0$ $(i \neq k)$ (and $C = 0$).]

2: N.B. The proof that we shall give of Baker in §33 does not go thru items (ii) or (iii).

3: THEOREM The following assertions are equivalent.

(i) If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and $\mathbb{Q}$-linearly independent, then $\lambda_1, \ldots, \lambda_n$ are $\bar{\mathbb{Q}}$-linearly independent (homogeneous Baker).

(ii) If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and if $\beta_1, \ldots, \beta_n$ are $\mathbb{Q}$-linearly independent elements of $\bar{\mathbb{Q}}$, then

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n \neq 0.$$

(iii) If $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and $\mathbb{Q}$-linearly independent and if $\beta_1, \ldots, \beta_n$ are $\mathbb{Q}$-linearly independent elements of $\bar{\mathbb{Q}}$, then

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n \neq 0.$$

The proof proceeds according to the scheme:

(i) => (iii), (ii) => (i), (iii) => (ii).

(i) => (iii): (cf. §31, #10).

(ii) => (i): To derive a contradiction, assume given $\mathbb{Q}$-linearly independent nonzero $\lambda_1 \in L, \ldots, \lambda_n \in L$ and a dependence relation

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n = 0.$$

Observe that since (ii) is in force, $\beta_1, \ldots, \beta_n$ are not $\mathbb{Q}$-linearly independent, so let $\gamma_1,\ldots,\gamma_m$ $(m < n)$ be a basis for the Q-span of $\{\beta_1,\ldots,\beta_n\}$, thus

$$\beta_i = \sum_{j=1}^{m} c_{ij}\gamma_j \qquad (1 \leq i \leq n).$$

Here the $c_{ij} \in Q$ and $\forall\ i, \exists\ j : c_{ij} \neq 0$. Next

$$0 = \beta_1\lambda_1 + \cdots + \beta_n\lambda_n$$

$$= (\sum_{j=1}^{m} c_{1j}\gamma_j)\lambda_1 + \cdots + (\sum_{j=1}^{m} c_{nj}\gamma_j)\lambda_n$$

$$= \sum_{j=1}^{m} \gamma_j(\sum_{i=1}^{n} c_{ij}\lambda_i).$$

On the other hand, a rational linear combination of the λ_i remains in L (cf. #2); thus in view of (ii),

$$\sum_{j=1}^{m} \gamma_j(\sum_{i=1}^{n} c_{ij}\lambda_i) \neq 0$$

provided

$$\sum_{i=1}^{n} c_{i1}\lambda_i, \ldots, \sum_{i=1}^{n} c_{im}\lambda_i$$

are nonzero (granted this, we have our contradiction). But $\lambda_1 \in L, \ldots, \lambda_n \in L$ are nonzero and Q-linearly independent. Therefore

$$\left[\begin{array}{l} \sum_{i=1}^{n} c_{i1}\lambda_i = 0 \Rightarrow c_{i1} = 0 \ (i = 1,\ldots,n) \\ \vdots \\ \sum_{i=1}^{n} c_{im}\lambda_i = 0 \Rightarrow c_{im} = 0 \ (i = 1,\ldots,n). \end{array}\right.$$

And this implies that $\beta_1 = 0,\ldots,\beta_n = 0$, a non sequitur.

(iii) => (ii): If

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n = 0,$$

where $\beta_1,\ldots,\beta_n$ are Q-linearly independent elements of $\bar{\bar{Q}}$, then it will be shown that

$$\lambda_1 = 0,\ldots,\lambda_n = 0,$$

from which the result. Renumbering the data if necessary, assume that $\lambda_1,\ldots,\lambda_m$ $(0 \leq m \leq n)$ is a basis for the Q-span of $\{\lambda_1,\ldots,\lambda_n\}$:

$$\lambda_i = \sum_{j=1}^{m} c_{ij}\lambda_j \quad (m + 1 \leq i \leq n),$$

where the $c_{ij} \in Q$. Then

$$0 = \sum_{j=1}^{m} \gamma_j\lambda_j \quad (\gamma_j = \beta_j + \sum_{i=m+1}^{n} c_{ij}\beta_i).$$

Now apply (iii) (with n replaced by m): $\lambda_1,\ldots,\lambda_m$ are Q-linearly independent, hence $\gamma_1,\ldots,\gamma_m$ are Q-linearly dependent. However $\beta_1,\ldots,\beta_n$ are Q-linearly independent, so the only possibility is $m = 0$, implying that

$$\lambda_1 = 0,\ldots,\lambda_n = 0.$$

[Note: If $C_j \in Q$ $(1 \leq j \leq m)$, then

$$\sum_{j=1}^{m} C_j\gamma_j = \sum_{j=1}^{m} C_j(\beta_j + \sum_{i=m+1}^{n} c_{ij}\beta_i)$$

$$= \sum_{j=1}^{m} C_j\beta_j + \sum_{i=m+1}^{n} (\sum_{j=1}^{m} c_{ij}C_j)\beta_i.]$$

4: REMARK One can add a fourth condition, viz.

(iv) If $\lambda_1,\ldots,\lambda_{n+1}$ are nonzero elements of L such that $\lambda_1,\ldots,\lambda_n$ are $\bar{Q}$-linearly independent and if $\beta_1,\ldots,\beta_n$ are elements of $\bar{Q}$ such that

$$\beta_1\lambda_1 + \cdots + \beta_n\lambda_n = \lambda_{n+1},$$

then $\beta_1,\ldots,\beta_n$ are rational.

[Note: Suppose that homogeneous Baker is in force. Consider item (ii) of #1 -- then the crux is to prove that $\beta_0 = 0$.]

5: N.B. Consider the arrow of inclusion:

$$L \rightarrow C.$$

Then it lifts to an arrow

$$L \otimes_Q \bar{Q} \rightarrow C$$

which remains injective iff item (iv) supra is in force.

6: LEMMA Baker's inhomogeneous theorem is equivalent to the conjunction of §31, #11 and §31, #16.

7: LEMMA Baker's homogeneous theorem is equivalent to §31, #11.

8: N.B.

§31, #11 <=> §31, #14.

§33. BAKER: PROOF

Our objective is to establish that if $\lambda_1 \in L,\ldots,\lambda_n \in L$ are nonzero and Q-linearly independent, then $1,\lambda_1,\ldots,\lambda_n$ are $\bar{Q}$-linearly independent (cf. §31, #8). I.e.: If $\gamma_0,\gamma_1,\ldots,\gamma_n$ are algebraic numbers and if

$$\gamma_0 + \gamma_1\lambda_1 + \cdots + \gamma_n\lambda_n = 0,$$

then

$$\gamma_0 = 0,\ \gamma_1 = 0,\ldots,\ \gamma_n = 0.$$

1: THEOREM Let K be an algebraic number field of degree d over Q, let $\{\beta_1,\ldots,\beta_d\}$ be a basis of the Q-vector space K, and let $\lambda_1,\ldots,\lambda_d$ be elements of L. Assume:

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d \in \bar{Q}.$$

Then

$$\lambda_1 = 0,\ldots,\lambda_d = 0.$$

2: REMARK Granted Baker's theorem (in its inhomogeneous version), it follows that #11 of §31 is in force. So, if

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d$$

is nonzero, then

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d$$

must be transcendental. On the other hand, under the assumption that it is algebraic, it must be zero:

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d = 0.$$

Still, this does not imply that

$$\lambda_1 = 0, \ldots, \lambda_d = 0.$$

The foregoing result can be used to give a quick proof of Baker's inhomogeneous theorem. So suppose that

$$\gamma_0 + \gamma_1\lambda_1 + \cdots + \gamma_n\lambda_n = 0.$$

Put $K = Q(\gamma_1, \ldots, \gamma_n)$, choose a basis $\{\beta_1, \ldots, \beta_d\}$ for the Q-vector space K, and write

$$\gamma_j = \sum_{i=1}^{d} c_{ji}\beta_i \quad (1 \leq j \leq n)$$

with $c_{ji} \in Q$ -- then

$$\begin{aligned} -\gamma_0 (\in \bar{Q}) & \\ &= \sum_{j=1}^{n} \gamma_j\lambda_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{d} c_{ji}\beta_i\right)\lambda_j \\ &= \sum_{i=1}^{d} \beta_i \sum_{j=1}^{n} c_{ji}\lambda_j \\ &= \sum_{i=1}^{d} \beta_i\lambda_i' , \end{aligned}$$

where

$$\lambda_i' = \sum_{j=1}^{n} c_{ji}\lambda_j \in L.$$

Owing to #1,

$$\lambda_1' = 0, \ldots, \lambda_d' = 0.$$

But $\lambda_1, \ldots, \lambda_n$ are nonzero and $\mathbb{Q}$-linearly independent, thus the relations

$$\sum_{j=1}^{n} c_{ji} \lambda_j = 0$$

imply that

$$c_{ji} = 0 \quad (1 \leq i \leq d,\ 1 \leq j \leq n),$$

hence

$$\gamma_1 = 0, \ldots, \gamma_n = 0$$

$$\Rightarrow \gamma_0 = 0.$$

<u>2:</u> RAPPEL Let K be an algebraic number field -- then the <u>trace</u> $K \to \mathbb{Q}$ is the $\mathbb{Q}$-linear map

$$\gamma \to \sum_{\sigma} \gamma^{\sigma},$$

where σ runs over the set of complex embeddings of K (a set of cardinality $[K:\mathbb{Q}]$) and γ^{σ} is the image of γ under σ.

<u>3:</u> NOTATION Let K be an algebraic number field, let $\{\beta_1, \ldots, \beta_d\}$ be a basis for the $\mathbb{Q}$-vector space K, and let $\sigma_1 : K \to \mathbb{C}, \ldots, \sigma_d : K \to \mathbb{C}$ be the complex embeddings of K (label matters so that σ_1 is the arrow $K \to \mathbb{C}$ of inclusion).

<u>4:</u> LEMMA

$$\det(\mathrm{tr}(\beta_i \beta_j))_{1 \leq i, j \leq d} = (\det B)^2,$$

where

$$B = (\beta_k^{\sigma_i})_{1 \leq i,k \leq d}$$

is nonsingular.

We shall now take up the proof of #1.

5: NOTATION Put

$$\Lambda_i = \sum_{k=1}^{d} \beta_k^{\sigma_i} \lambda_k \quad (1 \leq i \leq d).$$

Case 1: At least one but not all of the Λ_i vanish.

[Arrange the notation so that

$$\Lambda_1 \neq 0, \ldots, \Lambda_n \neq 0, \ \Lambda_{n+1} = 0, \ldots, \Lambda_d = 0.$$

- Define $\underline{x}_i \in \bar{\mathbb{Q}}^n$ by

$$\underline{x}_i = (\beta_i^{\sigma_1}, \ldots, \beta_i^{\sigma_n}) \quad (1 \leq i \leq d).$$

If $q_1, \ldots, q_d$ are rational numbers such that

$$q_1\underline{x}_1 + \cdots + q_d\underline{x}_d = 0,$$

then

$$0 = \sum_{i=1}^{d} q_i\beta_i^{\sigma_1} = \sum_{i=1}^{d} q_i\beta_i$$

=>

$$q_1 = 0, \ldots, q_d = 0.$$

Therefore $\underline{x}_1, \ldots, \underline{x}_d$ are $\mathbb{Q}$-linearly independent elements of $\bar{\mathbb{Q}}^n$.

- Define $\underline{y}_j \in C^n$ by

$$\underline{y}_j = (\beta_j^{\sigma_1}\Lambda_1,\ldots,\beta_j^{\sigma_n}\Lambda_n) \quad (1 \le j \le d).$$

Since the matrix

$$B = (\beta_k^{\sigma_i})_{1 \le i,\, k \le d}$$

has rank d, the $d \times n$ matrix

$$B_n = (\beta_k^{\sigma_i})_{1 \le k \le d,\ 1 \le i \le n}$$

has rank n (its n columns are independent in K^d). The product of B_n by the $n \times n$ diagonal matrix

$$\mathrm{diag}(\Lambda_1,\ldots,\Lambda_n)$$

is the $d \times n$ matrix whose row vectors are $\underline{y}_1,\ldots,\underline{y}_d$:

$$\begin{bmatrix} \beta_1^{\sigma_1}\Lambda_1 & \cdots & \beta_1^{\sigma_n}\Lambda_n \\ \vdots & & \vdots \\ \beta_d^{\sigma_1}\Lambda_1 & \cdots & \beta_d^{\sigma_n}\Lambda_n \end{bmatrix}$$

$$= \begin{bmatrix} \beta_1^{\sigma_1} & \cdots & \beta_1^{\sigma_n} \\ \vdots & & \vdots \\ \beta_d^{\sigma_1} & \cdots & \beta_d^{\sigma_n} \end{bmatrix} \times \begin{bmatrix} \Lambda_1 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & \Lambda_n \end{bmatrix}.$$

Therefore the set $\{\underline{y}_1,\ldots,\underline{y}_d\}$ contains a basis for C^n over C.]

The preceding considerations set the stage for an application of §30, #10, hence at least one of the

$$\underline{x}_i\underline{y}_j \quad (1 \leq i \leq d,\ 1 \leq j \leq n)$$

does not belong to L, which, however is false. To see this, recall that

$$\Lambda_{n+1} = 0, \ldots, \Lambda_d = 0,$$

and write

$$\underline{x}_i\underline{y}_j = \sum_{m=1}^{n} \beta_i^{\sigma_m}\beta_j^{\sigma_m}\Lambda_m$$

$$= \sum_{m=1}^{d} \beta_i^{\sigma_m}\beta_j^{\sigma_m}\Lambda_m$$

$$= \sum_{m=1}^{d} \beta_i^{\sigma_m}\beta_j^{\sigma_m} \sum_{k=1}^{d} \beta_k^{\sigma_m}\lambda_k$$

$$= \sum_{k=1}^{d} c_{ijk}\lambda_k,$$

where

$$c_{ijk} = \sum_{m=1}^{d} \beta_i^{\sigma_m}\beta_j^{\sigma_m}\beta_k^{\sigma_m}$$

$$= \mathrm{tr}(\beta_i\beta_j\beta_k) \in \mathbf{Q}.$$

But L is a $\mathbf{Q}$-vector space (cf. §31, #2). Consequently

$$\underline{x}_i\underline{y}_j \in L,$$

a contradiction.

<u>Case 2:</u> None of the Λ_i vanish.

[To begin with,

$$\Lambda_1 = \sum_{k=1}^{d} \beta_k^{\sigma_1}\lambda_k = \sum_{k=1}^{d} \beta_k\lambda_k \in \bar{Q}$$

by hypothesis.

- Define $\underline{x}_k \in C^d$ by

$$\underline{x}_k = (\beta_k^{\sigma_1},\ldots,\beta_k^{\sigma_d}) \quad (1 \le k \le d).$$

Since the matrix

$$B = (\beta_k^{\sigma_i}) \; 1 \le i,\, k \le d$$

is nonsingular, $\underline{x}_1,\ldots,\underline{x}_d$ are Q-linearly independent elements of $\bar{Q}^d$.

- Define $\underline{y}_j \in C^d$ by

$$\underline{y}_j = (\beta_j^{\sigma_1}\Lambda_1,\ldots,\beta_j^{\sigma_d}\Lambda_d) \quad (1 \le j \le d).$$

Since B has rank d and since

$$\begin{bmatrix} \beta_1^{\sigma_1}\Lambda_1 & \cdots & \beta_1^{\sigma_d}\Lambda_d \\ \vdots & & \vdots \\ \beta_d^{\sigma_1}\Lambda_1 & \cdots & \beta_d^{\sigma_d}\Lambda_d \end{bmatrix}$$

$$= \begin{bmatrix} \beta_1^{\sigma_1} & \cdots & \beta_1^{\sigma_d} \\ \vdots & & \vdots \\ \beta_d^{\sigma_1} & \cdots & \beta_d^{\sigma_d} \end{bmatrix} \times \begin{bmatrix} \Lambda_1 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & \Lambda_d \end{bmatrix},$$

it follows that $\underline{y}_1,\ldots,\underline{y}_d$ is a basis for C^d over C. In addition,

$$y_{1j} = \beta_j^{\sigma_1}\Lambda_1 = \beta_j\Lambda_1 \in \bar{Q}.]$$

Therefore the assumptions of §30, #12 are satisfied, hence at least one of the

$$\underline{x}_i\underline{y}_j \quad (1 \leq i \leq d,\ 1 \leq j \leq d)$$

does not belong to L. On the other hand,

$$\underline{x}_i\underline{y}_j = \sum_{k=1}^{d} \mathrm{tr}(\beta_i\beta_j\beta_k)\lambda_k \in L$$

and we again have a contradiction.

Case 3: All of the Λ_i vanish. Consider the system:

$$\begin{array}{l} \Lambda_1 : \beta_1^{\sigma_1}\lambda_1 + \cdots + \beta_d^{\sigma_1}\lambda_d = 0 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ \Lambda_d : \beta_1^{\sigma_d}\lambda_1 + \cdots + \beta_d^{\sigma_d}\lambda_d = 0. \end{array}$$

Its matrix is the transpose of B, thus is nonsingular, thus

$$\lambda_1 = 0,\ldots,\lambda_d = 0,$$

as desired.

§34. ESTIMATES

Given algebraic numbers $\alpha_1 \neq 0,1,\ldots,$ $\alpha_n \neq 0,1$ and nonzero integers $b_1,\ldots,$ b_n, put

$$\Lambda = b_1 \operatorname{Log} \alpha_1 + \cdots + b_n \operatorname{Log} \alpha_n.$$

Then for the applications, it is important to estimate $|\Lambda|$ from below.

1: NOTATION Put

$$B = \max \{2, |b_1|, \ldots, |b_n|\}.$$

2: THEOREM Assume: $\Lambda \neq 0$ -- then

$$|\Lambda| \geq B^{-C},$$

where $C > 0$ is a constant depending only on n and $\alpha_1,\ldots,\alpha_n$.

3: REMARK The reason for introducing the "2" is to accommodate the case when all the b_i are $\pm$ 1 since then

$$\max\{|b_1|,\ldots,|b_n|\} = 1 \text{ and } 1^C = 1.$$

4: EXAMPLE Suppose that $\frac{p}{q}$ is a nonzero rational number with $q \geq 2$. Let $\alpha > 0$ $(\alpha \neq 1)$, $\alpha' > 0$ $(\alpha' \neq 1)$ be algebraic numbers -- then

$$|p\ell n(\alpha) - q\ell n(\alpha')| \geq \frac{1}{\max\{|p|,q\}^C} \quad (\text{cf. §15, \#33}),$$

where $c > 0$ depends only on $\ell n(\alpha)$ and $\ell n(\alpha')$.

[Note: In the context of §15, #32, it is automatic that $\alpha' \neq 1$. For if

$\alpha^x = \alpha' = 1$, then

$$\ell n(\alpha^x) = \ell n(1) \Rightarrow x\ell n(\alpha) = 0 \Rightarrow \ell n(\alpha) = 0 \Rightarrow \alpha = 1,$$

which was ruled out at the beginning.]

Obviously

$$e^{\Lambda} = \exp(b_1 \operatorname{Log} \alpha_1 + \cdots + b_n \operatorname{Log} \alpha_n)$$

$$= \alpha_1^{b_1} \cdots \alpha_n^{b_n}.$$

5: THEOREM Assume

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1.$$

Then

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq B^{-C},$$

where $C > 0$ is a constant depending only on n and $\alpha_1, \ldots, \alpha_n$.

Some elementary preliminaries are needed in order to make the transition from #2 to #5.

[Note: The "C" in #5 is not the "C" in #2.]

6: RAPPEL

$$\operatorname{Log} z = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (z-1)^n \quad (|z-1| < 1) \quad (\text{cf. §23, #7}).$$

Put $z = 1 + w$, hence

$$\operatorname{Log}(1 + w) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} w^n \quad (|w| < 1).$$

7: LEMMA

$$|w| \leq \frac{1}{2} \Rightarrow |\text{Log}(1 + w)| \leq 2|w|.$$

Passing to the proof of #5, put $w = \alpha_1^{b_1} \cdots \alpha_n^{b_n}$ -- then there are two possibilities.

- $|w| > \frac{1}{2}$. By definition,

$$B = \max\{2, |b_1|, \ldots, |b_n|\}$$

$$\Rightarrow \quad B \geq 2 \Rightarrow \frac{1}{B} \leq \frac{1}{2} \Rightarrow \frac{1}{B} < |w|,$$

so $C = 1$ will work.

- $|w| \leq \frac{1}{2}$. To begin with, for some $k \in Z$,

$$\begin{aligned} \text{Log}(1 + w) &= \text{Log}(\alpha_1^{b_1} \cdots \alpha_n^{b_n}) \\ &= \text{Log } \alpha_1^{b_1} + \cdots + \text{Log } \alpha_n^{b_n} + 2\pi\sqrt{-1}\,k \quad (\text{cf. §23, \#5}) \\ &= b_1 \text{ Log } \alpha_1 + \cdots + b_n \text{ Log } \alpha_n + 2\pi\sqrt{-1}\,k. \end{aligned}$$

But

$$\begin{aligned} \text{Log } {-1} &= \ln(|-1|) + \pi\sqrt{-1} \\ &= \pi\sqrt{-1}. \end{aligned}$$

Therefore

$$\text{Log}(1 + w) = b_1 \text{ Log } \alpha_1 + \cdots + b_n \text{ Log } \alpha_n + 2k \text{ Log } {-1}.$$

The right hand side has the form needed for an application of #2 (ignore $2k$ Log -1 if $k = 0$), thus setting

$$B_0 = \max\{2, |b_1|, \ldots, |b_n|, |2k|\},$$

it follows that

$$|\mathrm{Log}(1 + w)| \geq B_0^{-C_0}$$

for some $C_0 > 0$. Now estimate $|2\pi \sqrt{-1}\, k|$:

$$
\begin{aligned}
|2\pi \sqrt{-1}\, k| &\leq |\mathrm{Log}(1 + w)| + \sum_{i=1}^{n} |b_i|\, |\mathrm{Log}\, \alpha_i| \\
&\leq 2|w| + \sum_{i=1}^{n} |b_i|\, |\mathrm{Log}\, \alpha_i| \\
&\leq 1 + B \sum_{i=1}^{n} |\mathrm{Log}\, \alpha_i| \\
&\leq B(1 + \sum_{i=1}^{n} |\mathrm{Log}\, \alpha_i|)
\end{aligned}
$$

=>

$$
\begin{aligned}
|2k| &\leq B(1 + \sum_{i=1}^{n} |\mathrm{Log}\, \alpha_i|)/\pi \\
&\leq B(1 + \sum_{i=1}^{n} |\mathrm{Log}\, \alpha_i|) \\
&\equiv C_1 B \,(C_1 > 1)
\end{aligned}
$$

=>

$$
\begin{aligned}
B_0 &= \max\{B, |2k|\} \\
&\leq \max\{B, C_1 B\} = C_1 B
\end{aligned}
$$

=>

$$
\begin{aligned}
2|w| &\geq |\mathrm{Log}(1 + w)| \\
&\geq B_0^{-C_0} > (C_1 B)^{-C_0}
\end{aligned}
$$

=>

$$|w| \geq \frac{1}{2} (C_1B)^{-C_0}.$$

Write

$$2(C_1B)^{C_0} = 2(C_1)^{C_0}B^{C_0}.$$

Choose D:

$$2(C_1)^{C_0} \leq B^D.$$

Then

$$2(C_1)^{C_0}B^{C_0} \leq B^DB^{C_0} = B^{D+C_0}.$$

Let $C = C + C_0$ to conclude that

$$\frac{1}{2} (C_1B)^{-C_0} \geq B^{-C},$$

so

$$|w| \geq B^{-C}$$

thereby completing the proof of #5.

Under certain circumstances, one can go beyond #5.

8: THEOREM Let

$$\left[\begin{array}{l} a_1,\ldots,a_n \\ b_1,\ldots,b_n \end{array}\right.$$

be nonzero integers. Assume:

$$a_1 \geq 2,\ldots,a_n \geq 2$$

and

$$a_1^{b_1} \cdots a_n^{b_n} \neq 1.$$

Then

$$|a_1^{b_1} \cdots a_n^{b_n} - 1| \geq \exp(-C(n)\ln(B)\ln(a_1) \cdots \ln(a_n)),$$

where $C(n) > 0$ is a constant depending only on n.

9: REMARK According to Waldschmidt, an admissible value for $C(n)$ is

$$2^{26n} n^{3n}.$$

FACT If $|b_1| \geq 2$, $|b_2| \geq 2$, then

$$|b_1\ln(2) + b_2\ln(3)| \geq B^{-13.3}.$$

APPENDIX

DEFINITION Complex numbers $\alpha_1,\ldots,\alpha_n$ are <u>multiplicatively independent</u> if none are zero and if for any relation

$$\alpha_1^{a_1} \cdots \alpha_n^{a_n} = 1,$$

where $(a_1,\ldots,a_n) \in \mathbb{Z}^n$, there follows

$$a_1 = 0,\ldots,a_n = 0.$$

LEMMA Suppose that $\alpha_1,\ldots,\alpha_n$ are multiplicatively independent -- then for any choice $(\lambda_1,\ldots,\lambda_n) \in \mathbb{C}^n$ with $e^{\lambda_i} = \alpha_i$ $(1 \leq i \leq n)$, the $n + 1$ complex numbers

$2\pi\sqrt{-1}$, $\lambda_1,\ldots,\lambda_n$ are $\mathbb{Q}$-linearly independent.

Suppose given algebraic numbers $\alpha_1 \neq 0,1,\ldots,\alpha_n \neq 0,1$ and assume that they are multiplicatively independent, hence that

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} \neq 1$$

if the exponents are not all zero.

Turning to #2, it can be shown that if

$$|\Lambda| < B^{-C}$$

for a sufficiently large positive constant C depending only on n and $\alpha_1,\ldots,\alpha_n$, then $\alpha_1,\ldots,\alpha_n$ must be multiplicatively dependent... .

§35. *MATRICES*

Let A be an $m \times n$ matrix with entries in the complex numbers (m rows and n columns).

1: DEFINITION The column space of A is the vector space spanned by its columns and the column rank of A is the dimension of the column space of A.

2: DEFINITION The row space of A is the vector space spanned by its rows and the row rank of A is the dimension of the row space of A.

3: THEOREM The column rank of A equals the row rank of A.

Therefore the number of linearly independent columns of A equals the number of linearly rows of A, their common value being the rank of A: rank A.

[Note: Only a zero matrix has rank 0.]

4: EXAMPLE

$$\text{rank} \begin{bmatrix} 1 & 0 & 1 \\ -2 & -3 & 1 \\ 3 & 3 & 0 \end{bmatrix} = 2.$$

[The first two rows are linearly independent, so the rank is at least 2 but the three rows in total are linearly dependent (the third is equal to the second subtracted from the first), thus the rank is less than 3.]

5: N.B. Denote by A^T the transpose of A -- then

$$\text{rank } A = \text{rank } A^T.$$

6: EXAMPLE

$$\operatorname{rank}\begin{bmatrix} 1 & 1 & 0 & 2 \\ -1 & -1 & 0 & -2 \end{bmatrix} = 1.$$

In fact, there are nonzero columns so the rank is positive. On the other hand

$$\operatorname{rank}\begin{bmatrix} 1 & -1 \\ 1 & -1 \\ 0 & 0 \\ 2 & -2 \end{bmatrix} = 1.$$

7: LEMMA The rank of A is the smallest integer k such that A can be factored as a product $A = BC$, where B is a $m \times k$ matrix and C is a $k \times n$ matrix.

8: LEMMA The rank of A is the largest integer r for which there exists a nonsingular $r \times r$ submatrix of A.

[Note: A nonsingular r-minor is a $r \times r$ submatrix with nonzero determinant.]

9: LEMMA The rank of A is the smallest integer k such that A can be written as a sum of k rank 1 matrices.

[Note: A matrix has rank 1 if it can be written as a nonzero product CR of a column vector C and a row vector R:

$$C = \begin{bmatrix} c_1 \\ \cdot \\ \cdot \\ \cdot \\ c_m \end{bmatrix}, \ R = [r_1 \cdots r_n]$$

=>

$$CR = \begin{bmatrix} c_1r_1 & \cdots & c_1r_n \\ \vdots & & \\ c_mr_1 & \cdots & c_mr_n \end{bmatrix}.]$$

<u>10:</u> Take A as in #6 — then

$$A = \begin{bmatrix} 1 \\ -1 \end{bmatrix} [1\ 1\ 0\ 2]$$

is rank 1.

<u>11:</u> LEMMA The rank of A is $\leq \min\{m,n\}$.

<u>12:</u> DEFINITION If

$$\text{rank } A = \min\{m,n\},$$

then A is said to have <u>full rank</u>; otherwise A is <u>rank deficient</u>.

<u>13:</u> LEMMA If A is a square matrix (i.e., if $m = n$), then A is invertible iff A has rank n, thus is full rank.

<u>14:</u> LEMMA If B is a $n \times k$ matrix, then

$$\text{rank } AB \leq \min\{\text{rank } A, \text{ rank } B\}$$

and if rank B = n, then

$$\text{rank } AB = \text{rank } A.$$

<u>15:</u> LEMMA The rank of A is equal to r iff there exists an invertible

$m \times m$ matrix X and an invertible $n \times n$ matrix Y such that

$$XAY = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix},$$

where I_r is the $r \times r$ identity matrix.

<u>16:</u> NOTATION $\bar{A}$ is the complex conjugate of A and A^* is the conjugate transpose of A.

<u>17:</u> LEMMA

$$\text{rank } A = \text{rank } \bar{A} = \text{rank } A^*$$

$$= \text{rank } A^*A = \text{rank } AA^*.$$

Attached to A is the linear map

$$f_A : \mathbb{C}^n \to \mathbb{C}^m$$

defined by

$$f_A(x) = Ax.$$

<u>18:</u> LEMMA The rank of A equals the dimension of the image of f_A.

<u>19:</u> LEMMA

- f_A is injective iff rank $A = n$.
- f_A is surjective iff rank $A = m$.

§36. *SIX EXPONENTIALS THEOREM*

This is the following statement.

<u>1:</u> THEOREM Suppose given $\mathbb{Q}$-linearly independent complex numbers

$$\{x_1,\ldots,x_m\} \text{ and } \{y_1,\ldots,y_n\}.$$

Assume:

$$mn > m + n.$$

Then at least one of the numbers

$$\exp(x_i y_j) \quad (1 \leq i \leq m, \ 1 \leq j \leq n)$$

is transcendental.

[As regards the proof, one can extend the ideas used in the proof of Gelfond-Schneider but we shall omit the details opting instead for a "geometric argument" later on (cf. §41, #1).]

Special Cases: $m = 3$, $n = 2$ or $m = 2$, $n = 3$.

<u>2:</u> EXAMPLE Take

$$x_1 = 1,\ x_2 = e,\ y_1 = e,\ y_2 = e^2,\ y_3 = e^3,$$

where §17, #2 has been silently invoked -- then the six exponentials are

$$e^e,\ e^{e^2},\ e^{e^3},\ e^{e^2},\ e^{e^3},\ e^{e^4},$$

thus at least one of the numbers

$$e^e,\ e^{e^2},\ e^{e^3},\ e^{e^4}$$

is transcendental.

3: EXAMPLE Take

$$x_1 = 1,\ x_2 = \pi,\ y_1 = \ln(2),\ y_2 = \pi\ln(2),\ y_3 = \pi^2\ln(2).$$

Then the six exponentials are

$$2,\ 2^{\pi},\ 2^{\pi^2},\ 2^{\pi},\ 2^{\pi^2},\ 2^{\pi^3},$$

thus at least one of the numbers

$$2^{\pi},\ 2^{\pi^2},\ 2^{\pi^3}$$

is transcendental.

[Note: Consider a dependence relation

$$q_1\ln(2) + q_2\pi\ln(2) + q_3\pi^2\ln(2) = 0,$$

where $q_1, q_2, q_3 \in \mathbb{Q}$ — then

$$q_1 + q_2\pi + q_3\pi^2 = 0$$

$$\Rightarrow$$

$$q_1 = 0,\ q_2 = 0,\ q_3 = 0,$$

π being transcendental (cf. §19, #1).]

4: REMARK It is unknown whether one of the numbers

$$2^{\pi},\ 2^{\pi^2}$$

is transcendental.

5: EXAMPLE Fix $t \in \mathbb{R}$, $t \notin \mathbb{Q}$. Take

$$x_1 = 1,\ x_2 = t,\ y_1 = \ln(2),\ y_2 = \ln(3),\ y_3 = \ln(5).$$

Then the six exponentials are

$$2,\ 3,\ 5,\ 2^t,\ 3^t,\ 5^t,$$

thus at least one of the numbers

$$2^t,\ 3^t,\ 5^t$$

is transcendental.

[Note: $\ell n(2)$, $\ell n(3)$, $\ell n(5)$ are $\mathbb{Q}$-linearly independent. To see this, consider a dependence relation

$$q_1 \ell n(2) + q_2 \ell n(3) + q_3 \ell n(5) = 0,$$

where $q_1, q_2, q_3 \in \mathbb{Q}$. Write

$$q_1 = \frac{m_1}{n_1},\ q_2 = \frac{m_2}{n_2},\ q_3 = \frac{m_3}{n_3}\ .$$

Here

$$n_1 \neq 0,\ n_2 \neq 0,\ n_3 \neq 0$$

and the claim is that

$$m_1 = 0,\ m_2 = 0,\ m_3 = 0.$$

Clear the denominators and exponentiate to get

$$2^{m_1 n_2 n_3}\ 3^{n_1 m_2 n_3}\ 5^{n_1 n_2 m_3} = 1$$

$\Rightarrow$

$$m_1 n_2 n_3 = 0,\ n_1 m_2 n_3 = 0,\ n_1 n_2 m_3 = 0,$$

so

$$m_1 = 0,\ m_2 = 0,\ m_3 = 0.]$$

6: EXAMPLE Let

$$E_\infty = \{t \in R: 2^t, 3^t, 5^t, \ldots \in N\}.$$

Then $E_\infty = N$.

[Introduce

$$E_1 = \{t \in R: 2^t \in N\}$$

$$E_2 = \{t \in R: 2^t, 3^t \in N\}$$

$$E_3 = \{t \in R: 2^t, 3^t, 5^t \in N\}.$$

Then

$$N \subset E_\infty \subset E_3 \subset E_2 \subset E_1$$

=>

$$N = N \cap Q \subset E_3 \cap Q \subset E_2 \cap Q \subset E_1 \cap Q = N$$

=>

$$E_3 \cap Q = N.$$

But, in view of #5,

$$(R - Q) \cap E_3 = \emptyset.$$

Therefore

$$N \subset E_\infty = (E_\infty \cap Q) \cup (E_\infty \cap (R - Q))$$

$$\subset (E_\infty \cap Q) \cup (E_3 \cap (R - Q))$$

$$= E_\infty \cap Q \subset E_3 \cap Q = N.]$$

[Note: True or False: $E_2 = N$ (cf. §44, #6).]

7: N.B. By definition,

$$E_1 = \{t \in R: 2^t \in N\}.$$

And

$$2^t = n \in N \Rightarrow \exp(\ln(2^t)) = n$$

$$\Rightarrow \ln(2^t) = \ln(n)$$

$$\Rightarrow t = \frac{\ln(n)}{\ln(2)} .$$

And if $t = m \in N$, then

$$m = \frac{\ln(2^m)}{\ln(2)} = m\,\frac{\ln(2)}{\ln(2)} = m.]$$

<u>8:</u> EXAMPLE Let x_1, x_2 be two elements of $R \cup \sqrt{-1}\, R$ which are Q-linearly independent. Let y_1, y_2 be two complex numbers subject to $y_1, y_2, \bar{y}_2$ being Q-linearly independent -- then at least one of the numbers

$$e^{x_1 y_1},\ e^{x_1 y_2},\ e^{x_2 y_1},\ e^{x_2 y_2}$$

is transcendental.

[Taking $y_3 = \bar{y}_2$, #1 is applicable so it is a matter of eliminating $e^{x_1 y_3}$, $e^{x_2 y_3}$ from consideration. E.g.:

(1) Suppose $x_1 \in R$ -- then

$$e^{x_1 y_3} = e^{x_1 \bar{y}_2} = e^{\bar{\bar{x}}_1 \bar{y}_2} = e^{\overline{\bar{x}_1 y_2}} = e^{\overline{x_1 y_2}} .$$

But $e^{\overline{x_1 y_2}}$ is transcendental iff $e^{x_1 y_2}$ is transcendental.

(2) Suppose $x_1 \in \sqrt{-1}\, R$ -- then

$$e^{x_1 y_3} = e^{x_1 \bar{y}_2} = e^{\bar{\bar{x}}_1 \bar{y}_2} = e^{\overline{\bar{x}_1 y_2}} = e^{\overline{-x_1 y_2}} .$$

But

$$e^{-x_1y_2} = \frac{1}{e^{x_1y_2}}$$

is transcendental iff $e^{x_1y_2}$ is transcendental. Meanwhile $e^{-x_1y_2}$ is transcendental iff $\overline{e^{-x_1y_2}}$ is transcendental.]

[Note: α transcendental <=> $\bar{\alpha}$ transcendental and α transcendental iff $\frac{1}{\alpha}$ transcendental.]

<u>9:</u> LEMMA Consider a nonzero $m \times n$ matrix

$$M = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{m1} & \cdots & \lambda_{mn} \end{bmatrix},$$

where $\lambda_{ij} \in L$. Assume:

- The m rows

$$[\lambda_{11} \cdots \lambda_{1n}], \ldots, [\lambda_{m1} \cdots \lambda_{mn}]$$

are Q-linearly independent in C^n.

- The n columns

$$\begin{bmatrix} \lambda_{11} \\ \vdots \\ \lambda_{m1} \end{bmatrix}, \ldots, \begin{bmatrix} \lambda_{1n} \\ \vdots \\ \lambda_{mn} \end{bmatrix}$$

are Q-linearly independent in C^m.

Then

$$mn > m + n$$

implies that the rank of M is ≥ 2.

PROOF To get a contradiction, suppose that

$$\text{rank } M = 1.$$

Write (cf. §35, #9)

$$\lambda_{ij} = x_i y_j.$$

The point then is to check that the conditions of #1 are satisfied, i.e., that

$$\left[\begin{array}{l} x_1, \ldots, x_m \\ \\ y_1, \ldots, y_n \end{array}\right. \quad \text{are Q-linearly independent.}$$

For then the conclusion is that there is a pair (x_i, y_j) such that

$$\exp(x_i y_j)$$

is transcendental. But

$$\exp(x_i y_j) = \exp(\lambda_{ij}) \in \overline{Q}^{\times},$$

a contradiction. So consider dependence relations

$$\left[\begin{array}{l} q_1 x_1 + \cdots + q_m x_m = 0 \\ \\ p_1 y_1 + \cdots + p_n y_n = 0 \end{array}\right. \qquad (q_i \in Q,\ p_j \in Q)$$

and for the sake of argument, set down a generic rational dependence relation for the columns:

$$A_1 \begin{bmatrix} x_1y_1 \\ \cdot \\ \cdot \\ \cdot \\ x_my_1 \end{bmatrix} + \cdots + A_n \begin{bmatrix} x_1y_n \\ \cdot \\ \cdot \\ \cdot \\ x_my_n \end{bmatrix} = \begin{bmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} \in \mathbf{C}^m$$

$\Rightarrow$

$$\begin{cases} A_1x_1y_1 + \cdots + A_nx_1y_n = 0 \\ \quad\quad\cdot \\ \quad\quad\cdot \\ \quad\quad\cdot \\ A_1x_my_1 + \cdots + A_nx_my_n = 0. \end{cases}$$

We have

$$p_1y_1 + \cdots + p_ny_n = 0$$

$\Rightarrow$

$$x_1p_1y_1 + \cdots + x_1p_ny_n = 0$$

$\Rightarrow$

$$p_1x_1y_1 + \cdots + p_nx_1y_n = 0$$

$$\vdots$$

$$x_mp_1y_1 + \cdots + x_mp_ny_n = 0$$

$\Rightarrow$

$$p_1x_my_1 + \cdots + p_nx_my_n = 0.$$

Take now

$$A_1 = p_1, \ldots, A_n = p_n.$$

Since by hypothesis, the columns are $\mathbf{Q}$-linearly independent in $\mathbf{C}^m$, it follows that $A_1 = 0, \ldots, A_n = 0$ or still, $p_1 = 0, \ldots, p_n = 0$.]

10: SCHOLIUM Take $m = 2$, $n = 3$ and consider a nonzero 2×3 matrix M with entries in L:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \end{bmatrix}.$$

Suppose that its rows are Q-linearly independent and its columns are Q-linearly independent -- then in view of #9, the rank of M is ≥ 2. However, on general grounds (cf. §35, #11), the rank of M is $\leq \min(2,3) = 2$. Therefore

$$\text{rank } M = 2,$$

hence M has full rank (cf. §35, #12).

11: N.B. We have seen above that #1 => #9. The converse is also true: #9 => #1.

[To begin with, the assumption that

$$\{x_1,\ldots,x_m\} \text{ and } \{y_1,\ldots,y_n\}$$

are Q-linearly independent implies the Q-linear independence of the rows and columns of M. E.g.: To deal with the columns, note that there is at least one $x_i \neq 0$, say $x_1 \neq 0$, thus from

$$A_1x_1y_1 + \cdots + A_nx_1y_n = 0$$

there follows

$$A_1y_1 + \cdots + A_ny_n = 0$$

$$\Rightarrow$$

$$A_1 = 0,\ldots,A_n = 0.$$

Put $\lambda_{ij} = x_i y_j$ and suppose that $\forall\, i,j:\lambda_{ij} \in L$ -- then the rank of

$$M = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{m1} & \cdots & \lambda_{mn} \end{bmatrix}$$

is ≥ 2 (bear in mind that $mn > m + n$). But this is false: rank $M = 1$. Consequently $\exists\, i,j:\lambda_{ij} \notin L$, so

$$\exp(\lambda_{ij}) = \exp(x_i y_j)$$

is transcendental.

APPENDIX

QUESTION If $mn/(m + n)$ is large, can one find a lower bound for the rank of M which is > 2? Without additional conditions, the answer is "no". To see this, consider

$$M_m = \begin{bmatrix} \ell n(2) & \ell n(3) & \cdots & \ell n(p_m) \\ \ell n(3) & & 0 & \\ \vdots & & & \\ \ell n(p_m) & & & \end{bmatrix},$$

where p_m is the m^{th} prime -- then rank $M_m = 2$ for each $m > 2$ (here $m = n$ and $m^2 > 2m \Rightarrow m > 2$). Therefore the mere Q-linear independence of the rows and columns does not suffice.

CRITERION Let

$$M = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{m1} & \cdots & \lambda_{mn} \end{bmatrix}$$

be an $m \times n$ matrix with entries in L. Assume:

$$\begin{cases} \forall\ (t_1,\ldots,t_m) \in Z^m - \{(0,\ldots,0)\} \\ \forall\ (s_1,\ldots,s_n) \in Z^n - \{(0,\ldots,0)\}, \end{cases}$$

the sum

$$\sum_{i=1}^{m} \sum_{j=1}^{n} (t_i s_j \lambda_{ij} \neq 0.$$

Then the rank of M is

$$\geq \frac{mn}{m + n}.$$

[Note:

$$\lambda_{ij} \neq 0 \ (\forall\ i,j).]$$

EXAMPLE Take $m = d > 1$, $n = d > 1$ -- then

$$\frac{mn}{m + n} = \frac{d^2}{2d} = \frac{d}{2}.$$

LEMMA Under these circumstances, the rows and columns are Q-linearly independent.

PROOF Consider

$$A_1 \begin{bmatrix} \lambda_{11} \\ \cdot \\ \cdot \\ \cdot \\ \lambda_{m1} \end{bmatrix} + \cdots + A_n \begin{bmatrix} \lambda_{1n} \\ \cdot \\ \cdot \\ \cdot \\ \lambda_{mn} \end{bmatrix},$$

where without loss of generality, the $A_j \in Z$ are not all zero -- then the claim is that this expression is $\neq 0$. To be specific, assume $A_1 \neq 0$ and tailor the expression

$$\sum_{i=1}^{m} \sum_{j=1}^{n} t_i s_j \lambda_{ij}$$

as follows: Choose

$$t_1 = 1, \ t_2 = 0, \ldots, \ t_m = 0$$

to get

$$\begin{aligned} \sum_{j=1}^{n} s_j \lambda_{1j} &= s_1 \lambda_{11} + s_2 \lambda_{12} + \cdots + s_n \lambda_{1n} \\ &\neq 0. \end{aligned}$$

Take

$$s_1 = A_1, \ s_2 = A_2, \ldots, \ s_n = A_n,$$

hence

$$A_1 \lambda_{11} + A_2 \lambda_{12} + \cdots + A_n \lambda_{1n} \neq 0.$$

Assume in addition that

$$mn > m + n.$$

Then what has been said above implies #9 which in turn implies #1 (cf. #11).

EXAMPLE Take $m = d > 1$, $n = d > 1$ — then the foregoing says that the rank of M is $\geq \frac{d}{2}$. On the other hand, the theory also says that the rank of M is ≥ 2 (cf. #9). To check consistency, note that

$$mn > m + n \text{ becomes } d^2 > 2d \Rightarrow d > 2 \Rightarrow \frac{d}{2} > 1.$$

<u>Case 1:</u> $d = 2r$ $(r = 1,2,\ldots)$ -- then

$$1 < \frac{d}{2} = r \Rightarrow r \geq 2$$

$$\Rightarrow$$

$$2 \leq r \leq \text{rank } M.$$

<u>Case 2:</u> $d = 2r + 1$ $(r = 1,2,\ldots)$

<u>$r = 1$:</u> Here

$$\frac{d}{2} = \frac{3}{2} \leq \text{rank } M.$$

But rank M is a positive integer, so rank $M \geq 2$.

<u>$r > 1$:</u> Simply write

$$2 \leq r \leq \frac{2r + 1}{2} = \frac{d}{2} \leq \text{rank } M.$$

Therefore matters are in fact consistent.

§37. *VECTOR SPACES*

Let K be a field, $k \subset K$ a subfield.

1: N.B. Typically,

$$K = C, \ k = \bar{Q} \text{ or } Q.$$

2: LEMMA Let $V \subset K^d$ be a K-vector subspace -- then the following conditions are equivalent.

(i) V has a basis whose elements belong to k^d.

(ii) V is the intersection of hyperplanes defined by linear forms with coefficients in k.

[Note: Such a subspace V is said to be rational over k.]

3: DEFINITION Let V be a K-vector subspace -- then a k-structure on V is a k-vector subspace V' of V such that any basis of V' over k is a basis of V over K.

4: LEMMA Let $V \subset K^d$ be a K-vector subspace -- then $V \cap k^d$ is a k-structure on V iff V is rational over k.

5: EXAMPLE

- Q^d is a Q-structure on C^d.
- $\bar{Q}^d$ is a $\bar{Q}$-structure on C^d.

6: DEFINITION Given K-vector subspaces

$$\begin{cases} V_1 \subset K^{d_1} \\ V_2 \subset K^{d_2} \end{cases}$$

endowed with k-structures

$$\begin{cases} V_1' \subset V_1 \\ V_2' \subset V_2, \end{cases}$$

a K-linear map $f: V_1 \to V_2$ is <u>rational over k</u> if $f(V_1') \subset V_2'$.

<u>7:</u> EXAMPLE Take $V_1 = C^{d_1}$, $V_2 = C^{d_2}$ to arrive at the notion of a C-linear map $f: C^{d_1} \to C^{d_2}$ which is rational over Q (or $\bar{Q}$).

APPENDIX

NOTATION Let $\underline{e}_1, \ldots, \underline{e}_d$ be the canonical basis for K^d.

Let $V \subset K^d$ be a K-vector subspace of dimension n. Consider the following properties.

(1) If $\pi_V: K^d \to K^d/V$ is the canonical projection, then $(\pi_V(\underline{e}_1), \ldots, \pi_V(\underline{e}_{d-n}))$ is a basis for K^d/V.

(2) Given $\underline{z} = (z_1, \ldots, z_d) \in V$, the conditions

$$z_{d-n+1} = \cdots + z_d = 0 \Rightarrow \underline{z} = \underline{0}.$$

(3) The restriction to V of the projection $K^d \to K^n$ of the last n coordinates is injective.

(4) V is the intersection of d − n hyperplanes defined by the equations

$$z_j = \sum_{i=d-n+1}^{d} a_{ij} z_i \quad (1 \le j \le d-n).$$

FACT Properties (1), (2), (3), (4) are equivalent.

§38. VECTOR SPACES: L

Recall that in §32, #3, various conditions were formulated which are equivalent to homogeneous Baker. What follows is a supplement to that list.

1: THEOREM The following assertions are equivalent to homogeneous Baker.

(i) Let $V \subset C^d$ be a C-vector subspace rational over $\bar{Q}$ with $V \cap Q^d = \{0\}$ -- then $V \cap L^d = \{0\}$.

(ii) Let $V \subset C^d$ be a C-vector subspace rational over $\bar{Q}$ -- then there exists a C-vector subspace V_0 of C^d rational over Q and contained in V such that

$$V \cap L^d = V_0 \cap L^d.$$

[E.g.: To see that (ii) => (i), note that if $V \cap Q^d = \{0\}$, then the only C-vector subspace V_0 of C^d rational over Q and contained in V is $\{0\}$, hence

$$V \cap L^d = V_0 \cap L^d = \{0\} \cap L^d = \{0\}.]$$

2: REMARK One can replace item (ii) by a weaker assertion, viz.: If $V \subset C^d$ is a C-vector subspace rational over $\bar{Q}$, then

$$V \cap L^d = \bigcup_{V_0} V_0 \cap L^d,$$

where V_0 ranges over the C-vector subspaces of C^d rational over Q and contained in V.

3: THEOREM Let $V \subset C^d$ be a C-vector subspace -- then the Q-vector space $V \cap L^d$ is finite dimensional iff $V \cap Q^d = \{0\}$.

The implication

$$\dim_Q(V \cap L^d) < \infty \Rightarrow V \cap Q^d = \{0\},$$

i.e.,

$$V \cap Q^d \neq \{0\} \Rightarrow \dim_Q(V \cap L^d) = \infty$$

is straightforward: Take

$$\underline{q} = (q_1,\ldots,q_d) \neq 0$$

in $V \cap Q^d$ -- then $\forall\ \lambda \in L$,

$$(q_1\lambda,\ldots,q_d\lambda) \in V \cap L^d \Rightarrow \dim_Q(V \cap L^d) = \infty.$$

As for the converse, i.e.,

$$V \cap Q^d = \{0\} \Rightarrow \dim_Q(V \cap L^d) < \infty,$$

it is not so easy to establish. However there is one situation when matters are immediate. For suppose that $V \cap Q^d = \{0\}$ AND in addition that V is rational over $\bar{Q}$ -- then $V \cap L^d = \{0\}$ (cf. #1 (i)).

4: N.B. If V is not rational over $\bar{Q}$ but $V \cap Q^d = \{0\}$, then

$$\dim_Q(V \cap L^d)$$

may very well be positive (but, of course, finite) (cf. #7).

5: THEOREM Let $V \subset C^d$ be a C-vector subspace such that $V \cap Q^d = \{0\}$ -- then

$$\dim_Q(V \cap L^d) \leq n(n+1),$$

where

$$n = \dim_C(V).$$

6: EXAMPLE Take for V a complex line in C^d, hence $n = 1$. Suppose that V contains three Q-linearly independent points of L^d -- then V contains a nonzero point of Q^d.

[In fact, if $V \cap Q^d = \{0\}$, then

$$\dim_Q(V \cap L^d) \le n(n+1) = 1(1+1) = 2.$$

But the assumption implies that

$$\dim_Q(V \cap L^d) \ge 3.$$

Therefore $V \cap Q^d \neq \{0\}$.]

It is conjectured that $n(n+1)$ in #5 can be replaced by $n(n+1)/2$ but this remains to be seen.

7: EXAMPLE Fix nonzero Q-linearly independent elements $\lambda_1,\ldots,\lambda_{n+1}$ of L and define V by the equations

$$\lambda_1 z_1 + \cdots + \lambda_{n+1} z_{n+1} = 0,\ z_{n+2} = \cdots = z_d = 0.$$

Then $V \cap Q^d = \{0\}$ and $V \cap L^d$ contains the $n(n+1)/2$ points

$$w_{ij} = (w_{ij1},\ldots,w_{ijd}) \in C^d \quad (1 \le i < j \le d),$$

where

$$w_{ijk} = \lambda_j\ (k=i),\ w_{ijk} = -\lambda_i\ (k = j),$$

and $w_{ijk} = 0$ otherwise $(1 \le k \le d)$. And these points are Q-linearly independent, hence

$$\dim_Q(V \cap L^d) \geq n(n+1)/2.$$

8: RAPPEL Let X be a vector space, $S \subset X$ a nonempty subset -- then the span $< S >$ of S is the intersection of all subspaces containing S or still, the set of all finite linear combinations of the elements of S.

9: NOTATION Given a C-vector subspace $V \subset C^d$, put

$$t = \dim_C < V \cap \bar{Q}^d >,$$

the dimension of the C-vector space spanned by $V \cap \bar{Q}^d$.

10: N.B. For the record,

$$0 \leq t \leq n < d,$$

it being assumed that $V \neq C^d$.

11: THEOREM Let $V \subset C^d$ be a C-vector subspace such that $V \cap Q^d = \{0\}$ -- then

$$\begin{aligned}\dim_Q(V \cap L^d) &\leq d(n-t)\\ &\leq d(d-1-t),\end{aligned}$$

where

$$n = \dim_C(V).$$

12: REMARK Sometimes this estimate is better than the one provided by #5 but it can also be worse.

- Suppose that

$$n = \dim_C(V) = d-1, \ t = n.$$

Then

$$d(n-t) = d(d-1-t)$$

$$= d(d-1-(d-1)) = 0$$

$$\Rightarrow \dim_Q(V \cap L^d) = 0 \Rightarrow V \cap L^d = \{0\}$$

in accordance with expectation (V being rational over $\bar{Q}$). As for #5, it just gives

$$\dim_Q(V \cap L^d) \leq (d-1)(d).$$

- Suppose that

$$n = \dim_C(V) = 1, \ t=0.$$

Then

$$d(n-t) = d(1-0) = d,$$

whereas

$$n(n+1) = 2$$

which is less than d if $d \geq 3$.

<u>13:</u> EXAMPLE Let $V \subset C^3$ be the hyperplane defined by the equation

$$\sqrt{2}\, z_1 + ez_2 + z_3 = 0.$$

Then $\sqrt{2}$, e, 1 are Q-linearly independent. To check this, consider a rational dependence relation

$$q_1 \sqrt{2} + q_2 e + q_3 = 0.$$

<u>Case 1:</u> $q_1 = 0 \Rightarrow q_2 e + q_3 = 0 \Rightarrow q_2 = 0, \ q_3 = 0.$

<u>Case 2:</u> $q_1 \neq 0 \Rightarrow$

$$\sqrt{2} + \frac{q_2}{q_1} e + \frac{q_3}{q_1} = 0$$

$$\Rightarrow \frac{q_2}{q_1} e = - \sqrt{2} - \frac{q_3}{q_1}$$

$$\Rightarrow e = \frac{q_1}{q_2} \left(- \sqrt{2} - \frac{q_3}{q_1}\right).$$

I.e.: e is algebraic which it isn't Consequently, $V \cap Q^3 = \{0\}$. Since here

$$d = 3,\ n = 2,\ t = 1,$$

it therefore follows from #11 that

$$\dim_Q(V \cap L^3) \leq 3(2-1) = 3.$$

[Note: There are three possibilities for t: 0,1,2. But

$$(1,\ 0,\ - \sqrt{2}) \in V \cap \bar{Q}^3$$

which implies that $t \geq 1$. And $t = 2$ is impossible (V is not rational over $\bar{Q}$), thus $t = 1$.]

It has been observed above that #1(i) is a particular instance of #11 (cf. #12 (first ●)). To repeat:

<u>14:</u> THEOREM Let $V \subset C^d$ be a C-vector subspace rational over $\bar{Q}$ with $V \cap Q^d = \{0\}$ -- then $V \cap L^d = \{0\}$.

<u>15:</u> APPLICATION Here is one version of Gelfond-Schneider: Let $\lambda_1 \in L$, $\lambda_2 \in L$, let $\beta \in \bar{Q}$, $\beta \notin Q$, and suppose that $\lambda_2 = \beta\lambda_1$ -- then the claim is that $\lambda_1 = \lambda_2 = 0$. To establish this, work in C^2 and let $V \subset C^2$ be the complex line $C(1,\beta)$ -- then $V \cap Q^2 = \{0\}$ ($(z,z\beta) = (q_1,q_2) \Rightarrow z = q_1 \Rightarrow q_1\beta = q_2 \Rightarrow \beta = q_2/q_1$ if $q_1 \neq 0$). Moreover V is rational over Q (V being defined by the equation

$z_2 = \beta z_1$). The assumptions of #14 are therefore satisfied, hence $V \cap L^2 = \{0\}$. But $(\lambda_1, \lambda_2) \in V \cap L^2$, thus $\lambda_1 = \lambda_2 = 0$, as contended.

<u>16:</u> APPLICATION Let $\beta_1 \neq 0, \ldots, \beta_d \neq 0$ be algebraic numbers. Denote by $V \subset \mathbb{C}^d$ the hyperplane defined by the equation

$$\beta_1 z_1 + \cdots + \beta_d z_d = 0.$$

Then V is rational over $\bar{\mathbb{Q}}$. Assume: $V \cap \mathbb{Q}^d = \{0\}$ -- then $V \cap L^d = \{0\}$ (cf. #14). Next $\beta_1, \ldots, \beta_d$ are $\mathbb{Q}$-linearly independent:

$$q_1\beta_1 + \cdots + q_d\beta_d = 0 \Rightarrow (q_1, \ldots, q_d) \in V \cap \mathbb{Q}^d = \{0\}.$$

To exploit this, take nonzero $\lambda_1 \in L, \ldots, \lambda_n \in L$ and consider

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d,$$

which we claim is nonzero. For otherwise,

$$(\lambda_1, \ldots, \lambda_d) \in V \cap L^d = \{0\}.$$

Now quote §32, #3(ii) to see that this setup implies homogeneous Baker.

[Note: In §32, #3(ii), the supposition is that $\beta_1, \ldots, \beta_d$ are $\mathbb{Q}$-linearly independent (replace n by d). This implies that $V \cap \mathbb{Q}^d = \{0\}$. Proof:

$$(z_1, \ldots, z_d) = (q_1, \ldots, q_d) \in V \cap \mathbb{Q}^d$$

$$\Rightarrow$$

$$\beta_1 z_1 + \cdots + \beta_d z_d = 0$$

$$\Rightarrow$$

$$\beta_1 q_1 + \cdots + \beta_d q_d = 0.]$$

§39. VECTOR SPACES: L_G

It will be useful to generalize the considerations in §38 as this provides a convenient forum for certain important applications.

<u>1:</u> NOTATION Let $d_0 \geq 0$, $d_1 \geq 1$ be integers and let $d = d_0 + d_1$. Put

$$\begin{cases} G_0 = C \times \cdots \times C & (d_0 \text{ factors}) \\ G_1 = C^\times \times \cdots \times C^\times & (d_1 \text{ factors}) \end{cases}$$

and set

$$G = G_0 \times G_1.$$

<u>2:</u> NOTATION

$$L_G = \bar{Q}^{d_0} \times L^{d_1}.$$

[Note: Accordingly an element of L_G is a $d_0 + d_1$ tuple

$$(\beta_1, \ldots, \beta_{d_0}, \lambda_1, \ldots, \lambda_{d_1}),$$

where $\beta_1, \ldots, \beta_{d_0}$ are algebraic numbers, i.e., are in $\bar{Q}$, and $\lambda_1, \ldots, \lambda_{d_1}$ are logarithms of algebraic numbers, i.e., are in L.]

<u>3:</u> <u>N.B.</u> The choice $d_0 = 0$ puts us back into the setting of §38.

<u>4:</u> LEMMA L_G is a Q-vector subspace of C^d.

<u>5:</u> LEMMA Let $V \subset C^d$ be a C-vector subspace.

• If $V \cap (\{0\} \times \mathbf{Q}^{d_1}) \neq \{0\}$, then

$$\dim_{\mathbf{Q}}(V \cap L_G) = \infty.$$

[Take

$$\underline{q} = (0,\ldots,0,\ q_1,\ldots,q_{d_1}) \neq 0$$

in $V \cap (\{0\} \times \mathbf{Q}^{d_1})$ -- then $\forall\ \lambda \in L$,

$$(0,\ldots,0,\ q_1\lambda,\ldots,q_{d_1}\lambda) \in V \cap L_G \Rightarrow \dim_{\mathbf{Q}}(V \cap L_G) = \infty.]$$

• If $V \cap (\bar{\mathbf{Q}}^{d_0} \times \{0\}) \neq \{0\}$, then

$$\dim_{\mathbf{Q}}(V \cap L_G) = \infty.$$

[Take

$$\underline{\beta} = (\beta_1,\ldots,\beta_{d_0},0,\ldots,0) \neq 0$$

in $V \cap (\bar{\mathbf{Q}}^{d_0} \times \{0\})$ -- then $\forall\ \gamma \in \bar{\mathbf{Q}}$,

$$(\beta_1\gamma,\ldots,\beta_{d_0}\gamma,0,\ldots,0) \in V \cap L_G \Rightarrow \dim_{\mathbf{Q}}(V \cap L_G) = \infty.]$$

<u>6:</u> SCHOLIUM If

$$\dim_{\mathbf{Q}}(V \cap L_G) < \infty,$$

then

$$V \cap (\{0\} \times \mathbf{Q}^{d_1}) = \{0\} \text{ and } V \cap (\bar{\mathbf{Q}}^{d_0} \times \{0\}) = \{0\}.$$

<u>7:</u> DEFINITION The relations

$$V \cap (\{0\} \times \mathbf{Q}^{d_1}) = \{0\} \text{ and } V \cap (\bar{\mathbf{Q}}^{d_0} \times \{0\}) = \{0\}$$

are the <u>canonical conditions</u>.

8: THEOREM Let $V \subset \underline{C}^d$ be a $\underline{C}$-vector subspace for which the canonical conditions are in force -- then

$$\dim_{\underline{Q}}(V \cap L_G) < \infty$$

and, in fact,

$$\dim_{\underline{Q}}(V \cap L_G) \leq d_1(n-t).$$

[Note: As in §38,

$$n = \dim_{\underline{Q}}(V) \text{ and } t = \dim_{\underline{C}} \langle V \cap \bar{\underline{Q}}^d \rangle.]$$

9: REMARK Taking $d_0 = 0$ recovers 38, #11. As for the proof, it will be omitted since it depends on the so-called "linear subgroup theorem" which we shall not stop to formulate.]

10: APPLICATION Homogeneous Baker is the assertion that if $\lambda_1 \in L, \ldots, \lambda_d \in L$ are nonzero and $\underline{Q}$-linearly independent, then $\lambda_1, \ldots, \lambda_d$ are $\bar{\underline{Q}}$-linearly independent.

[Suppose that $\lambda_1, \ldots, \lambda_d$ are $\bar{\underline{Q}}$-linearly dependent, say

$$\beta_1\lambda_1 + \cdots + \beta_{d-1}\lambda_{d-1} = \lambda_d,$$

where $\beta_1, \ldots, \beta_{d-1}$ are algebraic. It can be assumed in addition that $\lambda_1, \ldots, \lambda_{d-1}$ are $\bar{\underline{Q}}$-linearly independent. Take now for V the hyperplane in $\underline{C}^d$ defined by the equation

$$\lambda_1 z_1 + \cdots + \lambda_{d-1} z_{d-1} = z_d.$$

Explicate the parameters: $d_0 = n = d-1$, $d_1 = 1$ (so $d \equiv d_0 + d_1 = n + 1 = (d - 1) + 1 = d\ldots$), $t = 0$. The definitions imply that the canonical conditions are in force, thus by #8,

$$\dim_Q(V \cap L_G) \leq d_1(n-t) = 1(d-1-0) = d - 1.$$

On the other hand,

$$V \cap L_G = V \cap (\bar{Q}^{d-1} \times L)$$

contains d Q-linearly independent points $\zeta_1,\ldots,\zeta_d$, namely

$$\zeta_i = (\delta_{i1},\ldots,\delta_{i(d-1)},\lambda_i) \quad (1 \leq i \leq d-1)$$

and

$$\zeta_d = (\beta_1,\ldots,\beta_{d-1},\lambda_d).]$$

[Note: Take a point in $V \cap \bar{Q}^d$, say $(\beta_1,\ldots,\beta_d)$, subject to

$$\lambda_1\beta_1 + \cdots \lambda_{d-1}\beta_{d-1} = \beta_d.$$

Argue that necessarily $\beta_d = 0$ (cf. #14), hence $\beta_1 = 0,\ldots,\beta_{d-1} = 0$ ($\lambda_1,\ldots,\lambda_{d-1}$ are $\bar{Q}$-linearly independent), hence $V \cap \bar{Q}^d = \{0\}$, hence $t = 0$.]

<u>11:</u> APPLICATION Inhomogeneous Baker is the assertion that if $\lambda_1 \in L$, $\ldots,\lambda_d \in L$ are nonzero and Q-linearly independent, then $1,\lambda_1,\ldots,\lambda_d$ are $\bar{Q}$-linearly independent.

[Suppose that $1,\lambda_1,\ldots,\lambda_d$ are $\bar{Q}$-linearly dependent, say

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_{d-1}\lambda_{d-1} = \lambda_d,$$

where $\beta_0,\beta_1,\ldots,\beta_{d-1}$ are algebraic. It can be assumed in addition that $\lambda_1,\ldots,\lambda_d$ are Q-linearly independent and $1,\lambda_1,\ldots,\lambda_{d-1}$ are $\bar{Q}$-linearly independent. Take now for V the hyperplane in $\mathbb{C}^{d+1}$ defined by the equation

$$z_0 + \lambda_1 z_1 + \cdots + \lambda_{d-1} z_{d-1} = z_d.$$

Explicate the parameters: $d_0 = n = d$, $d_1 = 1$ (the role of d in the theory is played in this situation by $d + 1: d_0 + d_1 = d + 1$, $t \geq 1$ (since $(1,0,\ldots,0,1) \in V$). The definitions imply that the canonical conditions are in force, thus by #8

$$\dim_{\mathbb{Q}}(V \cap L_G) \leq d_1(n-t) = 1(d-t) \leq d - 1.$$

On the other hand,

$$V \cap L_G = V \cap (\bar{\mathbb{Q}}^d \times L)$$

contains d $\mathbb{Q}$-linearly independent points $\zeta_1,\ldots,\zeta_d$, namely

$$\zeta_i = (0,\delta_{i1},\ldots,\delta_{i(d-1)},\lambda_i) \quad (1 \leq i \leq d-1)$$

and

$$\zeta_d = (\beta_0,\beta_1,\ldots,\beta_{d-1},\lambda_d).]$$

[Note:

$$t \geq 1 \Rightarrow - t \leq -1 \Rightarrow d - t \leq d - 1.$$

Also, on general grounds, $\beta_0 = 0$ (cf. #14).]

12: THEOREM Let $V \subset \mathbb{C}^d$ be a $\mathbb{C}$-vector subspace rational over $\bar{\mathbb{Q}}$ and for which the canonical conditions are in force -- then $V \cap L_G = \{0\}$.

PROOF In #8, take $t = n$ to get

$$\dim_{\mathbb{Q}}(V \cap L_G) = \{0\}.$$

13: APPLICATION

- If α is a nonzero algebraic number, then e^{α} is transcendental (cf. §21, #4).

$\bullet\bullet$ If β is an algebraic number such that e^β is algebraic, then $\beta = 0$.

Claim: $\bullet\bullet \Rightarrow \bullet$ For if e^α was not transcendental, then it would be algebraic, hence that $\alpha = 0$, contradiction.

To establish $\bullet\bullet$, take $d_0 = 1$, $d_1 = 1$ so that $d = 1 + 1 = 2$ and $L_G = \bar{Q} \times L$. The complex line $V = C(1,1)$ in C^2 is rational over $\bar{Q}$ and contains $(\beta,\beta) \in L_G$. Moreover it is clear that the canonical conditions hold. Therefore

$$V \cap L_G = \{0\} \quad (\text{cf. \#12}) \Rightarrow \beta = 0.$$

14: APPLICATION Suppose given a relation

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_d\lambda_d = 0,$$

where $\beta_0,\beta_1,\ldots,\beta_d$ are algebraic and $\lambda_1 \in L,\ldots,\lambda_d \in L$ — then $\beta_0 = 0$.

[Argue by contradiction and assume that $\beta_0 \neq 0$ with d minimal, thus $\beta_1,\ldots,\beta_d$ are Q-linearly independent and $\lambda_1,\ldots,\lambda_d$ are $\bar{Q}$-linearly independent. Let $V \subset C^{d+1}$ be the hyperplane defined by the equation

$$\beta_0 z_0 + \beta_1 z_1 + \cdots + \beta_d z_d = 0.$$

Then V is rational over $\bar{Q}$ and the canonical conditions are satisfied. But

$$(1,\lambda_1,\ldots,\lambda_d) \in V$$

and

$$(1,\lambda_1,\ldots,\lambda_d) \in L_G = \bar{Q} \times L^d \quad (d_0 = 1,\ d_1 = d).$$

Meanwhile

$$V \cap L_G = \{0\} \quad (\text{cf. \#12}).]$$

15: SCHOLIUM Suppose given a relation

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d = 0,$$

where $\beta_1,\ldots,\beta_d$ are algebraic and $\lambda_1 \in L,\ldots,\lambda_d \in L$.

- If $(\beta_1,\ldots,\beta_d) \neq (0,\ldots,0)$, then $\lambda_1,\ldots,\lambda_d$ are $\mathbb{Q}$-linearly dependent.
- If $(\lambda_1,\ldots,\lambda_d) \neq (0,\ldots,0)$, then $\beta_1,\ldots,\beta_d$ are $\mathbb{Q}$-linearly dependent.

16: N.B. Recall that every nonzero linear combination

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d$$

is transcendental (cf. §31, #11).

17: LEMMA Suppose that $\lambda_1,\ldots,\lambda_d$ are nonzero elements of L and $\beta_1,\ldots,\beta_d$ are nonzero elements of $\bar{\mathbb{Q}}$. Assume:

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d = 0.$$

Then there exist nonzero integers $k_1,\ldots,k_d$ such that

$$k_1\beta_1 + \cdots + k_d\beta_d = 0.$$

§40. VECTOR SPACES: V_{max}, V_{min}

<u>1:</u> CONSTRUCTION Let $V \subset \mathbb{C}^d$ be a $\mathbb{C}$-vector subspace -- then V contains a unique maximal subspace V_{max} of the form $W_0 \times W_1$, where W_0 is a subspace of $\mathbb{C}^{d_0}$ rational over $\bar{\mathbb{Q}}$ and W_1 is a subspace of $\mathbb{C}^{d_1}$ rational over $\mathbb{Q}$.

<u>2:</u> LEMMA W_0 is the subspace of $\mathbb{C}^{d_0}$ spanned by

$$V \cap (\bar{\mathbb{Q}}^{d_0} \times \{0\})$$

and W_1 is the subspace of $\mathbb{C}^{d_1}$ spanned by

$$V \cap (\{0\} \times \mathbb{Q}^{d_1}).$$

<u>3:</u> RAPPEL (cf. §39, #7) The relations

$$V \cap (\{0\} \times \mathbb{Q}^{d_1}) = \{0\} \text{ and } V \cap (\bar{\mathbb{Q}}^{d_0} \times \{0\}) = \{0\}$$

are the <u>canonical conditions</u>.

<u>4:</u> <u>N.B.</u> $V_{max} = \{0\}$ iff the canonical conditions are in force.

<u>5:</u> THEOREM Let $V \subset \mathbb{C}^d$ be a $\mathbb{C}$-vector subspace. Assume: V is rational over $\bar{\mathbb{Q}}$ -- then

$$V \cap L_G = V_{max} \cap L_G.$$

PROOF Trivially,

$$V_{max} \cap L_G \subset V \cap L_G.$$

This said, if first the canonical conditions hold, then $V \cap L_G = 0$ (cf. §39, #12).

But also $V_{max} = \{0\}$ (cf. #4), hence $V_{max} \cap L_G = 0$. Proceeding in general, write

$$V_{max} = W_0 \times W_1,$$

put

$$d_0' = \dim_C(\frac{C^d}{W_0}),\ d_1' = \dim_C(\frac{C^d}{W_1}),$$

and introduce

$$\begin{cases} G_0' = C \times \cdots \times C & (d_0' \text{ factors}) \\ G_1' = C^\times \times \cdots \times C^\times & (d_1' \text{ factors}). \end{cases}$$

Let $C^{d_0} \to C^{d_0'}$ be a surjective linear map, rational over $\bar{Q}$, with kernel W_0 and let $C^{d_1} \to C^{d_1'}$ be a surjective linear map, rational over Q, with kernel W_1. Denote by φ their product

$$C^{d_0} \times C^{d_1} \to C^{d_0'} \times C^{d_1'}.$$

Then the kernel of φ is V_{max} and $\varphi(L_G) = L_{G'}$. Moreover the canonical conditions hold for the subspace $V' = \varphi(V)$ of $C^{d_0'} \times C^{d_1'}$, hence $V' \cap L_{G'} = \{0\}$. Therefore

$$V \cap L_G \subset \varphi^{-1}(V' \cap L_{G'}) = \text{Ker } \varphi = V_{max}$$

$$\Rightarrow$$

$$V \cap L_G \subset V_{max} \cap L_G.$$

<u>6:</u> CONSTRUCTION Let $V \subset C^d$ be a C-vector subspace -- then V is contained in a unique minimal subspace V_{min} of the form $W_0 \times W_1$, where W_0 is a subspace of C^{d_0} rational over $\bar{Q}$ and W_1 is a subspace of C^{d_1} rational over Q.

7: LEMMA W_0 is the intersection of all hyperplanes of C^{d_0} rational over $\bar{Q}$ which contain the projection of V onto C^{d_0} and W_1 is the intersection of all hyperplanes of C^{d_1} rational over Q which contain the projection of V onto C^{d_1}.

8: N.B. $V_{min} = C^d$ means that $W_0 = C^{d_0}$ and $W_1 = C^{d_1}$.

APPENDIX

FACT Let $V \subset C^d$ be a C-vector subspace. Assume: The canonical conditions are in force -- then there exists a hyperplane $H \subset C^d$ containing V and for which the canonical conditions are also in force.

§41. *EXPONENTIALS* (6 or 5)

Specialized to the case when $m = 2$, $n = 3$, the six exponentials theorem is the following statement (cf. §36, #1):

<u>1:</u> THEOREM Let $\{x_1,x_2\}$ and $\{y_1,y_2,y_3\}$ be two $\mathbb{Q}$-linearly independent sets of complex numbers -- then at least one of the six numbers

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_1y_3}, e^{x_2y_1}, e^{x_2y_2}, e^{x_2y_3}$$

is transcendental.

PROOF To arrive at a contradiction, assume that the six numbers x_iy_j $(i = 1,2,$ $j = 1,2,3)$ all belong to L (the vectors in a linearly independent set are nonzero, thus $x_i \neq 0$ $(i = 1,2)$, $y_j \neq 0$ $(j = 1,2,3)$, so $x_iy_j \neq 0$). Work in $\mathbb{C}^2$ and take for V the complex line $\mathbb{C}\underline{x} = \mathbb{C}\{x_1,x_2\}$ -- then $V \cap \mathbb{Q}^2 = \{0\}$. For suppose that

$$z\underline{x} = (zx_1,zx_2) \in V \cap \mathbb{Q}^2 \quad (z \in \mathbb{C},\ z \neq 0).$$

Then

$$\begin{cases} zx_1 = q_1 \\ zx_2 = q_2 \end{cases} \qquad (q_1,q_2 \in \mathbb{Q})$$

and the claim is that $q_1 = 0$, $q_2 = 0$. Consider the four possibilities.

- $q_1 \neq 0$, $q_2 \neq 0 \Rightarrow$

$$\frac{1}{z} = \frac{x_1}{q_1}, \quad \frac{1}{z} = \frac{x_2}{q_2}$$

$$\Rightarrow q_2x_1 = q_1x_2 \Rightarrow q_2x_1 - q_1x_2 = 0$$

$$\Rightarrow q_1 = 0,\ q_2 = 0,$$

$\{x_1,x_2\}$ being Q-linearly independent.

- $q_1 \neq 0,\ q_2 = 0 \Rightarrow zx_2 = 0 \Rightarrow x_2 = 0.$
- $q_1 = 0,\ q_2 \neq 0 \Rightarrow zx_1 = 0 \Rightarrow x_1 = 0.$

Therefore these three possibilities are untenable, leaving $q_1 = 0$, $q_2 = 0$, as claimed. Next, $V \cap L^2$ contains the points

$$y_1\underline{x},\ y_2\underline{x},\ y_3\underline{x}$$

which are Q-linearly independent. To see this, consider a rational dependence relation

$$q_1y_1\underline{x} + q_2y_2\underline{x} + q_3y_3\underline{x} = \underline{0},$$

i.e.,

$$\begin{cases} q_1x_1y_1 + q_2x_1y_2 + q_3x_1y_3 = 0 \\ q_1x_2y_1 + q_2x_2y_2 + q_3x_2y_3 = 0. \end{cases}$$

Dividing the first of these relations by $x_1 \neq 0$ (or the second of these relations by $x_2 \neq 0$) gives

$$q_1y_1 + q_2y_2 + q_3y_3 = 0$$

$$\Rightarrow$$

$$q_1 = 0,\ q_2 = 0,\ q_3 = 0,$$

$\{y_1,y_2,y_3\}$ being $\mathbb{Q}$-linearly independent. Therefore

$$3 \leq \dim_{\mathbb{Q}}(V \cap L^2).$$

On the other hand (cf. §38, #5),

$$\dim_{\mathbb{Q}}(V \cap L^2) \leq 1(1 + 1) = 2$$

Contradiction.

The next result is known as the five exponentials theorem.

2: THEOREM Let $\{x_1,x_2\}$ and $\{y_1,y_2\}$ be two $\mathbb{Q}$-linearly independent sets of complex numbers. Let further γ be a nonzero algebraic number -- then at least one of the five numbers

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_2y_1}, e^{x_2y_2}, e^{\gamma x_1/x_2}$$

is transcendental.

PROOF With §39, #8 in mind, take $d_0 = 1$, $d_1 = 2$ ($\Rightarrow d = 3$) and let V be the hyperplane in $\mathbb{C}^3$ defined by the equation

$$\gamma x_1z_1 - x_2z_2 + x_1z_3 = 0 \quad (\Rightarrow n = 2).$$

Note that

$$(1,0,-\gamma) \in V \cap \bar{\mathbb{Q}}^3,$$

hence $t \geq 1$. If both x_1,x_2 are algebraic, then $\gamma x_1/x_2 \neq 0$ is algebraic, so $e^{\gamma x_1/x_2}$ is transcendental (cf. §39, #13). It can therefore be assumed that either x_1 or x_2 is transcendental, thus V is not rational over $\bar{\mathbb{Q}}$, thus $t \neq 2 \Rightarrow t = 1$. Moving on, since x_1,x_2 are $\mathbb{Q}$-linearly independent and $\gamma \neq 0$, it follows that the canonical conditions are in force. Consequently

$$\dim_{\mathbb{Q}}(V \cap L_G) \le d_1(n - t) = 2(2 - 1) = 2.$$

On the other hand, V contains the $\mathbb{Q}$-linearly independent points

$$(1,\gamma x_1/x_2,0), \ (0,x_1y_1,x_2y_1), \ (0,x_1y_2,x_2y_2),$$

so at least one of these does not belong to

$$L_G = \bar{\mathbb{Q}} \times L^2 = \bar{\mathbb{Q}} \times L \times L.$$

E.g.: Suppose that

$$(0,x_1y_1,x_2y_1) \notin \bar{\mathbb{Q}} \times L \times L.$$

Then

$$x_1y_1 \notin L \text{ or } x_2y_1 \notin L \quad \text{(or both)}$$

=>

$$e^{x_1y_1} \text{ transcendental or } e^{x_2y_1} \text{ transcendental (or both)}.$$

3: EXAMPLE Suppose that $\lambda_1 \in L$, $\lambda_2 \in L$. Assume: $\{\lambda_1,\lambda_2\}$ is $\mathbb{Q}$-linearly independent. Let $w \in \mathbb{C}$ $(w \notin \mathbb{Q})$ and let $\beta \in \bar{\mathbb{Q}}$ $(\beta \neq 0)$ -- then at least one of the three numbers

$$e^{w\lambda_1}, e^{w\lambda_2}, e^{\beta w}$$

is transcendental.

[In #2, take $x_1 = w$ $(\notin \mathbb{Q})$, $x_2 = 1$, $y_1 = \lambda_1, y_2 = \lambda_2$ -- then at least one of

$$e^{w\lambda_1}, e^{w\lambda_2}, e^{\lambda_1}, e^{\lambda_2}, e^{\beta w}$$

is transcendental or still, at least one of

$$e^{w\lambda_1}, e^{w\lambda_2}, e^{\beta w}$$

is transcendental.]

[Note: Put

$$\begin{bmatrix} \alpha_1 = e^{\lambda_1} \\ \alpha_2 = e^{\lambda_2}. \end{bmatrix}$$

Then at least one of

$$\alpha_1^w, \alpha_2^w, e^{\beta w}$$

is transcendental.]

<u>4:</u> EXAMPLE Fix $\lambda \neq 0$ in L. Let $w \in \mathbb{C}$ ($w \notin \mathbb{Q}$) and let $\beta \in \bar{\mathbb{Q}}$ ($\beta \neq 0$) -- then at least one of the three numbers

$$e^{w^2\lambda}, e^{w\lambda}, e^{\beta w}$$

is transcendental.

[In #2, take $x_1 = w$ ($\notin \mathbb{Q}$), $x_2 = 1$, $y_1 = w\lambda$, $y_2 = \lambda$ -- then at least one of

$$e^{w^2\lambda}, e^{w\lambda}, e^{w\lambda}, e^{\lambda}, e^{\beta w}$$

is transcendental or still, at least one of

$$e^{w^2\lambda}, e^{w\lambda}, e^{\beta w}$$

is transcendental.]

[Note: Put $\alpha = e^{\lambda}$ -- then at least one of

$$\alpha^{w^2}, \alpha^w, e^{\beta w}$$

is transcendental.]

<u>5:</u> EXAMPLE Let $\lambda_0 \in L$ ($\lambda_0 \neq 0$), $\lambda_1 \in L$, $\lambda_2 \in L$, $\beta \in \bar{\mathbb{Q}}$ ($\beta \neq 0$), $\gamma = \frac{1}{\beta}$.

Assume: $\{\lambda_1, \lambda_2\}$ is $\mathbb{Q}$-linearly independent -- then at least one of the two numbers

$$e^{\beta\lambda_0\lambda_1}, e^{\beta\lambda_0\lambda_2}$$

is nonzero.

[In #2, take $x_1 = \lambda_0\beta$ ($\notin \mathbb{Q}$), $x_2 = 1$, $y_1 = \lambda_1$, $y_2 = \lambda_2$, hence at least one of

$$e^{\lambda_0\beta\lambda_1}, e^{\lambda_0\beta\lambda_2}, e^{\lambda_1}, e^{\lambda_2}, e^{\frac{1}{\beta}\lambda_0\beta} = e^{\lambda_0}$$

is transcendental or still, at least one of

$$e^{\beta\lambda_0\lambda_1}, e^{\beta\lambda_0\lambda_2}$$

is transcendental.]

[Note: $\lambda_0\beta$ is not rational (for if it were, then λ_0 would be algebraic whereas it is transcendental).]

<u>6:</u> EXAMPLE Let λ_0, λ_1 be nonzero elements of L and let $\beta \in \bar{\mathbb{Q}}$ ($\beta \neq 0$) -- then at least one of the two numbers

$$e^{\beta\lambda_0\lambda_1}, e^{(\beta\lambda_0)^2\lambda_1}$$

is transcendental.

[To illustrate, take $\beta = 1$, $\lambda_0 = \ln(2)$, $\lambda_1 = \ln(2)$ -- then at least one of

$$2^{\ln(2)}, 2^{(\ln(2))^2}$$

is transcendental.]

<u>7:</u> REMARK Is it true that

five exponentials $\Rightarrow$ six exponentials?

In the literature, it is asserted that this is the case but no proof has been offered.

[To see the difficulty, in #2, take $\gamma = 1$, and consider

$$\left[\begin{array}{l} e^{x_1y_1},\ e^{x_1y_2},\ e^{x_2y_1},\ e^{x_2y_2},\ e^{x_1/x_2} \\ \\ e^{x_1y_3},\ e^{x_2y_3},\ e^{x_1y_1},\ e^{x_2y_1},\ e^{x_1/x_2}. \end{array}\right.$$

If e^{x_1/x_2} is algebraic, then we are done since one of the exponentials in the first row preceding e^{x_1/x_2} or in the second row preceding e^{x_1/x_2} must be transcendental. However, if e^{x_1/x_2} is transcendental, then it is conceivable that the first four exponentials in both rows are algebraic... .]

§42. *SHARP SIX EXPONENTIALS THEOREM*

This is the following statement.

1: THEOREM Let $\{x_1,x_2\}$ and $\{y_1,y_2,y_3\}$ be two Q-linearly independent sets of complex numbers. Let further β_{ij} $(i = 1,2,\ j = 1,2,3)$ be algebraic numbers. Assume: The six numbers

$$e^{x_iy_j-\beta_{ij}}$$

are algebraic, hence that the $\lambda_{ij} = x_iy_j - \beta_{ij}$ are in L -- then

$$x_iy_j = \beta_{ij} \quad (i = 1,2,\ j = 1,2,3).$$

PROOF With §39, #8 in mind, take $d_0 = 2$, $d_1 = 2$ ($\Rightarrow d = 4$) and let $V \subset C^4$ be the hyperplane defined by the equation

$$x_2(z_1 + z_3) = x_1(z_2 + z_4) \quad (\Rightarrow n = 3).$$

Note that

$$\left[\begin{array}{l} (1,0,-1,0) \in V \cap \bar{Q}^4 \\ \\ (0,-1,0,1) \in V \cap \bar{Q}^4 \end{array}\right. \qquad \Rightarrow t \geq 2.$$

Note in addition that for $j = 1,2,3$,

$$\eta_j \equiv (\beta_{1j},\beta_{2j},\lambda_{1j},\lambda_{2j}) \in V \cap L_G = V \cap (\bar{Q}^2 \times L^2).$$

Since these points are Q-linearly independent (see below), the canonical conditions are not satisfied (see below). Therefore

$$V \cap (\bar{Q}^2 \times \{0\}) \neq \{0\},$$

say

$$(z_1,z_2,z_3,z_4) \in V \cap (\bar{Q}^2 \times \{0\})$$

$$\Rightarrow z_1 \in \bar{Q},\ z_2 \in \bar{Q} \ \&\ z_3 = 0,\ z_4 = 0.$$

And

$$x_2(z_1 + z_3) - x_1(z_2 + z_4) = 0$$

$$\Rightarrow$$

$$x_2(z_1) - x_1(z_2) = 0$$

$$\Rightarrow \frac{x_2}{x_1}(z_1) = z_2.$$

But neither z_1 nor z_2 can be zero (see below), thus

$$\frac{x_2}{x_1} = \frac{z_2}{z_1}$$

is an algebraic number not in Q (see below). Now put $\gamma = \frac{x_2}{x_1}$ and write

$$\lambda_{2j} + \beta_{2j} = \gamma(\lambda_{1j} + \beta_{1j}) \quad (j = 1,2,3)$$

or still,

$$\gamma\lambda_{1j} - \lambda_{2j} = \beta_{2j} - \gamma\beta_{1j} \quad (j = 1,2,3).$$

The entity $\beta_{2j} - \gamma\beta_{1j}$ is an algebraic number, thus on general grounds (see below)

$$\beta_{2j} - \gamma\beta_{1j} = 0$$

which then implies that

$$\gamma\lambda_{1j} - \lambda_{2j} = 0 \Rightarrow \gamma\lambda_{1j} = \lambda_{2j}.$$

To finish the proof, make the claim that

$$\begin{cases} \lambda_{1j} = 0 \\ \\ \lambda_{2j} = 0 \end{cases} \qquad (j = 1,2,3).$$

To argue this, assume that $\lambda_{1j} \neq 0$, so $\gamma = \dfrac{\lambda_{2j}}{\lambda_{1j}}$ is transcendental (see below) (recall that $\gamma \notin Q$). Accordingly

$$\gamma_{1j} = 0 \Rightarrow \gamma 0 - \lambda_{2j} = 0 \Rightarrow \lambda_{2j} = 0.$$

[Note: Details--

- Consider a dependence relation over Q:

$$q_1\eta_1 + q_2\eta_2 + q_3\eta_3 = (0,0,0,0)$$

which, when unraveled, becomes

$$q_1(\beta_{11}, \beta_{21}, x_1y_1 - \beta_{11}, x_2y_1 - \beta_{21})$$

$$+ q_2(\beta_{12}, \beta_{22}, x_1y_2 - \beta_{12}, x_2y_2 - \beta_{22})$$

$$+ q_3(\beta_{13}, \beta_{23}, x_1y_3 - \beta_{13}, x_2y_3 - \beta_{23})$$

$$= (0,0,0,0)$$

$\Rightarrow$

$$q_1\beta_{11} + q_2\beta_{12} + q_3\beta_{13} = 0$$

$\Rightarrow$

$$q_1(x_1y_1 - \beta_{11}) + q_2(x_1y_2 - \beta_{12}) + q_3(x_1y_3 - \beta_{13})$$

$$= q_1x_1y_1 + q_2x_1y_2 + q_3x_1y_3 = 0$$

or still, upon dividing by $x_1 \neq 0$,

$$q_1 y_1 + q_2 y_2 + q_3 y_3 = 0$$

$$\Rightarrow q_1 = 0,\ q_2 = 0,\ q_3 = 0.$$

- Suppose that the canonical conditions were satisfied -- then

$$\begin{aligned} \dim_Q(V \cap L) &\leq d_1(n - t) \\ &= 2(3 - t). \end{aligned}$$

There are two possibilities for t:

$$\left[\begin{array}{l} t = 2 \Rightarrow 2(3 - 2) = 2 \\ t = 3 \Rightarrow 2(3 - 3) = 0. \end{array}\right.$$

But

$$\dim_Q(V \cap L_G) \geq 3,$$

η_1, η_2, η_3 being three Q-linearly independent points of $V \cap L_G$.

- The formula

$$x_2(z_1) - x_1(z_2) = 0$$

is a $\bar{Q}$ dependence relation per $\{x_1, x_2\}$. Claim: $z_1 \neq 0$, $z_2 \neq 0$. E.g.: Suppose $z_1 = 0$, hence $x_1(z_2) = 0 \Rightarrow z_2 = 0$ $(x_1 \neq 0)$.

- $\frac{x_2}{x_1}$ is a nonzero algebraic number and $\frac{x_2}{x_1} \notin Q$. For if $\frac{x_2}{x_1} \in Q$, we could write

$$x_2 - (\frac{x_2}{x_1})\, x_1 = 0$$

and thereby contradict the $\mathbb{Q}$-linear independence of x_1, x_2.

- If

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_d\lambda_d = 0,$$

where $\beta_0, \beta_1, \ldots, \beta_d$ are algebraic and $\lambda_1 \in L, \ldots, \lambda_d \in L$, then $\beta_0 = 0$ (cf. §39, #14).

- The quotient $\frac{u}{v}$ of two nonzero elements of L is either rational or transcendental.

<u>2:</u> IMPLICATION

sharp six exponentials => six exponentials.

[Take $\beta_{ij} = 0$, so $\forall$ i, $\forall$ j, $x_iy_j = 0$, which is false ($\forall$ i, $x_i \neq 0$, $\forall$ j, $y_j \neq 0$). The supposition that the six numbers

$$e^{x_iy_j}$$

are algebraic is therefore contradictory, thus at least one of the

$$e^{x_iy_j}$$

is transcendental.]

<u>3:</u> IMPLICATION

sharp six exponentials => five exponentials.

[Explicate the parameters in §41, #2:

$$e^{x_1y_1},\ e^{x_1y_2},\ e^{x_2y_1},\ e^{x_2y_2},\ e^{\gamma x_1/x_2}.$$

Put

$$y_3 = \gamma/x_2,$$

let

$$\beta_{11} = \beta_{12} = \beta_{21} = \beta_{22} = \beta_{13} = 0,$$

and let

$$\beta_{23} = \gamma.$$

To incorporate the denial of §41, #2, assume that the six numbers

$$e^{x_i y_j - \beta_{ij}}$$

are algebraic. Note that

$$e^{x_1 y_3 - \beta_{13}} = e^{x_1 y_3 - 0} = e^{\gamma x_1/x_2}$$

and

$$e^{x_2 y_3 - \beta_{23}} = e^{\gamma - \gamma} = 1.$$

Now apply #1:

$$x_i y_j = \beta_{ij} \quad (i = 1,2,\ j = 1,2,3),$$

so

$$x_1 y_1 = \beta_{11} = 0,\ x_1 y_2 = \beta_{12} = 0,\ x_2 y_1 = \beta_{21} = 0,\ x_2 y_2 = \beta_{22} = 0,$$

so we have our contradiction. Of course,

$$x_1 y_3 = \beta_{13} = 0,\ x_2 y_3 = \beta_{23} = \gamma$$

but these formulas do not figure in the deduction and are merely part of the formalism.

[Note: There is a potential gap in the argument, viz. why is $\{y_1, y_2, y_3\}$ a Q-linearly independent set? Thus consider a rational dependence relation

$$q_1 y_1 + q_2 y_2 + q_3 \gamma / x_1 = 0.$$

Multiply through by x_1:

$$q_1 x_1 y_1 + q_2 x_1 y_2 + q_3 \gamma = 0.$$

Since

$$e^{x_1 y_1} \in \bar{Q},\ e^{x_1 y_2} \in \bar{Q},$$

it follows that

$$\lambda_1 \equiv x_1 y_1 \in L,\ \lambda_2 \equiv x_1 y_2 \in L$$

and our relation reads

$$q_3 \gamma + q_1 \lambda_1 + q_2 \lambda_2 = 0.$$

But $\{x_1, x_2\}$ is a Q-linearly independent set, $\lambda_1 \in L$, $\lambda_2 \in L$ are nonzero and Q-linearly independent, hence with

$$\beta_0 = q_3 \gamma,\ \beta_1 = q_1,\ \beta_2 = q_2,$$

we have

$$\beta_0 + \beta_1 \lambda_1 + \beta_2 \lambda_2 = 0.$$

Therefore $\beta_0 = 0$ (cf. §39, #14)

$$\Rightarrow q_3 = 0 \Rightarrow q_1 = 0,\ q_2 = 0.]$$

§43. *STRONG SIX EXPONENTIALS THEOREM*

Denote by L^* the $\bar{Q}$-vector space spanned by 1 and L in C, thus

$$L^* = \{\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n:$$

$$n \geq 0,\ (\beta_0,\beta_1,\ldots,\beta_n) \in \bar{Q}^{n+1},\ (\lambda_1,\ldots,\lambda_n) \in L^n\}.$$

[Note: L^*, like L, is stable under complex conjugation.]

<u>1:</u> THEOREM Let $\{x_1,x_2\}$ and $\{y_1,y_2,y_3\}$ be two $\bar{Q}$-linearly independent sets of complex numbers -- then

$$\{x_1y_1,\ x_1y_2,\ x_1y_3,\ x_2y_1,\ x_2y_2,\ x_2y_3\} \not\subset L^*,$$

i.e., $\exists\ i \in \{1,2\}$, $\exists\ j \in \{1,2,3\}$:

$$x_iy_j \notin L^*,$$

hence $e^{x_iy_j}$ is transcendental.

This result, due to Damien Roy, is the strong six exponentials theorem (proof omitted).

[Note: The reason for the appelation "strong" as compared with the six exponentials theorem per se is that one of the x_iy_j $(1 \leq i \leq 2,\ 1 \leq j \leq 3)$ is not in L but even more, viz. it is not in L^*.]

<u>2:</u> STRONG CONDITION X Suppose that $\lambda_0 \in L^*$, $\lambda_1 \in L^*$, $\lambda_2 \in L^*$, $\lambda_3 \in L^*$. Assume: $\{\lambda_0,\lambda_1\}$ is $\bar{Q}$-linearly independent and $\{\lambda_0,\lambda_2,\lambda_3\}$ is $\bar{Q}$-linearly independent --

then

$$\{\frac{\lambda_1\lambda_2}{\lambda_0}, \frac{\lambda_1\lambda_3}{\lambda_0}\} \not\subset L^*.$$

PROOF In #1, take

$$x_1 = 1, \ x_2 = \frac{\lambda_1}{\lambda_0}, \ y_1 = \lambda_0, \ y_2 = \lambda_2, \ y_3 = \lambda_3.$$

Then

$$\{\lambda_0, \lambda_2, \lambda_3, \lambda_1, \frac{\lambda_1\lambda_2}{\lambda_0}, \frac{\lambda_1\lambda_3}{\lambda_0}\} \not\subset L^*.$$

But by hypothesis,

$$\{\lambda_0, \lambda_2, \lambda_3, \lambda_1\} \subset L^*.$$

Therefore

$$\{\frac{\lambda_1\lambda_2}{\lambda_0}, \frac{\lambda_1\lambda_3}{\lambda_0}\} \not\subset L^*.$$

3: THEOREM The strong condition X implies the strong six exponential theorem.

PROOF To devise a contradiction, assume that the six products $x_i y_j$ $(1 \leq i \leq 2, 1 \leq j \leq 3)$ are in L^*. Apply strong condition X as follows: Take

$$\lambda_0 = x_1 y_1, \ \lambda_1 = x_2 y_1, \ \lambda_2 = x_1 y_2, \ \lambda_3 = x_1 y_3.$$

Then $\{\lambda_0, \lambda_1\}$ is $\bar{Q}$-linearly independent, as is $\{\lambda_0, \lambda_2, \lambda_3\}$. Consequently either

$$\frac{\lambda_1\lambda_2}{\lambda_0} \notin L^* \text{ or } \frac{\lambda_1\lambda_3}{\lambda_0} \notin L^* \quad \text{(or both)}.$$

But

$$\left[\begin{array}{l} \dfrac{\lambda_1\lambda_2}{\lambda_0} = \dfrac{x_2y_1x_1y_2}{x_1y_1} = x_2y_2 \in L^* \\ \\ \dfrac{\lambda_1\lambda_3}{\lambda_0} = \dfrac{x_2y_1x_1y_3}{x_1y_1} = x_2y_3 \in L^*. \end{array}\right.$$

Contradiction.

<u>4:</u> LEMMA Suppose that $\lambda_1, \lambda_2 \in L^*$ $(\lambda_2 \neq 0)$. Assume: $\{1, \lambda_1, 1/\lambda_2\}$ is $\bar{Q}$-linearly independent -- then

$$\{\lambda_1\lambda_2,\ 1/\lambda_2\} \not\subset L^*.$$

PROOF If $1/\lambda_2 \notin L^*$, then we are done. Otherwise, apply strong condition X to the family $\{1/\lambda_2, 1, \lambda_1, 1\}$ and conclude that

$$\{\lambda_1\lambda_2, \lambda_2\} \not\subset L^*,$$

hence $\lambda_1\lambda_2 \notin L^*$.

<u>5:</u> SCHOLIUM Suppose that $\lambda \in L^*(\lambda \neq 0)$ is transcendental -- then

$$\{\lambda^2, 1/\lambda\} \not\subset L^*.$$

[In #4, take $\lambda_1 = \lambda$, $\lambda_2 = \lambda$ -- then the issue is whether $\{1, \lambda, 1/\lambda\}$ is $\bar{Q}$-linearly independent. So consider a dependence relation

$$r + s\lambda + t(1/\lambda) = 0,$$

where $r, s, t \in \bar{Q}$. Multiply up by λ to get

$$r\lambda + s\lambda^2 + t = 0.$$

Since λ is transcendental, it follows that $\{\lambda, \lambda^2, 1\}$ is algebraically independent over Q, hence is algebraically independent over $\bar{Q}$ (cf. §20, #7), hence is $\bar{Q}$-linearly independent, hence $r = 0$, $s = 0$, $t = 0$.]

6: APPLICATION Take $\lambda = \pi\sqrt{-1}$ -- then $\lambda \in L \subset L^*$ and

$$\{ -\pi^2, 1/\pi\sqrt{-1}\} \not\subset L^*.$$

Therefore

$$\pi^2 \notin L^* \text{ or } 1/\pi \notin L^* \quad \text{(or both)}$$

which implies that either

$$e^{\pi^2} \text{ is transcendental or } e^{1/\pi} \text{ is transcendental} \quad \text{(or both).}$$

7: SUBLEMMA Let x_1,x_2,y_1,y_2 be complex numbers and let γ be a nonzero algebraic number. Suppose that $\{x_1,x_2\}$ is $\bar{Q}$-linearly independent and $\{y_1,y_2,\gamma/x_1\}$ is $\bar{Q}$-linearly independent. Assume:

$$\gamma x_2/x_1 \in L^*.$$

Then

$$\{x_1y_1, x_1y_2, x_2y_1, x_2y_2\} \not\subset L^*.$$

PROOF Apply #1 to

$$\{x_1,x_2\} \text{ and } \{y_1,y_2,\gamma/x_1\},$$

which leads to

$$\{x_1y_1, x_1y_2, x_1(\gamma/x_1), x_2y_1, x_2y_2, x_2(\gamma/x_1)\}.$$

Of course,

$$x_1(\gamma/x_1) = \gamma \in L^*$$

and by hypothesis,

$$x_2(\gamma/x_1) = \gamma x_2/x_1 \in L^*,$$

leaving

$$\{x_1y_1,\ x_1y_2,\ x_2y_1,\ x_2y_2\}.$$

8: LEMMA Let x_1,x_2,y_1,y_2 be complex numbers and let γ be a nonzero algebraic number. Suppose that $\{x_1,x_2\}$ is $\mathbb{Q}$-linearly independent and $\{y_1,y_2\}$ is $\mathbb{Q}$-linearly independent. Assume:

$$\gamma x_2/x_1 \in L^*.$$

Then

$$\{x_1y_1,\ x_1y_2,\ x_2y_1,\ x_2y_2\} \not\subset L.$$

PROOF Assume instead that

$$\{x_1y_1,\ x_1y_2,\ x_2y_1,\ x_2y_2\} \subset L.$$

- $\{x_1y_1,\ x_2y_1\}$ is $\mathbb{Q}$-linearly independent, hence is $\bar{\mathbb{Q}}$-linearly independent (Gelfond-Schneider) (for $x_1y_1 \in L$, $x_2y_1 \in L$), hence $\{x_1,x_2\}$ is $\bar{\mathbb{Q}}$-linearly independent.

- $\{x_1y_1,\ x_1y_2\}$ is $\mathbb{Q}$-linearly independent, hence $\{1,\ x_1y_1,\ x_1y_2\}$ is $\bar{\mathbb{Q}}$-linearly independent (inhomogeneous Baker) (for $x_1y_1 \in L$, $x_1y_2 \in L$), hence $\{\gamma/x_1,\ y_1,y_2\}$ is $\bar{\mathbb{Q}}$-linearly independent.

Therefore (cf. #7)

$$\gamma x_2/x_1 \notin L^*.$$

[Note: To check that $\{\gamma/x_1,y_1,y_2\}$ is $\bar{\mathbb{Q}}$-linearly independent, write

$$r(\gamma/x_1) + sy_1 + ty_2 = 0,$$

where $r,s,t \in \bar{Q}$ -- then

$$r\gamma + sx_1y_1 + tx_1y_2 = 0$$

$$\Rightarrow r\gamma = 0,\ s = 0,\ t = 0.$$

But $\gamma \in \bar{Q}$ is nonzero, so $r = 0$.]

9: N.B. The strong six exponentials theorem intervenes in #8 via an application of #7.

10: RAPPEL Let $\{x_1,x_2\}$ and $\{y_1,y_2\}$ be two Q-linearly sets of complex numbers. Let further γ be a nonzero algebraic number -- then at least one of the five numbers

$$e^{x_1y_1},\ e^{x_1y_2},\ e^{x_2y_1},\ e^{x_2y_2},\ e^{\gamma x_2/x_2}$$

is transcendental.

[This is the five exponentials theorem (cf. §41, #2) (switch the roles of x_1 and x_2).]

11: IMPLICATION

strong six exponentials => five exponentials.

[The claim is that at least one of the five numbers

$$e^{x_1y_1},\ e^{x_1/y_2},\ e^{x_2y_1},\ e^{x_2y_2},\ e^{\gamma x_2/x_1}$$

is transcendental.

- Case 1: $\gamma x_2/x_1 \notin L^*$ -- then

$$e^{\gamma x_2/x_1}$$

is transcendental.

- Case 2: $\gamma x_2/x_1 \in L^*$ -- then

$$\{x_1y_1,\ x_1y_2,\ x_2y_1,\ x_2y_2\} \not\subset L \quad \text{(cf. \#8)},$$

i.e., $\exists\ i \in \{1,2\}$, $\exists\ j \in \{1,2,3\}$:

$$x_iy_j \notin L,$$

hence $e^{x_iy_j}$ is transcendental.]

12: REMARK Refer to §41, #7. Make the assumption that $x_2/x_1 \in L^*$ -- then for some pair $(i,j): x_iy_j \notin L$, implying thereby that $e^{x_iy_j}$ is transcendental, as desired.

13: RAPPEL Let $\{x_1,x_2\}$ and $\{y_1,y_2,y_3\}$ be two Q-linearly independent sets of complex numbers -- then

$$\{x_1y_1,\ x_1y_2,\ x_1y_3,\ x_2y_1,\ x_2y_2,\ x_2y_3\} \not\subset L.$$

[This is the six exponentials theorem.]

14: CONDITION X Suppose that $\lambda_0 \in L$, $\lambda_1 \in L$, $\lambda_2 \in L$, $\lambda_3 \in L$. Assume: $\{\lambda_0,\lambda_1\}$ is Q-linearly independent and $\{\lambda_0,\lambda_2,\lambda_3\}$ is Q-linearly independent -- then

$$\{\frac{\lambda_1\lambda_2}{\lambda_0},\ \frac{\lambda_1\lambda_3}{\lambda_0}\} \not\subset L.$$

[In #2, replace $\bar{Q}$ by Q and L^* by L.]

Imitating the proof that the strong exponentials theorem is equivalent to strong condition X, it follows that the six exponentials theorem is equivalent to condition X.

15: IMPLICATION

strong six exponentials => six exponentials.

[Start with the data for condition X — then thanks to homogeneous Baker, $\{\lambda_0,\lambda_1\}$ is $\bar{Q}$-linearly independent and $\{\lambda_0,\lambda_2,\lambda_3\}$ is $\bar{Q}$-linearly independent, the setup for strong condition X, hence (cf. #2),

$$\{\frac{\lambda_1\lambda_2}{\lambda_0}, \frac{\lambda_1\lambda_3}{\lambda_0}\} \not\subset L^*$$

$$\Rightarrow$$

$$\{\frac{\lambda_1\lambda_2}{\lambda_0}, \frac{\lambda_1\lambda_3}{\lambda_0}\} \not\subset L\ .]$$

APPENDIX

It was established in §36 that the six exponentials theorem is equivalent to the following statement.

SCHOLIUM Consider a nonzero 2×3 matrix M with entries in L:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \end{bmatrix}.$$

Suppose that its rows are Q-linearly independent and its columns are Q-linearly independent -- then

$$\text{rank } M = 2.$$

Analogously, the strong six exponentials theorem is equivalent to the following statement.

SCHOLIUM Consider a nonzero 2×3 matrix M with entries in L^*:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \end{bmatrix}.$$

Suppose that its rows are $\bar{Q}$-linearly independent and its columns are $\bar{Q}$-linearly independent -- then

$$\text{rank } M = 2.$$

<u>N.B.</u> Once again,

strong six exponentials => six exponentials.

[Start with

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \end{bmatrix} \quad (\lambda_{ij} \in L).$$

Then the assumption of the Q-linear independence of its rows and columns implies the $\bar{Q}$-linear independence of its rows and columns (homogeneous Baker).]

Finally, the sharp six exponentials theorem is equivalent to the following statement.

SCHOLIUM Consider a nonzero 2×3 matrix M with entries in $\bar{Q} + L$:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \end{bmatrix}.$$

Suppose that its rows are $\bar{Q}$-linearly independent and its columns are $\bar{Q}$-linearly independent -- then

$$\text{rank } M = 2.$$

REMARK Consequently

strong six exponentials => sharp six exponentials.

To help keep it all straight, make a chart of the various implications:

$$\begin{tikzcd}
& \text{strong 6 exp} \arrow[ddl] \arrow[d, Rightarrow] \arrow[dd, bend left=60] \\
& \text{sharp 6 exp} \arrow[d, Rightarrow] \\
\text{5 exp} \arrow[r, "?"'] & \text{6 exp}
\end{tikzcd}$$

§44. *FOUR EXPONENTIALS CONJECTURE* (4EC)

This is the following statement.

1: CONJECTURE Let $\{x_1, x_2\}$ and $\{y_1, y_2\}$ be two $\mathbb{Q}$-linearly independent sets of complex numbers -- then

$$\{x_1y_1, x_1y_2, x_2y_1, x_2y_2\} \not\subset L,$$

thus at least one of the numbers

$$e^{x_1y_1}, e^{x_1y_2}, e^{x_2y_1}, e^{x_2y_2}$$

is transcendental.

In terms of matrices (see the Appendix to §43):

2: CONJECTURE Consider a 2×2 matrix M with entries in L:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix}.$$

Suppose that its rows are $\mathbb{Q}$-linearly independent and its columns are $\mathbb{Q}$-linearly independent -- then

$$\text{rank } M = 2.$$

3: EXAMPLE Consider the matrix

$$\begin{bmatrix} 1 & \pi \\ \pi & \pi^2 \end{bmatrix}.$$

Its determinant is 0 and its rank is 1. This is not a contradiction since $\pi, \pi^2 \notin L$.

[Note: Still, its rows and columns are Q-linearly independent.]

<u>4:</u> LEMMA #1 <=> #2.

<u>5:</u> REMARK The four exponentials conjecture is a long outstanding open problem in transcendence theory.

<u>6:</u> EXAMPLE (Admit 4EC) Use the notation of §36, #6. Introduce as there

$$E_2 = \{t \in R: 2^t, 3^t \in N\}.$$

Then

$$E_2 = N.$$

[Given $t \notin R$, $t \notin Q$, take in #1

$$\begin{cases} x_1 = 1 \\ x_2 = t, \end{cases} \qquad \begin{cases} y_1 = \ln(2) \\ y_2 = \ln(3). \end{cases}$$

Then the four exponentials are

$$2,\ 3,\ 2^t,\ 3^t$$

and either

$$2^t \text{ or } 3^t \text{ (or both)}$$

is transcendental. Therefore

$$(R - Q) \cap E_2 = \emptyset.$$

But

$$E_2 \cap Q = N.$$

And

$$E_2 \cap Q = E_2 \cap (Q \cup (R-Q))$$

$$= E_2 \cap R = E_2.]$$

7: EXAMPLE (Admit 4EC) Let $\lambda \in L$, $\lambda \notin R$ — then $e^{|\lambda|}$ is transcendental.

[In #1, take

$$\begin{cases} x_1 = 1 \\ x_2 = |\lambda|/\lambda, \end{cases} \qquad \begin{cases} y_1 = \lambda \\ y_2 = |\lambda|. \end{cases}$$

Then the four exponentials are

$$e^{\lambda}, e^{|\lambda|}, e^{|\lambda|}, e^{|\lambda|^2/\lambda}.$$

Here $e^{\lambda} \in \bar{Q}$. And

$$|\lambda|^2 = \lambda\bar{\lambda} \Rightarrow \frac{|\lambda|^2}{\lambda} = \frac{\lambda\bar{\lambda}}{\lambda} = \bar{\lambda}$$

$$\Rightarrow e^{|\lambda|^2/\lambda} = e^{\bar{\lambda}} \in \bar{Q}.$$

Therefore $e^{|\lambda|}$ is transcendental.]

[Note: One should check that $\{x_1,x_2\}$ and $\{y_1,y_2\}$ are Q-linearly independent.

E.g.: Suppose that

$$py_1 + qy_2 = 0 \quad (p,q \in Q)$$

or still, if $\lambda = a + \sqrt{-1}\, b$ $(b \neq 0)$,

$$p(a + \sqrt{-1}\, b) + q\sqrt{a^2 + b^2} = 0$$

$\Rightarrow$

$$\begin{cases} pa + q\sqrt{a^2 + b^2} = 0 \\ pb = 0 \end{cases}$$

$\Rightarrow$

$$p = 0 \Rightarrow q\sqrt{a^2 + b^2} = 0 \Rightarrow q = 0.]$$

8: EXAMPLE (Admit 4EC) In #1, take

$$\begin{cases} x_1 = 1 \\ x_2 = \sqrt{2}, \end{cases} \qquad \begin{cases} y_1 = \sqrt{-1}\,\pi \\ y_2 = \sqrt{-1}\,\pi\sqrt{2}. \end{cases}$$

Then the four exponentials are

$$e^{\sqrt{-1}\pi}, \ e^{\sqrt{-1}\pi\sqrt{2}}, \ e^{\sqrt{-1}\pi\sqrt{2}}, \ e^{2\sqrt{-1}\pi}.$$

The first of these is -1, the fourth is $+1$, leaving

$$e^{\sqrt{-1}\pi\sqrt{2}},$$

which must therefore be transcendental (a consequence already of Gelfond-Schneider:

$$e^{\sqrt{-1}\pi\sqrt{2}} = e^{\sqrt{2}\,\mathrm{Log}\,-1} = (-1)^{\sqrt{2}}).$$

9: EXAMPLE (Admit 4EC) Let $\lambda \in L - \{0\}$ and let $w \in \mathbb{C} - \mathbb{Q}$ (a complex irrational number) -- then at least one of the two numbers

$$e^{\lambda w}, \ e^{\lambda/w}$$

is transcendental.

[In #1, take

$$\begin{cases} x_1 = \lambda \\ x_2 = w\lambda, \end{cases} \qquad \begin{cases} y_1 = 1 \\ y_2 = 1/w. \end{cases}$$

Then the four exponentials are

$$e^{\lambda} \in \bar{Q},\ e^{\lambda/w},\ e^{w\lambda},\ e^{\lambda} \in \bar{Q}.$$

[Note: There are circumstances when 4EC need not be invoked. E.g.: Consider the situation when $w \in \bar{Q}-Q$. In view of §24, #8, one of the numbers w, e^{λ}, and $e^{w\lambda}$ is transcendental. But w is algebraic (by hypothesis), e^{λ} is algebraic (by definition), thus $e^{w\lambda}$ is transcendental.]

<u>10:</u> EXAMPLE (Admit 4EC). Let $w \in C-Q$ -- then

$$\exp(2\pi\sqrt{-1}\, w) \text{ and } \exp(-2\pi\sqrt{-1}/w)$$

are not simultaneously algebraic.

[Modify #9 in the obvious way.]

<u>11:</u> EXAMPLE (Admit 4EC). Let α_1,α_2 be positive algebraic numbers different from 1 -- then π^2 and $\ell n(\alpha_1)\ell n(\alpha_2)$ are Q-linearly independent.

[Proceed by contradiction and assume that π^2 and $\ell n(\alpha_1)\ell n(\alpha_2)$ are Q-linearly dependent, say for $n,m \in Z$ nonzero,

$$n(\ell n(\alpha_1))(\ell n(\alpha_2)) = 4m\pi^2.$$

Put

$$\beta_1 = \alpha_1^n,\ \beta_2 = \exp(\tfrac{1}{m}\,\ell n(\alpha_2)).$$

Then β_1,β_2 are algebraic, nonzero, and $|\beta_1| \neq 1$, $|\beta_2| \neq 1$. Moreover

$$\ell n(\beta_1)\ell n(\beta_2)$$

$$= (n\ell n(\alpha_1))(\tfrac{1}{m}\ell n(\alpha_2))$$

$$= \frac{n}{m} \ln(\alpha_1)\ln(\alpha_2)$$

$$= \frac{n}{m}\frac{4m}{n}\pi^2 = 4\pi^2.$$

Let now

$$w = \ln(\beta_1)/2\pi\sqrt{-1},$$

so

$$\ln(\beta_1) = 2\pi\sqrt{-1}\, w.$$

Then

$$\ln(\beta_2) = \frac{4\pi^2}{\ln(\beta_1)}$$

$$= -2\pi\sqrt{-1}/w.$$

Since

$$\begin{bmatrix} \exp(2\pi\sqrt{-1}\, w) = \beta_1 \\ \exp(-2\pi\sqrt{-1}/w) = \beta_2, \end{bmatrix}$$

it follows that

$$\exp(2\pi\sqrt{-1}\, w) \text{ and } \exp(-2\pi\sqrt{-1}/w)$$

are algebraic, which contradicts #10.]

[Note: In the literature, this result is known as Bertrand's conjecture.]

12: EXAMPLE (Admit 4EC) Let $w \in C-Q$. Assume: $|w|^2 \in Q$ -- then

$$\exp(2\pi\sqrt{-1}\, w)$$

is transcendental.

[Assume instead that

$$\exp(2\pi\sqrt{-1}\, w)$$

is algebraic and write $w = x + \sqrt{-1}\, y \quad (y \neq 0)$.

- $\exists\ (n_1,n_2) \in \mathbb{Z}^2\ ((n_1,n_2) \neq (0,0))$:

$$\exp(2\pi\sqrt{-1}\, wn_1 - 2\pi\sqrt{-1}\, \bar{w}n_2) = 0.$$

- $\exists\ m \in \mathbb{Z}: n_1 w - n_2 \bar{w} = m$.

- $(n_1 - n_2)x = m, \quad (n_1 + n_2)y = 0$

=>

$$(n_1 + n_2) = 0 \Rightarrow 2n_1 x = m \Rightarrow x \in \mathbb{Q}.$$

- $|w|^2 = x^2 + y^2$

$$\Rightarrow y^2 = |w|^2 - x^2 \in \mathbb{Q}.$$

Therefore y is algebraic. But y is not algebraic (for if so, then $w = x + \sqrt{-1}\, y$ would be algebraic (cf. §21, #3) and $\exp(2\pi\sqrt{-1}\, w)$ would be transcendental (apply Gelfond-Schneider)). Thus we have reached a contradiction.]

[Note: With the overbar standing for complex conjugation,

$$\overline{2\pi\sqrt{-1}\, wn_1} = \overline{2\pi\sqrt{-1}}\ \overline{wn_1} = \overline{2\pi\sqrt{-1}}\ \bar{w}n_1 = -\ 2\pi\sqrt{-1}\ \bar{w}n_1.]$$

<u>13:</u> EXAMPLE (Admit 4EC). Let $w \in \mathbb{C}$. Assume: $|w| \in \mathbb{Q}$ and $\exp(2\pi\sqrt{-1}\, w)$ algebraic -- then $w \in \mathbb{Q}$.

[In fact,

$$|w| \in \mathbb{Q} \Rightarrow |w|^2 \in \mathbb{Q},$$

so if $w \in C-Q$, then

$$\exp(2\pi\sqrt{-1}\, w)$$

is transcendental (cf. #12).]

<u>14:</u> REMARK (Admit 4EC) The <u>Diaz curve</u> is the set of points

$$\exp(2\pi\sqrt{-1}\, w) \quad (|w| = 1).$$

If $w = \pm 1$, then

$$\exp(2\pi\sqrt{-1}\, w)$$

is algebraic. Otherwise

$$\exp(2\pi\sqrt{-1}\, w)$$

is transcendental.

Here is one situation where the 4EC can be verified.

<u>15:</u> THEOREM Suppose that x_1, x_2 are elements of $R \cup \sqrt{-1}\, R$ which are Q-linearly independent and suppose that y is a nonreal complex number with irrational real part -- then at least one of the numbers

$$e^{x_1},\ e^{x_1 y},\ e^{x_2},\ e^{x_2 y}$$

is transcendental.

[Note: In the notation of #1, $y_1 = 1$, $y_2 = y$.]

Proceed in steps.

- The set $\{1, y, \bar{y}\}$ is Q-linearly independent.

[Consider a rational dependence relation

$$a + by + c\bar{y} = 0.$$

Then

$$\begin{cases} a + (b + c)\operatorname{Re} y = 0 \\ \quad (b - c)\operatorname{Im} y = 0. \end{cases}$$

Since y is nonreal, $\operatorname{Im} y = 0$, hence

$$b - c = 0 \Rightarrow b = c \Rightarrow a + 2b(\operatorname{Re} y) = 0 \Rightarrow a = 0,\ b = 0.]$$

- Apply the six exponentials theorem to $\{x_1, x_2\}$ and $\{1, y, \bar{y}\}$ (cf. §41, #1).

Therefore at least one of the six numbers

$$e^{x_1},\ e^{x_1 y},\ e^{x_1 \bar{y}},\ e^{x_2},\ e^{x_2 y},\ e^{x_2 \bar{y}}$$

is transcendental.

- By hypothesis,

$$\bar{x}_1 = \varepsilon_1 x_1,\ \bar{x}_2 = \varepsilon_2 x_2\ \ (\varepsilon_1, \varepsilon_2 \in \{1, -1\}),$$

so

$$e^{x_1 \bar{y}} = e^{\overline{\varepsilon_1 x_1 y}},\ e^{x_2 \bar{y}} = e^{\overline{\varepsilon_2 x_2 y}}\ .$$

Therefore at least one of the numbers

$$e^{x_1},\ e^{x_1 y},\ e^{x_2},\ e^{x_2 y}$$

is transcendental.

[Note: If $e^{x_1 y}$ (or $e^{x_2 y}$) were algebraic, then the same would be true of $e^{x_1 \bar{y}}$ (or $e^{x_2 \bar{y}}$).]

§45. *STRONG FOUR EXPONENTIALS CONJECTURE (S4EC)*

This is the following statement.

1: CONJECTURE Let $\{x_1,x_2\}$ and $\{y_1,y_2\}$ be two $\bar{Q}$-linearly independent sets of complex numbers -- then

$$\{x_1y_1, x_1y_2, x_2y_1, x_2y_2\} \not\subset L^*.$$

In terms of matrices (cf. §44, #2):

2: CONJECTURE Consider a nonzero 2×2 matrix M with entries in L^*:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix}.$$

Suppose that its rows are $\bar{Q}$-linearly independent and its columns are $\bar{Q}$-linearly independent -- then

$$\text{rank } M = 2.$$

3: IMPLICATION

strong four exponentials => four exponentials.

4: CONDITION PQ Let $\lambda_0,\lambda_1,\lambda_2 \in L^* - \{0\}$. Assume:

$$\lambda_1/\lambda_0 \notin \bar{Q} \text{ and } \lambda_2/\lambda_0 \notin \bar{Q}.$$

Then

$$(\lambda_1\lambda_2)/\lambda_0 \notin L^*.$$

5: LEMMA

$$S4EC \iff PQ.$$

PROOF

- S4EC => PQ.

[In #1, take

$$\left[\begin{array}{l} x_1 = \lambda_0 \\ \\ x_2 = \lambda_2 \end{array}\right., \quad \left[\begin{array}{l} y_1 = 1 \\ \\ y_2 = \lambda_1/\lambda_0 \end{array}\right.$$

to arrive at

$$\lambda_0, \lambda_1, \lambda_2, \ (\lambda_1\lambda_2)/\lambda_0.$$

But $\lambda_0, \lambda_1, \lambda_2 \in L^* - \{0\}$, thus it must be the case that

$$(\lambda_1\lambda_2)/\lambda_0 \notin L^*.]$$

- PQ => S4EC.

[Start with $\{x_1, x_2\}$ and $\{y_1, y_2\}$ $\bar{Q}$-linearly independent sets of complex numbers. Assume that

$$x_1y_1, \ x_1y_2, \ x_2y_2$$

are in L^* and then claim that $x_2y_1 \notin L^*$. Put

$$\lambda_0 = x_1y_2, \ \lambda_1 = x_1y_1, \ \lambda_2 = x_2y_2$$

which, by hypothesis, are in $L^* - \{0\}$. Since

$$\lambda_1/\lambda_0 = y_1/y_2 \notin \bar{Q}, \ \lambda_2/\lambda_0 = x_2/x_1 \notin \bar{Q},$$

it follows that

$$(\lambda_1\lambda_2)/\lambda_0 = x_2y_1 \notin L^*.$$

6: APPLICATION (Admit S4EC) Let $\lambda_1, \lambda_2 \in L^* - \bar{Q}$ -- then $\lambda_1 \lambda_2 \notin L^*$. [In #4 above, take $\lambda_0 = 1$.]

7: N.B. So in particular, if $\lambda_1, \lambda_2 \in L - \{0\}$, then $\lambda_1 \lambda_2 \notin L^*$, hence

$$\lambda_1 \lambda_2 \notin \bar{Q} \text{ and } \lambda_1 \lambda_2 \notin L.$$

[Note: Bear in mind that $L \cap \bar{Q} = \{0\}$.]

8: EXAMPLE (Admit S4EC) e^{π^2} is transcendental (cf. §43, #6).

[In #7, take

$$\lambda_1 = \lambda_2 \equiv \lambda = \pi\sqrt{-1}.$$

Then

$$\lambda^2 = -\pi^2 \notin L^* \Rightarrow \pi^2 \notin L^*.$$

Therefore e^{π^2} is transcendental.]

9: THEOREM (Admit S4EC) If $\lambda \in L$ is nonzero, then $|\lambda|$ is transcendental.

PROOF In #7, take $\lambda_1 = \lambda$, $\lambda_2 = \bar{\lambda}$, thus

$$\lambda_1 \lambda_2 = \lambda\bar{\lambda} = |\lambda|^2 \notin L^*,$$

thus $|\lambda|^2$ is transcendental, thus $|\lambda|$ is transcendental (if $|\lambda|$ were algebraic, then $|\lambda|^2$ would be algebraic).

10: EXAMPLE (Admit S4EC) Take

$$\lambda = \ln(2) + \sqrt{-1}\,\pi.$$

Then $\lambda \in L$ and

$$|\lambda| = (\ln(2)^2 + \pi^2)^{1/2}$$

is transcendental.

<u>11:</u> THEOREM (Admit S4EC) Let $w \in \mathbb{C} - \{0\}$. Assume: $|w|$ is algebraic -- then e^w is transcendental (cf. §44, #7).

[In #1, take

$$\begin{bmatrix} x_1 = 1 \\ \\ x_2 = e^w \end{bmatrix}, \quad \begin{bmatrix} y_1 = 1 \\ \\ y_2 = e^{\bar{w}}. \end{bmatrix}$$

Then

$$x_1y_1 = 1,\ x_1y_2 = e^{\bar{w}},\ x_2y_1 = e^w,\ x_2y_2 = e^we^{\bar{w}}.$$

- $\{x_1,x_2\}$, $\{y_1,y_2\}$ are $\bar{\mathbb{Q}}$-linearly independent.]

[To deal with $\{x_1,x_2\}$, suppose that

$$\alpha + \beta e^w = 0 \ (\alpha,\beta \in \bar{\mathbb{Q}}).$$

Then $\beta = 0 \Rightarrow \alpha = 0$. Otherwise $\beta \neq 0$

$$\Rightarrow e^w = -\frac{\alpha}{\beta} \in \bar{\mathbb{Q}} - \{0\}$$

$$\Rightarrow w \in L \Rightarrow |w| \text{ transcendental (cf. #9)},$$

contrary to the assumption that $|w|$ is algebraic. Therefore β must be zero, as must α.]

Consider now the relation

$$\{1,\ e^{\bar{w}},\ e^w,\ e^we^{\bar{w}}\} \not\subset L^*.$$

If e^w was algebraic, then the same would be true of $e^{\bar{w}}$ and $e^we^{\bar{w}}$, an impossibility.

[Note: One can proceed without S4EC when

$$w \in \mathbb{R} \cup \sqrt{-1}\,\mathbb{R} \ (w \neq 0).$$

For in this situation,

$$\begin{cases} |w| = \pm\, w \quad (w \in R) \\ |w| = \pm\, \sqrt{-1}\, w \quad (w \in \sqrt{-1}\, R). \end{cases}$$

Therefore

$$w \in \bar{Q} - \{0\} \Rightarrow e^w \text{ transcendental (Hermite-Lindemann (§21, #4)).]}$$

<u>12:</u> LEMMA (Admit S4EC) Let $\lambda \in L^*$. Assume: $\{\lambda, \bar{\lambda}\}$ is $\bar{Q}$-linearly independent -- then $|\lambda| \notin L^*$.

PROOF We shall utilize condition PQ. To this end, note that $\{\lambda, |\lambda|\}$ is also $\bar{Q}$-linearly independent:

$$|\lambda| = \alpha\lambda \ (\alpha \in \bar{Q}) \Rightarrow |\lambda|^2 = \alpha^2\lambda^2 \Rightarrow \lambda\bar{\lambda} = \alpha^2\lambda^2 \Rightarrow \bar{\lambda} = \alpha^2\lambda.$$

Supposing that $|\lambda| \notin L^*$, take in #4

$$\lambda_0 = \lambda, \ \lambda_1 = \lambda_2 = |\lambda|.$$

Then

$$\lambda_1/\lambda_0 \notin \bar{Q} \text{ and } \lambda_2/\lambda_0 \notin \bar{Q}$$

$$\Rightarrow$$

$$(\lambda_1\lambda_2)/\lambda_0 \notin L^*.$$

On the other hand,

$$(\lambda_1\lambda_2)/\lambda_0 = \bar{\lambda} \in L^*.$$

Contradiction.

<u>13:</u> LEMMA (Admit S4EC)

- If $\lambda \in L^* - \bar{Q}$, then the quotient $1/\lambda$ is not in L^*.

- If $\lambda_1, \lambda_2 \in L^* - \bar{Q}$, then the product $\lambda_1\lambda_2$ is not in L^*.

APPENDIX

Let $\lambda \in L - \{0\}$ and let $w \in C - \{0\}$ with $|w| \in \bar{Q}$. Assume: $e^{\lambda w}$ is algebraic -- then either $w \in Q$ or else $w\lambda/\bar{\lambda} \in Q$.

[Note: Tacitly S4EC is in force.]

§46. *TRANSCENDENTAL EXTENSIONS*

<u>1:</u> NOTATION Let K be a field — then the field $K(X_1,\ldots,X_n)$ of rational functions in $X_1,\ldots,X_n$ is the quotient field of the polynomial ring $K[X_1,\ldots,X_n]$, hence consists of all quotients

$$f(X_1,\ldots,X_n)/g(X_1,\ldots,X_n)$$

of polynomials in $X_1,\ldots,X_n$ with $g \neq 0$.

Let L be a field, $K \subset L$ a subfield.

<u>2:</u> NOTATION Fix a subset $S \subset L$.

- The ring $K[S]$ generated by K and S is the intersection of all subrings of L that contain K and S.

- The field $K(S)$ generated by K and S is the intersection of all subfields of L that contain K and S.

[Note: If $S = \{\alpha_1,\ldots,\alpha_n\}$ is finite, write

$$K[S] = K[\alpha_1,\ldots,\alpha_n]$$

and

$$K(S) = K(\alpha_1,\ldots,\alpha_n).]$$

<u>3:</u> <u>N.B.</u> If S is finite, then the field $K(S)$ is said to be a <u>finitely generated extension</u> of K.

[Note:

finite extension => finitely generated extension

finitely generated extension $\not\Rightarrow$ finite extension.]

4: LEMMA $K(S)$ is the set of all elements of L that can be expressed as quotients of finite linear combinations with coefficients in K of finite products of elements of S.

5: TERMINOLOGY Let L be a field, $K \subset L$ a subfield.

- A finite subset $S = \{\alpha_1,\ldots,\alpha_n\} \subset L$ is algebraically dependent over K

if there is a nonzero polynomial $P \in K[X_1,\ldots,X_n]$ such that

$$P(\alpha_1,\ldots,\alpha_n) = 0.$$

- A finite subset $S = \{\alpha_1,\ldots,\alpha_n\} \subset L$ is algebraically independent over K

if there is no nonzero polynomial $P \in K[X_1,\ldots,X_n]$ such that

$$P(\alpha_1,\ldots,\alpha_n) = 0.$$

6: EXAMPLE Take $L = K(X_1,\ldots,X_n)$, the field of rational functions in $X_1,\ldots,X_n$ -- then $\{X_1,\ldots,X_n\}$ is algebraically independent over K.

[Note: Suppose that $r_1,\ldots,r_n$ are positive integers — then $\{X_1^{r_1},\ldots,X_n^{r_n}\}$ is algebraically independent over K.]

7: EXAMPLE Working still with $L = K(X_1,\ldots,X_n)$, let $A = [a_{ij}]$ be an $n \times n$ matrix with coefficients in K. Put $f_j = \sum_i a_{ij}X_i$ -- then $\{f_1,\ldots,f_n\}$ is algebraically independent over K iff $\det A \neq 0$.

8: N.B. Take $S = \emptyset$, the empty set -- then it is deemed to be algebraically independent over K.

9: LEMMA If $\alpha_1,\ldots,\alpha_n \in L$ are algebraically independent over K, then

$K[\alpha_1,\ldots,\alpha_n]$ and $K[X_1,\ldots,X_n]$ are K-isomorphic rings, hence $K(\alpha_1,\ldots,\alpha_n)$ and $K(X_1,\ldots,X_n)$ are K-isomorphic fields.

[Note: The property is characteristic in that if $K(\alpha_1,\ldots,\alpha_n)$ and $K(X_1,\ldots,X_n)$ are K-isomorphic fields, then $\{\alpha_1,\ldots,\alpha_n\}$ is algebraically independent over K.]

<u>10:</u> REMARK The algebraic independence of $\alpha_1,\ldots,\alpha_n \in L$ over K is equivalent to the requirement that for each i, α_i is transcendental over $K(\alpha_1,\ldots,\alpha_{i-1})$.

<u>11:</u> DEFINITION A subset S of L is a <u>transcendence basis</u> for L/K if S is algebraically independent over K and if L is algebraic over K(S).

[Note: A priori, S is infinite, the convention being that S is algebraically independent over K if every finite subset of S is algebraically independent over K.]

<u>12:</u> EXAMPLE In the setup of #6, $\{X_1^{r_1},\ldots,X_n^{r_n}\}$ is algebraically independent over K. So, to establish that $\{X_1^{r_1},\ldots,X_n^{r_n}\}$ is a transcendence basis for L/K, it has to be shown that L is algebraic over $K(X_1^{r_1},\ldots,X_n^{r_n})$. But for each i, the element X_i is a zero of the polynomial $T^{r_i} - X_i^{r_i} \in L[T]$.

<u>13:</u> <u>N.B.</u> If $S = \emptyset$ is a transcendence basis for L/K, then L/K is algebraic (and conversely).

<u>14:</u> THEOREM There exists a transcendence basis for L/K.

15: REMARK If $S_1 \subset S_2 \subset L$, if S_1 is algebraically independent over K, if $L/K(S_2)$ is algebraic, then there exists a transcendence basis X for L/K with $S_1 \subset X \subset S_2$.

16: THEOREM If $S_1 \subset L$, $S_2 \subset L$ are transcendence bases for L/K, then

$$\text{card } S_1 = \text{card } S_2.$$

17: DEFINITION The transcendence degree

$$\text{trdeg}_K(L/K)$$

is the cardinality of any transcendence basis for L/K.

18: N.B. If

$$\text{trdeg}_K(L/K) = 0,$$

then L/K is algebraic (and conversely).

19: EXAMPLE Take $K = \mathbb{Q}$, $L = \mathbb{C}$ -- then

$$\text{trdeg}_{\mathbb{Q}}(\mathbb{C}/\mathbb{Q}) = \mathfrak{c}.$$

20: THEOREM Let $k \subset K \subset L$ be fields -- then

$$\text{trdeg}_k(L/k) = \text{trdeg}_K(L/K) + \text{trdeg}_k(K/k).$$

The situation when L is a finitely generated extension of K occupies center stage.

21: SCHOLIUM Let $L = K(\alpha_1,\ldots,\alpha_n)$ -- then a maximal algebraically independent subset of the set $\{\alpha_1,\ldots,\alpha_n\}$ is a transcendence basis for L/K and

$$\mathrm{trdeg}_K(L/K) \leq n$$

Assuming that $S = \{\alpha_1,\ldots,\alpha_m\}$, it follows that L is a finite extension of $K(\alpha_1,\ldots,\alpha_m)$ and if this is separable (which is always the case in characteristic 0), then

$$L = K(\alpha_1,\ldots,\alpha_m,\beta)$$

for some β in L (primitive element).

[Note: The extension L/K can be broken up into a series of subextensions, viz. let $K_i = K(\alpha_1,\ldots,\alpha_i)$ (put $K_0 = K$) -- then

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n = L,$$

where $K_{i+1} = K_i(\alpha_{i+1})$.]

22: LEMMA Let L be a field, $K \subset L$ a subfield. Let S be a subset of L with the property that each $\alpha \in S$ is algebraic over K -- then K(S) is algebraic over K and

$$S \text{ finite} \Rightarrow [K(S):K] \text{ finite}.$$

23: EXAMPLE Take $K = Q$ and consider $Q(\sqrt{2},\pi)$ -- then it is clear that $\{\sqrt{2}\}$ is not algebraically independent, nor is $\{\sqrt{2},\pi\}$, which leaves $\{\pi\}$, the claim being that it is a transcendence basis for $Q(\sqrt{2},\pi)/Q$ (per the theory spelled out in #21). To check this, in #22 take $K = Q(\pi)$, $L = Q(\sqrt{2},\pi)$, $S = \{\sqrt{2},\pi\}$.

- $\sqrt{2}$ is algebraic over $Q(\pi)$: Work with $X^2 - 2 \in Q(\pi)[X]$.

- π is algebraic over $Q(\pi)$: Work with $X - \pi \in Q(\pi)[X]$.

Therefore $Q(\pi)(\sqrt{2},\pi)$ is algebraic over $Q(\pi)$.

And

$$\mathrm{tr}_Q\, Q(\sqrt{2},\pi) = 1.$$

<u>24:</u> REMARK The transcendence degree

$$\mathrm{trdeg}_Q\, Q(\pi,e)$$

is either 1 or 2 but whether it is 1 or whether it is 2 is unknown since it is not known if π and e are algebraically independent or not.

<u>25:</u> RATIONAL RECAPITULATION Let M and N be finite subsets of $\mathbb{C}$.

- If $N \subset \bar{Q}$, then

$$\mathrm{trdeg}_Q\, Q(M \cup N) = \mathrm{trdeg}_Q\, Q(M).$$

Therefore algebraic numbers do not contribute to the transcendence degree.

- If $N \subset M$, then

$$\mathrm{trdeg}_Q\, Q(M \cup N) = \mathrm{trdeg}_Q\, Q(M).$$

Therefore only distinct numbers can contribute to the transcendence degree.

- If the transcendence degree

$$\deg_Q\, Q(M)$$

of the field $Q(M)$ is card M, then M is algebraically independent over Q and conversely.

- If $M = \{m\}$, then the transcendence degree

$$\deg_Q\, Q(m)$$

of the field $Q(m)$ is 0 if m is algebraic and 1 if m is transcendental.

- $Q \ldots \bar{Q}$:

$$\deg_Q Q(M) = \deg_{\bar{Q}} \bar{Q}(M).$$

<u>26:</u> LEMMA Suppose that $\alpha_1,\ldots,\alpha_n$ are algebraically independent over K -- then so are $\alpha_1^{p_1/q_1},\ldots,\alpha_n^{p_n/q_n}$ for nonzero rational numbers $p_1/q_1,\ldots,p_n/q_n$.

PROOF The transcendence degree of $K(\alpha_1,\ldots,\alpha_n)$ over K is n (cf. #9), whereas

$$K(\alpha_1^{1/q_1},\ldots,\alpha_n^{1/q_n})$$

is algebraic over $K(\alpha_1,\ldots,\alpha_n)$ since $(\alpha_j^{1/q_j})^{q_j} = \alpha_j$. Therefore the transcendence degree of

$$K(\alpha_1^{1/q_1},\ldots,\alpha_n^{1/q_n})$$

over K is also n. The numbers $\{\alpha_1^{1/q_1},\ldots,\alpha_n^{1/q_n}\}$ are algebraically independent over K, thus the same is true of the numbers $\{\alpha_1^{p_1/q_1},\ldots,\alpha_n^{p_n/q_n}\}$ (cf. #6).

<u>27:</u> LEMMA Suppose that $\alpha_1,\ldots,\alpha_n$ are algebraically independent over K. Let

$$\frac{A[X_1,\ldots,X_n]}{B[X_1,\ldots,X_n]}$$

be two nonzero polynomials whose quotient is not in K -- then

$$\frac{A(\alpha_1,\ldots,\alpha_n)}{B(\alpha_1,\ldots,\alpha_n)}$$

is not in K.

PROOF If the ratio was equal to some $\alpha \in K$, then

$$A(\alpha_1,\ldots,\alpha_n) - \alpha B(\alpha_1,\ldots,\alpha_n) = 0,$$

which contradicts the algebraic independence of the α_j's.

§47. *SCHANUEL'S CONJECTURE* (SCHC)

This is the following statement.

1: CONJECTURE Suppose that $x_1,\ldots,x_n$ are Q-linearly independent complex numbers — then among the 2n numbers

$$x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n},$$

at least n are algebraically independent over Q, i.e.,

$$\mathrm{trdeg}_Q\ Q(x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n}) \geq n \quad \text{(cf. §46, #21).}$$

This conjecture has many consequences, some of which are delineated below.

2: LEMMA The set of n-tuples $(x_1,\ldots,x_n)$ in C^n such that the 2n numbers

$$x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n}$$

are algebraically independent over Q is a G_δ-subset of C^n and its complement is a set of Lebesgue measure 0.

3: N.B. The transcendence degree can be as small as n (cf. #6).

4: THEOREM Take n = 1 and consider x, e^x $(x \neq 0)$ — then at least one of x, e^x is transcendental (cf. §31, #5), thus

$$\mathrm{trdeg}_Q\ Q(x,e^x) \geq 1,$$

which is Schanuel in the simplest situation.

5: N.B. Take $n = 2$ and consider $x_1, x_2, e^{x_1}, e^{x_2}$ -- then the claim is that

$$\mathrm{tr}_Q\, Q(x_1, x_2, e^{x_1}, e^{x_2}) \geq 2$$

but this has never been verified in general.

[Note: Let w_1, w_2 be two nonzero complex numbers -- then SCHC implies that

$$\mathrm{trdeg}_Q\, Q(w_1 w_2, e^{w_1}, e^{w_2}) \geq 1.]$$

6: THEOREM Suppose that $x_1,\ldots,x_n$ are Q-linearly independent algebraic numbers -- then the transcendental numbers $e^{x_1},\ldots,e^{x_n}$ are algebraically independent over Q (cf. §21, #12), so

$$\mathrm{tr}_Q\, Q(x_1,\ldots,x_n, e^{x_1},\ldots,e^{x_n}) \geq n,$$

thereby settling Schanuel in the particular case when $x_1,\ldots,x_n$ are algebraic.

7: THEOREM (Admit SCHC) Let $\lambda_1,\ldots,\lambda_n$ be Q-linearly independent elements of L (thus transcendental (cf. §31, #4)) -- then $e^{\lambda_1},\ldots,e^{\lambda_n}$ are algebraic numbers, hence

$$\begin{aligned}\mathrm{trdeg}_Q\, Q(\lambda_1,\ldots,\lambda_n, e^{\lambda_1},\ldots,e^{\lambda_n}) & \\ &= \mathrm{trdeg}_Q\, Q(\lambda_1,\ldots,\lambda_n) \\ &\leq n.\end{aligned}$$

On the other hand, by Schanuel,

$$\mathrm{trdeg}_Q\, Q(\lambda_1,\ldots,\lambda_n, e^{\lambda_1},\ldots,e^{\lambda_n}) \geq n.$$

Therefore

$$\operatorname{trdeg}_{Q} Q(\lambda_1,\ldots,\lambda_n) = n,$$

which implies that $\{\lambda_1,\ldots,\lambda_n\}$ is algebraically independent over Q (cf. §46, #9).

<u>8:</u> EXAMPLE It is not true in general that

linear independence => algebraic independence.

Thus, e.g., $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is linearly independent over Q but is not algebraically independent over Q as can be seen by noting that if

$$P(X_1,X_2,X_3,X_4) = X_2X_3 - X_4,$$

then

$$P(1,\sqrt{2},\sqrt{3},\sqrt{6}) = 0.$$

<u>9:</u> IMPLICATION

Schanuel => inhomogeneous Baker.

[If $\lambda_1 \in L,\ldots,\lambda_n \in L$ are Q-linearly independent, then $\lambda_1,\ldots,\lambda_n$ are Q-algebraically independent (cf. #7) or still, $\lambda_1,\ldots,\lambda_n$ are $\bar{Q}$-algebraically independent (cf. §20, #7), hence $1,\lambda_1,\ldots,\lambda_n$ are $\bar{Q}$-linearly independent. Proof: Given $\gamma,\gamma_1,\ldots,\gamma_n$ algebraic and

$$\gamma + \gamma_1\lambda_1 + \cdots + \gamma_n\lambda_n = 0,$$

work with

$$P(X_1,\ldots,X_n) = \gamma + \gamma_1X_1 + \cdots + \gamma_nX_n.]$$

<u>10:</u> THEOREM (Admit SCHC) Suppose given elements $\lambda_1,\ldots,\lambda_n$ in L and elements $\alpha_1,\ldots,\alpha_m$ in $\bar{Q}$. Assume: $\lambda_1,\ldots,\lambda_n$ are Q-linearly independent and

$\alpha_1,\ldots,\alpha_m$ are Q-linearly independent -- then

$$\operatorname{trdeg}_Q Q(\lambda_1,\ldots,\lambda_n, e^{\alpha_1},\ldots, e^{\alpha_m}) = m + n,$$

thus

$$\{\lambda_1,\ldots,\lambda_n, e^{\alpha_1},\ldots, e^{\alpha_m}\}$$

is algebraically independent over Q (cf. §46, #9).

PROOF Define $\beta_j : j = 1,\ldots, m + n$ by $\beta_j = \lambda_j$ for $j = 1,\ldots,n$ and $\beta_{j+n} = \alpha_j$ for $j = 1,\ldots,m$. Claim:

$$\beta_1,\ldots,\beta_{m+n}$$

is Q-linearly independent. For suppose that

$$q_1\beta_1 + \cdots + q_{m+n}\beta_{m+n} = 0$$

is a rational dependence relation, hence

$$q_1\lambda_1 + \cdots + q_n\lambda_n + q_{n+1}\alpha_1 + \cdots + q_{m+n}\alpha_m = 0.$$

From the definitions,

$$q_{n+1}\alpha_1 + \cdots + q_{m+n}\alpha_m$$

is an algebraic number, i.e., is in $\bar{Q}$. Accordingly, thanks to inhomogeneous Baker,

$$q_1 = 0,\ldots, q_n = 0 \text{ and } q_{n+1}\alpha_1 + \cdots + q_{m+n}\alpha_m = 0.$$

But $\alpha_1,\ldots,\alpha_m$ are Q-linearly independent. Therefore

$$q_{n+1} = 0,\ldots, q_{m+n} = 0,$$

hence the claim. Now apply Schanuel: The transcendence degree over Q of

$$Q(\beta_1,\ldots,\beta_{m+n}, e^{\beta_1},\ldots, e^{\beta_{m+n}})$$

is $\geq m + n$. To cut this down, note that

$$\beta_{1+n} = \alpha_1,\ldots, \beta_{m+n} = \alpha_m$$

are algebraic, as are

$$e^{\beta_1} = e^{\lambda_1}, \ldots, e^{\beta_n} = e^{\lambda_n}.$$

So we are left with

$$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\lambda_1, \ldots, \lambda_n, e^{\alpha_1}, \ldots, e^{\alpha_m}) \geq m + n,$$

which suffices.

<u>11:</u> THEOREM (Admit SCHC) If $\alpha \neq 0,1$ is algebraic and if $1, \beta_1, \ldots, \beta_n \in \bar{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then the numbers $\operatorname{Log} \alpha$ and

$$\alpha^{\beta_1}, \ldots, \alpha^{\beta_n} \quad \text{(principal powers)}$$

are algebraically independent over $\mathbb{Q}$, hence are transcendental (cf. §31, #17).

PROOF To begin with,

$$\beta_1 \operatorname{Log} \alpha, \ldots, \beta_n \operatorname{Log} \alpha, \operatorname{Log} \alpha$$

are $\mathbb{Q}$-linearly independent, thus the transcendence degree of the field

$$\mathbb{Q}(\beta_1 \operatorname{Log} \alpha, \ldots, \beta_n \operatorname{Log} \alpha, \operatorname{Log} \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}, \alpha)$$

is $\geq n + 1$ (quote Schanuel). But

$$\beta_1 = (\beta_1 \operatorname{Log} \alpha)(\operatorname{Log} \alpha)^{-1}, \ldots$$

$\Rightarrow$

$$\begin{aligned} &\mathbb{Q}(\beta_1 \operatorname{Log} \alpha, \ldots, \beta_n \operatorname{Log} \alpha, \operatorname{Log} \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}, \alpha) \\ &\qquad = \mathbb{Q}(\beta_1, \ldots, \beta_n, \operatorname{Log} \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}, \alpha) \end{aligned}$$

$\Rightarrow$

$$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\beta_1, \ldots, \beta_n, \operatorname{Log} \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}, \alpha)$$

$$= \operatorname{trdeg}_Q Q(\operatorname{Log} \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n})$$

$$\geq n + 1$$

$\Rightarrow$

$$\operatorname{trdeg}_Q Q(\operatorname{Log} \alpha, \alpha^{\beta_1}, \ldots, \alpha^{\beta_n}) = n + 1,$$

from which the algebraic independence over Q of $\operatorname{Log} \alpha$ and

$$\alpha^{\beta_1}, \ldots, \alpha^{\beta_n}.$$

12: N.B. In #11, take $n = 1$ and assume that $\beta \notin Q$ -- then $\operatorname{Log} \alpha$ and α^{β} are algebraically independent over Q.

13: THEOREM (Admit SCHC) If $\alpha \neq 0,1$ is algebraic and if $\beta \in \bar{Q}$ has degree $d \geq 2$, then

$$\operatorname{trdeg}_Q Q(\operatorname{Log} \alpha, \alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}}) = d.$$

PROOF First of all, $1, \beta, \ldots, \beta^{d-1}$ are linearly independent over Q. In fact, the minimal polynomial of β has degree $d \geq 2$, whereas a rational dependence relation

$$q + q_1 \beta + \cdots + q_{d-1} \beta^{d-1} = 0$$

leads to a contradiction upon consideration of

$$P(X_0, X_1, \ldots, X_{d-1})$$

$$= X_0 + q_1 X_1 + \cdots + q_{d-1} X^{d-1}.$$

So, applying #11, the numbers $\operatorname{Log} \alpha$ and

$$\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}} \quad \text{(principal powers)}$$

are algebraically independent over Q, from which the result.

[Note: It is not necessary to appeal to SCHC when d = 2 or d = 3 as these special cases have been resolved. For a case in point, take

$$d = 3, \ \alpha = 2, \ \beta = 2^{1/3}.$$

Then

$$\ell n(2), \ 2^{2^{1/3}}, \ 2^{2^{2/3}}$$

are algebraically independent over Q.]

14: REMARK It can be shown that unconditionally

$$\operatorname{trdeg}_Q Q(\alpha^{\beta},\ldots,\alpha^{\beta^{d-1}}) \geq \left\lfloor \frac{d+1}{2} \right\rfloor,$$

the symbol on the right standing for the greatest integer less than or equal to $\frac{d+1}{2}$.

15: THEOREM (Admit SCHC) If $x_1,\ldots,x_n$ are complex numbers linearly independent over Q and if y is a transcendental number, then

$$\operatorname{trdeg}_Q Q(e^{x_1},\ldots,e^{x_n}, e^{x_1 y},\ldots,e^{x_n y}) \geq n - 1.$$

PROOF Order the numbers $x_1,\ldots,x_n$ in such a way that a basis for the Q-vector space generated by

$$\{x_1,\ldots,x_n, x_1y,\ldots,x_ny\}$$

is

$$\{x_1,\ldots,x_n, x_1y,\ldots,x_my\} \quad (0 \leq m \leq n).$$

Claim:

$$\operatorname{trdeg}_Q Q(x_1,\ldots,x_n,y) \leq m + 1.$$

For y is transcendental (by hypothesis), so there is a transcendence basis for

$$Q(x_1,\ldots,x_n,y)$$

which is

$$\{x_{i_1},\ldots,x_{i_k},y\}$$

with

$$1 \leq i_1 < i_2 < \cdots < i_k \leq n.$$

Then

$$x_1,\ldots,x_n,x_{i_1}y,\ldots,x_{i_k}y$$

are Q-linearly independent, thus

$$k + n \leq m + n \Rightarrow k \leq m \Rightarrow k + 1 \leq m + 1,$$

which establishes the claim. Next, invoking SCHC,

$$\operatorname{trdeg}_Q Q(x_1,\ldots,x_n,\ x_1y,\ldots,x_my,$$

$$e^{x_1},\ldots,e^{x_n},\ e^{x_1y},\ldots,e^{x_my}) \geq n + m$$

$$\Rightarrow$$

$$\operatorname{trdeg}_Q Q(x_1,\ldots,x_n,x_1y,\ldots,x_ny,$$

$$e^{x_1},\ldots,e^{x_n},\ e^{x_1y},\ldots,e^{x_ny}) \geq n + m.$$

Taking into account the claim, it follows that at least n - 1 of the numbers e^{x_i}, e^{x_iy} (i = 1,...,n) are algebraically independent.

16: N.B. Specialized to the case n = 2, the upshot is that at least one of the numbers

$$e^{x_1}, e^{x_2}, e^{x_1 y}, e^{x_2 y}$$

is transcendental.

<u>17:</u> IMPLICATION

$$\text{SCHC} \Rightarrow \text{4EC}.$$

<u>18:</u> RAPPEL (4EC) Let $\{x_1, x_2\}$ and $\{y_1, y_2\}$ be two Q-linearly independent sets of complex numbers -- then

$$\{x_1 y_1, x_1 y_2, x_2 y_1, x_2 y_2\} \subset L,$$

thus at least one of the numbers

$$e^{x_1 y_1}, e^{x_1 y_2}, e^{x_2 y_1}, e^{x_2 y_2}$$

is transcendental.

When dealing with 4EC, there is a little trick that can be used to advantage, viz. let

$$w_1 = x_1 y_1, \ w_2 = x_2 y_1, \ z_1 = y_2/y_1, \ z_2 = 1.$$

Then

$$w_1 z_1 = x_1 y_2, \ w_1 z_2 = x_1 y_1, \ w_2 z_1 = x_2 y_2, \ w_2 z_2 = x_2 y_1.$$

So the list

$$e^{x_1 y_1}, e^{x_1 y_2}, e^{x_2 y_1}, e^{x_2 y_2}$$

becomes the list

$$e^{w_1 z_1}, e^{w_1 z_2}, e^{w_2 z_1}, e^{w_2 z_2},$$

i.e., the list

$$e^{w_1 z_1},\ e^{w_1},\ e^{w_2 z_1},\ e^{w_2},$$

i.e., the list

$$e^{w_1},\ e^{w_2},\ e^{w_1 z_1},\ e^{w_2 z_1},$$

i.e., the list

$$e^{w_1},\ e^{w_2},\ e^{w_1 (y_2/y_1)},\ e^{w_2 (y_2/y_1)},$$

i.e., the list

$$e^{w_1},\ e^{w_2},\ e^{w_1 y},\ e^{w_2 y},$$

where

$$y = y_2/y_1.$$

In order to utilize #16, it is necessary that y be transcendental.

Case 1: $y \notin L^*$ -- then y is transcendental (otherwise, y would be algebraic, while $\bar{Q} \subset L^*$).

Case 2: $y \in L^*$ -- then #16 need not be applicable but in view of §43, #8,

$$\{x_1 y_1,\ x_1 y_2,\ x_2 y_1,\ x_2 y_2\} \not\subset L,$$

thus at least one of the numbers

$$e^{x_1 y_1},\ e^{x_1 y_2},\ e^{x_2 y_1},\ e^{x_2 y_2}$$

is transcendental.

[Note: In the reference to §43, #8, take $\gamma = 1$ and replace x_2/x_1 by y_2/y_1 (as is certainly permissible).]

19: RAPPEL (Admit S4EC) Let $w \in C - \{0\}$. Assume: $|w|$ is algebraic -- then e^w is transcendental (cf. §45, #11).

[Drop S4EC, impose instead SCHC, and bear in mind that the crux is when $w \notin R \cup \sqrt{-1}\, R$, thus $w, \bar{w}$ are Q-linearly independent, so

$$\mathrm{trdeg}_Q\, Q(w, \bar{w}, e^w, e^{\bar{w}}) \geq 2.$$

If e^w was algebraic, then $e^{\bar{w}} = \overline{e^w}$ would be too, reducing matters to

$$\mathrm{trdeg}_Q\, Q(w,\bar{w}) \geq 2,$$

which is false since $|w| \in \bar{Q} \Rightarrow |w|^2 \in \bar{Q} = w\bar{w} \in \bar{Q}$.]

<u>20:</u> NOTATION Write

$$\underline{x} = (x_1,\ldots,x_n)$$

and

$$e^{\underline{x}} = (e^{x_1},\ldots,e^{x_n}).$$

<u>21:</u> <u>N.B.</u> SCHC can thus be abbreviated to

$$\mathrm{trdeg}_Q\, Q(\underline{x},e^{\underline{x}}) \geq n.$$

Consider a Q-linear combination

$$x_{n+1} = q_1x_1 + \cdots + q_nx_n.$$

Let M be a nonzero integer such that Mq_k is an integer for all $k = 1,\ldots,n$ and assume with out loss of generality that

$$Mq_1,\ldots,Mq_t$$

are nonnegative and

$$Mq_{t+1},\ldots,Mq_n$$

are negative for some $0 \leq t \leq n$. Let

$$P(X_1,\ldots,X_{n+1})$$

$$= \prod_{k=1}^{t} X_k^{Mq_k} - X_{n+1}^{M} \prod_{k=t+1}^{n} X_k^{-Mq_k} .$$

Then

$$P(e^{x_1},\ldots,e^{x_{n+1}})$$

$$= \prod_{k=1}^{t} e^{x_k Mq_k} - e^{x_{n+1}M} \prod_{k=t+1}^{n} e^{-x_k Mq_k}$$

$$= \prod_{k=1}^{t} e^{M(q_k x_k)} - e^{M(q_1 x_1+\cdots+q_n x_n)} \prod_{k=t+1}^{n} e^{-M(q_k x_k)}$$

$$= \exp(\sum_{k=1}^{t} Mq_k x_k) - \exp(M(\sum_{k=1}^{t} Mq_k x_k + \sum_{k=t+1}^{n} Mq_k x_k))\exp(-\sum_{k=t+1}^{n} Mq_k x_k)$$

$$= \exp(\sum_{k=1}^{t} Mq_k x_k)(1 - \exp(\sum_{k=t+1}^{n} Mq_k x_k)\exp(-\sum_{k=t+1}^{n} Mq_k x_k))$$

$$= \exp(\sum_{k=1}^{t} Mq_k x_k)(1 - \exp(\sum_{k=t+1}^{n} Mq_k x_k - \sum_{k=t+1}^{n} Mq_k x_k))$$

$$= \exp(\sum_{k=1}^{t} Mq_k x_k)(1 - 1) = 0.$$

<u>22:</u> SCHOLIUM The collection

$$e^{x_1},\ldots,e^{x_n},e^{x_{n+1}}$$

is Q-algebraically dependent.

So adding x_{n+1}, $e^{x_{n+1}}$ to

$$Q(x_1,\ldots,x_n, e^{x_1},\ldots,e^{x_n})$$

does not change the transcendence degree.

23: NOTATION Given complex numbers $x_1,\ldots,x_n$, let

$$\mathrm{lindim}_Q\, \underline{x}$$

denote the linear dimension of the vector space over Q spanned by $x_1,\ldots,x_n$.

24: CONJECTURE (SCHC) $\forall\, \underline{x}$,

$$\mathrm{trdeg}_Q\, Q(\underline{x},e^{\underline{x}}) \geq \mathrm{lindim}_Q\, \underline{x}.$$

To say that $\underline{x}$ is a counterexample to SCHC means that $x_1,\ldots,x_n$ are linearly independent over Q but

$$\mathrm{trdeg}_Q\, Q(\underline{x},e^{\underline{x}}) < n.$$

25: LEMMA If there is a counterexample to SCHC, then there is a dense subset of C^n comprised of counterexamples.

PROOF If $\underline{x}$ is a counterexample to SCHC, then for any nonzero $q_1,\ldots,q_n$ in Q, $q_1x_1,\ldots,q_nx_n$ is also a counterexample.

26: NOTATION Given $\underline{x}$, put

$$\delta(\underline{x}) = \mathrm{trdeg}_Q\, Q(\underline{x},e^{\underline{x}}) - \mathrm{lindim}_Q\, \underline{x},$$

the predimension of $\underline{x}$.

27: REMARK SCHC is thus the claim that $\forall\ \underline{x}$,

$$\delta(\underline{x}) \geq 0,$$

so a counterexample to Schanuel is an $\underline{x}$ with

$$\delta(\underline{x}) < 0.$$

If

$$\delta(\underline{x}) < -1,$$

then for any complex number C,

$$\delta(\underline{x}C) \leq \delta(\underline{x}) + 1 < 0,$$

leading therefore to continuum-many counterexamples.

28: LEMMA $\forall\ n \in \mathbb{N}$, the set $X_n \subset C^n$ of n-tuples which do not satisfy Schanuel's condition is first category and of Lebesgue measure 0.

APPENDIX

THEOREM (Admit SCHC) Let $\alpha \neq 1$ be a positive algebraic number and let β be a positive irrational number. Assume:

$$\alpha^{\alpha^{\beta}} = \beta.$$

Then β is transcendental.

PROOF Suppose to the contrary that β is algebraic, so by Gelfond-Schneider, α^{β} is transcendental. Claim: $1, \beta, \alpha^{\beta}$ are Q-linearly independent. For suppose that

$$r + s\beta + t\alpha^{\beta} = 0$$

is a rational dependence relation:

$$r + s\beta \in \bar{Q},\ t\alpha^{\beta} \notin \bar{Q} \quad (\text{if } t \neq 0)$$

$$\Rightarrow t = 0 \Rightarrow r,s = 0 \quad (\beta \in P).$$

Now multiply $1,\beta,\alpha^{\beta}$ by $\ell n(\alpha) \neq 1$, hence

$$\ell n(\alpha),\ \beta\ell n(\alpha),\ \alpha^{\beta}\ell n(\alpha)$$

are also Q-linearly independent, hence by SCHC,

$$\operatorname{trdeg}_{Q} Q(\ell n(\alpha),\ \beta\ell n(\alpha),\ \alpha^{\beta}\ell n(\alpha),\ \alpha,\ \alpha^{\beta},\ \alpha^{\alpha^{\beta}}) \geq 3,$$

i.e.,

$$\operatorname{trdeg}_{Q} Q(\ell n(\alpha),\ \beta\ell n(\alpha),\ \alpha^{\beta}\ell n(\alpha),\ \alpha^{\beta}) \geq 3,$$

i.e.,

$$\operatorname{trdeg}_{\bar{Q}} \bar{Q}(\ell n(\alpha),\ \beta\ell n(\alpha),\ \alpha^{\beta}\ell n(\alpha),\ \alpha^{\beta}) \geq 3.$$

But

$$\operatorname{trdeg}_{\bar{Q}} \bar{Q}(\ell n(\alpha),\ \beta\ell n(\alpha),\ \alpha^{\beta}\ell n(\alpha),\ \alpha^{\beta})$$

$$= \operatorname{trdeg}_{\bar{Q}} \bar{Q}(\ell n(\alpha),\ \alpha^{\beta}) \leq 2.$$

Contradiction.

§48. SCHC: *NUMERICAL EXAMPLES*

Unless stipulated to the contrary, throughout the § SCHC is in force.

<u>1:</u> EXAMPLE The numbers e and e^e are algebraically independent over Q.

[Take $x_1 = 1$, $x_2 = e$ -- then

$$\text{trdeg}_Q\ Q(1, e, e^1, e^e) \geq 2,$$

i.e.,

$$\text{trdeg}_Q\ Q(e, e^e) \geq 2.]$$

<u>2:</u> EXAMPLE The numbers $\ell n(2)$ and $2^{\ell n(2)}$ are algebraically independent over Q.

[Take $x_1 = \ell n(2)$, $x_2 = (\ell n(2))^2$ -- then

$$\text{trdeg}_Q\ Q(\ell n(2), (\ell n(2))^2, 2, 2^{\ell n(2)}) \geq 2,$$

i.e.,

$$\text{trdeg}_Q\ Q(\ell n(2), 2^{\ell n(2)}) \geq 2.]$$

<u>3:</u> EXAMPLE The numbers $\ell n(2)$ and $\ell n(3)$ are algebraically independent over Q.

[Take $x_1 = \ell n(2)$, $x_2 = \ell n(3)$ -- then

$$\text{trdeg}_Q\ Q(\ell n(2), \ell n(3), 2, 3) \geq 2,$$

i.e.,

$$\text{trdeg}_Q\ Q(\ell n(2), \ell n(3)) \geq 2.]$$

[Note: Recall that $\frac{\ell n(3)}{\ell n(2)}$ is transcendental (cf. §24, #10), hence irrational.]

4: EXAMPLE The numbers e and π are algebraically independent over Q.

[Take $x_1 = 1$, $x_2 = \sqrt{-1}\pi$ -- then

$$\operatorname{trdeg}_Q Q(1, \sqrt{-1}\,\pi, e^1, e^{\sqrt{-1}\,\pi} = -1) \geq 2,$$

i.e.,

$$\operatorname{trdeg}_Q Q(\sqrt{-1}\,\pi, e) \geq 2.$$

Therefore e and $\sqrt{-1}\,\pi$ are algebraically independent over Q. Suppose now that e and π are algebraically dependent over Q, so there exists $P(X,Y) \in Q[X,Y]$ nonzero such that $P(e,\pi) = 0$. Let $G(X,Y) = P(X, -\sqrt{-1}\,Y)$ and $H(X,Y) = \overline{P(X, -\sqrt{-1}\,Y)}$ -- then

$$G(e, \sqrt{-1}\,\pi) = P(e, (-\sqrt{-1})\sqrt{-1}\,\pi) = P(e,\pi) = 0$$

and

$$H(e, \sqrt{-1}\,\pi) = \overline{P(e, (-\sqrt{-1})\sqrt{-1}\,\pi)} = \overline{P(e,\pi)} = \bar{0} = 0.$$

Consequently

$$(G + H)(e, \sqrt{-1}\,\pi) = 0.$$

But G + H is a nonzero polynomial with rational coefficients, thereby contradicting the algebraic independence over Q of e and $\sqrt{-1}\,\pi$.]

[Three applications:

- $e + \pi$ is transcendental.

[Suppose $e + \pi = \alpha \in \bar{Q}$. Form

$$P(X,Y) = X + Y - \alpha,$$

an element of $\bar{Q}[X,Y]$ -- then

$$P(e,\pi) = e + \pi - \alpha = 0.$$

Contradiction.]

- $e\pi$ is transcendental.

[Suppose $e\pi = \alpha \in \bar{Q}$. Form

$$P(X,Y) = XY - \alpha,$$

an element of $\bar{Q}[X,Y]$ -- then

$$P(e,\pi) = e\pi - \alpha = 0.$$

Contradiction.]

- e/π is transcendental (hence π/e is too).

[Suppose $e/\pi = \alpha \in \bar{Q}$. Form

$$P(X,Y) = X - \alpha Y,$$

an element of $\bar{Q}[X,Y]$ -- then

$$P(e,\pi) = e - \alpha\pi = \alpha\pi - \alpha\pi = 0.$$

Contradiction.]]

5: REMARK It can be shown that unconditionally at least one of the following statements is true.

- The number e^{π^2} is transcendental.
- The numbers e and π are algebraically independent over Q.

[Note: It is unknown whether e^{π^2} is even irrational.]

6: EXAMPLE The numbers e, $\ell n(2)$, and π are algebraically independent over Q.

[Take $x_1 = 1$, $x_2 = \ell n(2)$, $x_3 = \sqrt{-1}\,\pi$ to arrive at

$$\operatorname{trdeg}_Q Q(1, \ell n(2), \sqrt{-1}\,\pi, e, 2, -1) \geq 3.]$$

[Note: The numbers 1, $\ell n(2)$, $\sqrt{-1}\,\pi$ are Q-linearly independent (because $\ell n(2)$ is irrational (cf. §10, #5).]

7: LEMMA The eight numbers

$$1,\ \sqrt{-1}\,\pi,\ \pi^2,\ e,\ e^2,\ \ln(2),\ 2^{1/3}\ln(2),\ 4^{1/3}\ln(2)$$

are $\mathbb{Q}$-linearly independent.

PROOF The numbers $\sqrt{-1}\,\pi$, e, $\ln(2)$ are algebraically independent over $\mathbb{Q}$, hence are algebraically independent over $\bar{\mathbb{Q}}$ (cf. §20, #7). Consider now a rational dependence relation

$$A + B\sqrt{-1}\,\pi + C\pi^2 + De + Fe^2 + G\ln(2) + H2^{1/3}\ln(2) + K4^{1/3}\ln(2) = 0.$$

Define a polynomial $P \in \bar{\mathbb{Q}}[X,Y,Z]$ by the preseription

$$\begin{aligned} P(X,Y,Z) &= A + BX - CX^2 + DY + FY^2 \\ &\quad + GZ + H2^{1/3}Z + K4^{1/3}Z. \end{aligned}$$

Then

$$\begin{aligned} P(\sqrt{-1}\,\pi,\ e,\ \ln(2)) &= A + B\sqrt{-1}\,\pi + C\pi^2 + De + Fe^2 \\ &\quad + G\ln(2) + H2^{1/3}\ln(2) + K4^{1/3}\ln(2) = 0. \end{aligned}$$

Therefore

$$A = B = C = D = F = G = H = K = 0.$$

8: APPLICATION The eight numbers

$$e,\ \pi,\ e^e,\ e^{e^2},\ e^{\pi^2},\ 2^{2^{1/3}},\ 2^{2^{2/3}},\ \ln(2)$$

are algebraically independent over $\mathbb{Q}$.

[Consider

$$1,\ \sqrt{-1}\,\pi,\ \pi^2,\ e,\ e^2,\ \ln(2),\ 2^{1/3}\ln(2),\ 4^{1/3}\ln(2),$$

$$e,\ -1,\ e^{\pi^2},\ e^e,\ e^{e^2},\ 2,\ 2^{2^{1/3}},\ 2^{2^{2/3}}.]$$

The next objective is #14 infra, the verification of which proceeds in a series of steps.

9: LEMMA Suppose that $x_1,\ldots,x_n$ is an algebraically independent set of positive real numbers -- then $x_1,\ldots,x_n$ is multiplicatively independent (cf. §34, Appendix).

10: EXAMPLE The numbers 2, 3, π, and $\ln(2)$ are multiplicatively independent:

$$2^a 3^b \pi^c (\ln(2))^d = 1 \qquad (a,b,c,d \in \mathbb{Z})$$

$$\Rightarrow a = b = c = d = 0.$$

[The numbers π and $\ln(2)$ are algebraically independent over $\mathbb{Q}$ (cf. #6). This said, suppose that

$$2^a 3^b \pi^c (\ln(2))^d = 1 \qquad (a,b,c,d \in \mathbb{Z}),$$

take for sake of argument $c \geq 0$, $d \geq 0$, and introduce the polynomial

$$P(X,Y) = 2^a 3^b X^c Y^d - 1.$$

Then

$$P(\pi,\ln(2)) = 2^a 3^b \pi^c (\ln(2))^d - 1$$

$$\Rightarrow c = 0,\ d = 0 \Rightarrow 2^a 3^b - 1 = 0 \Rightarrow a = 0,\ b = 0.]$$

11: LEMMA Suppose that $x_1,\ldots,x_n$ is a multiplicatively independent set of positive real numbers -- then the set $\ln(x_1),\ldots,\ln(x_n)$ is $\mathbb{Q}$-linearly independent.

12: EXAMPLE The numbers $\ln(\pi)$, $\ln(2)$, $\ln(3)$, $\ln(\ln(2))$ are $\mathbb{Q}$-linearly independent (cf. #10).

Therefore the numbers

$$\sqrt{-1}\,\pi,\ \ell n(\pi),\ \ell n(2),\ \ell n(3),\ \ell n(\ell n(2))$$

are Q-linearly independent (consider real and imaginary parts).

Now use SCHC to arrive at

$$\operatorname{trdeg}_Q Q(\sqrt{-1}\,\pi,\ \ell n(\pi),\ \ell n(2),\ \ell n(3),\ \ell n(\ell n(2)),$$
$$-1,\ \pi,\ 2,\ 3,\ \ell n(2)) \geq 5,$$

from which the conclusion that

$$\pi,\ \ell n(\pi),\ \ell n(2),\ \ell n(3),\ \ell n(\ell n(2))$$

are algebraically independent over Q.

Next the numbers

$$1,\ \sqrt{-1}\,\pi,\ \ell n(\pi),\ \ell n(2),\ \ell n(3),\ \ell n(\ell n(2))$$

are Q-linearly independent, thus invoking SCHC once again gives

$$\operatorname{trdeg}_Q Q(1,\ \sqrt{-1}\,\pi,\ \ell n(\pi),\ \ell n(2),\ \ell n(3),\ \ell n(\ell n(2)),$$
$$e,\ -1,\ \pi,\ 2,\ 3,\ \ell n(2)) \geq 6,$$

so

$$e,\ \pi,\ \ell n(\pi),\ \ell n(2),\ \ell n(3),\ \ell n(\ell n(2))$$

are algebraically independent over Q.

<u>13:</u> LEMMA The seventeen numbers

$$1,\ \sqrt{-1}\,\pi,\ \pi,\ \ell n(\pi),\ e,\ e\ell n(\pi),\ \pi\ell n(\pi),\ \ell n(2)$$
$$\pi\ell n(2),\ e\ell n(2),\ \sqrt{-1}\,\ell n(2),\ \sqrt{-1},\ \sqrt{-1}\,\ell n(\pi),\ \ell n(3)$$
$$\ell n(\ell n(2)),\ (\ell n(3))(\ell n(\ell n(2))),\ \sqrt{2}\,\ell n(2)$$

are Q-linearly independent (cf. #7).

14: THEOREM (Waldschmidt's menagerie) (Admit SCHC) The seventeen numbers

$$\pi, \ \ln(\pi), \ e, \ \ln(2), \ \ln(3), \ \ln(\ln(2)), \ e^{\pi}, \ e^{e}$$

$$\pi^{e}, \ \pi^{\pi}, \ 2^{\pi}, \ 2^{e}, \ 2^{\sqrt{-1}}, \ e^{\sqrt{-1}}, \ \pi^{\sqrt{-1}}, \ (\ln(2))^{\ln(3)}, \ 2^{\sqrt{2}}$$

are algebraically independent over Q.

15: REMARK e^{π} is transcendental (unconditionally) (cf. §20, #10) but it is not even known whether e^{e}, π^{π}, and π^{e} are irrational, let alone transcendental.

16: MISCELLANEA (Admit SCHC)

- $\sqrt{2}^{\sqrt{2}^{\sqrt{2}}}$ is transcendental.
- $\sqrt{-1}^{\sqrt{-1}^{\sqrt{-1}}}$ is transcendental.
- $\sqrt{-1}^{e^{\pi}}$ is transcendental.

§49. *THE ZERO CONDITION*

To begin with:

1: THE FUNDAMENTAL CONJECTURE (FDC) Let $\lambda_1,\ldots,\lambda_d$ be elements of L which are linearly independent over Q -- then $\lambda_1,\ldots,\lambda_d$ are algebraically independent over Q, hence are algebraically independent over $\bar{Q}$ (cf. §20, #7).

[Note: To appreciate how far away this conjecture lies, there is no known example of a Q-linearly independent pair $\{\lambda_1,\lambda_2\}$ which is algebraically independent over Q.]

2: N.B. Recall that the fundamental conjecture is implied by SCHC (cf. §47, #7).

3: NOTATION Fix $P \in Q[X_1,\ldots,X_d]$, put

$$Z(P) = \{\underline{x} \in C^d : P(\underline{x}) = 0\}.$$

4: DEFINITION A nonzero polynomial $P \in Q[X_1,\ldots,X_d]$ is said to satisfy the zero condition if

$$Z(P) \cap L^d = \bigcup_V V \cap L^d,$$

where V ranges over the C-vector subspaces of C^d rational over Q and contained in $Z(P)$.

5: EXAMPLE Suppose that

$$P(X_1,\ldots,X_d) = C_1X_1 + \cdots + C_dX_d,$$

where $C_1,\ldots,C_d \in Q$ -- then P satisfies the zero condition.

6: LEMMA If every nonzero $P \in Q[X_1,\ldots,X_d]$ satisfies the zero condition, then the fundamental conjecture is in force.

PROOF To get a contradiction, assume that $\lambda_1,\ldots,\lambda_d$ are linearly independent over Q but not algebraically independent over Q, hence there exists a nonzero polynomial P in $Q[X_1,\ldots,X_d]$ such that $P(\lambda_1,\ldots,\lambda_d) = 0$, hence there is a C-vector subspace V of C^d rational over Q and contained in $Z(P)$ with

$$\underline{\lambda} = (\lambda_1,\ldots,\lambda_d) \in V \cap L^d.$$

Using the rationality of V over Q, write V as the intersection of hyperplanes defined by linear forms with coefficients in Q (cf. §37, #2). Denoting by

$$\{(z_1,\ldots,z_d) \in C^d : \beta_1 z_1 + \cdots + \beta_d z_d = 0 \quad (\beta_1,\ldots,\beta_d \text{ in } Q)\}$$

a typical such hyperplane, we then have

$$\beta_1\lambda_1 + \cdots + \beta_d\lambda_d = 0,$$

thus

$$\beta_1 = 0,\ldots,\beta_d = 0$$

and so $V = \{0\}$. But

$$(\lambda_1,\ldots,\lambda_d) \in V \cap L^d = \{0\} \cap L^d = (0,\ldots,0).$$

7: REMARK It is also true that the fundamental conjecture implies that every nonzero $P \in Q[X_1,\ldots,X_d]$ satisfies the zero condition.

Our objective now will be to establish the four exponentials conjecture modulo yet another conjecture.

[Note: It was shown already in §47, #17 that

$$\text{SCHC} \Rightarrow \text{4EC.}]$$

8: CONJECTURE Work in C^4 and define $P \in Q[X_1,X_2,X_3,X_4]$ by

$$P(X_1,X_2,X_3,X_4) = X_1X_4 - X_2X_3.$$

Then P satisfies the zero condition.

9: CONJECTURE Consider a 2×2 matrix M with entries in L:

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix}.$$

Suppose that its rows are Q-linearly independent and its columns are Q-linearly independent -- then

$$\text{rank } M = 2 \quad (\text{cf. } §44, \#2).$$

10: N.B. The claim now is that

$$\#8 \Rightarrow \#9.$$

Here is another way to phrase it: If

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix}$$

is a 2×2 matrix with entries in L and if

$$\text{rank } M = 1,$$

then either its rows are Q-linearly dependent or its columns are Q-linearly dependent.

11: N.B. The condition

$$\operatorname{rank} M = 1$$

implies that

$$\det M = \lambda_{11}\lambda_{22} - \lambda_{12}\lambda_{21}$$

$$= 0.$$

Per #8, take for P the polynomial

$$P(X_1,X_2,X_3,X_4) = X_1X_4 - X_2X_3.$$

Substitute in

$$X_1 = \lambda_{11},\ X_4 = \lambda_{22},\ X_2 = \lambda_{12},\ X_3 = \lambda_{21},$$

thus

$$P(\lambda_{11},\lambda_{12},\lambda_{21},\lambda_{22}) = \lambda_{11}\lambda_{22} - \lambda_{12}\lambda_{21}$$

$$= 0$$

and so

$$(\lambda_{11},\lambda_{12},\lambda_{21},\lambda_{22}) \in Z(P) \cap L^4.$$

But

$$Z(P) \cap L^4 = \bigcup_{V} V \cap L^4.$$

Choose V: A C-vector subspace of C^4 rational over Q and contained in Z(P) with

$$(\lambda_{11},\lambda_{12},\lambda_{21},\lambda_{22}) \in V \cap L^4.$$

<u>12:</u> LEMMA $\exists$ $(a:b) \in P^1(Q)$ such that V is included either in the plane

$*_1: \{(z_1,z_2,z_3,z_4) \in C^4 : az_1 = bz_2,\ az_3 = bz_4\}$

or in the plane

$*_2: \{(z_1,z_2,z_3,z_4) \in C^4 : az_1 = bz_3,\ az_2 = bz_4\}$.

[Note: See the Appendix for the verification.]

<u>13:</u> <u>N.B.</u> $(a:b)$ is the class of (a,b) in the projective line $P^1(Q)$.

Return to

$$M = \begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix}.$$

- Assume $*_1$ in #12 and work with the columns of M:

$$\begin{bmatrix} \lambda_{11} \\ \lambda_{21} \end{bmatrix}, \quad \begin{bmatrix} \lambda_{12} \\ \lambda_{22} \end{bmatrix}.$$

Then

$$\left[\begin{array}{l} a\lambda_{11} = b\lambda_{12} \\ a\lambda_{21} = b\lambda_{22}. \end{array}\right.$$

Form now

$$-\ a \begin{bmatrix} \lambda_{11} \\ \lambda_{21} \end{bmatrix} + b \begin{bmatrix} \lambda_{12} \\ \lambda_{22} \end{bmatrix}$$

or still

$$\begin{bmatrix} -a\lambda_{11} + b\lambda_{12} \\ \\ -a\lambda_{21} + b\lambda_{22} \end{bmatrix} = \begin{bmatrix} -b\lambda_{12} + b\lambda_{12} \\ \\ -b\lambda_{22} + b\lambda_{22} \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since $(a{:}b) \in P^1(C)$, the columns of M are linearly dependent and the four exponentials conjecture is thereby established.

- Assume $*_2$ in #12 and work with the rows of M:

$$[\lambda_{11}\ \lambda_{12}]\ ,\ \ [\lambda_{21}\ \lambda_{22}].$$

This time

$$\begin{cases} a\lambda_{11} = b\lambda_{21} \\ \\ a\lambda_{12} = b\lambda_{22} \end{cases}$$

and one can consider

$$-\,a[\lambda_{11}\ \lambda_{12}] + b[\lambda_{21}\ \lambda_{22}].$$

It is not necessary to utilize #8 in order to arrive at a restricted but unconditional result, the idea being to reduce the elements $\underline{\lambda}$ in $Z(P) \cap L^4$ for which there is a V: A C-vector subspace of C^4 rational over Q and contained in $Z(P)$ with $\underline{\lambda} \in V \cap L^4$.

<u>13:</u> THEOREM Take a

$$\underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in Z(P) \cap L^4.$$

Then either $\underline{\lambda} \in V$ for some V per supra or else

$$\operatorname{trdeg}_{Q} Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \geq 2.$$

<u>14:</u> SCHOLIUM The statement of the four exponentials conjecture holds true for the set of those

$$\underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in Z(P) \cap L^4$$

with the property that

$$\operatorname{trdeg}_{Q} Q(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = 1.$$

[Note: The point, of course, is that for this set of λ, #12 is applicable.]

<u>15:</u> <u>N.B.</u> The λ_i $(i = 1,2,3,4)$ are transcendental (if not zero).

APPENDIX

The issue is the validity of #12. Write

$$\left[\begin{array}{l} *_1 = W_1(a:b) \\ \\ *_2 = W_2(a:b) \end{array}\right.$$

and note that

$$\left[\begin{array}{l} W_1(a:b) \\ \\ W_2(a:b) \end{array}\right. \subset Z(P).$$

Matters are trivial if V is contained in

$$W_1(0:1) \text{ or } W_1(1:0) \text{ or } W_2(0:1) \text{ or } W_2(1:0).$$

Assume, therefore, that there exists $v:(w,x,y,z) \in V$ such that $wxyz \neq 0$. Since $wz = xy$, we have $(x:w) = (z:y)$ and $(y:w) = (z:x)$, the claim then being that the supposition

$$V \not\subset W_1(x:w) \text{ and } V \not\subset W_2(y:w)$$

leads to a contradiction. Choose $v' = (w',x',y',z')$ in V which does not belong to

$$W_1(0:1) \cup W_1(1:0) \cup W_2(0:1) \cup W_2(1:0) \cup W_1(x:w) \cup W_2(y:w).$$

Accordingly

$$w'x'y'z' \neq 0.$$

Moreover

$$uv + u'v' \in V$$

for all $(u,u') \in C^2$, hence

$$P(uv + u'v') = 0$$

or still,

$$P((uw,ux,uy,uz) + (u'w',u'x',u'y',u'z')) = 0$$

or still,

$$P(uw + u'w',\ ux + u'x',\ uy + u'y',\ uz + u'z') = 0$$

or still,

$$(uw + u'w')(uz + u'z') - (ux + u'x')(uy + u'y') = 0$$

or still,

$$(wz - xy)u^2 + (w'z - xy' - x'y + wz')uu' + (w'z' - x'y')u'^2 = 0$$

$\Rightarrow$

$$wz = xy,\ w'z' = x'y',\ w'z + wz' = xy' + x'y,$$

$(u,u') \in C^2$ being arbitrary. Therefore

$$(yz' - y'z)(xz' - x'z)$$
$$= zz'(w'z - xy' - x'y + wz') = 0.$$

So at least one of the numbers

$$yz' - y'z,\ xz' - x'z$$

must vanish.

- $yz' - y'z = 0$

$\Rightarrow$

$$\frac{w}{x} = \frac{y}{z} = \frac{y'}{z'} = \frac{w'}{x'} \Rightarrow v' \in W_1(x:w),$$

a contradiction.

- $xz' - x'z = 0$

$\Rightarrow$

$$\frac{w}{y} = \frac{x}{z} = \frac{x'}{z'} = \frac{w'}{y'} \Rightarrow v' \in W_2(y:w),$$

a contradiction.

Since V is rational over Q (by hypothesis), there is a basis $e_1,\ldots,e_d$ for V $(d \le 2)$ with

$$e_i = (e_{i1}, e_{i2}, e_{i3}, e_{i4}) \in Q^4.$$

If V is included in $W_1(a:b)$ for some $(a:b) \in P^1(C)$, then the system of equations

$$ue_{i1} = u'e_{i2},\ ue_{i3} = u'e_{i4} \quad (i = 1,\ldots,d)$$

has a nontrivial solution $(u,u') \in C^2$, thus it has a nontrivial solution $(u,u') \in Q^2$. Consequently V is included in $W_1(a:b)$ for some $(a:b) \in P^1(Q)$. The story for $W_2(a:b)$ is analogous.

§50. *PROPERTY* $\begin{pmatrix} A & C \\ B & 0 \end{pmatrix}$

Let K be a field, $k \subset K$ a subfield.

1: DEFINITION Two $m \times n$ matrices M and N with entries in K are k-equivalent if there exist nonsingular matrices P and Q with entries in k such that $N = PMQ$.

[Note: The dimension of the Q-subspace of K^n generated by the rows of M (or N) is the same as the dimension of the Q-subspace of K^m generated by the columns of M (or N).]

2: N.B. The rank of M equals the rank of N, this being the largest integer r for which there exists a nonsingular $r \times r$ submatrix of M (or N) (cf. §35, #8).

3: THEOREM Let E be a k-vector subspace of K which is spanned by a family (finite or infinite) of elements of K which are algebraically independent over k -- then every matrix M with entries in E is k-equivalent to a matrix of the form

$$\begin{bmatrix} A & B \\ C & 0 \end{bmatrix},$$

where A is either zero-size or nonsingular.

To orient ourselves, here are two examples of the overall structural setup (ignoring for the time being the validity of the assumption on E).

4: EXAMPLE Take $K = C$, $k = Q$, let E_0 be the Q-vector space L of logarithms of algebraic numbers, and put $E = Q + L$.

[Note: The sum is direct. In fact,

$$\bar{Q} \cap L = \{0\} \quad (\text{cf. } §31, \#3) \Rightarrow Q \cap L = \{0\}.]$$

5: EXAMPLE Take $K = C$, $k = \bar{Q}$, let E_0 be the $\bar{Q}$-vector space of homogeneous linear combinations of elements of L with coefficients in $\bar{Q}$, and put $E = \bar{Q} + E_0$ (hence $E = L^*$).

[Note: The sum $\bar{Q} + E_0$ is direct (cf. §39, #14).]

6: LEMMA Suppose that E is a k-vector subspace of K -- then the following conditions are equivalent.

(i) E is spanned by a family (finite or infinite) of elements of K which are algebraically independent over k.

(ii) Subsets of E which are linearly independent over k are algebraically independent over k.

(iii) If E' is a vector subspace of E and x is an element of E which does not belong to E', then x is transcendental over $k(E')$.

PROOF

(i) => (ii) Per the assumption, fix a basis B for E over k consisting of elements of K which are algebraically independent over k. Let $x_1, \ldots, x_m$ be a set of k-linearly independent elements of E and write each x_i $(1 \leq i \leq m)$ as a linear combination with coefficients in k of elements $y_j \in B$ $(1 \leq j \leq n)$, say

$$x_i = \sum_{j=1}^{n} a_{ij} y_j.$$

Since the matrix $[a_{ij}]$ has rank m, it follows that there is a subset $\{z_1,\ldots,z_{n-m}\}$ of $\{y_1,\ldots,y_n\}$ such that

$$k(y_1,\ldots,y_n) = k(x_1,\ldots,x_m, z_1,\ldots,z_{n-m}).$$

And this relation implies that $x_1,\ldots,x_m$ are algebraically independent over k.

(ii) => (iii) Assume instead that $x \in E$, $x \notin E'$ is algebraic over $k(E')$. Choose $y_1,\ldots,y_n$ in E', linearly independent over k, such that x is algebraic over $k(y_1,\ldots,y_n)$ — then $y_1,\ldots,y_n,x$ are algebraically dependent over k, hence by (ii), are linearly dependent over k, say

$$a_1y_1 + \cdots + a_ny_n - ax = 0.$$

But a cannot be zero (since otherwise a = 0 would force $y_1,\ldots,y_n$ to be linearly dependent over k), hence

$$x = \frac{a_1}{a}\ y_1 + \cdots + \frac{a_n}{a} y_n \in E',$$

contradicting $x \notin E'$.

(iii) = (i): Let B be a basis for E over k. Claim: Any subset $\{y_1,\ldots,y_n\} \subset B$ of k-linearly independent elements of B consists of k-algebraically independent elements. To establish this, proceed by induction on n.

- $n = 1$: Use (iii) with $E' = \{0\}$:

$$y_1 \neq 0 \Rightarrow y_1 \notin E'.$$

Therefore y_1 is transcendental over k.

- $n \geq 2$: Assume the result holds at level $n - 1$ and let $y_1,\ldots,y_n$ be

k-linearly independent elements of B. Denote by E' the vector subspace of E over k spanned by $y_1,\ldots,y_{n-1}$. Owing to the induction hypothesis, $y_1,\ldots,y_{n-1}$ are algebraically independent over k. But $y_n \notin E'$, so by (iii), y_n is transcendental over the field $k(y_1,\ldots,y_{n-1})$ from which $y_1,\ldots,y_n$ are algebraically independent over k.

[Note: There is yet another equivalent condition that can be added to this list, viz:

(iv) For any nonzero polynomial $P \in k[X_1,\ldots,X_n]$,

$$Z(P) \cap E^n = \bigcup_{V} V \cap E^n,$$

where V ranges over the K-vector subspaces of K^n rational over k and contained in

$$Z(P) = \{\underline{x} \in K^n : P(\underline{x}) = 0\}.]$$

<u>7:</u> NOTATION Let E_0 be the k-vector subspace of E spanned by the entries of M.

The proof of #3 goes via induction in the dimension n of E_0.

• $n = 1$: Write $M = Nx$, where N has entries in k and $x \in E$, $x \neq 0$. Let r be the rank of N and let P and Q be nonsingular matrices with entries in k such that

$$PNQ = \begin{bmatrix} I_r & 0 \\ & \\ 0 & 0 \end{bmatrix}.$$

Then

$$PMQ = \begin{bmatrix} I_r x & 0 \\ & \\ 0 & 0 \end{bmatrix},$$

so matters are satisfied with the choices

$$A = I_r x,\ B = 0,\ C = 0.$$

- $n = 2$: Write

$$M = M_1 x_1 + M_2 x_2,$$

where M_1 and M_2 are matrices with entries in k and where $x_1, x_2 \in E$ are linearly independent over k (hence algebraically independent over k (cf. #6 (ii)). Denote by r_1 the rank of M_1. Choose nonsingular matrices P_1 and Q_1 with entries in k such that

$$P_1 M_1 Q_1 = \begin{bmatrix} I_{r_1} & 0 \\ & \\ 0 & 0 \end{bmatrix}.$$

Denote by A_2, B_2, C_2, D_2 the matrices with entries in k such that

$$P_1 M_2 Q_1 = \begin{bmatrix} A_2 & B_2 \\ & \\ C_2 & D_2 \end{bmatrix},$$

where A_2 is a $r_1 \times r_1$ matrix. Then

$$P_1 M Q_1 = \begin{bmatrix} I_{r_1} x_1 + A_2 x_2 & B_x x_2 \\ & \\ C_2 x_2 & D_2 x_2 \end{bmatrix}.$$

Choose nonsingular matrices P_2 and Q_2 with entries in k such that

$$P_2 D_2 Q_2 = \begin{bmatrix} I_{r_2} & 0 \\ 0 & 0 \end{bmatrix},$$

where r_2 is the rank of D_2. Then

$$\begin{bmatrix} I_{r_1} & 0 \\ 0 & P_2 \end{bmatrix} P_1 M Q_1 \begin{bmatrix} I_{r_1} & 0 \\ 0 & Q_2 \end{bmatrix}$$

equals

$$\begin{bmatrix} I_{r_1}x_1 + A_2x_2 & B_2'x_2 & B_2''x_2 \\ C_2'x_2 & I_{r_2}x_2 & 0 \\ C_2''x_2 & 0 & 0 \end{bmatrix},$$

where B_2', B_2'', C_2', C_2'' have entries in k. Put now

$$A = \begin{bmatrix} I_{r_1}x_1 + A_2x_2 & B_2'x_2 \\ C_2'x_2 & I_{r_2}x_2 \end{bmatrix}$$

and take for B,C what remains. To check that A is nonsingular, note that the determinant of A is a polynomial in x_1 and x_2 and the coefficient of $x_1^{r_1}x_2^{r_2}$ is 1. Therefore

$$\det A \neq 0.$$

- $n > 2$: Fix a nonzero element $x \in E_0$. Let E_1 be a subspace of E_0 such that $E_0 = E_1 \oplus kx$. Write $M = xN + M_1$, where N has entries in k and M_1 has entries in E_1. Denote by r the rank of N. Choose nonsingular matrices P and Q with entries in k such that

$$PNQ = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

Then

$$PMQ = \begin{bmatrix} xI_r + A_1 & B_1 \\ C_1 & D_1 \end{bmatrix},$$

where A_1, B_1, C_1, D_1 have their entries in E_1. Apply now the induction hypothesis to D_1:

$$P'D_1Q' = \begin{bmatrix} A' & B' \\ C' & 0 \end{bmatrix}.$$

Here A' is nonsingular with entries in E_1. Next

$$\begin{bmatrix} I_r & 0 \\ 0 & P' \end{bmatrix} \begin{bmatrix} xI_r + A_1 & B_1 \\ C_1 & D_1 \end{bmatrix} \begin{bmatrix} I_r & 0 \\ 0 & Q' \end{bmatrix}$$

equals

$$\begin{bmatrix} A & B \\ C & 0 \end{bmatrix}.$$

Here

$$A = \begin{bmatrix} xI_r + A_1 & B'' \\ C'' & A' \end{bmatrix}$$

and the entries of B'', C'' are in E_1. To assertain that A is nonsingular, note that the determinant of A is a polynomial in x with coefficients in $k(E_1)$ whose term of highest degree is $x^r \det A'$. Since $x \notin E_1$, it follows from #6 (iii) that x is transcendental over $k(E_1)$ and since A' is nonsingular, the bottom line is that

$$\det A \neq 0.$$

8: DEFINITION Let E be a k-vector subspace of K — then by property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ we shall understand the following: Any nonzero matrix M with entries in E is k-equivalent to a matrix of the form

$$\begin{bmatrix} A & B \\ C & 0 \end{bmatrix},$$

where A is nonsingular.

[Note: Strictly speaking this is a property of the triple

$$(k,K,E)$$

but usually one abuses the language and simply says that E has property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$.]

9: N.B. The upshot of #3 is that if E is a k-vector subspace of K spanned by k-algebraically independent elements, then E satisfies property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$.

10: LEMMA If E_0 is a k-vector subspace of K spanned by k-algebraically independent elements and if $E_0 \cap k = \{0\}$, then $E = k + E_0$ satisfies property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$.

PROOF As a k-vector space, E is isomorphic to the subspace $E' = kX + E_0$ of $K(X)$ and property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ holds for the triple

$$(k,K(X),E').$$

11: EXAMPLE As in #4, take $K = \mathbb{C}$, $k = \mathbb{Q}$, $E_0 = L$, and admit FDC (cf. §49, #1) -- then #6(ii) is in force which implies that #6(i) is in force. Accordingly, since $E_0 \cap k = \{0\}$, it follows that $E = k + E_0$ satisfies property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$.

[Note: Of course, E_0 also satisfies property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$.]

12: REMARK The satisfaction of property $\begin{pmatrix} A & B \\ C & 0 \end{pmatrix}$ is not automatic.

[To illustrate, choose elements x and u in K such that u, ux, ux^2 are k-linearly independent ($\Rightarrow x \notin k$). Denote by E the k-vector space $ku + kux + kux^2$ ($\Rightarrow \dim_k(E) = 3$) -- then the triple (k,K,E) does not satisfy property $\binom{A\ B}{C\ 0}$. Thus consider the line $V = K(1,x)$ in K^2 (the hyperplane defined by the equation $z_2 = xz_1$) and note that $V \cap k^2 = \{0\}$. Furthermore $V \cap E^2$ contains the k-linearly independent points

$$(u,ux),\ (ux,ux^2)$$

implying thereby that $\dim_k(V \cap E^2) \geq 2$. On the other hand, taking into account §51, #3 infra (with $d = 2$, $n = 1$),

$$\dim_k(V \cap E^2) \leq 1(1 + 1)/2 = 1.$$

So, on the basis of this contradiction, the triple (k,K,E) does not satisfy property $\binom{A\ B}{C\ 0}$.]

APPENDIX

Let K be a field, $k \subset K$ a subfield.

LEMMA Suppose that E is a k-vector subspace of K containing k -- then the following conditions are equivalent (cf. #6).

(i) There exists a basis $\{x_i : i \in I\}$ for E over k with $0 \in I$, $x_0 = 1$, and $\{x_i : i \in I,\ i \neq 0\}$ algebraically independent over k.

(ii) If $x_1,\ldots,x_n$ are elements in E such that $1, x_1,\ldots,x_n$ are linearly independent over k, then $x_1,\ldots,x_n$ are algebraically independent over k.

(iii) For any tuple $(x_0,\ldots,x_n)$ consisting of k-linearly independent elements of E and for any nonzero homogeneous polynomial $P \in k[X_0,\ldots,X_n]$, the number $P(x_0,\ldots,x_n)$ is not zero.

(iv) If $P \in k[X_0,\ldots,X_n]$ is a nonzero homogeneous polynomial, then

$$Z(P) \cap E^{n+1} = \bigcup_{V} V \cap E^{n+1},$$

where V ranges over the K-vector subspaces of K^{n+1} rational over k and contained in

$$Z(P) = \{\underline{x} \in K^{n+1} : P(\underline{x}) = 0\}.$$

§51. VECTOR SPACES: L(bis)

1: RAPPEL Let $V \subset C^d$ be a C-vector subspace such that $V \cap Q^d = \{0\}$ -- then

$$\dim_Q(V \cap L^d) \leq n(n+1) \quad (\text{cf. §38, \#5}),$$

where

$$n = \dim_C(V).$$

2: N.B. This result is unconditional.

Return now to the setup of §50.

3: THEOREM Let E be a k-vector subspace of K satisfying property $\binom{A\ B}{C\ 0}$. Let $V \subset K^d$ be a K-vector subspace -- then

$$\dim_k(V \cap E^d) \leq n(n+1)/2,$$

where

$$n = \dim_K(V).$$

PROOF When $d = 1$, $V = \{0\}$ and $V \cap E = \{0\}$. Assume now that $d \geq 2$ ($\Rightarrow n < d$).

- By induction on d, if $r < d$ and if W is a K-vector subspace of K^r such that $W \cap k^r = \{0\}$, then the k-vector space $W \cap E^r$ is finite dimensional, in fact

$$\dim_k(W \cap E^r) \leq r(r-1)/2 \quad (\text{see below}).$$

Take now ℓ elements $\underline{x}_1,\ldots,\underline{x}_\ell$ in $V \cap E^d$ which are linearly independent over k, the claim being that

$$\ell \leq n(n+1)/2.$$

Denote by M the $d \times \ell$ matrix whose columns are given by the coordinates of the $\underline{x}_i$ $(i = 1,\ldots,\ell)$ — then the entries of M are in E, so M is k-equivalent to a matrix

$$\begin{bmatrix} A & B \\ & \\ C & 0 \end{bmatrix},$$

where A is a nonsingular $r \times r$ matrix. In addition

$$d > n \geq \text{rank } M \geq r \Rightarrow r \leq n < d.$$

Put $t = \ell - r$, thus B is a $r \times t$ matrix. Let W be the K-vector space spanned by the columns of B in K^r. Since V contains $W \times \{0\}^{d-r}$, we have $W \cap k^r = \{0\}$. On the other hand, the columns of M are k-linearly independent, hence the same is true of

$$\begin{bmatrix} A & B \\ & \\ C & 0 \end{bmatrix},$$

hence too for B. Therefore

$$t = \dim_k(W \cap E^r)$$

and by the induction hypothesis,

$$t \leq r(r-1)/2$$

$\Rightarrow$

$$\begin{aligned} \ell &= t + r = r + t \\ &\leq r + r(r-1)/2 \\ &\leq n + n(n-1)/2 \\ &= n(n+1)/2. \end{aligned}$$

Finally

$$n \leq d - 1 \Rightarrow$$

$$\ell \leq (d-1)(d-1+1)/2 = d(d-1)/2$$

which completes the induction.

4: APPLICATION Take $K = \mathcal{C}$, $k = \mathcal{Q}$, and $E_0 = L$. Admit FDC (cf. §49, #1) -- then E_0 is a $\mathcal{Q}$-vector subspace of $\mathcal{C}$ satisfying property $\binom{A\ B}{C\ 0}$ (cf. §50, #11), so for any $\mathcal{C}$-vector subspace $V \subset \mathcal{C}^d$ such that $V \cap \mathcal{Q}^d = \{0\}$ there follows

$$\dim_{\mathcal{Q}}(V \cap L^d) \leq n(n+1)/2.$$

[Note: It is not known if

$$\operatorname{tr}_{\mathcal{Q}} \mathcal{Q}(L) \geq 2.$$

However the mere presence of property $\binom{A\ B}{C\ 0}$ is not enough to imply that there exists two algebraically independent logarithms of algebraic numbers.]

5: N.B. The estimate

$$\dim_{\mathcal{Q}}(V \cap L^d) \leq n(n+1)/2$$

is sharp (cf. §38, #7).

6: IMPLICATION

$$\text{FDC} \Rightarrow \text{4EC}.$$

PROOF Refer back to the proof of #1 in §41. Follow it line by line, working with $\{x_1,x_2\}$ and $\{y_1,y_2\}$ (drop the "y_3") — then $V = \mathcal{C}\underline{x}$ contains two $\mathcal{Q}$-linearly independent points (viz. $y_1\underline{x}$, $y_2\underline{x}$), hence

$$2 \leq \dim_{\mathcal{Q}}(V \cap L^2).$$

On the other hand (cf. #4),

$$\dim_{\mathbb{Q}}(V \cap L^2) \leq 1(1+1)/2 = 1.$$

Contradiction.

[Note: Recall that

$$\text{SCHC} \Rightarrow \text{4EC} \quad (\text{cf. §47, #17})$$

and

$$\text{SCHC} \Rightarrow \text{FDC} \quad (\text{cf. §47, #7 and §49, #1}).]$$

7: REMARK Under SCHC, it can be shown that a finite subset of L^* consisting of $\bar{\mathbb{Q}}$-linearly independent elements along with 1 is $\bar{\mathbb{Q}}$-algebraically independent. Agreeing to denote this property by the symbol SFDC, we therefore have the implication

$$\text{SCHC} \Rightarrow \text{SFDC}.$$

One can then work with the triple $(\bar{\mathbb{Q}}, \mathbb{C}, L^*)$, which thus satisfies property $\binom{A\ B}{C\ 0}$. So, for any $\mathbb{C}$-vector subspace $V \subset \mathbb{C}^d$ of dimension n such that $V \cap \bar{\mathbb{Q}}^d = \{0\}$, the $\bar{\mathbb{Q}}$-vector subspace $V \cap L^{*d}$ has dimension $\leq n(n+1)/2$.

8: N.B.

$$\text{SCHC} \Rightarrow \text{S4EC}.$$

§52. *ON THE EQUATION* $z + e^z = 0$

This equation has exactly one real root. Can it be expressed in "elementary" terms?

1: DEFINITION A subfield F of $\mathbb{C}$ is closed under exp and Log if

- $z \in F \Rightarrow \exp z \in F$
- $z \in F - \{0\} \Rightarrow \operatorname{Log} z \in F$.

2: NOTATION Write $\mathbb{E}$ for the intersection of all subfields of $\mathbb{C}$ that are closed under exp and Log, the elements of $\mathbb{E}$ being the elementary numbers.

3: CONSTRUCTION Set $\mathbb{E}_0 = \{0\}$ and for each $n > 0$, let $\mathbb{E}_n$ be the set of all complex numbers obtained by applying a field operation to a pair of elements of $\mathbb{E}_{n-1}$ or by applying exp or Log to an element of $\mathbb{E}_{n-1}$.

[Note: Division by zero or taking the logarithm of zero are not, of course, permitted.]

4: N.B. Therefore

$$\mathbb{Q} \subset \mathbb{E}.$$

5: LEMMA

$$\mathbb{E} = \bigcup_{n=0}^{\infty} \mathbb{E}_n.$$

[Note: Consequently $\mathbb{E}$ is countable.]

6: EXAMPLE

$$e = \exp(\exp 0) \in \mathbb{E}.$$

7: EXAMPLE

$$\sqrt{-1} = \exp\left(\frac{\operatorname{Log}(-1)}{2}\right) \in E.$$

8: EXAMPLE

$$\pi = -\sqrt{-1}\,\operatorname{Log}(-1) \in E.$$

9: EXAMPLE

$$\sqrt{2} = \exp\left(\frac{\ell n(2)}{2}\right) \in E.$$

10: THEOREM (Admit SCHC) The real root ρ of the equation $z + e^z = 0$ is not in E.

This is definitely not obvious and it will first be necessary to step through some preliminaries.

11: NOTATION Given a finite set

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

of nonzero complex numbers, if $A = \emptyset$ put $A_0 = Q$ and if $A \neq \emptyset$, put

$$A_i = Q(\alpha_1, e^{\alpha_1}, \ldots, \alpha_i, e^{\alpha_i}) \quad (i \in \{1, \ldots, n\}).$$

12: N.B. Each element of A_i is a rational function (with rational coefficients) of the numbers

$$\alpha_1, e^{\alpha_1}, \ldots, \alpha_i, e^{\alpha_i}.$$

13: DEFINITION A tower is a finite set

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

of nonzero complex numbers with the property that for each $i \in \{1, \ldots, n\}$ there exists an integer $m_i > 0$ such that $\alpha_i^{m_i} \in A_{i-1}$ or $e^{\alpha_i m_i} \in A_{i-1}$ (or both).

14: EXAMPLE

$$A = (\alpha_1, \alpha_2, \alpha_3) = (\ell n(2),\ \ell n(2)/3,\ \ell n(1 + e^{(\ell n(2))/3}))$$

is a tower.

[One can choose

$$m_1 = 1,\ m_2 = 1,\ m_3 = 1$$

because

$$e^{\alpha_1} = 2 \in A_0,\ \alpha_2 \in A_1,\ e^{\alpha_3} \in A_2.]$$

15: DEFINITION A reduced tower is a tower

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

such that $\{\alpha_1, \ldots, \alpha_n\}$ is linearly independent over Q.

16: N.B. The tower figuring in #14 is not reduced (in fact $\alpha_1 - 3\alpha_2 = 0$).

17: LEMMA Let

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

be a tower and suppose that $q_1, \ldots, q_n$ are nonzero integers. Set

$$B = \{\beta_1, \ldots, \beta_n\},$$

where

$$\beta_i = \frac{\alpha_i}{q_i} \ (i = 1,\ldots,n).$$

Then $\forall\ i$,

$$A_i \subset B_i$$

and B is a tower.

PROOF Since

$$\alpha_i = \beta_i q_i \text{ and } e^{\alpha_i} = (e^{\beta_i})^{q_i},$$

it follows that every element of A_i is a rational function (with rational coefficients) of the numbers

$$\beta_1, e^{\beta_1}, \ldots, \beta_i, e^{\beta_i},$$

hence $\forall$ i,

$$A_i \subset B_i \text{ (cf. \#12)}.$$

This said, let $i \in \{1,\ldots,n\}$, thus $\alpha_i^{m_i} \in A_{i-1}$ or $e^{\alpha_i m_i} \in A_{i-1}$ (or both) and put $n_i = m_i q_i$.

- Suppose that $\alpha_i^{m_i} \in A_{i-1}$ -- then

$$\beta_i^{n_i} = \left(\frac{\alpha_i^{m_i}}{q_i^{m_i}}\right)^{q_i} \in A_{i-1} \subset B_{i-1}.$$

- Suppose that $e^{\alpha_i m_i} \in A_{i-1}$ -- then

$$e^{\beta_i n_i} = e^{\alpha_i m_i} \in A_{i-1} \subset B_{i-1}.$$

Therefore B is a tower.

18: REDUCTION PRINCIPLE Given $\gamma \in E$, there is a reduced tower

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

such that $\gamma \in A_n$.

PROOF If $\gamma \in Q$, take for A the empty sequence. If $\gamma \notin Q$, let $T(\gamma)$ be the set of all towers

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

with the property that $\gamma \in A_n$ — then $T(\gamma)$ is not empty and, as will now be shown, the assumption that every element of $T(\gamma)$ is not reduced is a non sequitur. So choose a tower

$$A = \{\alpha_1, \ldots, \alpha_n\} \in T(\gamma)$$

and take n minimal ($n \geq 1$). Let i be the smallest integer such that $\{\alpha_1, \ldots, \alpha_i\}$ is linearly dependent over Q, hence

$$\alpha_i = \sum_{j=1}^{i-1} \frac{p_j}{q_j} \alpha_j$$

for certain integers $p_1, q_1, \ldots, p_n, q_n$. Consider the sequence

$$A' = \{\frac{\alpha_1}{q_1}, \ldots, \frac{\alpha_{i-1}}{q_{i-1}}, \alpha_{i+1}, \ldots, \alpha_n\}.$$

Then the claim is that $A' \in T(\gamma)$, which contradicts the minimality of n. To establish this, note that the sequence

$$\{\frac{\alpha_1}{q_1}, \ldots, \frac{\alpha_{i-1}}{q_{i-1}}\}$$

is a tower (cf. #17). In addition,

$$\alpha_i \in A'_{i-1} \text{ (by the formula above for } \alpha_i)$$

and

$$e^{\alpha_i} \in A'_{i-1} \text{ (it is a polynomial in the numbers } e^{\alpha_1/q_1}, \ldots, e^{\alpha_{i-1}/q_{i-1}}).$$

But

$$A_{i-1} \subset A'_{i-1} \text{ (cf. #17)}$$

$$\Rightarrow A_i = A_{i-1}(\alpha_i, e^{\alpha_i}) \subset A'_{i-1}.$$

Therefore the tower condition for A' is satisfied at the boundary between $\frac{\alpha_{i-1}}{q_{i-1}}$ and α_{i+1} and

$$\gamma \in A_n \subset A'_{n-1} \Rightarrow A' \in T(\gamma),$$

as claimed.

<u>19:</u> SUBLEMMA Suppose that

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

is a tower — then $\forall$ i,

$$\text{trdeg}_Q A_i \leq i.$$

PROOF Start with the situation when n = 1, say $\{\alpha, e^\alpha\}$, and for sake of argument, assume that $\alpha^m \in Q$ — then α is algebraic (consider $X^m - \alpha^m$), hence

$$\text{trdeg}_Q Q(\alpha, e^\alpha) = \text{trdeg}_Q Q(e^\alpha)$$

$$\leq 1.$$

Proceed from this point by induction, the underlying hypothesis being that

$$\text{trdeg}_Q A_{i-1} \leq i - 1.$$

Let r_i stand for α_i or e^{α_i} -- then

$$A_i = A_{i-1}(\alpha_i, e^{\alpha_i})$$
$$= A_{i-1}(r_i).$$

However, on general grounds (cf. §46, #20),

$$\text{trdeg}_Q\, A_{i-1}(r_i) = \text{trdeg}_{A_{i-1}}\, A_{i-1}(r_i) + \text{trdeg}_Q\, A_{i-1},$$

or still,

$$\text{trdeg}_Q\, A_{i-1}(r_i) \leq 1 + i - 1 = i.$$

I.e.:

$$\text{trdeg}_Q\, A_i \leq i.$$

<u>20:</u> LEMMA (Admit SCHC) Suppose that

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

is a reduced tower -- then not both α_i and e^{α_i} can be algebraic over A_{i-1}.

PROOF In the notation of §46, #20,

$$\text{trdeg}_Q(A_i/Q) = \text{trdeg}_{A_{i-1}}(A_i/A_{i-1}) + \text{trdeg}_Q(A_{i-1}/Q).$$

To get a contradiction, suppose that both α_i and e^{α_i} are algebraic over A_{i-1}, thus

$$A_{i-1}(\alpha_i, e^{\alpha_i})$$

is an algebraic extension of A_{i-1}, so A_i is an algebraic extension of A_{i-1}, hence

$$\text{trdeg}_{A_{i-1}}(A_i/A_{i-1}) = 0 \quad \text{(cf. §46, #18).}$$

Therefore

$$\mathrm{trdeg}_Q(A_i/Q) = \mathrm{trdeg}_Q(A_{i-1}/Q).$$

Owing now to Schanuel,

$$\mathrm{trdeg}_Q(A_i/Q) \geq i.$$

On the other hand (cf. #19),

$$\mathrm{trdeg}_Q(A_{i-1}/Q) \leq i - 1.$$

Contradiction.

<u>21:</u> <u>N.B.</u> $\forall\, i$,

$$\mathrm{trdeg}_Q\, A_i = i.$$

Turning finally to the proof of #10, suppose that $\rho \in E$ — then in view of #18, there is a reduced tower

$$A = \{\alpha_1, \ldots, \alpha_n\}$$

such that $\rho \in A_n$. Obviously $\rho \notin Q$ and it can be assumed without loss of generality that $\rho \notin A_i$ if $i < n$.

Put

$$A' = \{\alpha_1, \ldots, \alpha_n, \rho\}.$$

Then

$$\rho \in A_n' = Q(\alpha_1, e^{\alpha_1}, \ldots, \alpha_n, e^{\alpha_n}) = A_n$$

and

$$\rho + e^{\rho} = 0 \Rightarrow e^{\rho} \in A_n'.$$

Accordingly A' (which is clearly a tower) cannot be reduced (cf. #20). On the other hand, A is reduced, thus

$$\rho = \sum_{i=1}^{n} \frac{p_i}{q_i} \alpha_i$$

for certain integers $p_1, q_1, \ldots, p_n, q_n$. Here $p_n \neq 0$ since $\rho \notin A_i$ for $i < n$. In terms of this data

$$\rho + e^{\rho} = 0 \Rightarrow \sum_{i=1}^{n} \frac{p_i}{q_i} \alpha_i + \prod_{i=1}^{n} (e^{\alpha_i/q_i})^{p_i} = 0.$$

Let

$$B = \{\alpha_1/q_1, \ldots, \alpha_n/q_n\}.$$

Then B is a tower (cf. #17) and since A is reduced, the same is true of B. But $p_n \neq 0$, hence

$$\alpha_n/q_n \text{ algebraic over } B_{n-1} \Rightarrow e^{\alpha_n/q_n} \text{ algebraic over } B_{n-1}$$

and vice versa. It therefore follows that B cannot be reduced (cf. #20). Consequently the supposition that $\rho \in E$ has led to a contradiction.

22: NOTATION Write $\overline{E}$ for the smallest algebraically closed subfield of $\mathbf{C}$ that is closed under exp and Log.

23: N.B. Evidently

$$E \subset \overline{E}.$$

24: THEOREM (Admit SCHC) Suppose that $P(X,Y) \in \overline{\mathbf{Q}}[X,Y]$ is an irreducible polynomial such that

$$\begin{cases} \deg_X P \geq 1 \text{ per } C[Y][X] \\ \\ \deg_Y P \geq 1 \text{ per } C[X][Y]. \end{cases}$$

Assume: For some nonzero $\alpha \in C$,

$$P(\alpha, e^{\alpha}) = 0.$$

Then $\alpha \not\in \bar{E}$.

[Note: α is necessarily transcendental. For if α was algebraic, then the relation

$$P(\alpha, e^{\alpha}) = 0$$

implies that e^{α} would also be algebraic, which contradicts Hermite-Lindemann (cf. §21, #4).]

25: APPLICATION Take $P(X,Y) = X + Y$ and take $\alpha = \rho$ -- then

$$P(\rho, e^{\rho}) = \rho + e^{\rho} = 0$$

$$\Rightarrow \rho \not\in \bar{E} \Rightarrow \rho \not\in E,$$

thereby recovering #10.

§53. *ON THE EQUATION* $P(z,e^z) = 0$

<u>1:</u> RAPPEL Let f be an entire function. Assume: f has no zeros -- then there is an entire function g such that $f = e^g$.

[Note: If f is of finite order, then g is a polynomial (and the order of f is equal to the degree of g).]

<u>2:</u> RAPPEL Let f be an entire function. Assume: f has finitely many zeros $z_1 \neq 0, \ldots, z_n \neq 0$ (each counted with multiplicity), as well as a zero of order $m \geq 0$ at the origin -- then

$$f(z) = z^m e^{g(z)} \prod_{k=1}^{n} \left(1 - \frac{z}{z_k}\right),$$

where g(z) is entire.

[Note: If f is of finite order, then g is a polynomial (and the order of f is equal to the degree of g).]

<u>3:</u> DEFINITION A polynomial $P \in \mathbb{C}[X,Y]$ satisfies the <u>standard conditions</u> if P is irreducible and

$$\begin{cases} \deg_X P \geq 1 \text{ per } \mathbb{C}[Y][X] \\ \deg_Y P \geq 1 \text{ per } \mathbb{C}[X][Y]. \end{cases}$$

Given such a P, let

$$f(z) = P(z,e^z).$$

Then f(z) has order 1.

<u>4:</u> LEMMA f(z) has infinitely many zeros.

PROOF Suppose that $f(z)$ has finitely many zeros -- then there exist complex constants A,B and a polynomial $p(X) \in \mathbb{C}[X]$ such that

$$f(z) = e^{Az+B}p(z)$$

$$= e^{Az}e^{B}p(z) = e^{Az}q(z),$$

where

$$q(z) = e^{B}P(z) \in \mathbb{C}[X].$$

But the relation

$$P(z,e^{z}) - e^{Az}q(z) = 0$$

is possible only if $A \in \mathbb{N}$ (expand the data and compare coefficients), hence

$$P(X,Y) = Y^{A}q(X).$$

Since P depends on both X and Y, neither Y^{A} nor $q(X)$ are equal to 1, thus $P(X,Y)$ is reducible, which contradicts the fact that $P(X,Y)$ is irreducible.

[Note: To rule out from first principles the possibility that $A = 0$, observe that the relation

$$P(z,e^{z}) = q(z)$$

would imply that e^{z} is algebraic (cf. §20, #13), whereas e^{z} is transcendental (cf. §20, #15).]

We come now to the main result which is an illustration of the old adage "assume more, get more", there being, however, a price to pay, viz. the imposition of SCHC.

5: THEOREM (Admit SCHC) Suppose that P satisfies the standard conditions.

Suppose in addition that $P \in Q[X,Y]$ -- then

$$f(z) = P(z,e^z)$$

has infinitely many Q-algebraically independent zeros.

The proof is lengthy and will be developed in the lines that follow.

<u>6:</u> DEFINITION A zero $\alpha \neq 0$ of $f(z)$ is said to be <u>generic</u> if

$$\operatorname{trdeg}_Q Q(\alpha,e^\alpha) = 1.$$

[Note: Therefore the point (α,e^α) is a generic point of the curve $C \subset \mathbf{C} \times \mathbf{C}^\times$ given by $P(X,Y) = 0$.]

<u>7:</u> LEMMA Every zero $\alpha \neq 0$ of $f(z)$ is generic.

PROOF According to §52, #24, α is necessarily transcendental, hence

$$\operatorname{trdeg}_Q Q(\alpha) = 1.$$

But

$$P(\alpha,Y) \in Q(\alpha)[Y],$$

so e^α is algebraic over $Q(\alpha)$, which implies that

$$\operatorname{trdeg}_Q Q(\alpha,e^\alpha) = 1.$$

<u>8:</u> <u>N.B.</u> Distinct nonzero α,β with $f(\alpha) = 0$, $f(\beta) = 0$ are not automatically algebraically independent over Q.

[Take

$$P(X,Y) = 1 + X^2Y + Y^2.$$

Then

$$P(\alpha,e^\alpha) = 0 \Rightarrow P(-\alpha,e^{-\alpha}) = 0.]$$

However:

9: SUBLEMMA (Admit SCHC) Suppose that

$$\begin{cases} f(\alpha) = 0 \quad (\alpha \neq 0) \\ \\ f(\beta) = 0 \quad (\beta \neq 0) \end{cases} \qquad \text{and } \alpha \neq \pm \beta.$$

Then α and β are algebraically independent over Q.

PROOF Bear in mind that $\alpha \neq 0$, $\beta \neq 0$ are transcendental and generic (cf. #7). This said, assume that α and β are algebraically dependent over Q -- then

$$\text{trdeg}_Q\ Q(\alpha,\beta,e^\alpha,e^\beta) = \text{trdeg}_Q\ Q(\alpha,\beta) = \text{trdeg}_Q\ Q(\alpha) = 1.$$

Owing now to Schanuel's conjecture, α and β are linearly dependent over Q: Linear independence over Q would imply that

$$\text{trdeg}_Q\ Q(\alpha,\beta,e^\alpha,e^\beta) \geq 2.$$

Accordingly choose relatively prime integers m and n such that $m\alpha = n\beta$ (take $n > 0$ and suppose momentarily that $m > 0$). Put $\gamma = \frac{\alpha}{n}$, hence

$$e^\alpha = (e^\gamma)^n \text{ and } e^\beta = (e^\gamma)^m.$$

For every positive integer j, let

$$C_j \subset C \times C^\times$$

be the curve given by

$$P(jX,Y^j) = 0.$$

Then

$$\begin{cases} 0 = f(\alpha) = P(\alpha,e^\alpha) = P(n\gamma,(e^\gamma)^n) \\ \\ 0 = f(\beta) = P(\beta,e^\beta) = P(m\gamma,(e^\gamma)^m) \end{cases}$$

=>

$$(\gamma,e^{\gamma}) \in C_n \cap C_m.$$

Since C_n and C_m have a nonempty intersection, it follows that they have a common irreducible component and this means that

$$P(nX,Y^n) \text{ and } P(mX,Y^m)$$

have a common irreducible factor.

FACT The n^{th} roots of unity operate transitively on the irreducible components of C_n and the m^{th} roots of unity operate transitively on the irreducible components of C_m.

- Factor $P(nX,Y^n)$ into relatively prime irreducibles:

$$P(nX,Y^n) = \prod_{j=1}^{k} U_j(X,Y)^{s_j}.$$

Then it can be shown that each $U_j(X,Y)$ is of the form $U_1(X,\omega Y)$ for some n^{th} root of unity ω and $s_1 = \cdots = s_k$, call their common value s, hence

$$\deg_X P = ks \deg_X U_1$$

and

$$n \deg_Y P = ks \deg_Y U_1.$$

- Factor $P(mX,Y^m)$ into relatively prime irreducibles:

$$P(mX,Y^m) = \prod_{i=1}^{\ell} V_i(X,Y)^{t_i}.$$

Then it can be shown that each $V_i(X,Y)$ is of the form $V_1(X,\omega Y)$ for some m^{th} root of unity ω and $t_1 = \cdots = t_\ell$, call their common value t, hence

$$\deg_X P = \ell t \deg_X V_1$$

and

$$m \deg_Y P = \ell t \deg_Y V_1.$$

It can be assumed that

$$U_1(X,Y) = V_1(X,Y),$$

the common irreducible factor of $P(nX,Y^n)$ and $P(mX,Y^m)$ -- then

$$\begin{aligned} ks \deg_X U_1 = \deg_X P &= \ell t \deg_X V_1 \\ &= \ell t \deg_X U_1. \end{aligned}$$

But

$$\deg_X P \neq 0 \Rightarrow ks = \ell t \neq 0.$$

Next

$$\begin{aligned} n \deg_Y P = ks \deg_Y U_1 &= \ell t \deg_Y U_1 \\ &= \ell t \deg_Y V_1 \\ &= m \deg_Y P. \end{aligned}$$

But

$$\deg_Y P \neq 0 \Rightarrow n = m,$$

contradicting the assumption that m,n are relatively prime.

[Note: To treat the case when $m < 0$, consider the polynomial

$$T(X,Y) = Y^{-m \deg_Y P} P(mX,Y^m).$$

Then

$$\deg_X T = \deg_X P$$

and

$$\deg_Y T = -m \deg_Y P.$$

So as above,

$$m\alpha = n\beta \Rightarrow -n\alpha = n\beta \Rightarrow -\alpha = \beta \Rightarrow \alpha = -\beta,$$

whcih is forbidden by hypothesis.]

<u>10:</u> DEFINITION Under the assumptions of #5, P is said to be <u>primitive</u> if $\forall\, n \in N$, the curve C_n given by

$$P(nX, Y^n) = 0$$

is irreducible.

<u>11:</u> LEMMA (Admit SCHC) Suppose that P is primitive and let $\alpha_1, \ldots, \alpha_n$ be nonzero zeros of $f(z) = P(z, e^z)$ subject to $\alpha_i \neq \pm\, \alpha_j$ for all $i \neq j$ -- then $\alpha_1, \ldots, \alpha_n$ are algebraically independent over Q.

PROOF Searching for a contradiction, the first step is to tabulate the data. So assume that over Q there exists an algebraically dependent collection $\alpha_1, \ldots, \alpha_n$, α_{n+1} of $n + 1$ nonzero zeros of f such that $\alpha_i \neq \pm\, \alpha_j$ for all $i \neq j$ and take n minimal. In view of #9, two such zeros are algebraically independent over Q, hence $n \geq 2$, and, by the minimality of n, the collection $\alpha_1, \ldots, \alpha_n$ is algebraically independent over Q, hence

$$\operatorname{trdeg}_Q Q(\alpha_1, \ldots, \alpha_{n+1}, e^{\alpha_1}, \ldots, e^{\alpha_{n+1}}) = n < n + 1.$$

Meanwhile, by Schanuel, if $\alpha_1,\ldots,\alpha_n,\alpha_{n+1}$ were linearly independent over Q, then

$$\operatorname{trdeg}_Q Q(\alpha_1,\ldots,\alpha_{n+1},e^{\alpha_1},\ldots,e^{\alpha_{n+1}}) \geq n+1.$$

Since this cannot be, it follows that there exist nonzero integers $m_1,\ldots,m_n,m$ with no common factor such that

$$\sum_{k=1}^{n} m_k\alpha_k = m\alpha_{n+1} \quad (m > 0).$$

Put $\gamma_k = \dfrac{\alpha_k}{m}$. Let $C \subset C \times C^\times$ be the curve defined by $P(X,Y) = 0$ and let $C_m \subset C \times C^\times$ be the curve defined by $P(mX,Y^m) = 0$. Since P is primitive, C_m is irreducible and since $\alpha_1,\ldots,\alpha_n$ are algebraically independent over Q, the same is true of $\gamma_1,\ldots,\gamma_n$. Therefore $(\gamma_1,e^{\gamma_1}),\ldots,(\gamma_n,e^{\gamma_n})$ are generic points in C_m. Moreover

$$\operatorname{trdeg}_Q Q(\gamma_1,e^{\gamma_1},\ldots,\gamma_n,e^{\gamma_n}) = n.$$

<u>12:</u> CONSTRUCTION Define a map

$$\varphi: (C \times C^\times)^n \to C \times C^\times$$

by the prescription

$$(x_1,y_1,\ldots,x_n,y_n) \to \left(\sum_{k=1}^{n} m_kx_k, \prod_{k=1}^{n} y_k^{m_k}\right).$$

Then

$$\varphi(\gamma_1,e^{\gamma_1},\ldots,\gamma_n,e^{\gamma_n})$$

$$= \left(\sum_{k=1}^{n} m_k\gamma_k, \prod_{k=1}^{n} e^{\gamma_k m_k}\right)$$

$$= \left(\sum_{k=1}^{n} \frac{m_k \alpha_k}{m}, \prod_{k=1}^{n} e^{\frac{m_k \alpha_k}{m}} \right)$$

$$= (\alpha_{n+1}, e^{\alpha_{n+1}}),$$

a generic point in C, hence φ maps $(C_m)^n$ to C. So if $z_1, \ldots, z_n$ are zeros of f, then the pairs

$$\left(\frac{z_1}{m}, e^{\frac{z_1}{m}}\right), \ldots, \left(\frac{z_n}{m}, e^{\frac{z_n}{m}}\right)$$

lie in C_m, from which it follows that the sum

$$\sum_{k=1}^{m} \frac{m_k}{m} z_k$$

is a zero of f. In particular:

$$\alpha \equiv \frac{m_1+m_2}{m} \alpha_1 + \frac{m_3}{m} \alpha_3 + \cdots + \frac{m_n}{m} \alpha_n$$

is a zero of f (take $z_1 = z_2 = \alpha_1$ and $z_k = \alpha_k$ $(k > 2)$).

<u>$n > 2$:</u> In this situation, the collection $\alpha_1, \alpha_3, \ldots, \alpha_n, \alpha$ is algebraically dependent over Q and consists of n nonzero zeros of f, contradicting the minimality of n.

[Note: The condition $n > 2$ implies that α is nonzero and $\alpha \neq \pm \alpha_i \ \forall\ i$.]

<u>$n = 2$:</u> It is a question of dealing with the collection $\alpha_1, \alpha_2, \alpha_3$ of Q-algebraically dependent nonzero zeros of f such that $\alpha_i \neq \pm \alpha_j$ for all $i \neq j$ satisfying

$$m_1\alpha_1 + m_2\alpha_2 = m\alpha_3,$$

where, as above,

$$\alpha = \frac{m_1+m_2}{m}\,\alpha_1$$

is a zero of f. The claim then is that such a scenario is impossible. To this end, it will be shown below that each of the following conditions leads to a contradiction.

$$(1)\ m_1 + m_2 = 0;\ \ (2)\ m_1 + m_2 = m;\ \ (3)\ m_1 + m_2 = -\,m.$$

Therefore

$$\alpha \neq 0\ (\text{cf. }(1));\ \alpha \neq \alpha_1\ (\text{cf. }(2));\ \alpha \neq -\,\alpha_1\ (\text{cf. }(3)).$$

Consequently α and α_1 are algebraically independent over Q (cf. #9). But this is nonsense since α and α_1 are linearly dependent over Q:

$$1 \cdot \alpha - q \cdot \alpha_1 = 0\ \ (q = \frac{m_1+m_2}{m} \in Q).$$

<u>Ad(1)</u> ($m_1 + m_2 = 0$): To begin with, note that $\frac{m_1}{m}\alpha_1$ and α_1 are nonzero Q-algebraically dependent zeros of f, hence by #9,

$$\frac{m_1}{m}\alpha_1 = \pm\,\alpha_1 \Rightarrow m_1 = \pm\,m.$$

To pin things down, take $m_1 = +m$ -- then

$$\begin{aligned} m_1\alpha_1 + m_2\alpha_2 = m\alpha_3 &\Rightarrow m\alpha_1 - m\alpha_2 = m\alpha_3 \\ &\Rightarrow \alpha_1 = \alpha_2 + \alpha_3. \end{aligned}$$

Now interchange the roles of α_1 and α_2 to get

$$\alpha_2 = \alpha_1 + \alpha_3$$

or still,

$$\alpha_2 = \alpha_2 + \alpha_3 + \alpha_3 \Rightarrow 0 = 2\alpha_3.$$

Contradiction.

Ad(2) $(m_1 + m_2 = m)$: By switching the roles of the variables and multiplying by -1 if necessary, it can be assumed that $|m| \geq |m_1|, |m_2|$ and $m > 0$, $m_1 > 0$. Construct a sequence $\{z_k\}$ of zeros of f by the following procedure: Take $z_1 = \alpha_1$ and via recursion, take

$$z_{k+1} = \frac{m_1}{m} z_k + \frac{m_2}{m}\alpha_2.$$

Then the fact that

$$\frac{m_2}{m} = 1 - \frac{m_1}{m}$$

leads to the relation

$$z_{k+1} = \left(\frac{m_1}{m}\right)^k \alpha_1 + \left(1 - \left(\frac{m_1}{m}\right)^k\right)\alpha_2.$$

Since

$$0 < \frac{m_1}{m} < 1,$$

the coefficient $\left(\frac{m_1}{m}\right)^k$ of α_1 takes a different value for each k, thus thanks to the Q-algebraic independence of α_1 and α_2, the sequence $\{z_k\}$ assumes infinitely many distinct values. Put

$$M = \max\{|\alpha_1|, |\alpha_2|\}.$$

Then

$$|z_{k+1}| \leq \left| \left(\frac{m_1}{m}\right)^k \right| M + \left| 1 - \left(\frac{m_1}{m}\right)^k \right| M \leq 2M.$$

But this means that the entire function f has infinitely many zeros in the disc of radius 2M centered at the origin, so f = 0, a contradiction.

<u>Ad(3)</u> $(m_1 + m_2 = - m)$: Let $s = \dfrac{m_1}{m}$ -- then

$$\frac{m_2}{m} = -(1 + s)$$

and

$$m\alpha_3 = m_1\alpha_1 + m_2\alpha_2$$

$$\Rightarrow \quad \alpha_3 = \frac{m_1}{m}\alpha_1 + \frac{m_2}{m}\alpha_2$$

$$= s\alpha_1 - (1 + s)\alpha_2.$$

On the other hand,

$$s\alpha_3 - (1 + s)\alpha_2$$

is a zero of f. And

$$\begin{aligned} w \equiv{} & s\alpha_3 - (1 + s)\alpha_2 \\ ={} & s(s\alpha_1 - (1 + s)\alpha_2) - (1 + s)\alpha_2 \\ ={} & s^2\alpha_1 - s(1 + s)\alpha_2 - (1 + s)\alpha_2 \\ ={} & s^2\alpha_1 - (1 + s)(s\alpha_2 + \alpha_2) \\ ={} & s^2\alpha_1 - (1 + s)^2\alpha_2. \end{aligned}$$

Now treat α_1, α_2, w as a collection of $\mathbb{Q}$-algebraically dependent nonzero zeros of f. Invoking the earlier analysis, we thus have

$$s^2 - (1 + s)^2 = - 2s - 1 = 0 \text{ or } \pm 1.$$

- If $- 2s - 1 = 1$, then

$$s = - 1 \Rightarrow - 1 = \frac{m_1}{m}$$

$$\Rightarrow - m = m_1$$

$$\Rightarrow m_1 + m_2 = m_1$$

$$\Rightarrow m_2 = 0.$$

So

$$m\alpha_3 = m_1\alpha_1 + m_2\alpha_2$$

$$\Rightarrow m\alpha_3 = m_1\alpha_1$$

$$\Rightarrow - m_1\alpha_3 = m_1\alpha_1 \Rightarrow \alpha_3 = - \alpha_1.$$

Contradiction.

- If $- 2s - 1 = - 1$, then

$$s = 0 \Rightarrow m_1 = 0.$$

So

$$m\alpha_3 = m_1\alpha_1 + m_2\alpha_2$$

$$\Rightarrow - m_1\alpha_3 - m_2\alpha_3 = m_1\alpha_1 + m_2\alpha_2$$

$$\Rightarrow - m_2\alpha_3 = m_2\alpha_2 \Rightarrow \alpha_3 = - \alpha_2.$$

Contradiction.

- If $-2s - 1 = 0$, then

$$s^2 - (1 + s)^2 = s^2 - (1 + 2s + s^2)$$

$$= -1 - 2s = 0.$$

So matters reduce to "$m_1 + m_2 = 0$"... .

<u>13:</u> <u>N.B.</u> It won't hurt to repeat: $P \in \mathbb{Q}[X,Y]$ satisfies the standard conditions and

$$f(z) = P(z,e^z)$$

has infinitely many zeros (cf. #4).

PROOF OF #5 In view of #11, it can be assumed that P is not primitive. Choose, accordingly, an $n \in \mathbb{N}$ such that C_n is reducible (cf. #10) -- then C_n has an irreducible component defined by some polynomial $P_n(X,Y) \in \mathbb{Q}[X,Y]$ depending on both X and Y and

$$0 < \deg_X P_n < \deg_X P.$$

Noting that $\deg_X P > 1$, proceed by induction on $\deg_X P$, supposing that for all irreducible polynomials $T(X,Y) \in \mathbb{Q}[X,Y]$ satisfying the standard conditions such that

$$\deg_X T < \deg_X P$$

the entire function

$$T(z,e^z)$$

has infinitely many $\mathbb{Q}$-algebraically independent zeros -- then by hypothesis, the entire function

$$f_n(z) = P_n(z,e^z)$$

has infinitely many $\mathbb{Q}$-algebraically independent zeros, say $z_1, z_2, \ldots$. But $P_n(X,Y)$ is a factor of $P(nX, Y^n)$, hence

$$f(nz_k) = P(nz_k, e^{nz_k}) = 0 \quad (k = 1,2,\ldots).$$

Therefore

$$nz_1, nz_2, \ldots$$

is an infinite collection of $\mathbb{Q}$-algebraically independent zeros of f.

14: REMARK The result remains valid if $\mathbb{Q}$ is replaced by $\bar{\mathbb{Q}}$, i.e., granted SCHC, if $P \in \bar{\mathbb{Q}}[X,Y]$ satisfies the standard conditions, then

$$f(z) = P(z, e^z)$$

has infinitely many $\mathbb{Q}$-algebraically independent zeros.

15: EXAMPLE (Admit SCHC) Consider $P(X,Y) = X - Y$ -- then the entire function

$$f(z) = P(z, e^z) = z - e^z$$

has infinitely many $\mathbb{Q}$-algebraically independent zeros, thus the exponential function e^z has infinitely many $\mathbb{Q}$-algebraically independent fixed points (cf. §52, #10).

16: THEOREM (Admit SCHC) Suppose that $K \subset \mathbb{C}$ is a finitely generated field -- then for any $P \in K[X,Y]$ satisfying the standard conditions, the equation

$$P(z, e^z) = 0$$

has a solution α generic over K:

$$\operatorname{trdeg}_K K(\alpha, e^\alpha) = 1.$$

[This was proved in 2014 by V. Mantova.]

<u>17:</u> APPLICATION (Admit SCHC)

$$\#16 \Rightarrow \#14.$$

[Start with the field K obtained by adjoining the coefficients of P to Q. Choose an α per supra.]

Here is a word or two on the proof of #16. The key is to show that $P(z,e^z)$ has only finitely many zeros in $\bar{K}$, the algebraic closure of K (this forces the other zeros to be generic over K). The point of departure for this is the following result.

<u>18:</u> LEMMA (Admit SCHC) There exists a finite dimensional Q-vector space $F \subset \bar{K}$ containing all the zeros of $P(z,e^z)$ in $\bar{K}$.

[Without loss of generality, add to K the coefficients of P so that P is defined over K. Recall that for any $\underline{z} = (z_1,\ldots,z_n)$,

$$\operatorname{trdeg}_Q Q(\underline{z},e^{\underline{z}}) \geq \operatorname{lindim}_Q \underline{z} \quad (\text{cf. §47, \#24}).$$

If now each $z_i \in \underline{z}$ is in $\bar{K}$ and $P(z_i,e^{z_i}) = 0$, then $e^{z_i} \in \bar{K}$.]

§54. ZILBER FIELDS

These are fields subject to the following conditions.

- (EAC)
- (STD)
- (SCHP)
- (SEACP) $\subset$ (EACP)
- (CCP)

The meaning of these abbreviations will be explained below.

1: DEFINITION An E-field is a field $(K, +, \cdot, 0, 1)$ of characteristic 0 equipped with a surjective homomorphism E from its additive group $(K,+)$ to its multiplicative group $(K^{\times}, \cdot)$, thus

$$\forall\, x,y \in K,\ E(x+y) = E(x) \cdot E(y)$$

and $E(0) = 1$.

2: EXAMPLE To exhibit an E-field, take $K = \mathbf{R}$, take $a > 0$, and equip it with the exponential function to base a, i.e.,

$$\exp_a(x) = a^x \quad (x \in \mathbf{R}) \quad \text{(cf. §5, \#1)}.$$

[Note: Denote this setup by the symbol $\mathbf{R}_{\exp}$ when $a = e$.]

3: DEFINITION An E-field K is an EAC-field if K is algebraically closed.

4: EXAMPLE To exhibit an EA-field, take $K = \mathbf{C}$ and equip it with the usual exponential function $z \to e^z$.

[Note: Denote this setup by the symbol $\mathbf{C}_{\exp}$.]

5: N.B. If K is an E-field, then Q can be considered as a subfield of K, since K has characteristic 0.

6: DEFINITION Suppose that K is an E-field -- then the kernel of the exponential map, i.e.,

$$\{x \in K : E(x) = 1\},$$

is said to be standard (STD) if it is an infinite cyclic group generated by a transcendental element α, thus

$$\mathrm{Ker}(E) = \alpha Z.$$

[Note: α is transcendental provided that it is not the root of a nonzero polynomial with coefficients in the copy of Q in K.]

7: EXAMPLE Take $K = C_{\exp}$ -- then the kernel of the exponential map is $2\pi\sqrt{-1}\, Z$, hence is standard (take $\alpha = 2\pi\sqrt{-1}$).

8: DEFINITION Suppose that K is an E-field -- then to say that K has Schanuel's property (SCHP) means that if $x_1,\ldots,x_n$ are elements of K which are linearly independent over Q, then the field

$$Q(x_1,\ldots,x_n,E(x_1),\ldots,E(x_n))$$

has transcendence degree $\geq n$ over Q.

[Note: When $K = C$, SCHP is, of course, conjectural (SCHC).]

9: NOTATION Given an E-field K, transcribe §47, #20 from C to K and given $\underline{x}$, put

$$\delta_A(\underline{x}) = \mathrm{trdeg}_Q\, Q(\underline{x},E(\underline{x})) - \mathrm{lindim}_Q\, \underline{x},$$

the predimension of $\underline{x}$ (cf. §47, #26).

Therefore SCHP per K is the claim that $\forall\ \underline{x}$,

$$\delta_A(\underline{x}) \geq 0.$$

10: NOTATION (Admit SCHP) Given an E-field K and a finite set $X \subset K$, view X as a tuple — then $\delta_K(X) \geq 0$ and the dimension of X in K is

$$\dim_K(X) = \inf\{\delta_K(Y): X \subset Y \subset_f K\} \text{ (i.e., Y finite)}.$$

11: DEFINITION (Admit SCHP) Let K and L be E-fields — then L is a strong extension of K if $K \subset L$ and

$$\dim_K(X) = \dim_L(X)$$

for all $X \subset K$, where X is finite.

12: THEOREM (Admit SCHP) $C_{\exp}$ is not a strong extension of $R_{\exp}$.

PROOF It will be shown that

$$\dim_R(\pi) \neq \dim_C(\pi).$$

Owing to Nesterenko (cf. §20, #10):

- $\delta_R(\pi) = \text{trdeg}_Q\ Q(\pi,e^{\pi}) - \text{lindim}_Q(\pi)$

  $= 2 - 1 = 1.$

- $\delta_C(\pi,\pi\sqrt{-1}) = \text{trdeg}_Q\ Q(\pi,\pi\sqrt{-1},e^{\pi},e^{\pi\sqrt{-1}}) - \text{lindim}_Q(\pi,\pi\sqrt{-1})$

  $= \text{trdeg}_Q\ Q(\pi,\pi\sqrt{-1},e^{\pi},-1) - 2$

  $= \text{trdeg}_Q\ Q(\pi,\pi\sqrt{-1},e^{\pi}) - 2$

  $= \text{trdeg}_Q\ Q(\pi,e^{\pi}) - 2$

  $= 2 - 2 = 0,$

$\pi\sqrt{-1}$ being algebraic over $Q(\pi)$. Therefore

$$\dim_C(\pi) = 0.$$

If now C_{exp} was a strong extension of R_{exp}, then we'd have

$$\dim_R(\pi) = 0,$$

so there would be a finite subset $X \subset R$ with $\pi \in X$ such that $\delta_R(X) = 0$. Explicate:

$$X = \{\pi, x_1, \ldots, x_n\}$$

and suppose that

$$\operatorname{lindim}_Q X = k + 1.$$

Write

$$\begin{aligned} 0 &= \delta_R(\pi, x_1, \ldots, x_n) \\ &= \operatorname{trdeg}_Q Q(\pi, x_1, \ldots, x_n, e^{\pi}, e^{x_1}, \ldots, e^{x_n}) - \operatorname{lindim}_Q(\pi, x_1, \ldots, x_n) \end{aligned}$$

$\Rightarrow$

$$\operatorname{trdeg}_Q Q(\pi, x_1, \ldots, x_n, e^{\pi}, e^{x_1}, \ldots, e^{x_n})$$
$$= k + 1$$

$\Rightarrow$

$$\operatorname{trdeg}_Q Q(\pi, \pi\sqrt{-1}, x_1, \ldots, x_n, e^{\pi}, e^{\pi\sqrt{-1}}, e^{x_1}, \ldots, e^{x_n})$$
$$= k + 1.$$

On the other hand, thanks to Schanuel,

$$\operatorname{trdeg}_Q Q(\pi, \pi\sqrt{-1}, x_1, \ldots, x_n, e^{\pi}, e^{\pi\sqrt{-1}}, e^{x_1}, \ldots, e^{x_n})$$
$$\geq \operatorname{lindim}_Q(\pi, \pi\sqrt{-1}, x_1, \ldots, x_n)$$
$$= k + 2.$$

Contradiction.

The next definition, viz. that of strong exponential closure, is on the technical side.

Let K be an EAC-field. Put $G = K \times K^\times$ -- then G is a $\mathbb{Z}$-module:

$$(\cdot): \quad \mathbb{Z} \times G \to G$$

$$m \cdot (x,y) = (mx, y^m).$$

This action can be generalized to matrices with integer coefficients:

$$(\cdot): \quad M_{n \times n}(\mathbb{Z}) \times G^n \to G^n,$$

where a matrix $M = [m_{ij}]$ sends

$$(x_1,\ldots,x_n,y_1,\ldots,y_n)$$

to

$$\left(\sum_{j=1}^{n} m_{1j}x_j,\ldots,\sum_{j=1}^{n} m_{nj}x_j;\ \prod_{j=1}^{n} y_j^{m_{1j}},\ldots,\prod_{j=1}^{n} y_j^{m_{nj}}\right).$$

<u>13:</u> NOTATION If $V \subset G^n$, write $M \cdot V$ for its image and observe that if V is a subvariety of G^n, then so is $M \cdot V$.

<u>14:</u> DEFINITION A subvariety $V \subset G^n$ satisfies the <u>dimension condition</u> if for all $M \in M_{n \times n}(\mathbb{Z})$,

$$\dim M \cdot V \geq \operatorname{rank} M.$$

[Note: In particular, $\dim V \geq n$.]

<u>15:</u> DEFINITION A subset V of G^n is <u>additively free</u> if V is not contained in a set given by equations of the form

$$\{(\underline{x},\underline{y}): \sum_{i=1}^{n} m_i x_i = a\},$$

where the $m_i \in \mathbb{Z}$ are not all zero and $a \in K$.

16: DEFINITION A subset V of G^n is multiplicatively free if V is not contained in a set given by equations of the form

$$\{(\underline{x},\underline{y}): \prod_{i=1}^{n} y_i^{m_i} = b\},$$

where the $m_i \in \mathbb{Z}$ are not all zero and $b \in K^\times$.

17: N.B. Call V free if V is both additively and multiplicatively free.

18: DEFINITION A subvariety $V \subset G^n$ is admissible if V is irreducible, satisfies the dimension condition, and is free.

19: DEFINITION Suppose that K is an EAC-field -- then K has the exponential algebraic closure property (EACP) if for all admissible subvarieties V of G^n that are defined over K and of dimension n, there is an $\underline{x}$ in K^n such that $(\underline{x},E(\underline{x})) \in V$.

[Note: Therefore K is exponentially algebraically closed iff each such variety V intersects the graph of exponentiation.]

20: REMARK (Admit EACP) It can be shown that there are infinitely many $\mathbb{Q}$-algebraically independent $\underline{x}$ such that $(\underline{x},E(\underline{x})) \in V$.

21: EXAMPLE (Admit SCHC) Take $K = \mathbb{C}_{\exp}$ -- then it is unknown whether EACP obtains in general but the simplest case, namely when n = 1, can be dealt with. To see how this goes, recall that a variety V in $\mathbb{C}^2$ is the set of common zeros of a collection of polynomials in $\mathbb{C}[X,Y]$ and, in fact, is the zero set of a single polynomial, i.e., given V, there is a polynomial $P(X,Y) \in C[X,Y]$ such that

$$V = Z(P) = \{(X,Y) \in C \times C : P(X,Y) = 0\}.$$

And V is irreducible iff this is so of P. Working with $V \subset C \times C^{\times}$ (being interested only in solutions to $P(z,e^{z}) = 0$), transfer matters from V to P by imposing the standard conditions on P (cf. §53, #3) — then V is admissible. E.g.: To check freeness, $\forall$ nonzero $m \in Z$,

$$\begin{cases} V \not\subset \{(X,Y) \in C \times C^{\times} : mX = a\} \\ V \not\subset \{(X,Y) \in C \times C^{\times} : Y^{m} = b \neq 0\}. \end{cases}$$

Proceeding, to produce a point $(z,e^{z}) \in V$, what has been established in §53, #5 serves to settle things if $P \in Q[X,Y]$ or if instead $P \in \bar{Q}[X,Y]$ (cf. §53, #13) and the general situation can be handled by an appeal to §53, #15.

<u>22:</u> REMARK There is a reinforcement of EACP to SEACP, where the "S" stands for "strong". This is done by demanding that the outcomes $(\underline{x},E(\underline{x})) \in V$ be generic in a suitable sense.

[Note: The discussion in #21 is actually strong.]

Agreeing to admit SCHP, recall the notation of #10.

<u>23:</u> NOTATION Let K be an E-field with Schanuel's property. Given a finite set $X \subset K$, put

$$ec\ell_K(X) = \{x \in K : \dim_K(X \cup \{x\}) = \dim_K(X)\}.$$

<u>24:</u> <u>N.B.</u> $ec\ell_K(X)$ is called the <u>exponential closure</u> of X.

<u>25:</u> DEFINITION (Admit SCHP) An E-field K has the <u>countable closure</u>

property (CCP) if for any finite set $X \subset K$, $ec\ell_K(X)$ is countable.

There is another approach to exponential closure which forgoes SCHP and has the merit that it can be used to establish that C_{exp} has the CCP.

26: DEFINITION An exponential polynomial is a function of the form

$$f(\underline{x}) = P(\underline{x}, E(\underline{x})),$$

where

$$P \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_n].$$

27: N.B. Formal differentiation of polynomials can be extended to exponential polynomials in a unique way such that $\frac{\partial e^X}{\partial X} = e^X$.

28: DEFINITION A Khovanskii system of width n consists of exponential polynomials $f_1, \ldots, f_n$ with equations

$$f_i(x_1, \ldots, x_n) = 0 \quad (i = 1, \ldots, n)$$

and the inequation

$$\begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix} (x_1, \ldots, x_n) \neq 0,$$

the differentiation being the formal differentiation of exponential polynomials.

29: LEMMA (Admit SCHP) Let K be an E-field, $X \subset K$ a finite subset --

then $ec\ell_K(X)$ consists of those points $x \in K$ with the property that there are $n \in \mathbb{N}$, $x_1,\dots,x_n \in K$, and exponential polynomials $f_1,\dots,f_n$ with coefficients from $\mathbb{Q}(X)$ such that $x = x_1$ and $(x_1,\dots,x_n)$ is a solution to the Khovanskii system given by the f_i.

Now drop SCHP and for any E-field K take for the definition of $ec\ell_K(X)$ the property figuring in #29, thereby extending the definition of CCP to all E-fields K.

<u>30:</u> THEOREM $\mathbb{C}_{\exp}$ has the countable closure property.

PROOF Given a finite subset $X \subset \mathbb{C}_{\exp}$, there are only countably many Khovanskii systems with coefficients from $\mathbb{Q}(X)$. The inequation in a Khovanskii system amounts to saying that the Jacobian of the functions $f_1,\dots,f_n$ does not vanish, so by the implicit function theorem, solutions to a Khovanskii system are isolated, hence there are but countably many solutions to each system, thus implying that

$$ec\ell_{\mathbb{C}_{\exp}}(X)$$

is countable.

We come now to the fundamental definition: A <u>Zilber field</u> is a field K subject to the conditions listed at the beginning.

[Note: Denote this setup by the symbol K_E.]

<u>31:</u> THEOREM For κ uncountable, up to isomorphism there is a unique Zilber field of size κ.

<u>32:</u> CONJECTURE The Zilber field of size continuum is isomorphic to $\mathbb{C}_{\exp}$.

§55. *E-RINGS*

<u>1:</u> DEFINITION An <u>E-ring</u> is a pair (R,E), where R is a ring (commutative with 1) and

$$E:(R,+) \to (UR,\cdot)$$

is a map from the additive group of R to the multiplicative group of units of R such that

$$\forall\, x,y \in E,\ E(x + y) = E(x) \cdot E(y)$$

and $E(0) = 1$.

[Note: Every ring R becomes an E-ring via the stipulation

$$E(x) = 1 \quad (x \in R).]$$

<u>2:</u> EXAMPLE Every E-field is an E-ring (cf. §54, #1).

[Note: By definition, an E-field has characteristic 0, matters being trivial in positive characteristic. Thus suppose that K is a field of characteristic $p > 0$ -- then $\forall\, x \in K$,

$$\begin{aligned}1 = E(0) &= E(\underbrace{x + x + \cdots + x}_{p}) \\ &= E(x) + E(x) + \cdots + E(x) \\ &= E(x)^p\end{aligned}$$

$\Rightarrow$

$$\begin{aligned}(E(x) - 1)^p &= E(x)^p - 1^p \\ &= E(x)^p - 1 = 0 \Rightarrow E(x) = 1.]\end{aligned}$$

3: EXAMPLE Take $R = \mathbb{Z}$ and define E by the prescription

$$E(x) = 1 \quad (x \in \mathbb{Z}).$$

Another possibility is the prescription

$$E(x) = \begin{cases} 1 \text{ if } x \text{ is even} \\ -1 \text{ if } x \text{ is odd} \end{cases} \quad (x \in \mathbb{Z}).$$

[Note: These two are the only possibilities.]

4: RAPPEL If G is a multiplicative group (finite or infinite) and R is a ring (commutative with 1), then the group ring R[G] of G over R is the set of all finite linear combinations of elements of G with coefficients in R, thus

$$\sum_{g \in G} r_g g,$$

where $r_g = 0$ for all but finitely many elements of G and the ring operations are defined in the obvious way.

[Note: If 1 is the identity of R and e is the identity of G, then 1e is the identity of R[G].]

Let $X_1, \ldots, X_n$ be distinct indeterminants.

5: DEFINITION The free E-ring, denoted

$$[X_1, \ldots, X_n]^E,$$

is an E-ring containing $X_1, \ldots, X_n$ as elements and having the property that for each E-ring R and elements $r_1, \ldots, r_n \in R$ there is one and only one E-ring morphism

$$f:[X_1,\ldots,X_n]^E \to R$$

such that

$$f(X_i) = r_i \quad (i = 1,\ldots,n).$$

<u>6:</u> <u>N.B.</u> The free E-ring on no generators, denoted $[\emptyset]^E$ ("n = 0"), is admitted. It has the property that for each E-ring R there is an E-morphism from $[\emptyset]^E$ to R.

The existence of

$$[X_1,\ldots,X_n]^E$$

is established via an argument of recursion, itself a special case of the following considerations. Given an E-ring R, one can form the free E-ring extension of R on generators $X_1,\ldots,X_n$, denoted

$$R[X_1,\ldots,X_n]^E,$$

its elements being by definition the E-ring of exponential polynomials.

[Note: Take $R = \mathbb{Z}$ $(E \equiv 1)$ to recover

$$[X_1,\ldots,X_n]^E.]$$

<u>7:</u> CONSTRUCTION We shall construct three sequences:

- $(R_k, +, \cdot)_{k \geq -1}$ are rings;
- $(A_k, +)_{k \geq 0}$ are abelian groups;
- $(E_k)_{k \geq -1}$ are E-morphisms from R_k to UR_{k+1}.

Initial Step: Put $R_{-1} = R$,

$$R_0 = R[X_1,\ldots,X_n],$$

and let A_0 be the ideal generated by $X_1,\ldots,X_n$. So, as an additive group,

$$R_0 = R \oplus A_0 \quad (= R_{-1} \oplus A_0).$$

Define the morphism

$$E_{-1}:R_{-1} \to R_0$$

by the composition

$$R_{-1} = R \overset{E}{\to} R \overset{i}{\to} R[X_1,\ldots,X_n] = R_0.$$

Inductive Step: Suppose that $k \geq 0$ and R_{k-1}, R_k, A_k, And E_{k-1} have been defined in such a way that

$$R_k = R_{k-1} \oplus A_k,\ E_{k-1}:(R_{k-1},+) \to (UR_k,\cdot).$$

Let

$$t:(A_k,+) \to (t^{A_k},\cdot)$$

be a formal isomorphism (additive $\to$ multiplicative). Define

$$R_{k+1} = R_k[t^{A_k}].$$

Therefore R_k is a subring of R_{k+1} and as an additive group

$$R_{k+1} = R_k \oplus A_{k+1},$$

where A_{k+1} is the R_k-submodule of R_{k+1} freely generated by the t^a ($a \in A_k$, $a \neq 0$).

Next extend

$$E_k:(R_k,+) \to UR_{k+1},\cdot)$$

by

$$E_k(x) = E_{k-1}(y) \cdot t^a \quad (x = y + a, \text{ with } y \in R_{k-1}, a \in A_k).$$

In this way there is assembled a chain of partial E-rings (the domain of exponentiation of R_{k+1} is R_k):

$$R_0 \subset R_1 \subset \cdots .$$

Definition:

$$R[X_1,\ldots,X_n]^E = \bigcup_{k=0}^{\infty} R_k,$$

its E-ring morphism being the prescription

$$E(x) = E_k(x) \quad (x \in R_k).$$

8: N.B. R_{k+1} as an additive group is the direct sum

$$R \oplus A_0 \oplus A_1 \oplus \cdots \oplus A_{k+1}.$$

[Note: The group ring R_{k+1} is isomorphic to

$$R_0[t^{A_0 \oplus \cdots \oplus A_k}]$$

or still, is isomorphic to

$$R_1[t^{A_1 \oplus \cdots \oplus A_k}]$$

$$\cdots$$

or still, is isomorphic to

$$R_k[t^{A_k}].]$$

9: N.B.

$$R[X_1,\ldots,X_n]^E$$

as an additive group is

$$R \oplus A_0 \oplus A_1 \oplus \cdots \oplus A_k \oplus \cdots$$

and as a group ring is

$$R[X_1,\ldots,X_n]\,[t^{A_0 \oplus A_1 \oplus \cdots \oplus A_k \oplus \cdots}].$$

10: EXPONENTIATIONS

- Let $P \in R_k$ $(k \geq 0)$ -- then P can be written uniquely as

$$P = P_0 + P_1 + \cdots + P_k,$$

where $P_0 \in R_0$ and $P_\ell \in A_\ell$ $(\ell > 0)$.

- Let $P \in A_k$ $(k \geq 1)$ -- then P can be written uniquely as

$$P = \sum_{i=1}^{N} r_i E(a_i),$$

where $a_i \in A_{k-1} - \{0\}$ and $a_i \neq a_j$ for $i \neq j$ and $r_1,\ldots,r_N$ are nonzero elements of R_{k-1}.

[Note: The isomorphism $t:A_k \to t^{A_k}$ is the restriction of the exponential map E to A_k:

$$E(A_k) = t^{A_k}.]$$

11: EXAMPLE Take $n = 2$ and work with

$$[X_1,X_2]^E \equiv [X,Y]^E \equiv Z[X,Y]^E.$$

Then $(k = 2)$

$$P(X,Y) = -\,3X^2Y - X^5Y^7$$

$$+ (2XY + 5Y^2)E(-7X^3 + 11X^5Y^4)$$

$$+ (6 - 2XY^5)E((5X + 2X^7Y^2)E(5X - 10Y^2))$$

is an element of R_2 (per Z):

$$P = P_0 + P_1 + P_2.$$

12: EXAMPLE Consider the free E-ring $[\emptyset]^E$ on no generators -- then the elements of $[\emptyset]^E$ are "exponential constants", e.g., in suggestive notation,

$$e^{e^2+3} + 4 - 5e^{3+e^{-3}}.$$

13: LEMMA Given an E-ring T and elements $t_1,\ldots,t_n \in T$, every E-ring morphism $\phi:R \to T$ has a unique extension to an E-ring morphism

$$\Phi:R[X_1,\ldots,X_n]^E \to T$$

such that

$$\Phi(X_i) = t_i \quad (i = 1,\ldots,n).$$

[Use the corresponding property of

$$R[X_1,\ldots,X_n] = R_0$$

and extend stepwise to each R_k $(k > 0)$.]

Suppose that (R,E) is an E-ring. Given a set $I \neq \emptyset$, let R^I be the set of functions $I \to R$ -- the R^I is an E-ring: Let $f \in R^I$ and define Ef by the rule

$$(Ef)(i) = E(f(i)),$$

i.e., operations are pointwise.

Take $I = R^n$ and consider R^{R^n}, the functions from R^n to R. Define the coordinate functions $x_1,\ldots,x_n \in R^{R^n}$ by

$$x_i(r_1,\ldots,r_n) = r_i \quad (i = 1,\ldots,n).$$

In #13, take $T = R^{R^n}$. Embed R in R^{R^n} by assigning to each $r \in R$ the constant function C_r $(C_r(r_1,\ldots,r_n) = r)$ -- then the assignment

$$C:\begin{cases} R \to R^{R^n} \\ \\ r \to C_r \end{cases}$$

is an E-ring morphism, hence C admits a unique extension to an E-ring morphism

$$R[X_1,\ldots,X_n]^E \to R^{R^n}$$

that sends each X_i to x_i, the <u>canonical arrow</u>, call it Γ.

<u>14:</u> NOTATION Write

$$R[x_1,\ldots,x_n]^E$$

in place of

$$R^{R^n},$$

its elements being by definition the E-ring of exponential polynomial functions.

<u>15:</u> LEMMA If (R,E) is an E-ring and if R is an integral domain of characteristic 0, then $R[X_1,\ldots,X_n]^E$ is an integral domain (and its units are of the form $uE(P)$, where u is a unit of R and $P \in R[X_1,\ldots,X_n]^E$).

[Without going into detail, let us recall only that if R is an integral domain of characteristic 0 and G is a multiplicative group, then the group ring R[G] is an integral domain of characteristic 0 iff G is torsion free.]

16: N.B. By induction on $k \geq 0$, assume that R_k is an integral domain of characteristic 0 -- then A_k is torsion free. Therefore t^{A_k} is torsion free, which implies that

$$R_{k+1} = R_k[t^{A_k}]$$

is an integral domain of characteristic 0.

In general, the canonical arrow

$$\Gamma:R[X_1,\ldots,X_n]^E \to R[x_1,\ldots,x_n]^E$$

may have a nontrivial kernel.

17: EXAMPLE Consider a ring R equipped with the trivial exponentiation, i.e., $E(x) = 1$ for all $x \in R$ -- then $E(X_1) - 1$ is in the kernel of Γ.

[In fact,

$$\begin{aligned}\Gamma(E(X_1) - 1) &= \Gamma E(X_1) - \Gamma 1\\ &= E(\Gamma X_1) - C_1\\ &= E(x_1) - C_1.\end{aligned}$$

And

$$\begin{aligned}E(x_1)(r_1,\ldots,r_n) &= E(x_1(r_1,\ldots,r_n))\\ &= E(r_1)\\ &= 1 = C_1(r_1,\ldots,r_n)\end{aligned}$$

=>

$$E(x_1) = C_1.$$

Therefore

$$\Gamma(E(X_1) - 1) = E(x_1) - C_1$$

$$= C_1 - C_1 = 0.]$$

<u>18:</u> THEOREM Suppose that (R,E) is an E-ring and R is an integral domain of characteristic 0. Make the following assumptions.

- There are derivations $d_1,\ldots,d_n$ of $R[x_1,\ldots,x_n]^E$ which are trivial on R and satisfy the condition $d_i(x_j) = \delta_{ij}$ $(1 \leq i,j \leq n)$.

- There is a nonzero element $r \in R$ such that

$$d_i(E(f)) = rd_i(f)E(f)$$

for all f in $R[x_1,\ldots,x_n]^E$ $(i = 1,\ldots,n)$.

Then Γ is one-to-one.

Specialize now the theory outlined above and take $R = \mathbf{C}$, shifting matters to

$$\mathbf{C}[X_1,\ldots,X_n]^{\exp} \quad (E = \exp),$$

which, as will be recalled, is a group ring (cf. #9). Moreover, since $\mathbf{C}$ is an integral domain of characteristic 0, it follows from #15 that

$$\mathbf{C}[X_1,\ldots,X_n]^{\exp}$$

is an integral domain.

[Note: While $\mathbf{C}[X_1,\ldots,X_n]$ is noetherian, this is definitely not the case of

$$\mathbf{C}[X_1,\ldots,X_n]^{\exp}.]$$

<u>19:</u> THEOREM The canonical arrow

$$\Gamma : C[X_1,\ldots,X_n]^{\exp} \to C[x_1,\ldots,x_n]^{\exp}$$

is one-to-one.

[Apply #18 (take $d_1,\ldots,d_n$ as the partial derivatives $\partial/\partial x_1,\ldots,\partial/\partial x_n$ and choose $r = 1$).]

<u>20:</u> NOTATION Put

$$\mathrm{EXP}(C^n) = \Gamma C[X_1,\ldots,X_n]^{\exp}.$$

<u>21:</u> LEMMA (cf. #10) Each function f in $\mathrm{EXP}(C^n)$ can be written as a finite sum

$$f = \sum_i P_i \cdot \exp(g_i),$$

where

$$P_i \in C[X_1,\ldots,X_n] \text{ and } g_i \in \mathrm{EXP}(C^n).$$

<u>22:</u> EXAMPLE Take $n = 1$ and let $X_1 = X$ -- then the function $z \to e^z$ belongs to $\mathrm{EXP}(C)$.

[For

$$X \in A_0 \Rightarrow EX \in A_1.$$

And $\Gamma X = x$, where $x:C \to C$ is the function $z \to z$ (i.e., $x(z) = z$), hence

$$\Gamma EX = \exp \Gamma X = \exp x,$$

the function $C \to C$ that sends z to $\exp x(z) = \exp z$.

<u>23:</u> EXAMPLE The function

$$(z_1,z_2) \to z_1 z_2 \cdot \exp(\exp(z_1 + z_2))$$

belongs to $\mathrm{EXP}(C^2)$.

§56. *SCHANUEL => SHAPIRO*

1: DEFINITION Working over C, an exponential polynomial is an entire function f of the form

$$f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_n e^{\mu_n z},$$

where $\lambda_1,\ldots,\lambda_n$ and $\mu_1,\ldots,\mu_n$ are complex numbers.

Under addition and multiplication, the set of all such functions form a commutative ring E with 1.

[Note: The units are the elements of the form $\lambda e^{\mu z}$ $(\lambda \neq 0)$.]

2: REMARK This is the simplest situation since one could, e.g., allow $\lambda_1,\ldots,\lambda_n$ to be complex polynomials.

3: SHAPIRO'S CONJECTURE If f,g are two exponential polynomials with infinitely many zeros in common, then there exists an exponential polynomial h such that h is a common divisor of f,g in the ring E and h has infinitely many zeros in C.

As will be seen below, the proof of Shapiro's conjecture breaks up into two cases (terminology per infra).

Case 1: Either f or g is simple.

Case 2: Both f and g are irreducible.

4: N.B. It turns out that the proof of Case 1 does not require Schanuel but the proof of Case 2 does require Schanuel, hence the rubric

Schanuel => Shapiro.

To prepare for the case distinction, we shall need some definitions and a few classical facts.

5: DEFINITION Let

$$f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_n e^{\mu_n z}$$

be an exponential polynomial -- then its support, denoted spt(f), is the vector space over Q generated by $\mu_1,\ldots,\mu_n$.

6: DEFINITION An exponential polynomial f is said to be simple if

$$\dim_Q \operatorname{spt}(f) = 1.$$

7: EXAMPLE

$$f(z) = \sin z = \frac{e^{\sqrt{-1}\,z} - e^{-\sqrt{-1}\,z}}{2\sqrt{-1}}$$

is simple.

8: DEFINITION An exponential polynomial f is said to be irreducible if it is not a unit and has no divisors in the ring E other than associates.

Here is Ritt's factorization theorem.

9: THEOREM Every exponential polynomial f can be written uniquely up to order and multiplication by a unit as a product in E of the form

$$S_1 \cdots S_c\, I_1 \cdots I_d,$$

where all the S_j are simple with

$$\operatorname{spt}(S_j) \cap \operatorname{spt}(S_{j'}) = \{0\}$$

for $j \neq j'$ and all the I_k are irreducible.

Suppose that f,g are two exponential polynomials with infinitely many zeros in common and neither one is simple. Write per Ritt:

$$\begin{cases} f = S_1 \cdots S_c I_1 \cdots I_d \\ g = T_1 \cdots T_u J_1 \cdots J_v. \end{cases}$$

Then a common zero of f,g must be a zero of a factor of each function, thus two factors $\tilde{f},\tilde{g}$ of f,g respectively have infinitely many zeros in common, thus if $\tilde{f},\tilde{g}$ have a common divisor h in E with infinitely many zeros, then h is the common divisor of f,g postulated in Shapiro's conjecture.

Matters have accordingly been reduced to Case 1 and Case 2 formulated at the beginning.

APPENDIX

Let R be a commutative ring with 1.

DEFINITION 1 Let $x,y \in R$ -- then y divides x (or y is a divisor of x) and x is divisible by y (or x is a multiple of y) if there exists $z \in R$ such that $x = yz$.

[Note: The only elements of R which are divisors of 1 are the units of R, i.e., the elements of UR.]

DEFINITION 2 If $x,y \in R$ and if $x = yu$, where $u \in UR$, then x and y are said to be associates.

[Note: Therefore y divides x. But also $y = xu^{-1}$, thus x divides y.]

DEFINITION 3 The associates of an element $x \in R$ are the <u>improper divisors</u> of x.

[Note: A unit $u \in UR$ divides every element x of R: $x = u(u^{-1}x)$. Still, the convention is not to include UR in the set of divisors of x.]

DEFINITION 4 An element $x \in R$ is <u>irreducible</u> if it is not a unit and its only divisors are associates, i.e., are improper.

DEFINITION 5 Irreducible elements $x,y \in R$ are <u>distinct</u> if they are not unit multiples of one another.

LEMMA Distinct irreducibles $x,y \in R$ do not have a common divisor.

PROOF Suppose that a is a common divisor:

$$\left[\begin{array}{l} x = au \\ \\ y = av \end{array}\right. \qquad (u,v \in UR).$$

Then

$$a = yv^{-1} \Rightarrow x = yv^{-1}u,$$

i.e., x is a unit multiple of y. Contradiction.

§57. *SHAPIRO'S CONJECTURE: CASE 1*

Recall the setup: f,g are two exponential polynomials with infinitely many zeros in common and either f or g is simple (cf. #3).

<u>1:</u> THEOREM (Skolem-Mahler-Lech) Let $f \in E$ and let $A \subset Z$ be the set of integers on which f vanishes -- then A is the finite union of arithmetic progressions, i.e., sets of the form $\{m + kd: k \in Z\}$ for some $m,d \in Z$. Moreover, if A is infinite, then at least one of these arithmetic progressions has a nonzero difference d.

This is a wellknown result on the distribution of zeros of exponential polynomials and will be taken without proof.

<u>2:</u> LEMMA Let $f \in E$. Suppose that $f(k) = 0 \ \forall \ k \in Z$ -- then $\sin(\pi z)$ divides f in the ring E.

PROOF Let

$$f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_n e^{\mu_n z},$$

with $\lambda_1,\ldots,\lambda_n \neq 0$. It can be assumed that f is not identically zero and that $n \geq 2$ (since $\lambda_1 e^{\mu_1 z} = 0$ only if $\lambda_1 = 0$). Proceed by induction on the length n of f.

- <u>$n = 2$:</u>

$$f(z) = \lambda_1 e^{\mu_1 z} + \lambda_2 e^{\mu_2 z}$$

with $\lambda_1,\lambda_2 \neq 0$. Put $z = 0$ to get

$$\lambda_1 + \lambda_2 = 0 \Rightarrow f(z) = \lambda_1 (e^{\mu_1 z} - e^{\mu_2 z}).$$

Put z = 1 to get

$$e^{\mu_1} - e^{\mu_2} = 0$$

$$\Rightarrow \mu_2 = \mu_1 + 2k\pi\sqrt{-1} \quad (\exists\, k \in Z - \{0\})$$

$$\Rightarrow f(z) = \lambda_1 e^{\mu_1 z}\,(1 - e^{2k\pi\sqrt{-1}\,z}).$$

Without loss of generality, take $k > 0$ (otherwise switch the roles of μ_1 and μ_2).

Next

$$\sin z = \frac{e^{\sqrt{-1}\,z} - e^{-\sqrt{-1}\,z}}{2\sqrt{-1}}$$

$$\Rightarrow$$

$$-\,2\sqrt{-1}\,e^{\pi\sqrt{-1}\,z}\sin(\pi z) = 1 - e^{2\pi\sqrt{-1}\,z}$$

$$\Rightarrow$$

$$(1 + e^{2\pi\sqrt{-1}\,z} + e^{4\pi\sqrt{-1}\,z} + \cdots + e^{2(k-1)\pi\sqrt{-1}\,z})(-\,2\sqrt{-1}\,e^{\pi\sqrt{-1}\,z}\sin(\pi z)$$

$$= (1 + e^{2\pi\sqrt{-1}\,z} + e^{4\pi\sqrt{-1}\,z} + \cdots + e^{2(k-1)\pi\sqrt{-1}\,z})(1 - e^{2\pi\sqrt{-1}\,z})$$

$$= 1 + e^{2\pi\sqrt{-1}\,z} + e^{4\pi\sqrt{-1}\,z} + \cdots + e^{2(k-1)\pi\sqrt{-1}\,z}$$

$$- e^{2\pi\sqrt{-1}\,z} - e^{4\pi\sqrt{-1}\,z} - \cdots - e^{2(k-1)\pi\sqrt{-1}\,z} - e^{2k\pi\sqrt{-1}\,z}$$

$$= 1 - e^{2k\pi\sqrt{-1}\,z}$$

$$\Rightarrow$$

$$f(z) = \lambda_1 e^{\mu_1 z}(1 - e^{2k\pi\sqrt{-1}\,z})$$

$$= \lambda_1 e^{\mu_1 z} F(z)(-\,2\sqrt{-1}\,e^{\pi\sqrt{-1}\,z}\sin(\pi z))$$

if

$$F(z) = 1 + e^{2\pi\sqrt{-1}\,z} + e^{4\pi\sqrt{-1}\,z} + \cdots + e^{2(k-1)\pi\sqrt{-1}\,z}.$$

Therefore $\sin(\pi z)$ divides $f(z)$.

- $\underline{n > 2:}$ Suppose now that for all exponential polynomials $h(z)$ of length $\leq n - 1$ which vanish at the integers, $\sin(\pi z)$ divides $h(z)$. Setting $z = 1,2,\ldots,n$ in $f(z)$ leads to the relations

$$\lambda_1 e^{\mu_1} + \cdots + \lambda_n e^{\mu_n} = 0$$

$$\lambda_1 (e^{\mu_1})^2 + \cdots + \lambda_n (e^{\mu_n})^2 = 0$$

$$\vdots$$

$$\lambda_1 (e^{\mu_1})^n + \cdots + \lambda_n (e^{\mu_n})^n = 0.$$

Let $\delta_j = e^{\mu_j}$ $(j = 1,\ldots,n)$, hence in matrix notation

$$\begin{bmatrix} \delta_1 & \delta_2 & \cdots & \delta_n \\ \delta_1^2 & \delta_2^2 & \cdots & \delta_n^2 \\ & \vdots & & \\ \delta_1^n & \delta_2^n & \cdots & \delta_n^n \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since $\lambda_1,\ldots,\lambda_n \neq 0$, they constitute a nontrivial solution of the corresponding system of linear equations, thus the determinant of the matrix vanishes:

$$\begin{vmatrix} \delta_1 & \delta_2 & \cdots & \delta_n \\ \delta_1^2 & \delta_2^2 & \cdots & \delta_n^2 \\ & \vdots & & \\ \delta_1^n & \delta_2^n & \cdots & \delta_n^n \end{vmatrix} = 0$$

or still,

$$\delta_1\delta_2 \cdots \delta_n \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \delta_1 & \delta_2 & \cdots & \delta_n \\ & & \vdots & \\ \delta_1^{n-1} & \delta_2^{n-1} & \cdots & \delta_n^{n-1} \end{vmatrix} = 0.$$

This is a Vandermonde determinant, so we are led to

$$\delta_1 \cdots \delta_n \prod_{1 \leq i < j \leq n} (\delta_i - \delta_j) = 0.$$

Since all the δ_i are nonzero, it must be the case that $\delta_i = \delta_j$ for some $i < j$. Without loss of generality, assume that $\delta_1 = \delta_2$, i.e., $e^{\mu_1} = e^{\mu_2}$. Put

$$h(z) = (\lambda_1 + \lambda_2)e^{\mu_1 z} + \sum_{j=3}^{n} \lambda_j e^{\mu_j z}.$$

Then

$$h(z) - \lambda_2(e^{\mu_1 z} - e^{\mu_2 z})$$

$$= \lambda_1 e^{\mu_1 z} + \lambda_2 e^{\mu_1 z} - \lambda_2 e^{\mu_1 z} + \lambda_2 e^{\mu_2 z} + \sum_{j=3}^{n} \lambda_j e^{\mu_j z}$$

$$= \lambda_1 e^{\mu_1 z} + \lambda_2 e^{\mu_2 z} + \sum_{j=3}^{n} \lambda_j e^{\mu_j z}$$

$$= f(z).$$

And $\forall\ k \in Z$,

$$h(k) = f(k) + \lambda_2(e^{\mu_1 k} - e^{\mu_2 k})$$

$$= 0.$$

Consequently $h(z)$ vanishes at the integers. But its length is $< n$, hence by the induction hypothesis, $\sin(\pi z)$ divides $h(z)$. On the other hand, arguing as in the case $n = 2$, $\sin(\pi z)$ divides $\lambda_2(e^{\mu_1 z} - e^{\mu_2 z})$. So finally $\sin(\pi z)$ divides $f(z)$.

[Note:

$$e^{\mu z} = \sum_{n=0}^{\infty} \frac{(\mu z)^n}{n!}$$

is, in general, not the same as

$$(e^{\mu})^z = e^{z \operatorname{Log} e^{\mu}} = e^{z(\mu + 2\pi\sqrt{-1}\, m)}.$$

But they are the same if $z = k \in \mathbb{Z}$:

$$(e^{\mu})^k = e^{k(\mu + 2\pi\sqrt{-1}\, m)} = e^{k\mu} = e^{\mu k}.]$$

3: THEOREM If f,g are two exponential polynomials with infinitely many zeros in common such that at least one of f,g is simple, then there exists an exponential polynomial h such that h is a common divisor of f,g in the ring E and h has infinitely many zeros in $\mathbb{C}$.

PROOF Take f simple and write

$$f(z) = u(z) \prod_{\ell=1}^{L} (1 - \alpha_\ell e^{\rho z}),$$

where $\alpha_1,\ldots,\alpha_L,\rho$ are nonzero complex numbers and $u(z) \in E$ is a unit (the simplicity of f implies that there is a nonzero $\kappa \in \mathbb{C}$ and $s_1,\ldots,s_n \in \mathbb{Z}$ such that $\mu_1 = s_1\kappa,\ldots,\mu_n = s_n\kappa$). Since this is a finite product, g must have infinitely many zeros in common with one of the factors, say $1 - \alpha_1 e^{\rho z}$. So suppose that

$$1 - \alpha_1 e^{\rho z} = 0.$$

Then

$$\frac{1}{\alpha_1} = e^{\rho z}$$

=>

$$e^{\text{Log}\,\frac{1}{\alpha_1}} = e^{\rho z}$$

=>

$$\rho z - \text{Log}\,\frac{1}{\alpha_1} = 2k\pi\sqrt{-1} \quad (\exists\, k \in Z)$$

=>

$$z = \frac{\text{Log}(\frac{1}{\alpha_1}) + 2k\pi\sqrt{-1}}{\rho}.$$

Therefore the exponential polynomial

$$G(z) = g\left(\frac{\text{Log}(\frac{1}{\alpha_1}) + 2z\pi\sqrt{-1}}{\rho}\right)$$

vanishes at infinitely many integers. Now apply #1 -- then for some $m_0, d_0 \in Z$ ($d_0 \neq 0$), G vanishes on $\{m_0 + kd_0 : k \in Z\}$, thus $G(m_0 + zd_0)$ is an exponential polynomial which vanishes at all the integers, so $\sin(\pi z)$ divides $G(m_0 + zd_0)$ (cf. #2). Moving on, any integer is a zero of the exponential polynomial

$$F(z) = f\left(\frac{\text{Log}(\frac{1}{\alpha_1}) + 2z\pi\sqrt{-1}}{\rho}\right).$$

Therefore $F(m_0 + zd_0)$ is an exponential polynomial which vanishes at all the integers, so $\sin(\pi z)$ divides $F(m_0 + zd_0)$ (cf. #2). To conclude, consider

$$h(z) = \sin\left(\frac{\pi}{d_0}\left(\frac{\rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{2\pi\sqrt{-1}} - m_0\right)\right).$$

To analyze G (ditto for F), start from

$$G(m_0 + zd_0) = \sin(\pi z) G_0(z).$$

Then

$$G\left(m_0 + \frac{1}{d_0}\left(\frac{\rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{2\pi\sqrt{-1}} - m_0\right) d_0\right)$$

$$= G\left(m_0 + \frac{\rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{2\pi\sqrt{-1}} - m_0\right)$$

$$= G\left(\frac{\rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{2\pi\sqrt{-1}}\right)$$

$$= g\left(\frac{\mathrm{Log}(\frac{1}{\alpha_1}) + 2\left(\frac{\rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{2\pi\sqrt{-1}}\right)\pi\sqrt{-1}}{\rho}\right)$$

$$= g\left(\frac{\mathrm{Log}(\frac{1}{\alpha_1}) + \rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{\rho}\right)$$

$$= g(z)$$

$$= \sin\left(\frac{\pi}{d_0}\left(\frac{\rho z - \mathrm{Log}(\frac{1}{\alpha_1})}{2\pi\sqrt{-1}} - m_0\right)\right) G_0\ (\cdots)$$

$$= h(z)\ G_0\ (\cdots).$$

§58. *SHAPIRO'S CONJECTURE: CASE 2*

In this situation, both f,g are irreducible. If f = gu for some unit u $\in$ $\mathcal{E}$, (technically, f,g are associates), then g can serve as the "h" in §56, #3. On the other hand, if f,g are distinct irreducibles (meaning that they are not unit multiples of one another), then they cannot have a common divisor (see the Lemma in the Appendix to §56). Matters thus reduce to the following statement.

1: THEOREM (Admit SCHC). Let f,g be distinct irreducible exponential polynomials in $\mathcal{E}$ -- then f,g have at most a finite number of zeros in common.

The proof is difficult and lengthy, thus an outline of the argument will have to do.

2: REMARK Let f,g be exponential polynomials and assume that f is irreducible. Suppose further that f,g have infinitely many zeros in common -- then f divides g in the ring $\mathcal{E}$ (i.e., g/f is entire).

[Note: This assertion is equivalent to #1.]

Proceeding to #1, assume that f,g are distinct irreducibles with infinitely many zeros in common, the objective being to show that this forces a contradiction (namely that g divides f).

[Note: If g divides f, then g must be an associate of f, say f = gu (u $\in$ U$\mathcal{E}$), thereby forcing f to be a unit multiple of g, contradicting the supposition of "distinct".]

3: NOTATION Let S be the infinite set of nonzero common zeros of f,g.

4: MAIN LEMMA (Admit SCHC) There exists an infinite subset S' of S such that the Q-vector space spanned by S' is finite dimensional.

Without changing the notation, assume henceforth that S spans a finite dimensional vector space over Q.

Write

$$f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_n e^{\mu_n z}$$

and let Γ be the divisible hull of the multiplicative group generated by

$$\{e^{\mu_j s} : 1 \leq j \leq n,\ s \in S\},$$

that is, $\forall\ \gamma \in \Gamma$ and any nonzero integer ℓ, $\exists\ \zeta \in \Gamma$ such that $\zeta^{\ell} = \gamma$ and Γ is the smallest such group containing

$$\{e^{\mu_j s} : 1 \leq j \leq n,\ s \in S\}.$$

Since span_Q S is finite dimensional, Γ has finite rank.

5: DEFINITION A solution $\alpha_1,\ldots,\alpha_N$ of the linear equation

$$a_1 x_1 + \cdots + a_N x_N = 1$$

over C is nondegenerate if for every proper nonempty subset J of $\{1,\ldots,N\}$,

$$\sum_{j \in J} a_j \alpha_j \neq 0.$$

6: THEOREM (Evertse-Schlickewei-Schmidt) Let N be a positive integer and let Λ be a subgroup of $(C^{\times})^N$ of finite rank r — then any linear equation

$$a_1 x_1 + \cdots + a_N x_N = 1$$

over C with $a_1,\ldots,a_N \neq 0$ has at most

$$\exp((6N)^{3N}(r+1))$$

many nondegenerate solutions in Λ.

[Note: Only the fact that there exists a finite upper bound on the number of nondegenerate solutions in Λ will actually be used.]

7: DISCUSSION Let $q = \ell\text{in} - \dim_Q S$ and fix a Q-basis $\{s_1,\ldots,s_q\}$ of $\text{span}_Q S$. Let $s \in S$ -- then there exist $c_1,\ldots,c_q \in Q$ such that

$$s = \sum_{i=1}^{q} c_i s_i$$

=>

$$0 = f(s) = \lambda_1 \prod_{i=1}^{q} e^{\mu_1 c_i s_i} + \cdots + \lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}$$

=>

$$\left(\prod_{i=1}^{q} e^{\mu_1 c_i s_i}, \ldots, \prod_{i=1}^{q} e^{\mu_n c_i s_i}\right) \in \Gamma$$

is a solution of the equation

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0.$$

Put

$$\lambda_j' = \left(-\lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}\right)^{-1} \lambda_j \quad (1 \leq j \leq n - 1).$$

Then

$$\lambda_1' \prod_{i=1}^{q} e^{\mu_1 c_i s_i} + \cdots + \lambda_{n-1}' \prod_{i=1}^{q} e^{\mu_{n-1} c_i s_i}$$

$$= \left(-\lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}\right)^{-1} \lambda_1 \prod_{i=1}^{q} e^{\mu_1 c_i s_i}$$

$$+ \cdots + \left(-\lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}\right)^{-1} \lambda_{n-1} \prod_{i=1}^{q} e^{\mu_{n-1} c_i s_i}$$

$$= \frac{\lambda_1}{-\lambda_n} \frac{\prod_{i=1}^{q} e^{\mu_1 c_i s_i}}{\prod_{i=1}^{q} e^{\mu_n c_i s_i}} + \cdots + \frac{\lambda_{n-1}}{-\lambda_n} \frac{\prod_{i=1}^{q} e^{\mu_{n-1} c_i s_i}}{\prod_{i=1}^{q} e^{\mu_n c_i s_i}}$$

$$= - \frac{\lambda_1 \prod_{i=1}^{q} e^{\mu_1 c_i s_i} + \cdots + \lambda_{n-1} \prod_{i=1}^{q} e^{\mu_{n-1} c_i s_i}}{\lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}}$$

$$= - \frac{-\lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}}{\lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i}} = 1$$

$\Rightarrow$

$$\left(\prod_{i=1}^{q} e^{\mu_1 c_i s_i}, \ldots, \prod_{i=1}^{q} e^{\mu_{n-1} c_i s_i} \right)$$

is a solution of the equation

$$\lambda_1' y_1 + \cdots + \lambda_{n-1}' y_{n-1} = 1,$$

all solutions of which lie in some group Γ_0, a subgroup of Γ of finite rank. Now apply #6 to conclude that there are only finitely many nondegenerate solutions of

$$\lambda_1' y_1 + \cdots + \lambda_{n-1}' y_{n-1} = 1$$

in Γ_0.

<u>8:</u> LEMMA Let $\alpha, \beta \in S$ $(\alpha \neq \beta)$. Suppose that

$$\underline{a} = (a_1, \ldots, a_n)$$

is the solution of

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$$

corresponding to α and

$$\underline{b} = (b_1, \ldots, b_n)$$

is the solution of

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$$

corresponding to β. Then

$$\underline{a} \neq \underline{b}.$$

PROOF If $\underline{a} = \underline{b}$, then for $j = 1, \ldots, n$,

$$\prod_{i=1}^{q} (e^{\mu_j s_i})^{c_{\underline{a},i}} = \prod_{i=1}^{q} (e^{\mu_j s_i})^{c_{\underline{b},i}}$$

iff

$$\prod_{i=1}^{q} (e^{\mu_j s_i})^{c_{\underline{a},i} - c_{\underline{b},i}} = 1$$

iff

$$\mu_j \sum_{i=1}^{q} s_i (c_{\underline{a},i} - c_{\underline{b},i}) \in 2\pi\sqrt{-1}\, Z.$$

So, for any $j = 1,\ldots,n$,

$$\sum_{i=1}^{q} s_i(c_{\underline{a},i} - c_{\underline{b},i}) = \frac{2\pi\sqrt{-1}}{\mu_j} N_j,$$

where $N_j \in \mathbb{Z}$. Therefore

$$\frac{2\pi\sqrt{-1}}{\mu_1} N_1 = \frac{2\pi\sqrt{-1}}{\mu_2} N_2 = \cdots = \frac{2\pi\sqrt{-1}}{\mu_n} N_n$$

$\Rightarrow$

$$\mu_2 = \frac{\mu_1}{N_1} N_2$$

$$\mu_3 = \frac{\mu_1}{N_1} N_3$$

$$\vdots$$

$$\mu_n = \frac{\mu_1}{N_1} N_n.$$

Now put $\gamma = \frac{\mu_1}{N_1}$ -- then $f(z)$ is a polynomial in $e^{\gamma z}$, i.e., f is simple, a contradiction since f is not simple.

With this preparation, we are ready to tackle the proof of #1 (as reformulated at the beginning: f,g are distinct irreducibles with infinitely many zeros in common). It will be shown by induction on the length n of f that g divides f. Since f,g are distinct irreducibles, this is a contradiction.

$\underline{n = 2:}$ Suppose that

$$f(z) = \lambda_1 e^{\mu_1 z} + \lambda_2 e^{\mu_2 z}$$

or still,

$$f(z) = \lambda_1 e^{\mu_1 z} (1 + \lambda_1^{-1}\lambda_2 e^{(\mu_2-\mu_1)z}).$$

Then g(z) has infinitely many zeros in common with

$$(1 + \lambda_1^{-1}\lambda_2 e^{(\mu_2-\mu_1)z})$$

and as in §57 there is an exponential polynomial of the form sin(T(z)) dividing both f(z) and g(z). Since g is irreducible, this implies that g divides f.

Proof:

$$\begin{cases} f = \sin(T)u \\ \\ g = \sin(T)v \end{cases} \qquad (u,v \in UE)$$

=>

$$gv^{-1} = \sin(T)$$

=>

$$f = gv^{-1}u.$$

<u>Induction Hypothesis:</u> Assume that for every exponential polynomial $h \neq g$ and of length < n, if h and g have infinitely many zeros in common, then g divides h.

<u>n > 2:</u> Let as above

$$\lambda_1' y_1 + \cdots + \lambda_{n-1}' y_{n-1} = 1$$

be the linear equation associated with

$$f(z) = \lambda_1 e^{\mu_1 z} + \cdots + \lambda_n e^{\mu_n z}.$$

Then Γ_0 contains just a finite number of nondegenerate solutions of this equation (cf. #7). Consider the equation

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0.$$

Then each $s \in S$ gives rise to a solution and since S is infinite, it follows from #8 that this equation has infinitely many distinct solutions

$$\underline{\omega}_s \equiv (\omega_1^{(s)}, \ldots, \omega_n^{(s)}) \in \Gamma,$$

where

$$\omega_1^{(s)} = \prod_{i=1}^{q} e^{\mu_1 c_i s_i}, \ldots, \omega_n^{(s)} = \prod_{i=1}^{q} e^{\mu_n c_i s_i}.$$

Each $\underline{\omega}_s$ can be turned into a solution of

$$\lambda_1' y_1 + \cdots + \lambda_{n-1}' y_{n-1} = 1$$

by simply removing its last component. Bottom line: There are an infinity of distinct solutions to

$$\lambda_1' y_1 + \cdots + \lambda_{n-1}' y_{n-1} = 1,$$

any such being determined by an $s \in S$. Moreover all but finitely many are degenerate (cf. #6) and for a degenerate $\underline{\omega}_s$ there exists a proper nonempty $J_s \subset \{1,\ldots,n\}$ such that

$$\sum_{j \in J_s} \lambda_j \omega_j^{(s)} = 0.$$

In fact, if

$$\sum_{j \in J_s} \lambda_j' \prod_{i=1}^{q} e^{\mu_j c_i s_i} = 0,$$

then

$$\sum_{j \in J_s} \left(- \lambda_n \prod_{i=1}^{q} e^{\mu_n c_i s_i} \right)^{-1} \lambda_j \prod_{i=1}^{q} e^{\mu_j c_i s_i} = 0$$

$$\Rightarrow$$

$$\sum_{j \in J_s} \lambda_j \prod_{i=1}^{q} e^{\mu_j c_i s_i} = 0$$

$$\Rightarrow$$

$$\sum_{j \in J_s} \lambda_j \omega_j^{(s)} = 0.$$

Owing now to the Box Principle (cf. §7, #15), we can find a proper nonempty subset

$$T = \{j_1, \ldots, j_t\} \subset \{1, \ldots, n\}$$

such that for infinitely many $s \in S$,

$$\sum_{j \in T} \lambda_j \omega_j^{(s)} = 0.$$

Therefore the equation

$$\lambda_{j_1} x_{j_1} + \cdots + \lambda_{j_t} x_{j_t} = 0$$

has infinitely many solutions corresponding to common zeros of f, g.

<u>9:</u> LEMMA g divides f.

PROOF Put

$$f_T(z) = \lambda_{j_1} e^{\mu_{j_1} z} + \cdots + \lambda_{j_t} e^{\mu_{j_t} z} .$$

Then g has infinitely many zeros in common with f_T which are also zeros of f, thus also zeros of $f - f_T$. Both f_T and $f - f_T$ are elements of $\mathcal{E}$ of length strictly less than n (the length of f). Thanks to §56, #9, g has infinitely many zeros in common with either an irreducible or a simple factor of f_T in E, call this factor h_T. If h_T is simple, then we are in Case 1 and g, h_T must have a common divisor. Since g is irreducible, it then divides h_T ($g = au$, $h_T = ab$, $gu^{-1} = a$, $h_T = gu^{-1}b$). If h_T is irreducible, then it is either a unit multiple of g, in which case g divides h_T, or g and h_T are distinct irreducibles, in which case g divides h_T (induction hypothesis). So, in all cases g divides h_T, thus it also divides f_T. Analogously, g divides $f - f_T$. Therefore g divides f.

10: <u>N.B.</u> #9 is the sought for contradiction.

§59. DIFFERENTIAL ALGEBRA

Let K/k be fields of characteristic 0, where k is algebraically closed in K.

1: DEFINITION Suppose that V is a K-vector space -- then a linear map $d:K \to V$ is a k-derivation if $\forall\, x,y \in K$,

$$d(xy) = xd(y) + yd(x)$$

and if $\forall\, a \in k$,

$$d(a) = 0.$$

[Note: In particular, $d(1) = 1$.]

2: RAPPEL There is a K-vector space $\Omega_{K/k}$ and a k-derivation $d_{K/k}:K \to \Omega_{K/k}$ with the property that for any K-vector space V and any k-derivation $d:K \to V$ there is a unique K-linear map $\xi:\Omega_{K/k} \to V$ such that $d = \xi \circ d_{K/k}$:

$$\begin{tikzcd} K \arrow[r, "d_{K/k}"] \arrow[d, "d"'] & \Omega_{K/k} \arrow[d, equal] \\ V & \Omega_{K/k}. \arrow[l, "\xi"] \end{tikzcd}$$

3: SCHOLIUM Associated with every k-derivation $d:K \to K$ there is a unique derivation $D:\Omega_{K/k} \to \Omega_{K/k}$ such that $\forall\, x_1,x_2 \in K$,

$$D(x_1 d_{K/k}(x_2)) = d(x_1)d_{K/k}(x_2) + x_1 d_{K/k}(d(x_2)).$$

4: SUBLEMMA Suppose given a k-derivation $d:K \to V$ -- then for $y \in K$,

$z \in K^{\times}$,

$$D(d_{K/k}(y) - \frac{d_{K/k}(z)}{z} = 0$$

if

$$d(y) = \frac{d(z)}{z} .$$

PROOF The LHS equals

$$d_{K/k}(d(y)) - \frac{1}{z} d_{K/k}(d(z)) + \frac{d(z)}{z^2} d_{K/k}(z)$$

or still,

$$d_{K/k}(\frac{d(z)}{z}) - \frac{1}{z} d_{K/k}(d(z)) + \frac{d(z)}{z^2} d_{K/k}(z)$$

$$= \frac{zd_{K/k}(d(z)) - (d(z))d_{K/k}(z)}{z^2}$$

$$- \frac{1}{z} d_{K/k}(d(z)) + \frac{d(z)}{z^2} d_{K/k}(z)$$

$$= 0.$$

5: SUBLEMMA Suppose given a k-derivation $d:K \to V$ — then for $y \in K$,

$$D(d_{K/k}(y)) = 0$$

if $d(y) = 1$.

PROOF The LHS equals

$$D(1d_{K/k}(y))$$

$$= d(1)d_{K/k}(y) + 1d_{K/k}(d(y))$$

$$= 0 + d_{K/k}(1) = 0.$$

6: NOTATION Given $y_i \in K$, $z_i \in K^\times$ $(i = 1,\ldots,n)$, put

$$\omega_i = d_{K/k}(y_i) - \frac{d_{K/k}(z_i)}{z_i} \in \Omega_{K/k}.$$

7: LEMMA Suppose that $d:K \to V$ is a k-derivation. Assume that $d(y_1) = 1$ and that $y_i \in K$, $z_i \in K^\times$ are connected by the relation

$$d(y_i) = \frac{d(z_i)}{z_i} \quad (i = 1,\ldots,n).$$

Then for $f_1,\ldots,f_n$, $g \in K$,

$$D(\sum_i f_i\omega_i + g d_{K/k}(y_1))$$

$$= \sum_i (d(f_i)\omega_i + f_i D\omega_i) + d(g)d_{K/k}(y_1) + gD(d_{K/k}(y_1))$$

$$= \sum_i (d(f_i)\omega_i + f_i 0) + d(g)d_{K/k}(y_1) + g0$$

$$= \sum_i d(f_i)\omega_i + d(g)d_{K/k}(y_1).$$

In what follows, $d:K \to K$ is a derivation such that

$$\text{Ker } d = k(\supset Q).$$

8: CRITERION Let $K \supset F \supset k$, where F is a field and

$$\text{trdeg}_k F < \infty.$$

Denote by E the K-vector subspace of $\Omega_{K/k}$ generated by $d_{K/k}F$ -- then

$$\dim_K E = \text{trdeg}_k F.$$

9: EXAMPLE Take $F = K$ -- then

$$\dim_K \Omega_{K/k} = \mathrm{trdeg}_k K.$$

[• If $x_1,\ldots,x_n \in K$ are algebraically dependent over k, then $d_{K/k}(x_1),\ldots,$ $d_{K/k}(x_n) \in \Omega_{K/k}$ are linearly dependent over K.

• If $x_1,\ldots,x_n \in K$ are algebraically independent over k, then $d_{K/k}(x_1),\ldots,$ $d_{K/k}(x_n) \in \Omega_{K/k}$ are linearly independent over K.]

[Note: Therefore $d_{K/k}(x) = 0$ iff x is algebraic over k.]

Keep to the setup of #7 and in #8, let

$$F = k(y_1,\ldots,y_n, z_1,\ldots,z_n)$$

and suppose that $\mathrm{trdeg}_k F < n + 1$ — then there are elements $f_1,\ldots,f_n, g \in K$ not all zero such that

$$\sum_i f_i\omega_i + gd_{K/k}(y_1) = 0.$$

It can be assumed that $f_1,\ldots,f_n, g \in K$ have been chosen so that a minimal number of them are nonzero and at least one of them is 1.

Write

$$\begin{aligned} 0 &= D0 \\ &= D(\sum_i f_i\omega_i + gd_{K/k}(y_1)) \\ &= \sum_i d(f_i)\omega_i + d(g)d_{K/k}(y_1) \end{aligned}$$

to conclude by minimality that

$$d(f_1) = 0,\ldots,d(f_n) = 0, \ d(g) = 0,$$

thus

$$f_1 \in k, \ldots, f_n \in k,\ g \in k,$$

the field of constants of d being k (by hypothesis). Bearing in mind that

$$\sum_i f_i \omega_i + g d_{K/k}(y_1) = 0,$$

let $c_i = f_i$, $c_0 = g$, hence

$$\sum_i c_i \omega_i + c_0 d_{K/k}(y_1) = 0.$$

<u>10:</u> NOTATION Put

$$C = c_0 + c_1 y_1 + \cdots + c_n y_n.$$

<u>11:</u> LEMMA

$$d_{K/k}(C) = \sum_i c_i \frac{d_{K/k}(z_i)}{z_i}.$$

PROOF In fact,

$$\sum_i c_i \omega_i + c_0 d_{K/k}(y_1) = 0$$

or still,

$$\sum_i c_i \left(d_{K/k}(y_i) - \frac{d_{K/k}(z_i)}{z_i}\right) + c_0 d_{K/k}(y_1) = 0$$

=>

$$\sum_i c_i d_{K/k}(y_i) + c_0 d_{K/k}(y_1) = \sum_i c_i \frac{d_{K/k}(z_i)}{z_i}$$

=>

$$c_0 d_{K/k}(y_1) + \sum_i c_i d_{K/k}(y_i) = \sum_i c_i \frac{d_{K/k}(z_i)}{z_i}$$

=>

$$d_{K/k}(C) = \sum_i c_i \frac{d_{K/k}(z_i)}{z_i} .$$

Suppose that $c_1,\ldots,c_L$ is a Q-basis for $c_1,\ldots,c_n$, hence

$$c_i = \sum_{\ell=1}^{L} q_{\ell,i} c_\ell \quad (i = 1,\ldots,n).$$

Here, at least a priori, the $q_{\ell,i} \in Q$ but there is no loss of generality in taking $q_{\ell,i} \in Z$.

Accordingly

$$\begin{aligned} d_{K/k}(C) &= \sum_{i=1}^{n} c_i \frac{d_{K/k}(z_i)}{z_i} \\ &= \sum_{i=1}^{n} \sum_{\ell=1}^{L} q_{\ell,i} c_\ell \frac{d_{K/k}(z_i)}{z_i} \\ &= \sum_{\ell=1}^{L} c_\ell \Big(\sum_{i=1}^{n} q_{\ell,i} \frac{d_{K/k}(z_i)}{z_i}\Big) \\ &= \sum_{\ell=1}^{L} c_\ell \frac{d_{K/k}(w_\ell)}{w_\ell} , \end{aligned}$$

where

$$w_\ell = \prod_{i=1}^{n} z_i^{q_{\ell,i}} .$$

<u>12:</u> LEMMA Let $a_1,\ldots,a_L \in k$ be linearly independent over Q, let $u_1,\ldots,u_L \in K^\times$, let $v \in K$, and assume that

$$d_{K/k}(v) = \sum_{\ell=1}^{L} a_\ell \frac{d_{K/k}(u_\ell)}{u_\ell} .$$

Then

$$d_{K/k}(u_1) = 0,\ldots,d_{K/k}(u_L) = 0.$$

<u>13:</u> APPLICATION Take $a_1 = c_1,\ldots,a_L = c_L$, take $v = C$, and take

$$u_1 = w_1,\ldots,u_L = w_L.$$

Then

$$d_{K/k}(w_1) = 0,\ldots,d_{K/k}(w_L) = 0.$$

<u>14:</u> <u>N.B.</u> Since the standing assumption is that k is algebraically closed in K, each $w_\ell \in k$ (cf. #9).

<u>15:</u> APPLICATION For $\ell = 1,\ldots,L$,

$$\prod_{i=1}^{n} z_i^{q_{\ell,i}} \in k.$$

Finally

$$w_\ell \in k \Rightarrow d(w_\ell) = 0$$

$\Rightarrow$

$$0 = \frac{d(w_\ell)}{w_\ell} = \sum_{j=1}^{L} q_{\ell,j} \frac{d(z_j)}{z_j}$$

$$= \sum_{j=1}^{L} q_{\ell,j}\, d(y_j)$$

$$= d(\sum_{j=1}^{L} q_{\ell,j}\, y_j)$$

=>

$$\sum_{j=1}^{L} q_{\ell,j} y_j \in k.$$

<u>16:</u> SCHOLIUM There exist integers $m_1,\ldots,m_n$ not all zero such that

$$\sum_{i=1}^{n} m_i y_i \in k.$$

Recall:

- $y_i \in K$, $z_i \in K^\times$, and

$$d(y_i) = \frac{d(z_i)}{z_i} \quad (i = 1,\ldots,n).$$

- $F = k(y_1,\ldots,y_n, z_1,\ldots,z_n)$ and

$$\operatorname{trdeg}_k F < n + 1.$$

Then under these assumptions:

(1) There are $m_1,\ldots,m_n \in Z$ not all zero such that

$$\prod_{i=1}^{n} z_i^{m_i} \in k.$$

(2) There are $m_1,\ldots,m_n \in Z$ not all zero such that

$$\sum_{i=1}^{n} m_i y_i \in k.$$

<u>17:</u> STATEMENT Maintain the supposition that

$$d(y_i) = \frac{d(z_i)}{z_i} \quad (i = 1,\ldots,n)$$

but assume that the y_i are Q-linearly independent modulo k, i.e.,

$$\sum_{i=1}^{n} q_i y_i \in k \Rightarrow q_i = 0 \quad (i = 1,\ldots,n).$$

Then

$$\operatorname{trdeg}_k F \geq n + 1.$$

§60. *FORMAL SCHANUEL*

This is a version of Schanuel that can be established rigorously. However, before proceeding to the particulars, let us review the situation.

As is usually formulated, Schanuel's conjecture is the following statement (cf. §47, #1).

1: CONJECTURE Suppose that $x_1,\ldots,x_n$ are Q-linearly independent complex numbers — then among the 2n numbers

$$x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n},$$

at least n are algebraically independent over Q, i.e.,

$$\text{trdeg}_Q\ Q(x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n}) \geq n.$$

There are other equivalent formulations. E.g.: $\forall\ \underline{x}$,

$$\delta(\underline{x}) \geq 0 \quad (\text{cf. §47, \#24 and \#27}).$$

Here are two more.

2: CONJECTURE Suppose that $x_1,\ldots,x_n$ are complex numbers such that

$$\text{trdeg}_Q\ Q(x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n})$$

is $< n$ — then there are integers $m_1,\ldots,m_n$ not all zero such that

$$\sum_{i=1}^{n} m_i x_i = 0.$$

3: CONJECTURE Suppose that $x_1,\ldots,x_n$ are complex numbers such that

$$(x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n})$$

lie in an algebraic subvariety V of $\mathbb{C}^{2n}$ defined over $\mathbb{Q}$ and of dimension strictly less than n -- then there are integers $m_1,\ldots,m_n$ not all zero such that

$$\sum_{i=1}^{n} m_i x_i = 0.$$

[The assumption that

$$(x_1,\ldots,x_n,\ e^{x_1},\ldots,e^{x_n}) \in V \ (\dim V < n)$$

forces

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

We shall turn now to a setting in which an analog of Schanuel's conjecture is true.

4: NOTATION Let R be a commutative ring with 1 -- then

$$R[[X]]$$

is the ring of formal power series over R, a typical element of which is denoted by

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \quad (\forall\, n,\ a_n \in R).$$

5: N.B. If R is an E-ring, then R[[X]] is also an E-ring.

[Given $f \in R[[X]]$, write

$$f = a_0 + g \quad (g(X) = \sum_{n=1}^{\infty} a_n X^n)$$

and put

$$\exp(f) = E(a_0)\exp(g),$$

where $E(a_0)$ is that derived from R and

$$\exp(g) = \sum_{n=0}^{\infty} \frac{(g)^n}{n!} .]$$

6: CONSTRUCTION Let

$$\begin{cases} f(X) = \sum_{n=1}^{\infty} a_n X^n = a_1 X + a_2 X^2 + \cdots \\ g(X) = \sum_{n=0}^{\infty} b_n X^n = b_0 + b_1 X + b_2 X^2 + \cdots . \end{cases}$$

Then their composite $g \circ f$ is the formal power series

$$g(f(X)) = \sum_{n=0}^{\infty} b_n (f(X))^n = \sum_{n=0}^{\infty} c_n X^n.$$

7: REMARK The foregoing operation is valid only when $f(X)$ has no constant term (for then each c_n depends on but a finite number of coefficients of $f(X)$ and $g(X)$).

[To illustrate, let

$$\exp(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \frac{X^4}{4!} + \cdots .$$

Then it makes sense to form

$$\exp(\exp(X) - 1) = 1 + X + X^2 + \frac{5}{6} X^3 + \frac{5}{8} X^4 + \cdots$$

but

$$\exp(\exp(X)) \ldots ?]$$

[Note: If $f(X)$ has no constant term, then $E(a_0) = E(0) = 1$ and one can form

$$\exp \circ f,$$

which agrees with #5.]

8: LEMMA If R is an integral domain, then so is R[[X]].

9: DEFINITION A formal Laurent series over R is a series of the form

$$f(X) = \sum_{n \in Z} a_n X^n,$$

where $a_n = 0$ for all but finitely many negative indices n.

10: N.B. The formal Laurent series form a ring, denoted by R((X)).

11: LEMMA If R = K is a field, then K((X)) is a field.

[Note: K((X)) can be identified with the field of fractions of the integral domain K[[X]].]

12: DEFINITION Take R = K of characteristic 0 -- then the formal derivative of the formal Laurent series

$$f(X) = \sum_{n \in Z} a_n X^n$$

is

$$f' = \partial f = \sum_{n \in Z} n a_n X^{n-1}.$$

13: N.B.

$$\partial : K((X)) \to K((X))$$

is a K-derivation (Ker ∂ = K).

Having dispensed with the formalities, specialize and take per §59,

$$K = \mathbf{C}((X)),\ k = \mathbf{C},\ d = \partial.$$

Let

$$y_1 \in X\mathbf{C}[[X]], \ldots, y_n \in X\mathbf{C}[[X]]$$

be Q-linearly independent and put

$$z_1 = \exp(y_1), \ldots, z_n = \exp(y_n).$$

<u>14:</u> THEOREM

$$\operatorname{trdeg}_C C(y_1,\ldots,y_n, z_1,\ldots,z_n) \geq n + 1.$$

[Quote §59, #17 (obviously, if the y_i are Q-linearly independent, then they are Q-linearly independent modulo C).]

This result can be rephrased.

<u>15:</u> RAPPEL (cf. §46, #20) Given fields $k \subset K \subset L$,

$$\operatorname{trdeg}_k(L/k) = \operatorname{trdeg}_K(L/K) + \operatorname{trdeg}_k(K/k).$$

Abbreviate

$$(y_1,\ldots,y_n, z_1,\ldots,z_n)$$

to

$$(\underline{y},\underline{z}).$$

Take in #15

$$k = C,\ K = C(X),\ L = C(X)(\underline{y},\underline{z}).$$

Then

$$\operatorname{trdeg}_C C(X)(\underline{y},\underline{z}) = \operatorname{trdeg}_{C(X)} C(X)(\underline{y},\underline{z}) + \operatorname{trdeg}_C C(X).$$

From #14

$$\operatorname{trdeg}_C C(X)(\underline{y},\underline{z}) > \operatorname{trdeg}_C C(\underline{y},\underline{z}) \geq n + 1.$$

And

$$\operatorname{trdeg}_C C(X) = 1.$$

Therefore

$$n + 1 \leq \operatorname{trdeg}_C C(X)(\underline{y},\underline{z})$$

$$= \operatorname{trdeg}_{C(X)} C(X)(\underline{y},\underline{z}) + 1$$

=>

$$n \leq \operatorname{trdeg}_{C(X)} C(X)(\underline{y},\underline{z}).$$

16: SUMMARY The fact that

$$\operatorname{trdeg}_{C(X)} C(X)(y_1,\ldots,y_n, z_1,\ldots,z_n) \geq n$$

is formal Schanuel, a result due to J. Ax. It is the power series analog of #1 (which remains conjectural).

17: N.B.

$$\begin{array}{ccccc} C & \subset & C[X] & \subset & C[[X]] \\ & & \cap & & \cap \\ & & C(X) & \subset & C((X)). \end{array}$$

§61. *AN ARITHMETIC CRITERION*

Recall:

1: SCHANUEL'S CONJECTURE Suppose that $x_1,\ldots,x_n$ are Q-linearly independent complex numbers -- then

$$\operatorname{trdeg}_Q Q(x_1,\ldots,x_n, e^{x_1},\ldots,e^{x_n}) \geq n.$$

2: NOTATION The symbol $\mathcal{D}$ stands for the derivation

$$\mathcal{D} = \frac{\partial}{\partial X_0} + X_1 \frac{\partial}{\partial X_1}$$

in the ring $C[X_0,X_1]$.

3: DEFINITION The height $H(P)$ of a polynomial $P \in C[X_0,X_1]$ is the maximum of the absolute values of its coefficients.

4: DATA Let n be a positive integer, let $x_1,\ldots,x_n$ be Q-linearly independent complex numbers, and let $\alpha_1 \in C^\times,\ldots,\alpha_n \in C^\times$.

5: PARAMETERS Let s_0,s_1,t_0,t_1,u be positive real numbers subject to

$$\max\{1,t_0,2t_1\} < \min\{s_0,2s_1\}$$

and

$$\max\{s_0,s_1 + t_1\} < u < \frac{1}{2}(1 + t_0 + t_1).$$

6: ROY'S CONJECTURE In the presence of #4 and #5, assume that for any sufficiently large positive integer N, there exists a nonzero polynomial

$P_N \in \mathbb{Z}[X_0,X_1]$ with partial degree $\leq N^{t_0}$ in X_0, with partial degree $\leq N^{t_1}$ in X_1, and with height $\leq e^N$ which satisfies

$$|(\mathcal{D}^k P_N)(\sum_{j=1}^n m_j x_j, \prod_{j=1}^n \alpha_j^{m_j})| \leq \exp(-N^u)$$

for all nonnegative integers $k,m_1,\ldots,m_n$, where

$$k \leq N^{s_0} \text{ and } \max\{m_1,\ldots,m_n\} \leq N^{s_1}.$$

Then

$$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(x_1,\ldots,x_n, \alpha_1,\ldots,\alpha_n) \geq n.$$

7: THEOREM Roy's conjecture is equivalent to Schanuel's conjecture.

This result is due to Damien Roy. While we shall omit the proof, some hints will be given below.

[Note: Spelled out: If Roy's conjecture is true for some n and some choice of s_0,s_1,t_0,t_1,u (per #5), then Schanuel's conjecture is true for this value of n. Conversely, if Schanuel's conjecture is true for some n, then Roy's conjecture is true for the same value of n and any choice of s_0,s_1,t_0,t_1,u (per #5).]

In one direction, assume that the conditions in Roy's conjecture are in force -- then it can be shown that there exists an integer $K \geq 1$ with the property that

$$\alpha_j^K = e^{Kx_j} \quad (j = 1,\ldots,n).$$

Since $x_1,\ldots,x_n$ are $\mathbb{Q}$-linearly independent, the same is true of $Kx_1,\ldots,Kx_n$, hence by Schanuel

$$\mathrm{trdeg}_Q\ Q(Kx_1,\ldots,Kx_n,\ e^{Kx_1},\ldots,e^{Kx_n}) \geq n$$

or still,

$$\mathrm{trdeg}_Q\ Q(Kx_1,\ldots,Kx_n,\ \alpha_1^K,\ldots,\alpha_n^K) \geq n$$

or still,

$$\mathrm{trdeg}_Q\ Q(x_1,\ldots,x_n,\ \alpha_1,\ldots,\alpha_n) \geq n.$$

Therefore

SCHANUEL => ROY.

In the other direction, take the data as in #4 and put $\alpha_j = e^{x_j}$ $(j = 1,\ldots,n)$. Take the parameters s_0,s_1,t_0,t_1,u as in #5 and impose the inequalities to be found there.

8: NOTATION Given $R > 0$, let

$$B(0,R) = \{(z_1,z_2) \in C^2 : |z_1| \leq R,\ |z_2| \leq R\}$$

and for any continuous function $F:B(0,R) \to C$, put

$$|F|_R = \sup\{|F(z_1,z_2)| : |z_1| = R,\ |z_2| = R\}.$$

[Note: By the maximum modulus principle, when F is holomorphic in the interior of $B(0,R)$, $|F|_R$ is the supremum of $|F|$ on $B(0,R)$.]

9: EXAMPLE Let L be a positive integer, let r_0,r,R be positive real numbers with $r \geq r_0$, $R \geq 2r$ -- then

$$|F|_r \leq \sum_{j,k\geq 0} \frac{1}{j!k!} \left| \frac{\partial^{j+k}}{\partial z^j \, \partial w^k} (0,0) \right| r^{j+k}$$

or still,

$$|F|_r \leq \sum_{j+k<L} \left(\frac{r}{r_0}\right)^{j+k} |F|_{r_0} + \sum_{j+k\geq L} \left(\frac{r}{R}\right)^{j+k} |F|_R$$

or still,

$$|F|_r \leq \binom{L+1}{2} \left(\frac{r}{r_0}\right)^L |F|_{r_0} + (2L+4)\left(\frac{r}{R}\right)^L |F|_{R'}$$

where

$$\sum_{j+k\geq L} 2^{L-j-k} = 2L + 4.$$

[Note: The conditions on F are, of course, the obvious ones... .]

<u>10:</u> LEMMA For any sufficiently large positive integer N, there exists a nonzero polynomial $P_N \in \mathbb{Z}[X_0,X_1]$ with partial degree $\leq N^{t_0}$ in X_0, with partial degree $\leq N^{t_1}$ in X_1, and with height $\leq e^N$ such that the function

$$f_N(z) = P_N(z,e^z)$$

satisfies

$$|f_N|_r \leq \exp(-2N^u).$$

[Note: Here

$$r = 1 + AN^{s_1},$$

where

$$A = |x_1| + \cdots + |x_n|.]$$

The claim now is that

$$\text{ROY} \Rightarrow \text{SCHANUEL}.$$

To verify that this is so, let $k, m_1, \ldots, m_n$ be nonnegative integers, where

$$k \leq N^{s_0} \text{ and } \max\{m_1, \ldots, m_n\} \leq N^{s_1}.$$

Then

$$|(\mathcal{D}^k P_N)(\sum_{j=1}^{n} m_j x_j, \prod_{j=1}^{n} \alpha_j^{m_j})|$$

$$= \left| \frac{d^k f_N}{dz^k} (\sum_{j=1}^{n} m_j x_j) \right|$$

$$\leq k! \ |f_N|_r \leq \exp(-N^u)$$

if N is sufficiently large. Consequently

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

thus

$$\text{ROY} \Rightarrow \text{SCHANUEL}$$

as claimed.

<u>11:</u> <u>N.B.</u> Consider the situation when $n = 1$ --- then

$$|(\mathcal{D}^k P_N)(mx, \alpha^m)|$$

$$= \left| \frac{d^k f_N}{dz^k} (mx) \right|$$

$$\leq k! \ |f_N|_{|mx| + 1}.$$

Next

$$|mx| + 1 \leq |x|N^{s_1} + 1 = r$$

=>

$$|(\mathcal{D}^k P_N)(mx, \alpha^m)| \leq k! \ |f_N|_r.$$

Since $s_0 < u$, it can be assumed that

$$N^{s_0} \ \ell n(N^{s_0}) \leq N^u,$$

from which

$$\exp(N^u) \geq \exp(N^{s_0} \ \ell n(N^{s_0}))$$

$$= \exp(\ell n((N^{s_0})^{N^{s_0}}))$$

$$= (N^{s_0})^{N^{s_0}}$$

=>

$$k! \leq k^k \leq (N^{s_0})^{N^{s_0}} \leq \exp(N^u)$$

=>

$$|(\mathcal{D}^k P_N)(mx, \alpha^m)| \leq \exp(N^u)|f_N|_r$$

$$\leq \exp(N^u)\exp(-2N^u) = \exp(-N^u).$$

<u>12:</u> REMARK When $n = 1$, Schanuel is an acquired fact: If $x \in C^\times$, then at least one of the two numbers x, e^x is transcendental (Hermite-Lindemann), hence

$$\mathrm{trdeg}_Q \ Q(x, e^x) \geq 1,$$

so Roy is automatic in this case.

APPENDIX

PRETHEOREM Let $(x,\alpha) \in \mathbb{C} \times \mathbb{C}^\times$ and let s_0, s_1, t_0, t_1, u be positive real numbers satisfying the inequalities of #5 — then the following conditions are equivalent:

(i) There exists an integer $K \geq 1$ such that $\alpha^K = e^{Kx}$.

(ii) For any sufficiently large positive integer N, there exists a nonzero polynomial $P_N \in \mathbb{Z}[X_0, X_1]$ with partial degree $\leq N^{t_0}$ in X_0, with partial degree $\leq N^{t_1}$ in X_1, and with height $\leq e^N$ which satisfies

$$|(\mathcal{D}^k P_N)(mx, \alpha^m)| \leq \exp(-N^u)$$

for all nonnegative integers k,m with

$$k \leq N^{s_0} \text{ and } m \leq N^{s_1}.$$

In what follows, we shall sketch the proof that

$$\text{(ii)} \Rightarrow \text{(i) or } \neg\text{(i)} \Rightarrow \neg\text{(ii)}.$$

Now $\neg$ (i) means that $\forall\, K \in \mathbb{N}$, $\alpha^K \neq e^{Kx}$, hence αe^{-x} is not a root of unity:

$$\alpha e^{-x} = \zeta \ (\zeta^K = 1) \Rightarrow \alpha^K = \zeta^K e^{Kx} = e^{Kx}.$$

OBJECTIVE Let $(x,\alpha) \in \mathbb{C} \times \mathbb{C}^\times$ and let s_0, s_1, t_0, t_1, u be positive real numbers such that

$$\max\{1, t_0, 2t_1\} < \min\{s_0, 2s_1\} < u.$$

Suppose that αe^{-x} is not a root of unity — then condition (ii) does not hold for the pair (x,α).

[Note: The stated assumption on the parameters s_0,s_1,t_0,t_1,u is weaker than that of #5. Observe too that there is no restriction from above on u.]

NOTATION Given $\gamma \in C - Q$ and a positive integer N, put

$$\Gamma_\gamma(N) = \min\{|m + n\gamma| : m,n \in Z,\ 0 < \max\{|m|, |n|\} < N .$$

LEMMA For infinitely many N,

$$\Gamma_\gamma(N) \geq \frac{1}{2N} ,$$

i.e., for infinitely many N,

$$|m + n\gamma| \geq \frac{1}{2N}$$

for any pair $(m,n) \in Z^2$ with

$$0 < \max\{|m|, |n|\} < N.$$

PROOF Assume to the contrary that for any integer N larger than some N_0, there are integers $m(N)$ and $n(N)$ such that

$$0 < \max\{|m(N)|, |n(N)|\} < N$$

and

$$|m(N) + n(N)\gamma| < \frac{1}{2N} .$$

Then $n(N) \neq 0$ and

$$\begin{aligned} &|m(N)n(N + 1) - m(N + 1)n(N)| \\ &\leq |m(N) + n(N)\gamma| \cdot |n(N + 1)| \\ &+ |m(N + 1) + n(N + 1)\gamma| \cdot |n(N)| < 1, \end{aligned}$$

$$\Rightarrow$$

$$m(N)n(N+1) - m(N+1)n(N) = 0.$$

Therefore the ratio

$$\frac{m(N)}{n(N)}$$

is a constant $q \in Q$. But

$$|q + \gamma| = |m(N) + n(N)\gamma|/|n(N)|$$

$$< \frac{1}{2N}$$

for any $N > N_0$, hence $\gamma = -q$, a contradiction.

One can thus attach to each $\gamma \in C - Q$ an infinite subset S_γ of N, where the elements of S_γ are the N figuring in the definition of $\Gamma_\gamma(N)$.

N.B. Choose λ such that $e^\lambda = \alpha$ — then the ratio

$$\gamma = \frac{\lambda - x}{2\pi\sqrt{-1}} \in C - Q.$$

[Suppose instead that

$$\frac{\lambda - x}{2\pi\sqrt{-1}} = q \ (\in Q),$$

say $q = \frac{m}{n}$ $(n > 0)$, so

$$\lambda - x = q(2\pi\sqrt{-1}) = \frac{m}{n}(2\pi\sqrt{-1})$$

$$\Rightarrow$$

$$e^{\lambda - x} = \exp\left(\frac{m}{n} 2\pi\sqrt{-1}\right)$$

=>

$$\alpha e^{-x} = \exp(\frac{m}{n} 2\pi\sqrt{-1})$$

=>

$$(\alpha e^{-x})^n = \exp(m 2\pi\sqrt{-1}) = 1.]$$

NOTATION Let

$$\underline{u} = (0,\ 2\pi\sqrt{-1}),\ \underline{v} = (x,\lambda),\ \underline{w} = (1,1).$$

[Note:

$$\underline{v} - \gamma\underline{u} = (x,\lambda) - \gamma(0,\ 2\pi\sqrt{-1})$$

$$= (x,\lambda) - \frac{\lambda - x}{2\pi\sqrt{-1}}(0,\ 2\pi\sqrt{-1})$$

$$= (x,\lambda) - (\lambda - x)(0,1)$$

$$= (x,\lambda) + (0,\ x - \lambda)$$

$$= (x,\ \lambda + x - \lambda) = (x,x) = x\underline{w}.]$$

FACT There exists a constant $C \geq 1$ (with $\underline{u},\underline{v} \in B(0,C)$) such that for any $N \in S_\gamma$ and for any pair of real numbers r,R with $R \geq 2r$ and $r \geq CN$ and for any continuous function $F:B(0,R) \to \mathbb{C}$ which is holomorphic in the interior of $B(0,R)$, the estimate

$$|F|_r \leq \left(\frac{Cr}{N}\right)^{N^2}$$

$$\times \max\{\frac{1}{k!}\,|D_{\underline{w}}^k F(m\underline{u} + n\underline{v})|N^k : 0 \leq k < N^2,\ 0 \leq m,n < N\}$$

$$+ \left(\frac{Cr}{R}\right)^{N^2} |F|_R$$

obtains.

[Note: Here

$$D_{\underline{w}} = \frac{\partial}{\partial z_1} + \frac{\partial}{\partial z_2} \,.]$$

To establish our objective, proceed in steps.

Step 1: Take

$$\gamma = \frac{\lambda - x}{2\pi\sqrt{-1}} \in \mathbf{C} - \mathbf{Q}.$$

Then S_γ is an infinite subset of $\mathbf{N}$, a generic element $N \in S_\gamma$ being allowed to "float".

Step 2: Put

$$s = \min\{s_0/2, s_1\}$$

and let M denote the smallest positive integer such that $N \leq M^s$ (tacitly, $N \in S_\gamma$). Note that M dpends on N (but M need not belong to S_γ) and we shall actually work with M rather than N in the statement of the objective.

Step 3: Choose a nonzero polynomial $Q_M \in \mathbf{Z}[X_0, X_1]$ with partial degree $\leq M^{t_0}$ in X_0, with partial degree $\leq M^{t_1}$ in X_1, and with height $\leq e^M$.

Step 4: Let

$$\left[\begin{array}{l} 0 \leq k \leq M^{s_0} \\ \\ 0 \leq m \leq M^{s_1} \end{array}\right.$$

and put

$$A = \max_{k,m} |(\mathcal{D}^k Q_M)(mx, \alpha^m)|,$$

the claim being that if N is sufficiently large, then

$$A > \exp(-M^u)\ (\exists\, u >> 0),$$

hence for some k, for some m,

$$|(\mathcal{D}^k Q_M)(mx, \alpha^m)| > \exp(-M^u),$$

thereby completing the proof.

Step 5: Define an entire function $G_M: C^2 \to C$ by the prescription

$$G_M(z,w) = Q_M(z, e^w).$$

Let

$$\partial = \partial/\partial z + \partial/\partial w.$$

Then

$$\partial^k G_M(z,w) = (\mathcal{D}^k Q_M)(z, e^w)$$

for any integer $k \geq 0$ and any $(z,w) \in C^2$.

Step 6: For any $(n,m) \in Z^2$,

$$(\partial^k G_M)(n\underline{u} + m\underline{v}) = (\mathcal{D}^k Q_M)(mx, \alpha^m).$$

Step 7: $N^2 \leq M^{s_0}$, $N \leq M^{s_1}$

=>

$$\max\{\frac{1}{k!}\,|(\partial^k G_M)(m\underline{u} + n\underline{v})|N^k : 0 \leq k < N^2,\ 0 \leq m,n < N\}$$

$$\leq A \sum_{k=0}^{\infty} \frac{N^k}{k!} = Ae^N.$$

<u>Step 8</u>: Introduce the constant $C \geq 1$ as above and specialize r, R by taking $r = CN$ and $R = eCR$ -- then in review

$$|F|_r \leq \left(\frac{Cr}{N}\right)^{N^2}$$

$$\times \max\left\{\frac{1}{k!}\,|(\partial^k F)(m\underline{u} + n\underline{v})|N^k : 0 \leq k < N^2,\ 0 \leq m,n < N\right\}$$

$$+ \left(\frac{Cr}{R}\right)^{N^2} |F|_R$$

and in the situation at hand ($F = G_M$)

$$\left[\begin{array}{l} \left(\frac{Cr}{N}\right)^{N^2} = (C \cdot C)^{N^2} = (C^2)^{N^2} = C^{2N^2} \\ \\ \left(\frac{Cr}{R}\right)^{N^2} = \left(\frac{Cr}{eCr}\right)^{N^2} = e^{-N^2}, \end{array}\right.$$

so

$$|G_M|_r \leq C^{2N^2} Ae^N + e^{-N^2} |G_M|_R.$$

<u>Step 9</u>: Since $\max\{1, t_0, s + t_1\} < 2s$, the definitions imply that

$$|G_M|_R \leq (M^{t_0} + 1)(M^{t_1} + 1)$$

$$\times \exp(M + M^{t_0} \ell n(R) + RM^{t_1})$$

$$\leq e^{N^2}/2$$

provided N is sufficiently large.

Step 10: Q_M is a nonzero polynomial with integral coefficients, hence

$$1 \le H(Q_M) \le |Q_M|_1 \le |G_M|_\pi \le |G_M|_r$$

if $r \le \pi$.

Step 11: Explicate the relation

$$|G_M|_r \le C^{2N^2} Ae^N + e^{-N^2} |G_M|_R$$

to arrive at

$$1 \le |G_M|_{CN} \le C^{2N^2} Ae^N + e^{-N^2} (e^{N^2}/2)$$

for N large enough.

I.e.:

$$1 \le C^{2N^2} e^N A + \frac{1}{2} .$$

I.e.:

$$\frac{1}{2} \le C^{2N^2} e^N A.$$

I.e.:

$$A \ge \frac{1}{2} C^{-2N^2} e^{-N}.$$

Step 12: Apart from the restriction that

$$\min\{s_0, 2s_1\} < u,$$

the parameter $u >> 0$ is at our disposal and can be chosen as large as we please. Bearing in mind that $2s$ is $< u$, or now, as will be notationally convenient, $2s$ is $< v$, write

$$N \le M^s \Rightarrow N^2 \le M^{2s} < M^v$$

$$\Rightarrow e^{N^2} < \exp(M^v).$$

Consequently for some $u > v >> 0$,

$$A \geq \frac{1}{2} C^{-2N^2} e^{-N} > \exp(-M^u).$$

[To see this, ignore the $\frac{1}{2}$ and for simplicity take $C = e$ -- then

$$\begin{aligned} N^2 < M^v \Rightarrow 2N^2 &< 2M^v \\ &< 2^v M^v = (2M)^v \\ &= M^w. \end{aligned}$$

Here

$$w = v\,\frac{\ln(2M)}{\ln(M)} > v.$$

In fact,

$$\begin{aligned} (2M)^v = M^w &\Rightarrow \ln((2M)^v) = \ln(M^w) \\ &\Rightarrow v\ln(2M) = w\ln(M). \end{aligned}$$

Therefore

$$\begin{aligned} e^{2N^2} e^N &< \exp(M^w)\exp(M^v) \\ &= \exp(M^w + M^v) \\ &< \exp(2M^w) \\ &< \exp(2^w M^w) \\ &= \exp((2M)^w) \\ &= \exp(M^u) \end{aligned}$$

if

$$u = w \frac{\ell n(2M)}{\ell n(M)} > w \ (> v).$$

Accordingly

$$e^{-2N^2}\, e^{-N} > \exp(-M^u).]$$

§62. *REAL NUMBERS* (bis)

"Few mathematical structures have undergone as many revisions or have been presented in as many guises as the real numbers. Every generation re-examines the reals in the light of its ... mathematical objectives."

[F. Faltin et al., Advances in Mathematics 16 (1975), p. 278.]

* * * * * * * * * * *

"How do we get future generations to take the validity of real numbers for granted? We indoctrinate them early in their careers when they are eager but impressionable undergraduates. Here's how we do it. First we soften them up with a "Constructing the Real Numbers" blurb in their first calculus course. Needless to say we don't really construct real numbers as they are by definition unconstructible. But the phrase sticks in their minds long after the details are forgotten."

[N. J. Wildberger, The Mathematical Intelligencer 21 (1999), pp. 4-7.]

* * * * * * * * * * *

"How real are real numbers? ... The frightening features are the unsolvability of the halting problem (Turing, 1936), the fact that most reals are uncomputable, and last but not least, the halting probability Ω, which is irreducibly complex (algorithmically random), maximally unknowable, and dramatically illustrates the limits of reason."

[Gregory Chaitin, arXiv:math/0411418 v 3 [math. HO] 29 Nov 2004.

* * * * * * * * * * *

APPENDIX

In algorithmic information theory, a <u>halting probability</u> (or <u>Chaitin constant</u>) is a real number Ω which represents the probability that a randomly constructed program will halt.

To be precise, let P_F be the domain of a prefix-free universal computable function F -- then the halting probability Ω_F of P_F is by definition

$$\Omega_F = \sum_{p \in P_F} 2^{-|p|},$$

where $|p|$ denotes the length of a binary string p. The sum defining Ω_F is infinite and converges to a real number lying between 0 and 1.

FACT Ω_F is transcendental.

There is a probabilistic interpretation of Ω_F, from which the terminology. Thus let (X,μ) be the Cantor space and suppose that F is a prefix-free universal computable function -- then the domain P_F of F consists of an infinite set of binary strings:

$$P_F = \{p_1, p_2, \ldots\}.$$

Each of these strings p_i determines a subset S_i of Cantor space (viz. all sequences in Cantor space that begin with p_i). Moreover the S_i are pairwise disjoint and

$$\Omega_F = \mu\left(\bigcup_{i \in N} S_i\right).$$

REMARK Ω_F is not computable, i.e., there is no algorithm which, given n, returns the first n digits of Ω_F.

For more information on this material, consult George Barmpalias (arXiv:1707.08109 v 3 [math. LO]).

SUPPLEMENT

TRANSCENDENCE OF SERIES

The overall theme is to discuss the transcendence of numbers of the form

$$\sum_{n=1}^{\infty} \frac{A(n)}{B(n)} \qquad \left(\text{or} \quad \sum_{n=0}^{\infty} \frac{A(n)}{B(n)}\right)$$

or

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)} \equiv \lim_{N \to \infty} \sum_{|n|<N} \frac{A(n)}{B(n)} .$$

The literature on this subject is extensive and no attempt will be made at a systematic exposition. Foregoing this, we shall first examine a number of instructive special cases and then take a look at the general picture.

[Note: Omitted details are to be regarded as exercises ad libitum.]

§1. *CANONICAL ILLUSTRATIONS*

1: EXAMPLE

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+1}\right) = 1.$$

2: EXAMPLE

$$\sum_{n=0}^{\infty} \frac{1}{n!} = e \text{ and } \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1} = \frac{\pi}{4},$$

both of which are transcendental.

3: EXAMPLE

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ell n(2),$$

a transcendental number (cf. §21, #9).

4: EXAMPLE

$$\sum_{n=1}^{\infty} \frac{1}{n^3} = \zeta(3),$$

an irrational number, the transcendence of which has yet to be shown.

5: EXAMPLE

$$\sum_{n=1}^{\infty} \left(\frac{1}{n} - \ell n\left(1 + \frac{1}{n}\right)\right) = \gamma,$$

γ being Euler's constant, which is not known to be irrational, let alone transcendental.

6: EXAMPLE

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2} = G,$$

G being Catalan's constant, whose irrationality status is unknown.

[Note: By comparison,

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^3} = \frac{\pi^3}{32}\ .]$$

7: LEMMA The zeros of the polynomial $X^2 - X - 1$ are $\phi = \frac{1+\sqrt{5}}{2}$ (the golden ratio) and $\psi = \frac{1-\sqrt{5}}{2}$ $(= 1 - \phi = -\frac{1}{\phi})$.

[Note: ϕ and ψ are quadratic irrationals (cf. §8, #4).]

8: EXAMPLE

$$\sum_{n=-\infty}^{\infty} \frac{2n-1}{n^2 - n - 1} = \sum_{n=-\infty}^{\infty} \left(\frac{1}{n-\phi} + \frac{1}{n-\psi}\right) = 0.$$

9: DEFINITION The integers 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ... are the Fibonacci numbers:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}\ (n \geq 2).$$

10: LEMMA

$$F_n = \frac{\phi^n - \psi^n}{\phi - \psi} = \frac{\phi^n - \psi^n}{\sqrt{5}}\ .$$

11: N.B. ϕ and ψ are both solutions to the equations

$$X^n = X^{n-1} + X^{n-2},$$

hence

$$\begin{cases} \phi^n = \phi^{n-1} + \phi^{n-2} \\ \psi^n = \psi^{n-1} + \psi^{n-2} . \end{cases}$$

12: EXAMPLE

$$\sum_{n=1}^{\infty} \frac{F_n}{n2^n} = \frac{1}{\sqrt{5}} \sum_{n=1}^{\infty} \frac{1}{n} \left(\left(\frac{\phi}{2}\right)^n - \left(-\frac{1}{2\phi}\right)^n\right)$$

$$= \frac{1}{\sqrt{5}} \ell n(1 + \phi) - \frac{1}{\sqrt{5}} \ell n(2 - \phi),$$

a transcendental number (cf. §31, #11).

13: EXAMPLE

$$\sum_{n=1}^{\infty} \frac{1}{F_n F_{n+2}} = 1.$$

14: EXAMPLE

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{F_n F_{n+1}} = \frac{1 - \sqrt{5}}{2} \quad (= \psi).$$

15: LEMMA If $\alpha_1, \ldots, \alpha_n$ are positive algebraic numbers and if $\beta_0, \beta_1, \ldots, \beta_n$ are algebraic numbers with $\beta_0 \neq 0$, then

$$\beta_0 \pi + \sum_{j=1}^{n} \beta_j \ell n(\alpha_j)$$

is a transcendental number.

PROOF Replace $-\pi$ by $\sqrt{-1}\,\mathrm{Log}(-1)$ and quote §31, #11.

[The underlying supposition is that

$$\beta_0\pi + \sum_{j=1}^{n} \beta_j \ell n(\alpha_j)$$

is nonzero. To see this, let $\{\ell n(\alpha_j); j \in S\}$ be a maximal Q-linearly independent subset of

$$\ell n(\alpha_1), \ldots, \ell n(\alpha_n),$$

hence

$$\beta_0\pi + \sum_{j=1}^{n} \beta_j \ell n(\alpha_j) = - \sqrt{-1}\ \beta_0 \operatorname{Log}(-1) + \sum_{j\in S} C_j \ell n(\alpha_j)$$

for algebraic numbers C_j. The claim now is that

$$\operatorname{Log}(-1),\ \ell n(\alpha_j) \quad (j \in S)$$

are linearly independent over Q, thus are linearly independent over $\bar{Q}$ (homogeneous Baker), thereby implying that

$$- \sqrt{-1}\ \beta_0 \operatorname{Log}(-1) + \sum_{j\in S} C_j \ell n(\alpha_j)$$

is nonzero. So consider a rational dependence relation

$$q_0 \operatorname{Log}(-1) + \sum_{j\in S} q_j \ell n(\alpha_j) = 0.$$

The sum over $j \in S$ is a real number, while $\operatorname{Log}(-1)$ is pure imaginary, which forces $q_0 = 0$. But then $q_j = 0\ \forall\ j \in S$.]

<u>16:</u> EXAMPLE (Lehmer)

$$\sum_{n=0}^{\infty} \prod_{j=1}^{6} \frac{1}{6n + j}$$

$$= \frac{1}{4320} (192\ \ell n(2) - 81\ \ell n(3) + 7\sqrt{3}\ (-\pi)),$$

a transcendental number.

§2. *THE ROLE OF THE COTANGENT*

1: RAPPEL $\forall\, z \in C - Z$,

$$\pi \cot(\pi z) = \sum_{n=-\infty}^{\infty} \frac{1}{n+z}.$$

2: THEOREM Let $C \in Q - Z$ -- then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n+C}$$

is transcendental if $C \not\equiv \frac{1}{2} \bmod Z$.

PROOF Write

$$\pi \cot(\pi C) = \pi \sqrt{-1}\, \frac{e^{\pi \sqrt{-1}\, C} + e^{-\pi \sqrt{-1}\, C}}{e^{\pi \sqrt{-1}\, C} - e^{-\pi \sqrt{-1}\, C}}$$

$$= \pi \sqrt{-1}\, \frac{e^{2\pi \sqrt{-1}\, C} + 1}{e^{2\pi \sqrt{-1}\, C} - 1} \neq 0.$$

Let $C = \frac{p}{q}$:

$$\Rightarrow e^{2\pi \sqrt{-1}\, C} = (e^{2\pi \sqrt{-1}/q})^p \in \bar{Q}.$$

Therefore

$$\sum_{n=-\infty}^{\infty} \frac{1}{n+C}$$

is transcendental (being π times a nonzero algebraic number).

[Note: If $C \equiv \frac{1}{2} \bmod Z$, then the series vanishes. In fact, $\forall\, m \in Z$,

$$e^{2\pi \sqrt{-1}(\frac{1}{2} + m)} = e^{\pi \sqrt{-1}} = -1.$$

One can also argue directly without an appeal to the formula: $\forall\, m \in Z$,

$$\sum_{n=-\infty}^{\infty} \frac{1}{n + \frac{1}{2} + m} = \sum_{n=-\infty}^{\infty} \frac{1}{n - 1 - 2m + \frac{1}{2} + m}$$

$$= \sum_{n=-\infty}^{\infty} \frac{1}{n - \frac{1}{2} - m} = \sum_{n=-\infty}^{\infty} \frac{1}{-n - \frac{1}{2} - m}$$

$$= - \sum_{n=-\infty}^{\infty} \frac{1}{n + \frac{1}{2} + m} .]$$

3: LEMMA $\forall\, k \geq 2$, $\forall\, z \in C - Z$,

$$\frac{d^{k-1}}{dz^{k-1}} \Big(\sum_{n=-\infty}^{\infty} \frac{1}{n + z} \Big) = (-1)^{k-1} (k-1)! \sum_{n=-\infty}^{\infty} \frac{1}{(n+z)^k} .$$

Therefore

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+z)^k} = \frac{(-1)^{k-1} (\pi \cot(\pi z))^{(k-1)}}{(k - 1)!}$$

4: LEMMA $\forall\, k \geq 2$, $\forall\, z \in C - Z$,

$$\frac{d^{k-1}}{dz^{k-1}} (\pi \cot(\pi z))$$

$$= (2\pi \sqrt{-1})^k \Big(\frac{A_{k,1}}{e^{2\pi \sqrt{-1}\, z} - 1} + \cdots + \frac{A_{k,k}}{(e^{2\pi \sqrt{-1}\, z} - 1)^k} \Big),$$

where $A_{i,j} \in Z$ and $A_{k,1} \neq 0$, $A_{k,k} \neq 0$.

PROOF Write

$$\pi \cot(\pi z) = \pi \sqrt{-1} \frac{e^{2\pi \sqrt{-1} z} + 1}{e^{2\pi \sqrt{-1} z} - 1}$$

$$= \pi \sqrt{-1} \frac{e^{2\pi \sqrt{-1} z} - 1 + 1 + 1}{e^{2\pi \sqrt{-1} z} - 1}$$

$$= \pi \sqrt{-1} \left(\frac{e^{2\pi \sqrt{-1} z} - 1}{e^{2\pi \sqrt{-1} z} - 1} + \frac{2}{e^{2\pi \sqrt{-1} z} - 1}\right)$$

$$= \pi \sqrt{-1} \left(1 + \frac{2}{e^{2\pi \sqrt{-1} z} - 1}\right).$$

Differentiating this gives the result for $k = 2$. Proceeding by induction, assume matters have been established at level $\ell - 1$, hence

$$A_{\ell-1,1}, \ldots, A_{\ell-1,\ell-1} \in Z$$

with $A_{\ell-1,1} \neq 0$, $A_{\ell-1,\ell-1} \neq 0$ and

$$\frac{d}{dz}\left(\frac{d^{\ell-2}}{dz^{\ell-2}} (\pi \cot(\pi z))\right)$$

$$= (2\pi \sqrt{-1})^{\ell-1} \frac{d}{dz}\left(\frac{A_{\ell-1,1}}{e^{2\pi \sqrt{-1} z} - 1} + \cdots + \frac{A_{\ell-1,\ell-1}}{(e^{2\pi \sqrt{-1} z} - 1)^{\ell-1}}\right)$$

or still,

$$(2\pi \sqrt{-1})^{\ell}\left(- A_{\ell-1,1} \frac{e^{2\pi \sqrt{-1} z}}{(e^{2\pi \sqrt{-1} z} - 1)^2} - \cdots - (\ell-1)A_{\ell-1,\ell-1} \frac{e^{2\pi \sqrt{-1} z}}{(e^{2\pi \sqrt{-1} z} - 1)^{\ell}}\right)$$

or still,

$$(2\pi\sqrt{-1})^{\ell}\Big(-A_{\ell-1,1}\frac{e^{2\pi\sqrt{-1}z}-1+1}{(e^{2\pi\sqrt{-1}z}-1)^2}-\cdots-(\ell-1)A_{\ell-1,\ell-1}\frac{e^{2\pi\sqrt{-1}z}-1+1}{(e^{2\pi\sqrt{-1}z}-1)^{\ell}}\Big),$$

which equals $(2\pi\sqrt{-1})^{\ell}$ times

$$-\frac{A_{\ell-1,1}}{e^{2\pi\sqrt{-1}z}-1}-\frac{A_{\ell-1,1}}{(e^{2\pi\sqrt{-1}z}-1)^2}$$

$$-\cdots-\frac{(\ell-1)A_{\ell-1,\ell-1}}{(e^{2\pi\sqrt{-1}z}-1)^{\ell-1}}-\frac{(\ell-1)A_{\ell-1,\ell-1}}{(e^{2\pi\sqrt{-1}z}-1)^{\ell}},$$

thereby leading to the result at level ℓ.

[Note: To see the pattern, take $\ell = 3$ and put $w = e^{2\pi\sqrt{-1}z} - 1$ -- then

$$\frac{A_{2,1}}{w}+\frac{A_{2,1}}{w^2}+\frac{2A_{2,2}}{w^2}+\frac{2A_{2,2}}{w^3}$$

$$=\frac{A_{2,1}}{w}+\frac{A_{2,1}+2A_{2,2}}{w^2}+\frac{2A_{2,2}}{w^3}.]$$

Therefore

$$\sum_{n=-\infty}^{\infty}\frac{1}{(n+z)^k}=\frac{(-1)^{k-1}}{(k-1)!}(2\pi\sqrt{-1})^k$$

$$\times\Big(\frac{A_{k,1}}{e^{2\pi\sqrt{-1}z}-1}+\cdots+\frac{A_{k,k}}{(e^{2\pi\sqrt{-1}z}-1)^k}\Big).$$

5: NOTATION Put

$$A_k(z)=\frac{(-1)^{k-1}}{(k-1)!}(2\sqrt{-1})^k\Big(\frac{A_{k,1}}{e^{2\pi\sqrt{-1}z}-1}+\cdots+\frac{A_{k,k}}{(e^{2\pi\sqrt{-1}z}-1)^k}\Big).$$

Therefore

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+z)^k} = \pi^k A_k(z).$$

<u>6:</u> <u>N.B.</u> $\forall\, C \in Q - Z$, $A_k(C)$ is an algebraic number.

<u>7:</u> THEOREM $\forall\, k \geq 2$, $\forall\, C \in Q - Z$, the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+C)^k}$$

is either transcendental or zero.

<u>8:</u> REMARK It can happen that

$$\frac{d^{k-1}}{dz^{k-1}} (\pi \cot(\pi z)) \Big|_{z=C} \quad (k \geq 2)$$

$$= 0.$$

To see this, take k odd and observe that $\forall\, m \in Z$,

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n + \frac{1}{2} + m)^k} = \sum_{n=-\infty}^{\infty} \frac{1}{(- n - \frac{1}{2} - m)^k}$$

$$= (-1)^k \sum_{n=-\infty}^{\infty} \frac{1}{(n + \frac{1}{2} + m)^k}.$$

[Note: The series does not vanish if k is even and in that case we have transcendence.]

§3. *APPLICATION OF NESTERENKO*

1: CRITERION For any positive integer D, π and $e^{\pi\sqrt{D}}$ are algebraically independent over Q (cf. §20, #10) (proof omitted).

[Note: In particular, π and e^{π} are algebraically independent over Q.]

2: N.B. If r and s are nonzero rational numbers, then π^r and $(e^{\pi\sqrt{D}})^s$ are algebraically independent over Q (cf. §46, #26).

3: THEOREM Let $C \in Q - \{0\}$ -- then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C^2}$$

is transcendental.

PROOF Take $C > 0$ and let

$$f(x) = \frac{\pi}{C} e^{-2\pi C|x|}.$$

Then, using Poisson summation,

$$\sum_{n=-\infty}^{\infty} f(n+t) = \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{2\pi\sqrt{-1}\,tn}.$$

Now put $t = 0$ to get

$$\frac{\pi}{C} \sum_{n=-\infty}^{\infty} e^{-2\pi C|n|} = \sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C^2}$$

or still,

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C^2} = \frac{\pi}{C} \left(\frac{e^{2\pi C} + 1}{e^{2\pi C} - 1}\right),$$

a transcendental number (cf. infra).

[Note: Let

$$C = \frac{p}{q} \quad (p,q \in \mathbb{N})$$

and write

$$2C = 2\,\frac{p}{q} = \frac{\sqrt{4p^2}}{q} \equiv \frac{\sqrt{D}}{q}.$$

If

$$\frac{\pi}{C}\left(\frac{e^{2\pi C}+1}{e^{2\pi C}-1}\right) = \alpha \in \bar{\mathbb{Q}} - \{0\},$$

then

$$\frac{\pi}{C}(e^{2\pi C}+1) - \alpha(e^{2\pi C}-1) = 0.$$

Define a polynomial $P \in \bar{\mathbb{Q}}[X,Y]$ by the prescription

$$P(X,Y) = \frac{X}{C}(Y+1) - \alpha(Y-1).$$

Then

$$P(\pi, e^{\pi\sqrt{D}/q}) = 0.$$

But π and $e^{\pi\sqrt{D}/q}$ are algebraically independent over $\mathbb{Q}$ (cf. #2), hence are algebraically independent over $\bar{\mathbb{Q}}$ (cf. §20, #7).]

4: N.B. For any positive real number C (not necessarily rational),

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2+C^2} = \frac{\pi}{C}\left(\frac{e^{2\pi C}+1}{e^{2\pi C}-1}\right)$$

$$= \frac{\pi}{C}\left(\frac{e^{\pi C}+e^{-\pi C}}{e^{\pi C}-e^{-\pi C}}\right).$$

5: RAPPEL

$$\coth z = \frac{\cosh z}{\sinh z} = \frac{e^z + e^{-z}}{e^z - e^{-z}}.$$

6: N.B. So, for any positive real number C (not necessarily rational),

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C^2} = \frac{\pi}{C} \coth(\pi C).$$

[There is another approach to this result using complex variables. Thus let

$$f(z) = \frac{1}{z^2 + C^2} \quad (C > 0).$$

Then $f(z)$ has simple poles at $z = \pm C\sqrt{-1}$.

- The residue of

$$\frac{\pi \cot(\pi z)}{z^2 + C^2}$$

at $z = C\sqrt{-1}$ is

$$\lim_{z \to C\sqrt{-1}} (z - C\sqrt{-1}) \frac{\pi \cot(\pi z)}{(z - C\sqrt{-1})(z + C\sqrt{-1})}$$

$$= \frac{\pi \cot(\pi C\sqrt{-1})}{2C\sqrt{-1}} = -\frac{\pi}{2C} \coth(\pi C).$$

- The residue of

$$\frac{\pi \cot(\pi z)}{z^2 + C^2}$$

at $z = -C\sqrt{-1}$ is

$$\frac{-\pi}{2C} \coth(\pi C).$$

Since the sum of the residues is

$$\frac{-\pi}{C} \coth(\pi C),$$

it follows that

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C^2} = - \text{ (sum of residues)}$$

$$= \frac{\pi}{C} \coth(\pi C).]$$

[Note: The formalism here is that

$$\sum_{n=-\infty}^{\infty} f(n) = - S,$$

where S is the sum of the residues of $\pi \cot(\pi z) f(z)$ at the poles of $f(z)$.]

7: LEMMA For any positive real number C (not necessarily rational),

$$\sum_{n=1}^{\infty} \frac{1}{n^2 + C^2} = \frac{\pi}{2C} \coth(\pi C) - \frac{1}{2C^2} .$$

PROOF Write

$$\sum_{n=-\infty}^{-1} \frac{1}{n^2 + C^2} + \frac{1}{C^2} + \sum_{n=1}^{\infty} \frac{1}{n^2 + C^2} = \frac{\pi}{C} \coth(\pi C) .$$

8: EXAMPLE Take C = 1 -- then

$$\sum_{n=0}^{\infty} \frac{1}{n^2 + 1} = \frac{1}{2} + \frac{\pi}{2} \frac{e^{\pi} + e^{-\pi}}{e^{\pi} - e^{-\pi}} .$$

By comparison,

$$\sum_{n=0}^{\infty} \frac{1}{n^2 - 1} = \frac{3}{4} .$$

[Note: For the record,

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} .]$$

9: REMARK It is also possible to sum the series

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{n^2+1},$$

the result being

$$\frac{2\pi}{e^{\pi} - e^{-\pi}}.$$

10: THEOREM Let $C \in \mathbb{Q}_{>0}$ — then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C}$$

is transcendental.

PROOF Write

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2+C} = \frac{\pi}{\sqrt{C}} \left(\frac{e^{2\pi\sqrt{C}} + 1}{e^{2\pi\sqrt{C}} - 1}\right)$$

and let

$$C = \frac{p}{q} \ (p,q \in \mathbb{N}) \Rightarrow \sqrt{C} = \left(\frac{p}{q}\right)^{1/2} = \frac{\sqrt{pq}}{q}$$

$$\Rightarrow 2\pi\sqrt{C} = \pi\sqrt{4}\,\frac{\sqrt{pq}}{q}$$

$$= \pi\,\frac{\sqrt{4pq}}{q}.$$

Now apply #2.

11: EXAMPLE Take $C = 3$ — then

$$\sum_{n=0}^{\infty} \frac{1}{n^2+3} = \frac{\pi}{2\sqrt{3}}\,\frac{e^{2\pi\sqrt{3}} + 1}{e^{2\pi\sqrt{3}} - 1} + \frac{1}{6}.$$

12: THEOREM Let $C \in \mathbb{Q} - \{0\}$ -- then for every positive integer k, the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n^2 + C^2)^k}$$

is transcendental.

PROOF Write

$$\frac{1}{(n^2 + C^2)^k} = \frac{1}{(n + \sqrt{-1}\, C)^k (n - \sqrt{-1}\, C)^k}$$

and decompose the term on the right into partial fractions:

$$\sum_{n=1}^{k} \frac{\alpha_j}{(n + \sqrt{-1}\, C)^j} + \frac{\beta_j}{(n - \sqrt{-1}\, C)^j} \quad (\alpha_j, \beta_j \in \bar{\mathbb{Q}}).$$

Proceed... .

13: EXAMPLE Take $C = 1$ -- then

$$\sum_{n=0}^{\infty} \frac{1}{(n^2 + 1)^2} = \frac{\pi}{4} \frac{e^{2\pi} + 1}{e^{2\pi} - 1} + \frac{\pi^2}{4} \frac{e^{2\pi}}{(e^{2\pi} - 1)^2} + \frac{1}{2}.$$

[Consider

$$R(X,Y) = \frac{X}{4} \frac{Y + 1}{Y - 1} + \frac{X^2}{4} \frac{Y}{(Y - 1)^2} + \frac{1}{2}$$

and write

$$e^{2\pi} = e^{\pi\sqrt{4}} \quad (\text{so } D = 4).]$$

14: THEOREM Let $C \in \mathbb{Q}_{>0}$ — then for every positive integer k, the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n^2 + C)^k}$$

is transcendental.

§4. *INTRODUCTION OF SCHC*

<u>1:</u> THEOREM Let $C \in Q - Z$ -- then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^3 + C^3}$$

is transcendental.

PROOF Since

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^3 - C^3} = \sum_{n=-\infty}^{\infty} \frac{1}{(-n)^3 - C^3} = - \sum_{n=-\infty}^{\infty} \frac{1}{n^3 + C^3},$$

it can be assumed that C is positive. This said, write

$$n^3 + C^3 = (n + C)(n + C\rho)(n + C\rho^2),$$

where

$$\rho = (-1 - \sqrt{-1}\,\sqrt{3})/2$$

is a primitive cube root of unity. Decompose $\dfrac{1}{n^3 + C^3}$ into partial fractions:

$$\frac{1}{3C^2}\frac{1}{n + C} + \frac{\rho}{3C^2}\frac{1}{n + C\rho} + \frac{\rho^2}{3C^2}\frac{1}{n + C\rho^2}.$$

Then

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^3 + C^3}$$

equals

$$\frac{\pi\sqrt{-1}}{3C^2}\left[\frac{e^{2\pi\sqrt{-1}\,C} + 1}{e^{2\pi\sqrt{-1}\,C} - 1} + \rho\,\frac{e^{2\pi\sqrt{-1}\,C\rho} + 1}{e^{2\pi\sqrt{-1}\,C\rho} - 1} + \rho^2\,\frac{e^{2\pi\sqrt{-1}\,C\rho^2} + 1}{e^{2\pi\sqrt{-1}\,C\rho^2} - 1}\right].$$

Here we have used the formula for the cotangent in terms of exponentials (see §2,

#2) (proof thereof). Expand the data to arrive at a fraction

$$2\pi\sqrt{-1}\,\frac{A}{B},$$

where A equals

$$(e^{-2\pi\sqrt{-1}\,C} + e^{2\pi\sqrt{-1}\,C}) + \rho(e^{\pi\sqrt{-1}\,C}e^{\pi C\sqrt{3}} + e^{-\pi\sqrt{-1}\,C}e^{-\pi C\sqrt{3}})$$

$$+ \rho^2(e^{\pi\sqrt{-1}\,C}e^{-\pi C\sqrt{3}} + e^{-\pi\sqrt{-1}\,C}e^{\pi C\sqrt{3}})$$

and B equals

$$3C^2(e^{2\pi\sqrt{-1}\,C} - 1)(e^{2\pi\sqrt{-1}\,C\rho} - 1)(e^{2\pi\sqrt{-1}\,C\rho^2} - 1).$$

Owing now to §3, #2, π and $(e^{\pi\sqrt{3}})^C = e^{\pi C\sqrt{3}}$ are algebraically independent over Q, hence the numerator is either transcendental or zero. If the numerator is zero, then the algebraic coefficients of $e^{\pi C\sqrt{3}}$ and $e^{-\pi C\sqrt{3}}$ must both be zero, which implies that

$$\begin{cases} \rho e^{\pi\sqrt{-1}\,C} + \rho^2 e^{-\pi\sqrt{-1}\,C} = 0 \\ \rho^2 e^{\pi\sqrt{-1}\,C} + \rho e^{-\pi\sqrt{-1}\,C} = 0. \end{cases}$$

The first equation implies that

$$C = \frac{1}{6} + K_1 \quad (\exists\, K_1 \in Z)$$

and the second equation implies that

$$C = -\frac{1}{6} + K_2 \quad (\exists\, K_2 \in Z)$$

$\Rightarrow$

$$\frac{1}{6} + K_1 = -\frac{1}{6} + K_2 \Rightarrow \frac{1}{3} = K_2 - K_1,$$

a contradiction. Therefore the series is transcendental.

<u>2:</u> REMARK At least one of

$$\sum_{n=1}^{\infty} \frac{1}{n^3 + C^3} \quad \text{and} \quad \sum_{n=1}^{\infty} \frac{1}{n^3 - C^3}$$

is transcendental.

<u>3:</u> THEOREM Let $C \in Q - Z$ -- then for every positive integer k, the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n^3 + C^3)^k}$$

is transcendental or zero (transcendental if k is even).

[Start by decomposing

$$\frac{1}{(n + C)^k \ (n + \rho C)^k \ (n + \rho^2 C)^k}$$

into partial fractions.]

<u>4:</u> CRITERION (Admit SCHC) If $\alpha_1,\ldots,\alpha_n$ are algebraic numbers such that $\sqrt{-1}$, $\alpha_1,\ldots,\alpha_n$ are linearly independent over Q, then

$$\pi, e^{\pi\alpha_1}, \ldots, e^{\pi\alpha_n}$$

are algebraically independent over Q.

<u>5:</u> <u>N.B.</u> Take $n = 1$, $\alpha_1 = 1$ -- then the conclusion is that π and e^{π} are algebraically independent over Q (cf. §3, #1) (no need for SCHC in this situation).

<u>6:</u> EXAMPLE (Admit SCHC) Take $n = 2$, $\alpha_1 = \sqrt[3]{C}\,\sqrt{3}$, $\alpha_2 = \sqrt{-1}\,\sqrt[3]{C}$, where

$$C \in Q - Z, \ C \neq D^3 \ (D \in Q).$$

Then

$$\pi,\ e^{\pi \sqrt[3]{C} \sqrt{3}},\ e^{\pi \sqrt{-1} \sqrt[3]{C}}$$

are algebraically independent over Q.

[To check that $\sqrt{-1}, \alpha_1, \alpha_2$ are linearly independent over Q, consider a rational dependence relation

$$r \sqrt{-1} + s\alpha_1 + t\alpha_2$$

$$= r \sqrt{-1} + s \sqrt[3]{C} \sqrt{3} + t \sqrt{-1} \sqrt[3]{C} = 0.$$

Then $s = 0$, leaving

$$r \sqrt{-1} + t \sqrt{-1} \sqrt[3]{C} = 0$$

or still,

$$r + t \sqrt[3]{C} = 0 \Rightarrow \sqrt[3]{C} = -\frac{r}{t}$$

$$\Rightarrow C = (-\frac{r}{t})^3.]$$

7: THEOREM (Admit SCHC) Suppose that $C \in Q - Z$ is not a cube in Q -- then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^3 + C}$$

is transcendental.

PROOF The verification is an elaboration of that used in #1 (which considers the situation when "C" is a cube). So, to begin with, recast matters into the form

$$\frac{\pi\sqrt{-1}}{3\sqrt[3]{C^2}}\left[\frac{e^{2\pi\sqrt{-1}\sqrt[3]{C}}+1}{e^{2\pi\sqrt{-1}\sqrt[3]{C}}-1}+\rho\,\frac{e^{2\pi\sqrt{-1}\sqrt[3]{C}\rho}+1}{e^{2\pi\sqrt{-1}\sqrt[3]{C}\rho}-1}+\rho^2\,\frac{e^{2\pi\sqrt{-1}\sqrt[3]{C}\rho^2}+1}{e^{2\pi\sqrt{-1}\sqrt[3]{C}\rho^2}-1}\right].$$

This done, combine terms in the sum to form a fraction and, using #6, check that its numerator is not zero.

§5. *INTRODUCTION OF* SCHC (bis)

1: EXAMPLE

$$\sum_{n=0}^{\infty} \frac{1}{n^4 + 4} = \frac{\pi}{8} \frac{e^{4\pi} - 1}{e^{4\pi} - e^{2\pi} + 1} + \frac{1}{8}.$$

[To ascertain that the right hand side is transcendental, suppose that

$$\pi \frac{e^{4\pi} - 1}{e^{4\pi} - e^{2\pi} + 1} = \alpha \in \bar{Q} - \{0\}.$$

Then

$$\pi(e^{4\pi} - 1) - \alpha(e^{4\pi} - e^{2\pi} + 1) = 0.$$

Define a polynomial $P \in \bar{Q}[X,Y]$ by the prescription

$$P(X,Y) = X(Y^4 - 1) - \alpha(Y^4 - Y^2 + 1) = 0.$$

Then

$$P(\pi,e^{\pi}) = \pi(e^{4\pi} - 1) - \alpha(e^{4\pi} - e^{2\pi} + 1) = 0,$$

which contradicts the fact that π and e^{π} are algebraically independent over $\bar{Q}$.]

2: LEMMA (Admit SCHC)

$$\pi,\ e^{\pi\sqrt{2}},\ e^{\pi\sqrt{-1}\sqrt{2}}$$

are algebraically independent over Q.

PROOF In §4, #4, take $n = 2$, $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{-1}\sqrt{2}$.

3: THEOREM (Admit SCHC) Let $C \in \bar{Q} - \{0\}$ -- then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^4 + C^4}$$

is transcendental.

PROOF Write

$$\frac{1}{n^4 + C^4} = \frac{1}{n^4 - (\xi C)^4},$$

where

$$\xi = e^{\pi\sqrt{-1}/4} = \sqrt{2}/2 + \sqrt{-1}\,\sqrt{2}/2.$$

Then

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^4 + C^4}$$

equals

$$\frac{\pi}{2\xi^3 C^3}\left[\frac{(e^{2\pi\sqrt{-1}\,\xi C} + 1)(e^{2\pi\xi C} - 1) - \sqrt{-1}(e^{2\pi\xi C} + 1)(e^{2\pi\sqrt{-1}\,\xi C} - 1)}{\sqrt{-1}\,(e^{2\pi\sqrt{-1}\,\xi C} - 1)(e^{2\pi\xi C} - 1)}\right].$$

Note that

$$e^{2\pi\sqrt{-1}\,\xi C} = e^{\pi\sqrt{-1}\,C\sqrt{2}}\,e^{-\pi C/\sqrt{2}}$$

and use the fact that

$$\pi,\ e^{\pi\sqrt{2}},\ e^{\pi\sqrt{-1}\,\sqrt{2}}$$

are algebraically independent over Q (cf. #2).

§6. *CONSOLIDATION*

Our objective here is to analyze the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^p + C^p},$$

where p = 1 or p is a prime ≥ 2 and $C \in Q - Z$.

- $\underline{p = 1}$:

$$\sum_{n=-\infty}^{\infty} \frac{1}{n + C}$$

is transcendental or zero (cf. §2, #2).

- $\underline{p = 2}$:

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^2 + C^2}$$

is transcendental (cf. §3, #3).

- $\underline{p = 3}$:

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^3 + C^3}$$

is transcendental (cf. §4, #1).

<u>1:</u> THEOREM (Admit SCHC) Let p be a prime ≥ 5 and let $C \in Q - Z$ — then the series

$$\sum_{n=-\infty}^{\infty} \frac{1}{n^p + C^p}$$

is transcendental or zero.

PROOF Let

$$\zeta = e^{2\pi \sqrt{-1}/p}$$

be a primitive p^{th} root of unity — then

$$1, \zeta, \ldots, \zeta^{p-2}$$

are linearly independent over Q, thus

$$\sqrt{-1}, \sqrt{-1}\,\zeta, \ldots, \sqrt{-1}\,\zeta^{p-2}$$

are also linearly independent over Q. Therefore

$$\pi, e^{\pi\sqrt{-1}\,\zeta}, \ldots, e^{\pi\sqrt{-1}\,\zeta^{p-2}}$$

are algebraically independent over Q (cf. §4, #4). Write

$$n^p + C^p = (n + C) \ldots (n + \zeta^{p-1}C)$$

to arrive at

$$\pi\sqrt{-1}\left(\alpha_0 \frac{e^{2\pi\sqrt{-1}\,C} + 1}{e^{2\pi\sqrt{-1}\,C} - 1} + \cdots + \alpha_{p-1} \frac{e^{2\pi\sqrt{-1}\,C\zeta^{p-1}} + 1}{e^{2\pi\sqrt{-1}\,C\zeta^{p-1}} - 1}\right),$$

where the $\alpha_i \in \bar{Q}$. Using the fact that

$$\zeta^{p-1} = -1 - \zeta - \cdots - \zeta^{p-2},$$

the sum inside the parenthesis can be reduced to a rational function in algebraically independent terms which can be transcendental, zero, or algebraic nonzero but the π out in front rules out the last possibility.

§7. CONSIDERATION OF $\frac{A}{B}$

Let $A(X)$, $B(X)$ be elements of $\bar{Q}[X]$ with

$$\deg A < \deg B.$$

Assume:

$$B(X) = (X + \alpha_1)^{m_1} \cdots (X + \alpha_k)^{m_k},$$

where $\alpha_1,\ldots,\alpha_k$ are algebraic, nonintegral, and such that

$$1, \alpha_1,\ldots,\alpha_k$$

are linearly independent over Q.

<u>1:</u> THEOREM (Admit SCHC) The series

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)}$$

is transcendental or zero.

<u>2:</u> RAPPEL (cf. §2, #3) $\forall\, j \geq 2$, $\forall\, z \in C - Z$,

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n + z)^j} = \frac{(-1)^{j-1}(\pi \cot(\pi z))^{(j-1)}}{(j - 1)!}.$$

<u>3:</u> <u>N.B.</u> When $j = 1$,

$$\sum_{n=-\infty}^{\infty} \frac{1}{n + z} = \pi \cot(\pi z).$$

Using partial fractions, write

$$\frac{A(n)}{B(n)} = \sum_{i=1}^{k} \sum_{j=1}^{m_i} C_{ij} \frac{1}{(n + \alpha_i)^j}.$$

Then

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)} = \sum_{n=-\infty}^{\infty} \left(\sum_{i=1}^{k} \sum_{j=1}^{m_i} C_{ij} \frac{1}{(n + \alpha_i)^j} \right)$$

$$= \sum_{i=1}^{k} \sum_{j=1}^{m_i} C_{ij} \sum_{n=-\infty}^{\infty} \frac{1}{(n + \alpha_i)^j}$$

$$= \sum_{i=1}^{k} \sum_{j=1}^{m_i} C_{ij} \frac{(-1)^{j-1}(\pi \cot(\pi\alpha_i))^{(j-1)}}{(j - 1)!}$$

$$= \pi \sum_{i=1}^{k} \sum_{j=1}^{m_i} D_{ij}(\cot(\pi\alpha_i))^{(j-1)},$$

where

$$D_{ij} = C_{ij} \frac{(-1)^{j-1}}{(j - 1)!}.$$

FACT For any integer $m > 1$,

$$\left(\frac{d}{dz}\right)^m \cot z$$

is a polynomial in cot z.

[The formula is

$$\left(\frac{d}{dt}\right)^m \cot z$$

equals

$$(2\sqrt{-1})^m (\cot z - \sqrt{-1}) \sum_{\ell=1}^{m} \frac{\ell!}{2^\ell} S(m,\ell)(\sqrt{-1}\cot z - 1)^\ell.$$

Here the $S(m,\ell) \in Z$ are the Stirling subset numbers (a.k.a. the Stirling numbers of the second kind).]

[Note: $\forall\, k \geq 2$, $\forall\, z \in C - Z$,

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n + z)^k} = \frac{(-2\pi \sqrt{-1})^k}{(k - 1)!} \sum_{\ell=1}^{k} \frac{(\ell - 1)!S(k,\ell)}{(e^{-2\pi \sqrt{-1}\, z} - 1)^\ell} \quad \text{(cf. §2, \#3).]}$$

4: RAPPEL

$$\cot(\pi z) = \sqrt{-1}\, \frac{e^{2\pi \sqrt{-1}\, z} + 1}{e^{2\pi \sqrt{-1}\, z} - 1}\,.$$

5: APPLICATION

$$(\cot(\pi\alpha_i))^{(j-1)}$$

is an algebraic linear combination of rational functions evaluated at $e^{2\pi \sqrt{-1}\, \alpha_i}$.

The assumption on the α_i is that

$$1, \alpha_1, \ldots, \alpha_k$$

are linearly independent over Q or still, that

$$\sqrt{-1}, \sqrt{-1}\, \alpha_1, \ldots, \sqrt{-1}\, \alpha_k$$

are linearly independent over Q or still, that

$$\sqrt{-1}, 2\sqrt{-1}\, \alpha_1, \ldots, 2\sqrt{-1}\, \alpha_k$$

are linearly independent over Q. Therefore

$$\pi, e^{2\pi \sqrt{-1}\, \alpha_1}, \ldots, e^{2\pi \sqrt{-1}\, \alpha_k}$$

are algebraically independent over Q (cf. §4, #4).

To finish the proof, rearrange the sum so as to form a polynomial in π, the coefficients of a given power of π being a rational expression in

$$e^{2\pi\sqrt{-1}\,\alpha_1}, \ldots, e^{2\pi\sqrt{-1}\,\alpha_k}.$$

Complete the argument by citing algebraic independence over Q (which eliminates the algebraic nonzero possibility).

There is one set of circumstances under which the series

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)}$$

is transcendental (thereby ruling out the zero contingency).

Assume: The roots of $B(X)$ are simple, hence

$$m_1 = 1, \ldots, m_k = 1.$$

To proceed, write

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)} = \pi \sum_{i=1}^{k} C_i \cot(\pi\alpha_i)$$

or still,

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)} = \pi\sqrt{-1} \sum_{i=1}^{k} C_i \frac{e^{2\pi\sqrt{-1}\,\alpha_i} + 1}{e^{2\pi\sqrt{-1}\,\alpha_i} - 1},$$

the claim being that the expression on the right is nonzero, thus that the series

$$\sum_{n=-\infty}^{\infty} \frac{A(n)}{B(n)}$$

is transcendental.

Rewrite the expression as

$$\frac{\pi\sqrt{-1}}{\prod_{i=1}^{k}(e^{2\pi\sqrt{-1}\,\alpha_i}-1)}\sum_{i=1}^{k} C_i(e^{2\pi\sqrt{-1}\,\alpha_i}+1)\prod_{a\neq i}(e^{2\pi\sqrt{-1}\,\alpha_a}-1).$$

Matters then reduce to showing that the polynomial

$$\sum_{i=1}^{k} C_i(X_i+1)\prod_{a\neq i}(X_a-1)$$

is not identically zero. Suppose it were identically zero. Given i, take

$$X_i = 0,\ X_j = -1\ (j \neq i),\ X_a = 2\ (a \neq i)$$

to see that $C_i = 0$. But i is arbitrary, so $C_i = 0\ \forall\ i$, contradicting the tacit assumption that $A \neq 0$.

§8. *AN ALGEBRAIC SERIES*

Instead of looking for a transcendental series, this time we shall exhibit an algebraic series.

1: THEOREM Suppose that $P(X) \in \bar{\mathbb{Q}}[X]$ and $z \in \bar{\mathbb{Q}}$ $(0 < |z| < 1)$ -- then the series

$$\sum_{n=0}^{\infty} z^n P(n)$$

is algebraic.

PROOF First of all, the manipulations infra are justified by the absolute convergence of our series, so if

$$P(X) = \sum_{i=0}^{k} a_i X^i,$$

then

$$\sum_{n=0}^{\infty} z^n P(n) = \sum_{i=0}^{k} a_i \sum_{n=0}^{\infty} z^n n^i.$$

Write

$$X^i = \sum_{j=0}^{i} S(i,j)(X)_j,$$

where $(X)_0 = 1$ and for $j \geq 1$,

$$(X)_j = X(X-1) \cdots (X-j+1).$$

Inserting this data leads to

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) \sum_{n=0}^{\infty} (n)_j z^n$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) \sum_{n=0}^{\infty} n(n-1) \cdots (n-j+1) z^n$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) \sum_{n=1}^{\infty} n(n-1) \cdots (n-j+1) z^n$$

$$\vdots$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) \sum_{n=j-1}^{\infty} n(n-1) \cdots (n-j+1) z^n$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) \sum_{n=j}^{\infty} n(n-1) \cdots (n-j+1) z^n$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) z^j \sum_{n=0}^{\infty} (n+1) \cdots (n+j) z^n$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} S(i,j) z^j \left(\frac{z^j}{1-z}\right)^{(j)}$$

or still,

$$\sum_{i=0}^{k} a_i \sum_{j=0}^{i} \frac{S(i,j) j! z^j}{(1-z)^{j+1}},$$

an algebraic number.

SUPPLEMENT

ZETA FUNCTION VALUES

§1. *BERNOULLI NUMBERS*

Define the Bernoulli polynomials $B_n(x)$ $(n = 0,1,2,\ldots)$ via the generating function

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}.$$

[Note:

$$B_0(x) = 1,\ B_1(x) = x - \frac{1}{2},\ B_2(x) = x^2 - x + \frac{1}{6}.]$$

There are two sign conventions at play here.

(+) Define the Bernoulli numbers B_n^+ $(n = 0,1,2,\ldots)$ by taking $x = 1$, hence the generating function

$$\frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n^+ \frac{t^n}{n!}.$$

[Note: $B_0^+ = 1$, $B_1^+ = \frac{1}{2}$, $B_2^+ = \frac{1}{6}$.]

(−) Define the Bernoulli numbers B_n^- $(n = 0,1,2,\ldots)$ by taking $x = 0$, hence the generating function

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n^- \frac{t^n}{n!}.$$

[Note: $B_0^- = 1$, $B_1^- = -\frac{1}{2}$, $B_2^- = \frac{1}{6}$.]

<u>1:</u> REMARK A Bernoulli number is real and rational.

2: LEMMA

$$B_n^+ = (-1)^n B_n^-.$$

3: LEMMA If n is an odd integer ≥ 3, then

$$B_n^+ = 0,\ B_n^- = 0.$$

4: N.B. In formulas involving even index Bernoulli numbers, it is permissible to drop the $\pm$ and simply use the symbol B_n.

5: EXAMPLE

$$x \cot x = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n}}{(2n)!} B_{2n} x^{2n} \quad (0 < |x| < \pi).$$

6: LEMMA $\forall\ n \geq 1$,

$$\int_0^1 B_n(x)dx = 0.$$

7: LEMMA $\forall\ n \geq 1$,

$$\int_0^1 B_n(x)B_m(x)dx = (-1)^{n-1} \frac{m!n!}{(m+n)!} B_{m+n}^-.$$

8: LEMMA $\forall\ n \geq 1$,

$$\frac{d}{dx} B_n(x) = nB_{n-1}(x).$$

APPENDIX

LEMMA (MULTIPLICATION FORMULA)

$$B_n(mx) = m^{n-1} \sum_{k=0}^{m-1} B_n\left(x + \frac{k}{m}\right).$$

APPLICATION Take $x = 0$, $m = 2$ -- then

$$B_{2n}(\tfrac{0}{2}) + B_{2n}(\tfrac{1}{2}) = 2^{1-2n} B_{2n}(0),$$

i.e.,

$$B_{2n}(\tfrac{1}{2}) = 2^{1-2n} B_{2n} - B_{2n}$$

$$= (2^{1-2n} - 1)B_{2n}.$$

LEMMA (ADDITION FORMULA)

$$B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x)y^{n-k}.$$

§2. $\zeta(2n)$

1: THEOREM $\forall\ n \geq 1$,

$$\zeta(2n) \equiv \sum_{k=1}^{\infty} \frac{1}{k^{2n}}$$

$$= (-1)^{n-1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n}$$

or still,

$$\zeta(2n) = (-1)^{n-1} \frac{2^{2n-1}}{(2n)!} B_{2n}\pi^{2n}.$$

2: APPLICATION $\zeta(2n)$ is transcendental.

[Recall that π is transcendental, hence π^{2n} is transcendental.]

The stated formula for $\zeta(2n)$ can be proved in mnay different ways. What follows is one of them.

3: NOTATION Given an $f \in L^1[0,1]$, put

$$\hat{f}(k) = \int_0^1 f(x)e^{-2\pi\sqrt{-1}\,kx}\,dx \quad (k \in Z).$$

4: PLANCHEREL Given an $f \in L^2[0,1]$,

$$\int_0^1 |f(x)|^2 dx = \sum_{-\infty}^{\infty} |\hat{f}(k)|^2.$$

[Note: Recall that

$$L^2[0,1] \subset L^1[0,1].]$$

5: LEMMA Take $f(x) = B_n(x)$ — then

$$\hat{B}_n(k) = -\frac{n!}{(2\pi\sqrt{-1}\,k)^n}$$

if $k \neq 0$ while $\hat{B}_n(0) = 0$.

PROOF The second point is covered by §1, #6. As for the first point, take $n \geq 1$ and write

$$\hat{B}_n(k) = \int_0^1 B_n(x) e^{-2\pi\sqrt{-1}\,kx}\,dx$$

$$= -\frac{1}{2\pi\sqrt{-1}\,k}\int_0^1 B_n(x)\frac{d}{dx}e^{-2\pi\sqrt{-1}\,kx}\,dx$$

$$= -\frac{1}{2\pi\sqrt{-1}\,k} B_n(x) e^{-2\pi\sqrt{-1}\,kx}\Big|_0^1$$

$$+\frac{1}{2\pi\sqrt{-1}\,k}\int_0^1 \frac{d}{dx}B_n(x) e^{-2\pi\sqrt{-1}\,kx}\,dx.$$

<u>$n = 1$</u>:

$$\hat{B}_1(k) = -\frac{1}{2\pi\sqrt{-1}\,k}\left(x - \frac{1}{2}\right)e^{-2\pi\sqrt{-1}\,kx}\Big|_0^1$$

$$-\frac{1}{2\pi\sqrt{-1}\,k}\int_0^1 1\cdot e^{-2\pi\sqrt{-1}\,kx}\,dx$$

$$= -\frac{1}{2\pi\sqrt{-1}\,k}\left(\frac{1}{2}+\frac{1}{2}\right)$$

$$-\frac{1}{2\pi\sqrt{-1}\,k}\,0 \quad (k \neq 0)$$

$$= -\frac{1}{2\pi\sqrt{-1}\,k}.$$

$\underline{n > 1}$: To begin with

$$-\frac{1}{2\pi\sqrt{-1}\,k} B_n(x)e^{-2\pi\sqrt{-1}\,kx}\Big|_0^1$$

$$= -\frac{1}{2\pi\sqrt{-1}\,k}(B_n(1) - B_n(0)).$$

And

$$\begin{aligned} B_n(1) - B_n(0) &= B_n^+ - B_n^- \\ &= (-1)^n B_n^- - B_n^- \quad (\text{cf. §1, \#2}) \\ &= B_n^-((-1)^n - 1). \end{aligned}$$

But

$$\begin{cases} n \text{ even}, \geq 2 \Rightarrow (-1)^n = 1 \Rightarrow B_n^-((-1)^n - 1) = 0 \\ n \text{ odd}, \geq 3 \Rightarrow B_n^- = 0 \ (\text{cf. §1, \#3}) \Rightarrow B_n^-((-1)^n - 1) = 0. \end{cases}$$

Therefore

$$B_n(1) - B_n(0) = 0,$$

leaving

$$\frac{1}{2\pi\sqrt{-1}\,k}\int_0^1 \frac{d}{dx} B_n(x)e^{-2\pi\sqrt{-1}\,kx}\,dx.$$

Using §1, #8, replace $\frac{d}{dx} B_n(x)$ by $n\,B_{n-1}(x)$ to arrive at

$$\hat{B}_n(k) = \frac{n}{2\pi\sqrt{-1}\,k}\int_0^1 B_{n-1}(x)e^{-2\pi\sqrt{-1}\,kx}\,dx$$

$$= \frac{n}{2\pi\sqrt{-1}\,k}\hat{B}_{n-1}(k),$$

so, inductively,

$$\begin{aligned}
\hat{B}_n(k) &= \frac{n}{2\pi\sqrt{-1}\,k} \cdot \frac{n-1}{2\pi\sqrt{-1}\,k}\,\hat{B}_{n-2}(k) \\
&\;\vdots \\
&= \frac{n(n-1)\ldots 2}{(2\pi\sqrt{-1}\,k)^{n-1}}\,\hat{B}_1(k) \\
&= \frac{n!}{(2\pi\sqrt{-1}\,k)^{n-1}}\left(-\frac{1}{2\pi\sqrt{-1}\,k}\right) \\
&= -\frac{n!}{(2\pi\sqrt{-1}\,k)^{n}}\,.
\end{aligned}$$

Hence the lemma.

To prove the theorem, take $f = B_n$ $(n \geq 1)$ in Plancherel:

$$\int_0^1 |B_n(x)|^2 dx = \sum_{-\infty}^{\infty} |\hat{B}_n(k)|^2.$$

Here

$$\begin{aligned}
&\int_0^1 |B_n(x)|^2 dx \\
&\quad = \int_0^1 B_n(x) B_n(x)\, dx \\
&\quad = (-1)^{n-1} \frac{(n!)^2}{(2n)!}\, \bar{B}_{2n} \qquad (\text{cf. } \S 1, \#7) \\
&\quad = (-1)^{n-1} \frac{(n!)^2}{(2n)!}\, B_{2n} \qquad (\text{cf. } \S 1, \#4).
\end{aligned}$$

On the other hand,

$$\sum_{-\infty}^{\infty} |\hat{B}_n(k)|^2 = \sum_{k \neq 0} \left| -\frac{n!}{(2\pi\sqrt{-1}\,k)^n} \right|^2$$

$$= 2 \sum_{k=1}^{\infty} \frac{(n!)^2}{(2\pi k)^{2n}}$$

$$= 2 \frac{(n!)^2}{(2\pi)^{2n}} \sum_{k=1}^{\infty} \frac{1}{k^{2n}}$$

$$= 2 \frac{(n!)^2}{(2\pi)^{2n}} \zeta(2n).$$

Now cancel the $(n!)^2$ to get

$$\zeta(2n) = (-1)^{n-1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n}.$$

<u>6:</u> SCHOLIUM

$$Q[\zeta(2),\zeta(4),\zeta(6),\ldots,] = Q[\pi^2].$$

§3. $\zeta(2)$

In §2, #1, take n = 1 to get

$$\zeta(2) = \frac{\pi^2}{6}.$$

Of course there are a "million" proofs of this result but for motivational purposes we shall single out one of these.

1: NOTATION The symbol

$$\int_0^1 \int_0^1 f(x,y)\,dxdy$$

stands for a double integral over the unit square $[0,1] \times [0,1]$, possibly improper.

2: SUBLEMMA

$$\frac{3}{4}\zeta(2) = \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2}.$$

PROOF

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2}$$

$$= \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} + \sum_{n=1}^{\infty} \frac{1}{(2n)^2}$$

$$= \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} + \frac{1}{4} \sum_{n=1}^{\infty} \frac{1}{n^2}$$

$$= \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} + \frac{1}{4}\zeta(2)$$

$\Rightarrow$

$$\frac{3}{4}\zeta(2) = \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2}.$$

<u>3:</u> LEMMA

$$\int_0^1 \int_0^1 \frac{1}{1-x^2y^2}\,dxdy = \int_0^1 \int_0^1 \sum_{n=0}^{\infty} (xy)^{2n} dxdy$$

$$= \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2}$$

$$= \frac{3}{4}\,\zeta(2)\ .$$

[Note: The singularity at the corner $(x,y) = (1,1)$ can be safely ignored... .]

Define a bijective map from

$$\Pi_2 \equiv \{(u,v): u > 0,\ v > 0,\ u + v < \frac{\pi}{2}\}$$

to $]0,1[\times]0,1[$ by the prescription

$$(u,v) \rightarrow \left(\frac{\sin u}{\cos v}, \frac{\sin v}{\cos u}\right)$$

with Jacobian

$$\frac{\partial(x,y)}{\partial(u,v)} = \begin{vmatrix} \cos u/\cos v & \sin u \sin v/\cos^2 v \\ \sin u \sin v/\cos^2 u & \cos v/\cos u \end{vmatrix}$$

$$= 1 - \frac{\sin^2 u \sin^2 v}{\cos^2 u \cos^2 v} = 1 - x^2y^2.$$

[Note: The details are in the Appendix to this §.]

Therefore

$$\frac{3}{4}\,\zeta(2) = \int_0^1 \int_0^1 \frac{1}{1-x^2y^2}\,dxdy$$

$$= \text{Area}(\Pi_2) = \frac{\pi^2}{8}$$

=>

$$\zeta(2) = \frac{\pi^2}{6}.$$

<u>4:</u> LEMMA

$$\zeta(2) = \int_0^1\int_0^1 \frac{1}{1-xy}\,dxdy.$$

PROOF The RHS equals

$$\int_0^1\int_0^1 \sum_{n=0}^{\infty} x^n y^n dxdy$$

or still,

$$\sum_{n=0}^{\infty} (\int_0^1 x^n dx) \cdot (\int_0^2 y^n dy)$$

or still,

$$\sum_{n=0}^{\infty} \frac{x^{n+1}}{n+1}\Bigg|_0^1 \cdot \frac{y^{n+1}}{n+1}\Bigg|_0^1$$

or still,

$$\sum_{n=0}^{\infty} \frac{1}{(n+1)^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2).$$

To establish the connection between #3 and #4, write

- $\int_0^1 \int_0^1 (\frac{1}{1-xy} - \frac{1}{1+xy})\,dxdy$

$$= \int_0^1 \int_0^1 (\frac{2xy}{1-x^2y^2})\,dxdy$$

$$= \frac{1}{2} \int_0^1 \int_0^1 \frac{1}{1-xy}\,dxdy.$$

- $\int_0^1 \int_0^1 \left(\frac{1}{1-xy} + \frac{1}{1+xy}\right) dxdy$

$$= 2 \int_0^1 \int_0^1 \frac{1}{1-x^2y^2}\, dxdy.$$

Then

$$2 \int_0^1 \int_0^1 \frac{1}{1-xy}\, dxdy$$

$$= \frac{1}{2} \int_0^1 \int_0^1 \frac{1}{1-xy}\, dxdy + 2 \int_0^1 \int_0^1 \frac{1}{1-x^2y^2}\, dxdy$$

$\Rightarrow$

$$2\zeta(2) = \frac{1}{2}\zeta(2) + 2 \int_0^1 \int_0^1 \frac{1}{1-x^2y^2}\, dxdy$$

$\Rightarrow$

$$\frac{3}{4}\zeta(2) = \int_0^1 \int_0^1 \frac{1}{1-x^2y^2}\, dxdy.$$

APPENDIX

NOTATION

$$\Pi_n = \{(u_1,u_2,\ldots,u_n) \in R^n : u_i > 0,\ u_i + u_{i+1} < \frac{\pi}{2}\ (1 \le i \le n)\}.$$

[Note: In what follows the indices i of the n coordinates of a point in R^n are to be regarded as integers modulo n, thus

$$x_i = \frac{\sin u_i}{\cos u_{i+1}} \quad (i \in N \bmod n).]$$

Introduce

$$x_1 = \frac{\sin u_1}{\cos u_2},\ x_1 = \frac{\sin u_2}{\cos u_3},\ldots,\ x_{n-1} = \frac{\sin u_{n-1}}{\cos u_n},\ x_n = \frac{\sin u_n}{\cos u_1}$$

to get an arrow $\Pi_n \to R^n$.

LEMMA 1 The arrow $\Pi_n \to R^n$ is one-to-one and its range is the open unit cube $(]0,1[)^n$.

LEMMA 2 The Jacobian

$$\frac{\partial(x_1,\ldots,x_n)}{\partial(u_1,\ldots,u_n)}$$

equals

$$1 \pm (x_1\ldots x_n)^2,$$

the sign - or + according to whether n is even or odd.

The volume of Π_n is

$$\int_{\Pi_n} 1du_1\ldots du_n$$

or still,

$$\int_0^1 \cdots \int_0^1 \frac{1}{1 \pm (x_1\ldots x_n)^2}\, dx_1\ldots dx_n$$

or still,

$$\int_0^1 \cdots \int_0^1 \sum_{k=0}^{\infty} (-1)^{nk} (x_1\ldots x_n)^{2k}\, dx_1\ldots dx_n.$$

[Note: When n is even, the integrand in the second integral is singular at

$$(x_1,\ldots,x_n) = (1,\ldots,1)$$

but the change of variable remains valid since the integrand is elsewhere positive.]

Take now $n \geq 2$ — then in view of absolute convergence, the third integral equals

$$\sum_{k=0}^{\infty} (-1)^{nk} \int_0^1 \cdots \int_0^1 (x_1 \cdots x_n)^{2k} \, dx_1 \cdots dx_n.$$

But

$$\int_0^1 \cdots \int_0^1 (x_1 \cdots x_n)^{2k} \, dx_1 \cdots dx_n$$

$$= \left(\int_0^1 x_1^{2k} \, dx_1\right) \cdots \left(\int_0^1 x_n^{2k} \, dx_n\right)$$

$$= \frac{1}{(2k+1)^n} .$$

Therefore the volume of Π_n is

$$\sum_{k=0}^{\infty} \frac{(-1)^{nk}}{(2k+1)^n} ,$$

a rational multiple of π^n.

<u>N.B.</u> When $n = 1$, Π_n reduces to the line segment $0 < u_1 < \pi/4$ and the bottom line is the wellknown formula

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots ,$$

the value of

$$\int_0^1 \frac{1}{1+x^2} \, dx.$$

REMARK Take n even — then

$$\sum_{k=0}^{\infty} \frac{(-1)^{nk}}{(2k+1)^n} = (1 - 2^{-n}) \zeta(n) .$$

§4. $\zeta(2)$ (bis)

Since $\zeta(2) = \frac{\pi^2}{6}$, it follows that $\zeta(2)$ is transcendental, hence irrational. But let's ignore this, the objective being to prove from first principles that $\zeta(2)$ is irrational, the point being that the methods utilized can be extended in the next § to establish that $\zeta(3)$ is irrational.

1: NOTATION Let d_n be the least common multiple of $1,2,\ldots,n$ and set $d_0 = 1$.

2: LEMMA $\forall\ K > e$,

$$d_n < K^n$$

if $n >> 0$.

PROOF

$$d_n = \prod_{p \leq n} p^{[\ell n(n)/\ell n(p)]}$$

$$\leq \prod_{p \leq n} p^{\ell n(n)/\ell n(p)}$$

$$= \prod_{p \leq n} n = n^{\pi(n)},$$

$\pi(n)$ the prime counting function. Owing now to the prime number theorem,

$$\lim_{n \to \infty} \frac{\pi(n)\ell n(n)}{n} = 1,$$

so if $A > 1$, then

$$n >> 0 \Rightarrow \frac{\pi(n)\ell n(n)}{n} < A$$

or still,

$$n >> 0 \Rightarrow \pi(n)\ell n(n) < nA$$

$$\Rightarrow n^{\pi(n)} < (e^A)^n = K^n,$$

where $K = e^A > e$, i.e.,

$$n >> 0 \Rightarrow d_n = n^{\pi(n)} < K^n.$$

3: N.B. In particular,

$$n >> 0 \Rightarrow d_n < 3^n.$$

4: NOTATION Let

$$P_n(x) = \frac{1}{n!}\frac{d^n}{dx^n}(x^n(1-x)^n).$$

Then

$$P_n(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k}\binom{n+k}{k} x^k,$$

a polynomial of degree n with integral coefficients.

5: SUBLEMMA For $i \leq n - 1$,

$$\begin{cases} \dfrac{d^i}{dx^i}(x^n(1-x)^n)(0) = 0 \\[2ex] \dfrac{d^i}{dx^i}(x^n(1-x)^n)(1) = 0. \end{cases}$$

6: LEMMA Suppose that $f(x)$ is sufficiently differentiable -- then

$$\left| \int_0^1 P_n(x) f(x) dx \right| = \left| \int_0^1 \frac{1}{n!} x^n (1-x)^n \frac{d^n}{dx^n} f(x) dx \right| .$$

PROOF Write

$$\int_0^1 P_n(x) f(x) dx = \int_0^1 \frac{1}{n!} \frac{d^n}{dx^n} (x^n (1-x)^n) \; f(x) dx$$

$$= \frac{1}{n!} \frac{d^{n-1}}{dx^{n-1}} (x^n (1-x)^n) \; f(x) \Big|_0^1$$

$$- \int_0^1 \frac{1}{n!} \frac{d^{n-1}}{dx^{n-1}} (x^n (1-x)^n) \; \frac{d}{dx} f(x) dx$$

$$= - \int_0^1 \frac{1}{n!} \frac{d^{n-1}}{dx^{n-1}} (x^n (1-x)^n) \; \frac{d}{dx} f(x) dx.$$

Proceed from here by iteration.

7: INTEGRAL FORMULAS

- Let r be a nonnegative integer -- then

$$\int_0^1 \int_0^1 \frac{x^r y^r}{1-xy} dxdy = \sum_{n=1}^{\infty} \frac{1}{(n+r)^2} .$$

So

$$r = 0 \Rightarrow \int_0^1 \int_0^1 \frac{1}{1-xy} dxdy = \zeta(2) \qquad \text{(cf. §3, \#4).}$$

$$r > 0 \Rightarrow \int_0^1 \int_0^1 \frac{x^r y^r}{1-xy} dxdy$$

$$= \zeta(2) - \left(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{r^2}\right).$$

- Let r,s be nonnegative integers with $r > s$ -- then

$$\int_0^1 \int_0^1 \frac{x^r y^s}{1-xy}\, dxdy = \frac{1}{r-s}\left\{\frac{1}{s+1} + \frac{1}{s+2} + \cdots + \frac{1}{r}\right\}.$$

8: APPLICATION

$$\int_0^1 \int_0^1 \frac{x^r y^r}{1-xy}\, dxdy = \zeta(2) - \frac{a}{d_r^2}$$

and

$$\int_0^1 \int_0^1 \frac{x^r y^s}{1-xy}\, dxdy = \frac{b}{d_r^2},$$

where a,b are integers.

Therefore:

9: LEMMA If $P(x)$, $Q(y)$ are polynomials of degree n with integer coefficients, then

$$\int_0^1 \int_0^1 \frac{P(x)Q(y)}{1-xy}\, dxdy = \frac{A\zeta(2)+B}{d_n^2},$$

where A,B are integers.

10: NOTATION Put

$$I_n = \int_0^1 \int_0^1 \frac{P_n(x)(1-y)^n}{1-xy}\, dxdy.$$

Take $Q(y) = (1-y)^n$ to get

$$I_n = \frac{A_n\zeta(2)+B_n}{d_n^2},$$

where A_n, B_n are integers depending on n.

11: LEMMA

$$|I_n| = \int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n(1-y)^n}{(1-xy)^{n+1}} dxdy.$$

PROOF Taking into account #6,

$$|I_n| = \left| \int_0^1 \frac{x^n(1-x)^n}{n!} \frac{d^n}{dx^n} \left(\int_0^1 \frac{(1-y)^n}{1-xy} dy\right) dx \right|$$

$$= \left| \int_0^1 \frac{x^n(1-x)^n}{n!} \left(\int_0^1 \frac{d^n}{dx^n} \left(\frac{(1-y)^n}{1-xy}\right) dy\right) dx \right|$$

$$= \left| \int_0^1 \frac{x^n(1-x)^n}{n!} \left(\int_0^1 \frac{n! y^n(1-y)^n}{(1-xy)^{n+1}} dy\right) dx \right|$$

$$= \int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n(1-y)^n}{(1-xy)^{n+1}} dxdy.$$

12: N.B. I_n is nonzero (the integrand is positive for all $x,y \in]0,1[$).

The function

$$f(x,y) = \frac{x(1-x)y(1-y)}{1-xy} \quad (0 \le x < 1,\ 0 \le y < 1)$$

vanishes on the boundary of $[0,1] \times [0,1]$ and, although not defined at $(1,1)$, it does however tend to 0 as $x,y \uparrow 1$.

13: LEMMA The maximum of $f(x,y)$ in $0 < x < 1$, $0 < y < 1$ is

$$\left(\frac{\sqrt{5}-1}{2}\right)^5.$$

PROOF Consider the relations

$$\frac{\partial}{\partial x} f(x,y) = 0, \quad \frac{\partial}{\partial y} f(x,y) = 0,$$

i.e.,

$$1 - 2x + yx^2 = 0, \; 1 - 2y + xy^2 = 0.$$

Then

$$y = \frac{2x-1}{x^2} \Rightarrow 1 - 2\left(\frac{2x-1}{x^2}\right) + x\left(\frac{2x-1}{x^2}\right)^2 = 0$$

$$\Rightarrow x^3 - 2x + 1 = 0,$$

the roots of which are

$$1, \; \frac{-1 \pm \sqrt{5}}{2}, \text{ so } x = \frac{\sqrt{5}-1}{2}.$$

Analogously

$$y = \frac{\sqrt{5}-1}{2}.$$

Therefore $f(x,y)$ achieves its maximum at

$$\left(\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}-1}{2}\right),$$

the value being

$$\left(\frac{\sqrt{5}-1}{2}\right)^5.$$

14: APPLICATION

$$|I_n| = \int_0^1 \int_0^1 f(x,y)\, \frac{1}{1-xy}\, dxdy$$

$$\leq \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \int_0^1 \int_0^1 \frac{1}{1-xy}\, dxdy$$

$$= \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \zeta(2) \qquad \text{(cf. §3, #4).}$$

15: N.B.

$$\frac{\sqrt{5}-1}{2} = \frac{2.27-1}{2} = \frac{1.27}{2} = .635.$$

And

$$(.635)^5 \approx \frac{1}{10} \Rightarrow 9^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n}$$

$$= \left(9 \cdot \left(\frac{\sqrt{5}-1}{2}\right)^5\right)^n$$

$$\approx \left(9 \cdot \frac{1}{10}\right)^n = \left(\frac{9}{10}\right)^n \to 0 \quad (n \to \infty).$$

<u>16:</u> THEOREM $\zeta(2)$ is irrational.

PROOF Suppose instead that $\zeta(2)$ was rational, say $\zeta(2) = \frac{a}{b}$ $(a,b \in \mathbb{N})$. Write

$$I_n = \frac{A_n\zeta(2) + B_n}{d_n^2} \quad \text{(cf. \#10)}$$

$$= \frac{A_n\left(\frac{a}{b}\right) + B_n}{d_n^2}$$

$\Rightarrow$

$$\left|A_n\left(\frac{a}{b}\right) + B_n\right| \leq d_n^2 \, |I_n|$$

$\Rightarrow$ $(n >> 0)$

$$\left|A_n\left(\frac{a}{b}\right) + B_n\right| \leq 9^n \, |I_n| \quad \text{(cf. \#3)}$$

$$\leq 9^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n} \zeta(2)$$

$\Rightarrow$ $(n >> 0)$

$$|A_n a + B_n b| \leq 9^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n} b$$

$$\approx b\left(\frac{9}{10}\right)^n \to 0.$$

But I_n is nonzero (cf. #12), hence

$$0 < |A_n a + B_n b| \to 0 \quad (n \to \infty),$$

a contradiction (a sequence of positive integers cannot tend to 0).

§5. $\zeta(2n)$ (bis)

1: RAPPEL

$$\pi x \cot(\pi x) = 1 + 2x^2 \sum_{k=1}^{\infty} \frac{1}{x^2-k^2}.$$

2: RAPPEL

$$\pi x \cot(\pi x) = 1 + \sum_{n=1}^{\infty} (-1)^n \frac{2^{2n} B_{2n}}{(2n)!} \pi^{2n} x^{2n}.$$

3: N.B. These expansions are valid for $|x|$ sufficiently small.

Given k, expand

$$\frac{2x^2}{x^2-k^2}$$

in powers of x:

$$\frac{2x^2}{x^2-k^2} = -2 \sum_{n=1}^{\infty} \left(\frac{x^2}{k^2}\right)^n.$$

Therefore the coefficient of x^{2n} is

$$-2 \sum_{n=1}^{\infty} \frac{1}{k^{2n}}.$$

And then

$$\sum_{k=1}^{\infty} \frac{2x^2}{x^2-k^2} = -2 \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \left(\frac{x^2}{k^2}\right)^n$$

$$= -2 \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{x^{2n}}{k^{2n}}$$

$$= -2 \sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} \frac{1}{k^{2n}} \right) x^{2n}$$

$$= -2 \sum_{n=1}^{\infty} \zeta(2n) x^{2n},$$

i.e., $-2\zeta(2n)$ is the coefficient of x^{2n}. But the coefficient of x^{2n} is also

$$(-1)^n \frac{2^{2n} B_{2n}}{(2n)!} \pi^{2n}.$$

Consequently

$$\zeta(2n) = (-1)^{n-1} \frac{2^{2n-1}}{(2n)!} B_{2n} \pi^{2n}$$

as predicted by the considerations of #2.

§6. $\zeta(3)$

1: THEOREM $\zeta(3)$ is irrational.

The proof is similar to that for $\zeta(2)$ (cf. §4, #16), albeit technically more complicated. In outline form, here is how it goes.

Step 1:

- Let r be a nonnegative integer -- then

$$-\int_0^1 \int_0^1 \frac{\ln(xy)}{1-xy} x^r y^r \, dxdy = 2(\zeta(3) - \sum_{k=1}^{r} \frac{1}{k^3}) \in 2\zeta(3) + \frac{1}{d_r^3} Z.$$

In particular:

$$-\int_0^1 \int_0^1 \frac{\ln(xy)}{1-xy} \, dxdy = 2\zeta(3).$$

- Let r,s be nonnegative integers with $r > s$ -- then

$$-\int_0^1 \int_0^1 \frac{\ln(xy)}{1-xy} x^r y^s \, dxdy = \frac{1}{r-s} (\frac{1}{(s+1)^2} + \cdots + \frac{1}{r^2}) \in \frac{1}{d_r^3} Z.$$

Step 2:

$$\begin{aligned} I_n &\equiv -\int_0^1 \int_0^1 \frac{P_n(x)P_n(y)}{1-xy} \ln(xy)\,dxdy \\ &= \frac{A_n\zeta(3)+B_n}{d_n^3}, \end{aligned}$$

where $A_n, B_n \in Z$.

Step 3:

$$-\frac{\ln(xy)}{1-xy} = \int_0^1 \frac{1}{1-(1-xy)z} \, dz.$$

Step 4:

$$|I_n| = \left| \int_0^1 \int_0^1 \int_0^1 \frac{P_n(x)P_n(y)}{1-(1-xy)z}\, dzdxdy \right|$$

$$= \left| \int_0^1 \frac{x^n(1-x)^n}{n!} \frac{d^n}{dx^n} \left(\int_0^1 \int_0^1 \frac{P_n(y)}{1-(1-xy)z}\, dydz\right) dx \right|$$

$$\vdots$$

$$= \left| \int_0^1 P_n(y) \left(\int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n z^n}{(1-(1-xy)z)^{n+1}}\, dxdz\right) dy \right| .$$

Step 5: Let $D = \{(u,v,w): u,v,w \in]0,1[\}$ -- then the map

$$(u,v,w) \to (x,y,z)$$

defined by $x = u$, $y = v$ and

$$z = \frac{1-w}{1-(1-uv)w}$$

from D to D is one-to-one and onto. In addition,

$$\frac{\partial(x,y,z)}{\partial(u,v,w)} = -\frac{uv}{(1-(1-uv)w)^2} .$$

Step 6: The function

$$\frac{u(1-u)v(1-v)w(1-w)}{1-(1-uv)w}$$

is bounded above by $\frac{1}{27}$ in the region D.

Step 7: In I_n make a change of variable and use the relations

$$z^n = \frac{(1-w)^n}{(1-(1-uv)w)^n}$$

$$(1-(1-xy)z)^{n+1} = (1-(1-uv)\frac{1-w}{1-(1-uv)w})^{n+1}$$

$$= \frac{(uv)^{n+1}}{(1-(1-uv)w)^{n+1}}$$

to get

$$|I_n| = \int_0^1 \int_0^1 \int_0^1 \frac{u^n(1-u)^n v^n(1-v)^n w^n(1-w)^n}{(1-(1-uv)w)^{n+1}} \, dudvdw.$$

Step 8: Therefore

$$0 < |I_n| \leq (\tfrac{1}{27})^n \int_0^1 \int_0^1 \int_0^1 \frac{1}{1-(1-uv)w} \, dudvdw$$

$$= (\tfrac{1}{27})^n \int_0^1 \int_0^1 - \frac{\ell n(uv)}{1-uv} \, dudv$$

$$= 2(\tfrac{1}{27})^n \zeta(3).$$

Step 9:

$$0 < |I_n| = \frac{|A_n \zeta(3) + B_n|}{d_n^3}$$

$$\leq 2(\tfrac{1}{27})^n \zeta(3).$$

Step 10: To derive a contradiction, suppose that $\zeta(3)$ is rational, say $\zeta(3) = \frac{a}{b}$ $(a,b \in N)$ -- then

$$0 < |A_n(\tfrac{a}{b}) + B_n| \leq 2(\tfrac{1}{27})^n \zeta(3) d_n^3$$

=>

$$0 < |A_n a + B_n b| \leq 2b(\frac{1}{27})^n d_n^3$$

$$< 2b(\frac{1}{27})^n (2.8)^{3n} \quad \text{(cf. §4, \#2 (take K = 2.8))}$$

$$= 2b(\frac{(2.8)^3}{27})^n < 2b(0.9)^n \to 0 \quad (n \to \infty).$$

2: N.B. The irrationality of $\zeta(3)$ is thereby established but the issue of its transcendence remains open.

3: REMARK It was shown by T. Rivoal that the Q-vector space generated by

$$1, \zeta(3), \zeta(5), \zeta(7), \ldots$$

is infinite dimensional, hence there exist infinitely many n such that $\zeta(2n+1)$ is irrational (but it is unknown whether $\zeta(5)$ is irrational).

[Note: For an account, consult S. Fischler (arXiv:math.0303066).]

In the book "Zeta and q-Zeta Functions and Associated Series and Integrals" by H.M. Srivastava and Junesang Choi, the reader will find a large collection of formulas for $\zeta(2n+1)$.

§7. CONJUGATE BERNOULLI NUMBERS

1: DEFINITION If f is a 1-periodic function, then its periodic Hilbert transform H[f] is given by

$$H[f](x) = \mathrm{PV} \int_{-1/2}^{1/2} f(x-y)\cot(\pi y)\,dy.$$

2: CONSTRUCTION Start with the Bernoulli polynomial $B_n(x)$ and put

$$\mathcal{B}_n(x) = B_n(x-[x]),$$

a so-called Bernoulli function. It is 1-periodic and

$$\frac{\mathcal{B}_n(x)}{n!} = - \sum_{\substack{k\in Z \\ k\neq 0}} \frac{e^{2\pi\sqrt{-1}\,kx}}{(2\pi\sqrt{-1}\,k)^n},$$

a formula which holds for all real x if $n \geq 2$ and for all $x \notin Z$ if $n = 1$.

3: DEFINITION The conjugate Bernoulli functions $\tilde{B}_n(x)$ are defined for $x \in [0,1[$ $(x \neq 0$ if $n = 1)$ by the restriction of $H[\mathcal{B}_n]$ to $[0,1[$.

4: EXAMPLE For $0 < x < 1$,

$$\tilde{B}_1(x) = -\frac{1}{\pi}\ln(2\sin(\pi x)).$$

5: EXAMPLE

$$\begin{aligned}\tilde{B}_{2n+1}\left(\tfrac{1}{2}\right) &= H[\mathcal{B}_{2n+1}]\left(\tfrac{1}{2}\right) \\ &= \mathrm{PV}\int_{-1/2}^{1/2} \mathcal{B}_{2n+1}\left(\tfrac{1}{2} - y\right)\cot(\pi y)\,dy\end{aligned}$$

$$= \text{PV} \int_{-1/2}^{1/2} B_{2n+1} \left(\frac{1}{2} - y\right)\cot(\pi y)\,dy.$$

[Note: By definition

$$B_{2n+1} \left(\frac{1}{2} - y\right) = B_{2n+1} \left(\frac{1}{2} - y - \left[\frac{1}{2} - y\right]\right).$$

But

$$-\frac{1}{2} < y < \frac{1}{2} \Rightarrow \frac{1}{2} > -y > -\frac{1}{2}$$

$$\Rightarrow \frac{1}{2} + \frac{1}{2} > \frac{1}{2} - y > \frac{1}{2} - \frac{1}{2}$$

$$\Rightarrow 1 > \frac{1}{2} - y > 0$$

$$\Rightarrow \left[\frac{1}{2} - y\right] = 0.]$$

<u>6:</u> <u>N.B.</u>

$$\tilde{B}_n(x) = -2(n!) \sum_{k=1}^{\infty} \frac{\sin(2\pi kx - n\pi/2)}{(2\pi k)^n} \quad (x \neq 0 \text{ if } n = 1).$$

<u>7:</u> LEMMA $\forall\, n \in \mathbb{N}$,

$$\tilde{B}_n(1-x) = (-1)^{n+1}\, \tilde{B}_n(x) \quad (0 < x < 1).$$

PROOF From #6,

$$\tilde{B}_n(1-x) = -2(n!) \sum_{k=1}^{\infty} \frac{\sin(2\pi k(1-x) - n\pi/2)}{(2\pi k)^n}.$$

Write

$$\sin(2\pi k(1-x) - n\pi/2)$$

$$= \sin(2\pi k - 2\pi kx - n\pi/2 + n\pi/2 - n\pi/2)$$

$$= \sin((-2\pi kx + n\pi/2) + (2\pi k - n\pi))$$

$$= \sin(-2\pi kx+n\pi/2)\cos(2\pi k-n\pi)$$

$$+ \sin(2\pi k-n\pi)\cos(-2\pi kx+n\pi/2)$$

$$= - \sin(2\pi kx-n\pi/2)\cos(-n\pi)$$

$$+ \sin(-n\pi)\cos(-2\pi kx+n\pi/2)$$

$$= \sin(2\pi kx-n\pi/2)(-1)\cos(n\pi)$$

$$+ (0)\cos(-2\pi kx+n\pi/2)$$

$$= \sin(2\pi kx-n\pi/2)(-1)(-1)^n$$

$$= (-1)^{n+1}\sin(2\pi kx-n\pi/2),$$

matters then being manifest.

8: APPLICATION Take $x = \frac{1}{2}$ -- then

$$\tilde{B}_{2n}(\tfrac{1}{2}) = (-1)^{2n+1}\tilde{B}_{2n}(\tfrac{1}{2}) = -\tilde{B}_{2n}(\tfrac{1}{2})$$

$$\Rightarrow$$

$$\tilde{B}_{2n}(\tfrac{1}{2}) = 0.$$

9: DEFINITION The conjugate Bernoulli numbers $\tilde{\tilde{B}}_n$ are defined by

$$\tilde{\tilde{B}}_n = \tilde{B}_n(0) \quad (n > 1).$$

10: RAPPEL $\forall\ n > 1$,

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{(2\pi k)^n} = (2\pi)^{-n}(1 - 2^{1-n})\zeta(n).$$

11: LEMMA $\forall\ n > 1$,

$$\tilde{B}_n(\tfrac{1}{2}) = (2^{1-n} - 1)\tilde{\tilde{B}}_n.$$

PROOF From #6,

$$\tilde{B}_n(\tfrac{1}{2}) = -2(n!)\sum_{k=1}^{\infty}\frac{\sin(\pi k-n\pi/2)}{(2\pi k)^n}.$$

But

$$\sin(\pi k-n\pi/2) = \sin(\pi k)\cos(\tfrac{n\pi}{2}) - \sin(\tfrac{n\pi}{2})\cos(\pi k)$$

$$= -\sin(\tfrac{n\pi}{2})\cos(\pi k)$$

$$= -\sin(\tfrac{n\pi}{2})(-1)^k$$

$$= \sin(\tfrac{n\pi}{2})(-1)^{k+1}.$$

Therefore

$$\tilde{B}_n(\tfrac{1}{2}) = -2(n!)\sin_{k=1}(\tfrac{n\pi}{2})\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{(2\pi k)^n}$$

$$= -2(n!)\sin(\tfrac{n\pi}{2})(2\pi)^{-n}(1-2^{1-n})\zeta(n)$$

$$= (2^{1-n}-1)2(n!)\sin(\tfrac{n\pi}{2})(2\pi)^{-n}\zeta(n).$$

However

$$\tilde{B}_n = \tilde{B}_n(0) = -2(n!)\sum_{k=1}^{\infty}\frac{\sin(-\frac{n\pi}{2})}{(2\pi k)^n}$$

$$= 2(n!)\sin(\tfrac{n\pi}{2})\sum_{k=1}^{\infty}\frac{1}{(2\pi k)^n}$$

$$= 2(n!)\sin(\tfrac{n\pi}{2})(2\pi)^{-n}\zeta(n).$$

Therefore

$$\tilde{B}_n(\tfrac{1}{2}) = (2^{1-n}-1)\tilde{B}_n.$$

12: DEFINITION Given $x \in R$, put

$$\Omega(x) = \mathrm{PV} \int_{-1/2}^{1/2} e^{xy} \cot(\pi y)\, dy,$$

the omega function.

13: N.B. Therefore the omega function is the periodic Hilbert transform at 0 of the 1-periodic function f defined by periodic extension of $f(y) = e^{-xy}$ $(y \in [-\frac{1}{2}, \frac{1}{2}[)$:

$$\Omega(x) = \mathrm{PV} \int_{-1/2}^{1/2} e^{-(0-y)x} \cot(y\pi)\, dy$$

$$= H[e^{-\cdot\, x}]\ (0).$$

14: LEMMA There is an expansion

$$\Omega(x) = \sum_{j=0}^{\infty} \frac{\Omega_j}{j!} x^j,$$

where

$$\Omega_j = D_x^j \Omega(x) \Big|_{x=0} = \mathrm{PV} \int_{-1/2}^{1/2} y^j \cot(\pi y)\, dy.$$

The omega function figures in the generating function for the $\tilde{B}_n(\frac{1}{2})$.

15: THEOREM For $|x| < 2\pi$,

$$-\frac{xe^{x/2}}{e^x - 1} \Omega(x) = \sum_{k=0}^{\infty} \tilde{B}_k(\tfrac{1}{2}) \frac{x^k}{k!}.$$

PROOF Ignoring the minus sign, on the LHS, it is a question of the Cauchy product of two infinite series:

$$\left(\sum_{k=0}^{\infty} B_k(\tfrac{1}{2}) \frac{x^k}{k!}\right) \times \left(\sum_{k=0}^{\infty} \frac{\Omega_k}{k!} x^k\right),$$

a generic term being

$$\sum_{j=0}^{k} B_{k-j}(\tfrac{1}{2}) \frac{x^{k-j}}{(k-j)!} \Omega_j \frac{x^j}{j!}$$

or still,

$$\left(\sum_{j=0}^{k} \binom{k}{j} B_{k-j}(\tfrac{1}{2})\Omega_j\right) \frac{x^k}{k!} .$$

Owing to the addition formula (see the Appendix to §1),

$$B_k(\tfrac{1}{2} - y) = \sum_{j=0}^{k} \binom{k}{j} B_{k-j}(\tfrac{1}{2}) (-y)^j.$$

On the other hand,

$$\Omega_j = \mathrm{PV} \int_{-1/2}^{1/2} y^j \cot(\pi y)\, dy.$$

And $\Omega_{2j} = 0$. So in the sum

$$\sum_{j=0}^{k} \binom{k}{j} B_{k-j}(\tfrac{1}{2}) \Omega_j,$$

only the odd j contribute. This said, consider

$$\mathrm{PV} \int_{-1/2}^{1/2} \sum_{j=0}^{k} \binom{k}{j} B_{k-j}(\tfrac{1}{2}) y^j \cot(\pi y)\, dy$$

or still,

$$- \mathrm{PV} \int_{-1/2}^{1/2} \sum_{j=0}^{k} \binom{k}{j} B_{k-j}(\tfrac{1}{2}) (-1) y^j \cot(\pi y)\, dy.$$

Assume that j is odd, say $j = 2\ell+1$ -- then

$$(-y)^j = (-y)^{2\ell+1} = (-1)^{2\ell+1}(y)^{2\ell+1}$$
$$= (-1)^1(y)^{2\ell+1} = (-1)y^j.$$

The data thus reduces to

$$- \text{PV} \int_{-1/2}^{1/2} B_k(\tfrac{1}{2} - y)\cot(\pi y)dy$$
$$\equiv - \tilde{B}_k(\tfrac{1}{2}),$$

from which the result.

16: THEOREM

$$\Omega(2\pi x) = \frac{1}{\pi}(e^{-\pi x} - e^{\pi x}) \sum_{k=1}^{\infty} (-1)^k \frac{k}{x^2+k^2}.$$

[It can be shown that

$$2 \sum_{k=1}^{\infty} (-1)^{k+1} \int_0^1 e^{2\pi xy}\sin(2\pi ky)dy$$
$$= \frac{1}{\pi}(e^{2\pi x}-1) \sum_{k=1}^{\infty} (-1)^k \frac{k}{x^2+k^2}$$

or still,

$$e^{\pi x}\Omega(-2\pi x) = \frac{1}{\pi}(e^{2\pi x}-1) \sum_{k=1}^{\infty} (-1)^k \frac{k}{x^2+k^2}$$

or still,

$$\Omega(-2\pi x) = \frac{1}{\pi}(e^{\pi x}-e^{-\pi x}) \sum_{k=1}^{\infty} (-1)^k \frac{k}{x^2+k^2}.]$$

17: REMARK By way of comparison, recall that

$$\frac{\pi}{\sin(\pi x)} = \frac{1}{x} + 2 \sum_{k=1}^{\infty} (-1)^k \frac{x}{x^2-k^2}.$$

§8. $\zeta(2n + 1)$

The formula for $\zeta(2n)$ in terms of Bernoulli numbers (cf. §2, #1) admits an analog for $\zeta(2n+1)$ in terms of conjugate Bernoulli numbers.

1: THEOREM

$$\zeta(2n+1) = (-1)^n \, 2^{2n} \pi^{2n+1} \frac{\tilde{B}_{2n+1}}{(2n+1)!} \, .$$

PROOF

Step 1: $|x| < 1$

=>

$$\sum_{k=1}^{\infty} (-1)^k \frac{k}{x^2+k^2} = \sum_{k=1}^{\infty} \frac{(-1)^k}{k} \sum_{n=0}^{\infty})-1)^n \left(\frac{x}{k}\right)^{2n}$$

$$= \sum_{k=1}^{\infty} \frac{(-1)^k}{k} \sum_{n=1}^{\infty} (-1)^n \left(\frac{x}{k}\right)^{2n} + \sum_{k=1}^{\infty} \frac{(-1)^k}{k}$$

$$= \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} (-1)^k \frac{2}{k^{2n+1}}\right) (-1)^n x^{2n}.$$

Step 2: Write (cf. §7, #15)

$$\sum_{k=0}^{\infty} \frac{\tilde{B}_k(\frac{1}{2})}{k!} (2\pi x)^k = - 2\pi x \frac{e^{\pi x}}{e^{2\pi x}-1} \Omega(2\pi x)$$

$$= - 2\pi x \frac{e^{\pi x}}{e^{2\pi x}-1} \frac{e^{-\pi x}}{e^{-\pi x}} \Omega(2\pi x)$$

$$= - 2\pi x \frac{1}{e^{\pi x}-e^{-\pi x}} \Omega(2\pi x)$$

$$= 2\pi x \frac{1}{e^{-\pi x}-e^{\pi x}} \Omega(2\pi x)$$

$$= 2x \frac{\pi}{e^{-\pi x}-e^{\pi x}} \Omega(2\pi x)$$

$$= 2x \sum_{k=1}^{\infty} (-1)^k \frac{k}{x^2+k^2} \qquad \text{(cf. §7, \#26)}$$

$$= 2x \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} (-1)^k \frac{1}{k^{2n+1}}\right) (-1)^n x^{2n}.$$

Accordingly

$$\frac{1}{2x} \sum_{k=0}^{\infty} \frac{\tilde{B}_k(\frac{1}{2})}{k!} (2\pi)^k x^k$$

$$= \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} (-1)^k \frac{1}{k^{2n+1}}\right) (-1)^n x^{2n}.$$

So, comparing coefficients,

$$\tilde{B}_{2n}(\tfrac{1}{2}) = 0 \qquad \text{(cf. §7, \#8)},$$

and

$$\frac{\tilde{B}_{2n+1}(\frac{1}{2})}{(2n+1)!} 2^{2n}\pi^{2n+1} = (-1)^n \sum_{k=1}^{\infty} (-1)^k \frac{1}{k^{2n+1}} .$$

<u>Step 3</u>: First (cf. §7, #10)

$$\sum_{k=1}^{\infty} (-1)^k \frac{1}{k^{2n+1}} = (2^{-2n}-1)\zeta(2n+1).$$

Therefore

$$\zeta(2n+1) = \frac{1}{2^{-2n}-1} (-1)^n 2^{2n}\pi^{2n+1} \frac{\tilde{B}_{2n+1}(\frac{1}{2})}{(2n+1)!} .$$

But (cf §7, #11)

$$\tilde{B}_{2n+1}(\tfrac{1}{2}) = (2^{-2n}-1)\tilde{B}_{2n+1},$$

thus

$$\zeta(2n+1) = \frac{1}{2^{-2n}-1} (-1)^n \, 2^{2n}\pi^{2n+1} \frac{(2^{-2n}-1)\tilde{B}_{2n+1}}{(2n+1)!}$$

$$= (-1)^n \, 2^{2n}\pi^{2n+1} \frac{\tilde{B}_{2n+1}}{(2n+1)!},$$

the statement of #1.

Question: Is

$$\frac{\zeta(2n+1)}{\pi^{2n+1}}$$

rational or irrational? Ans: Nobody knows. Of course, part of the problem is the structure of $\tilde{B}_{2n+1}$ which appears to be complicated. E.g.:

$$\tilde{B}_3(\tfrac{1}{2}) = \frac{\ell n(2)}{4\pi} - 2 \int_{0^+}^{1/2} y^3 \cot(\pi y)\,dy$$

$$= (2^{-2}-1)\tilde{B}_3.$$

2: THEOREM

$$\zeta(2n+1) = (-1)^{n+1} \frac{2^{2n}\pi^{2n+1}}{(2n+1)!} \int_0^1 B_{2n+1}(y) \cot(\pi y)\,dy.$$

PROOF In fact

$$\tilde{B}_{2n+1} \equiv \tilde{B}_{2n+1}(0) \qquad (\text{cf. §7, \#9})$$

$$= - \text{PV} \int_0^1 B_{2n+1}(y) \cot(\pi y)\,dy$$

$$= - \int_0^1 B_{2n+1}(y) \cot(\pi y)dy$$

after replacing y by -y and taking into account the 1-periodicity.

[Note: The PV is not necessary since

$$\lim_{x \to 0} x \cot x = 1.]$$

<u>3:</u> REMARK In a similar vein,

$$\zeta(2n) = (-1)^{n+1} \frac{2^{2n-1}\pi^{2n}}{(2n)!} \int_0^1 \tilde{B}_{2n}(y) \cot(\pi y)dy.$$