The Constructive Theory of Transcendental Numbers,

or

The LIOUVILLE-THUE-SIEGEL-MAHLER-ROTH-SCHNEIDER Theorem

by George Mark Bergman

submitted in fulfilment
of a minor requirement
for the degree of
Doctor of Philosophy
in Mathematics at
Harvard University.

Explanation: One of the requirements in the Math Ph.D. program at Harvard is the "minor thesis", which consists of producing, in a limited period of time, an expository write-up of a subject outside the student's main area of research. The procedure at the time I was a student was that one said one was ready to do one's minor thesis, and shortly thereafter, one received a slip of paper stating the topic, and had a few weeks in which to learn about the subject, and prepare and submit the write-up. (One faculty member's explanation for the skill this requirement was meant to develop and test was, "Your distinguished colleague who has taught the same graduate course for the last 30 years has just fallen ill, and you have three weeks to prepare to teach it in his stead.")

My slip said "Transcendental numbers". I found that there were too many areas therein to cover well, so I concentrated on one of them. This was probably in my last Semester of graduate school, Spring 1967.

George Bergman, 2011

Introduction

We shall here be concerned rather exclusively with one aspect of the theory of transcendental numbers, the "constructive" theory, which dates from the Liouville construction. The main result we shall prove is equivalent to Satz 6 of Schneider, |1|. If, like the chemist, we adopt a structural terminology, then, as we shall see, this should be called the

Liouville-Thue-Siegel-Roth
        Schneider-Mahler >Schneider Theorem.

In sections 1 and 2 we discuss, and give applications of, some of the earlier results leading up to this theorem. In section 3 we state the theorem and the two lemmas we shall use in proving it. In sections 4, 5 and 6 we prove the theorem, and then the two lemmas used. Section 7 consists of a hurried discussion of several topics related to the theorem and the constructive study of transcendental numbers in general. In section 8 we list the most important results from the rest of the theory of transcendental numbers.

Our principal innovations here are (1) to show that Schneider's Satz 6 is equivalent to a formally stronger statement*, and (2) to give a more natural proof of the lemma on "generalized Wronskians". We have also introduced some terminology making it easier to state and compare this type of results, and have sharpened the estimates in some of the lemmas used. On the other hand, our attempts to reorganize proofs so as to be conceptually clearer may have made some of them computationally messier.

One thing I have learned from this work is that I had better have my typewriter rehauled before doing the final copy of my major thesis.

The word "integer" is here used to mean "member of Z" unless we specify "algebraic integer" or "integer in the field K".

*Schneider's Satz 6, though stated somewhat differently, is essentially what we have left to prove after we have made the first two reductions of Step 1 in the proof of our Theorem.

§1 Liouville-Thue-Siegel-Roth

J. Liouville initiated the "constructive" study of transcendental numbers in 1844 with the following observation:

Let α be an irrational algebraic real number, say a root of the irreducible polynomial P of degree $n > 1$, with integral coefficients. Suppose p/q is a rational fraction near to α. Then P(p/q) can be written as a rational fraction with denominator q^n, hence has absolute value $\geqslant q^{-n}$. If C is an upper bound for the derivative of P in some fixed neighborhood of α, say $(\alpha-1,\alpha+1)$, we can see that $|\alpha-\frac{p}{q}|$ cannot be less than $1/Cq^n$ (for p/q in this neighborhood. If we take the bound C to be > 1, this will clearly also be true for p/q outside $(\alpha-1,\alpha+1)$.) i.e., cannot be the limit of a seq

That is, α cannot be the limit of a sequence of rational fractions which converges too rapidly, compared with the ~~right~~ rate at which the denominators increase. To set up a precise terminology, let f be an non-negative real-valued function on the positive integers, and let us say say that a real number α is f(q)-approximable if it is the limit of a sequence of rational fractions p_n/q_n with $|\alpha-p_n/q_n| \leqslant f(q_n)$.* Clearly, we can similarly define the statement that a number is O(f(q))-approximable, or o(f(q))-approximable. Then Liouville's result is that an algebraic number of degree $n > 1$ cannot be $o(q^{-n})$-approximated. It follows that an irrational number which is $o(q^{-n})$-approximable for all n must be transcendental. Such numbers are called Liouville numbers. Examples are $\sum a^{-i!}$, and $1/a + 1/a! + 1/a!! + \ldots$, where a is an integer >1. (The latter example is, in fact, 2/q!-approximable.) It is clear that we can get more Liouville numbers by giving the terms of either of these series integral coefficients, with very generous bounds on their magnitudes; in fact, we can get uncountably many distinct Liouville numbers using 0 and 1 as coefficients.

*When we speak of an approximating sequence of rational numbers, p_i/q_i, we shall understand the numerators p_i and the denominators q_i to be specified, not just their ratio. We do not require them to be relatively prime, but we do require $q_i > 0$.

One might expect that the sum of two Liouville numbers would still be a Liouville number unless it was rational. But consider the following counterexample. We shall form two numbers a and b using the decimal expansion of $\sqrt{2}$ as follows: the initial digits of a will be 0.0, and those of b 1.4; for integers $m > 1$, if m satisfies inequalities $(2k-1)! < m \leqslant (2k)!$ for some k, then the m^{th} digit of a to the right of the decimal point will be taken to be the corresponding digit of $\sqrt{2}$, while the m^{th} digit of b will be 0; for m satisfying $(2k)! < m \leqslant (2k+1)!$, the reverse will hold.

We note that for any $k > 0$, the first $(2k)!$ digits of a give an approximation of a which is rational with denominator $10^{(2k)!}$ but actually gives a to $10^{(2k+1)!}$ places. Calling this p_k/q_k $(q_k = 10^{(2k)!})$, we have $|a - p_k/q_k| < 10^{-(2k+1)!} = q_k^{-2k-1} = o(q_k^{-n})$ for any n. Hence a is a Liouville number. The same clearly applies to b. But their sum is $\sqrt{2}$ by construction (which is not even $o(q^{-2})$-approximable, by Liouville's argument).

In 1909 Thue strengthened Liouville's result, showing that an algebraic number of degree n is not $q^{-\mu}$-approximable for any $\mu > \frac{n}{2} + 1$. Given two functions f and g simultaneously approaching 0, let us write $g = oo(f)$ if there exists a constant $\varepsilon > 0$ such that $|g|$ is eventually $\leqslant |f|^{1+\varepsilon}$. Then Thue's result was that an algebraic number of degree n is not $oo(q^{-n/2\ -1})$-approximable.

Note that this implies that an algebraic number of degree $n > 2$ is not $O(q^n)$-approximable. We can now work Liouville's pump backwards: if P is the minimal polynomial of this number, we see that $P(p/q) = q^{-n}$ cannot have infinitely many solutions (near to this root, at least. But the other roots behave similarly.) Thus, if we write $f(p,q)$ for the homogeneous form $q^nP(p/q)$, $f(p,q) = 1$ has only finitely many solutions in integers. We could obtain stronger implications, but we shall leave this topic until section 7.

Siegel and Dyson were able to replace the function $\frac{n}{2}+1$ by still smaller functions of n in this result. Finally, in 1955, Roth showed that no irrational algebraic number is $oo(q^{-2})$-approximable. This allows us to construct larger classes of transcendental numbers than the Liouville numbers. For instance for a an integer >1, $\sum a^{-3^n}$ will be transcendental, since it is $O(q^{-3})$-approximable. (Clearly, it was not constructed as a Liouville number; the problem of proving that such a number is actually not a Liouville number — we should expect that it is not even $o(q^{-3})$-approximable — is not difficult, but will not be dealt with here. The reader will find such a proof for the example to be given in the next section in Schneider [1], last part of Satz 9.)

That Roth's result is the best possible concerning "q^{λ}-approximability" is shown by the following observation:

<u>Lemma 1</u> Every real number α is q^{-2}-approximable; in fact, $1/q(q+1)$-approximable.

<u>Proof</u> Given $n>0$, consider the images of the numbers $0, \alpha, 2\alpha, \ldots, n\alpha$ in the group $\mathbb{R}/\mathbb{Z}$, thought of as a closed curve of length 1. Then some two of them, $a\alpha$ and $(a+q)\alpha$ must lie within $\leq 1/(n+1)$ of each other. Hence the image of $q\alpha$ will lie within $1/(n+1)$ of 0. Hence in $\mathbb{R}$, $q\alpha$ will lie within $1/(n+1)$ of some integer p. Then $|\alpha-p/q| \leq 1/q(n+1) \leq 1/q(q+1)$. Since this difference is also $\leq 1/(n+1)$, we can, by taking n sufficiently large, get such fractions p/q to approach α.|

If we limit ourselves to approximations of α by fractions $p/q \neq \alpha$, however, we find that the above argument fails precisely if α is a rational number, while Liouville's original argument now holds for n=1, and shows us that α is not even $o(q^{-1})$-approximable. So the rationals are in one sense the easiest and in another the hardest numbers to approximate by rationals!

§ 2 <u>Schneider-Mahler</u>

It is clear that real numbers cannot in general be so quickly approximated

§2 Schneider-Mahler

It is clear that real numbers cannot in general be as quickly approximated by fractions whose denominators are required to be powers of a fixed integer $b > 1$ as by fractions with arbitrary denominator. In contrast to Lemma 1, the best result here is that any real number can be $\frac{1}{2}q^{-1}$-approximated by such a sequence, as we can see for the case $b=10$ by looking at decimal expansions, and for other b similarly.

In 1936, Schneider sketched a proof that no irrational algebraic number can be $oo(q^{-1})$-approximated by a sequence p_i/q_i in which the q_i have the form b^{λ_i}, and do not increase too rapidly — explicitly, $\overline{\lim}\ \lambda_{i+1}/\lambda_i < \infty$. For $b=10$, this means that a number α is transcendental if we can find integers $\lambda_1 < \mu_1 < \lambda_2 < \mu_2 < \ldots$ such that the decimal expansion of α has a straight string of zeroes or 9's from λ_1 to μ_1, from λ_2 to μ_2 etc., where the μ_i/λ_i have lower bound greater than 1 (essentially, the $1+\varepsilon$ in our definition of $oo(q^{-1})$, and the λ_{i+1}/λ_i are bounded above. Examples of numbers to which this applies are $\sum(7/10)^{3^i}$, $\sum 10^{-[(\frac{3}{2})^i]}$, and $\sum 10^{-f_i}$ (where [ ] is the "greatest integer" function, and f_i the Fibonacci series.)

In 1937, Mahler proved a strengthened version of Schneider's result: the denominators could now be of the form $b^{\lambda_i}q_i'$, where λ_i is as above, and the q_i' are arbitrary integers with $\log q_i' = o(\lambda_i)$. As an amusing application, he proved that if we take any nonnegative integral-valued polynomial function $P(x)$, and form a decimal (more generally: b-ary) fraction by juxtaposing the decimal expressions of $P(1), P(2), \ldots$ (written as blocks of digits not beginning with zero): $0.P(1)P(2)P(3)\ldots$, the resulting real number is transcendental.

The key fact he used is that for any integral-valued polynomial P of degree n, the series $\sum_0^\infty P(j)x^{-j}$ converges for $x>1$ to a rational function of x with integral coefficients and denominator $(x-1)^{n+1}$.* Because our decimal fraction

*This is easily seen if we recall that $\sum \binom{n}{j}x^{-j} = (x-1)^{-n-1}$.

expression breaks up into "runs" of rapidly increasing length which can be written as sums $\sum P(j)(10^k)^{-j}$, we can get good rational approximations to α. We shall illustrate the argument for $P(j)= j$, whence $\alpha =$ 0.123456789101112131415...

We first note that α can be approximated to essentially 9 places by $10/(10-1)^2 = 10/81 = .12345... = \sum^{\infty} j10^{-j}$. Actually, the error is slightly $> 10^{-10}$ because in the expansion of 10/81, a 1 is carried from the 10th place. But the error is $<2\cdot 10^{-10}$

If we look at the next ninety 2-digit units, 10 11 12 ... 99, we find that they must agree with the corresponding digits of a certain fraction of denominator 99^2. Adding to this a fraction with denominator 10^9, we can also make the first nine digits agree with those of α. Hence we have approximated α to essentially $9+2\cdot 90$ places (actually $9 + 2\cdot 90 -1$) by a fraction with denominator $10^9\cdot 99^2$.

In general, let us write $\lambda_i = 9 + 2\cdot 90 + ...+ i(10^i - 10^{i-1})$. Then we find that α can be approximated to within $10^{-\lambda_{i+1}}$ by a fraction with denominator $10^{\lambda_i}\cdot(10^i-1)^2$. Since λ_{i+1}/λ_i approaches 10 from above, this gives us a q^{-10}-approximation of α. The denominators do not increase too fast, and $\log q'_i = 2 \log (10^i-1) = O(i) = o(\lambda_i)$. So Mahler's result is applicable. (Roth's result, which had not been proved then, is also applicable, but fails when we use base-2 expansions!).

§3 Schneider's generalization

Th. Schneider, in [1], extends Roth's proof to get a result including Mahler's.* His statement is equivalent to the following:

Theorem Let a real number α be the limit of a sequence of rational fractions $p_k/q_k = p_k/q''_k q'_k$, where the q''_k have all their prime divisors in a fixed finite set. Suppose $0 < |\alpha - p_k/q_k| = oo(q''^{-1}_k q'^{-2}_k)$. Then α is transcendental.

*It is not clear whether Mahler's result originally required the approximating fractions to have the stated properties when in lowest terms or not. If not, it is not quite included in Schneider's original result, which did require this, as is clear from the proof though not from the statement. However for our restatement, lowest terms are clearly immaterial, so we see that Mahler's result is implied.

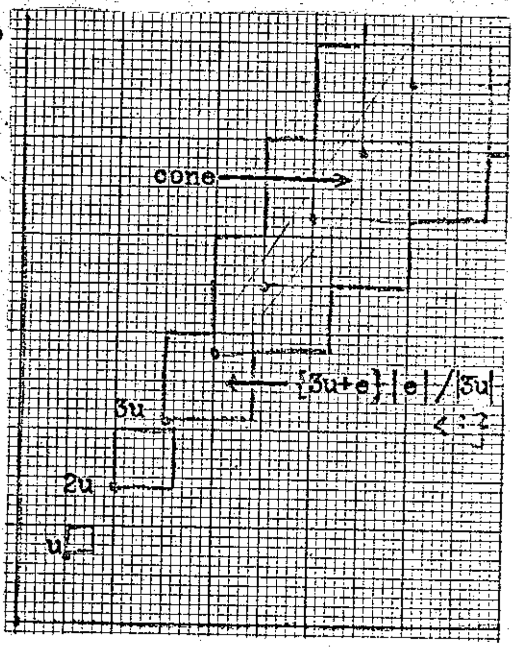
Indeed, if we make the $q_k^{\sim}=1$, this is Roth's result, while if we make the q_k' small and the $q_k^{\sim}$ powers of some b, it is Mahler's.

Schneider stated the result with the assumption that the $q_k^{\sim}$ are powers of a fixed integer. The equivalence of the above statement to his results from the following lemma (actually, the corollary), which allows us to pick from a sequence with our more general property a subsequence that approximately satisfies his condition, and can be transformed into one that does so precisely.

Let $\mathbb{R}_{\geqslant 0}$ denote the nonnegative real numbers, let n be a positive integer, and let us partially order $\mathbb{R}^n_{\geqslant 0}$ by writing $(u_1,\ldots,u_n)\geqslant(v_1,\ldots,v_n)$ if every $u_k\geqslant v_k$. Let $|(u_1,\ldots,u_n)|$ designate $\sum u_i$.

<u>Lemma 2</u> Let $c_1,\ldots,c_n$ be positive real constants, ε an arbitrarily small positive real number, and X an unbounded set in $\mathbb{R}^n_{\geqslant 0}$. Then there exists an element u of the form $(a_1c_1,\ldots,a_nc_n)$ $(a_i\in\mathbb{Z}_{\geqslant 0})$ and an unbounded sequence (x_i) of elements of X such that every x_i can be written $\lambda_i u + e_i$, with $|e_i|/|\lambda_i u|<\varepsilon$.

<u>Proof</u> We shall give the geometric idea, and leave the details to the reader. Let u be any nonzero element of $\mathbb{R}^n_{\geqslant 0}$. We note as shown in the diagram at right that the set of elements of the form $x = \lambda u + e$ with $|e|/|\lambda u|\leqslant\varepsilon$ $(\lambda\in\mathbb{Z}_{\geqslant 0})$ will contain all but a bounded portion of a convex "cone" of elements. Given any ray through O, it is easy to find a point u of the lattice described in the hypothesis with which we can associate an open cone containing this ray. By the compactness of projective n-1-space, finitely many such cones cover $\mathbb{R}^n_{\geqslant 0}$. Hence we can choose a sequence from X approaching infinity and lying in one such cone. All but finitely many of its terms (which we delete) will be of the desired form with respect to u.|



<u>Corollary</u> Let be an arbitrarily small positive number, and Y an infinite set of positive integers having all their prime divisors in a common finite set. Then there exists a positive integer b and an infinite sequence (y_i) in Y such that every y_i can be factored $b^{\lambda_i}f_i$ with $f_i < b^{\lambda_i \varepsilon}$.

<u>Proof</u> Let the finite set consist of n primes, $p_1,\ldots,p_n$. Let us map Y into $\mathbb{R}^n_{\geq 0}$ by sending $p_1^{k_1}\ldots p_n^{k_n}$ to $(k_1 \ln p_1,\ldots, k_n \ln p_n)$. Note that if y goes to $x \in \mathbb{R}^n_{\geq 0}$, we have $y = \exp|x|$. Let us also choose $c_j = \ln p_j$, and apply the above lemma. It is clear that each of the remainder terms e_i we get will also have j^{th} coordinate a multiple of $\ln p_j$ for all j. Taking $b = \exp|u|$, $f_i = \exp|e_i|$, we get the desired decomposition.|

When we apply this to our series of approximations, with Y the set of $\tilde{q_i}$'s, we shall see that the terms f_i can be "transferred" to the q_i'.

Let us now preview the essential idea of the proof of the theorem. If is based on two lemmas stated at the end of this section, which we shall put off proving until later. The first says that given a fixed algebraic number α, we can construct a polynomial in a large number of indeterminates, with integral coefficients, satisfying certain bounds on the degrees and magnitudes of the terms appearing, which vanishes to a high order in an appropriate sense at $(\alpha,\ldots,\alpha)$. The second says that a polynomial satisfying such bounds cannot vanish to too high an order at a point having rational coordinates with very large denominators.

We now consider a polynomial gotten from the first lemma at a point $(p_1/q_1,\ldots,p_m/q_m)$ whose coordinates are appropriately chosen from our sequence of approximations.* Since it cannot vanish to too high an order at this point, we can, by applying an appropriate mixed partial derivative, take it to be nonzero there, while still vanishing to a high order at $(\alpha,\ldots,\alpha)$.

*Throughout our proof, whenever we modify our sequence or choose a subsequence, we shall understand that all terms are relabeled so that our chosen terms are called $p_1/q_1,\ldots$.

We now use the fact that $(p_1/q_1,\dots,p_m/q_m)$ lies very close to $(\alpha,\dots,\alpha)$. From the fact that our polynomial vanishes to a high order at the latter point, we deduce that it will take on a very small value at the former point. But working with the denominators of $p_1/q_1,\dots,p_m/q_m$, and bounds on the degrees of the terms of our polynomial, we get an upper bound on the denominator of the value of our polynomial at this point, from which we conclude that this value cannot be as small as we had concluded, giving a contradiction.

A noteworthy aspect of the proof is the way in which we weight the variables, both in counting the degree of our polynomial, and the order to which it vanishes at a point. The earlier coordinates are given lower weights, and thus tend to appear with higher exponents. Thus the terms which approximate α more roughly, and have smaller denominators, ap pear to higher powers than the finer approximations with larger denominators, and so, both in our estimate of the value of the polynomial at $(p_1/q_1,\dots,p_m/q_m)$, and our estimate of the denominator, the rough and find approximations are made to contribute more or less equally!.

There remains the quation of how the $q_i^{\sim}$ and q_i' parts of our denominator come to behave differently. The idea is that we put a bound on the total (weighted) degree of our polynomial, which gives us a bound on the total power of b that the $q_i^{\sim}$'s can bring into the denominator of any term. But when we work with the q_i', the best we can do for a common denominator is the product of the highest powers to which each occurs.— the l.c.m. function is nicer on

The two lemmas we shall use are:

<u>Lemma 3</u> (Schneider's Hilfsatz 11) Let α be an algebraic number of degree $s > 0$. Let ε be a real number with $0<\varepsilon<1/2$, and m a positive integer such that $2m^{1/2}\varepsilon > 2s+1$. Let $r_1,\dots,r_m$ be positive integers.

Then there exists a polynomial $\phi(x_1,\dots,x_m)$ such that:

a) When ϕ is expanded about $(\alpha,\dots,\alpha)$, all terms $(x_1-\alpha)^{t_1}\dots(x_m-\alpha)^{t_m}$ with nonzero coefficient have: $t_i/r_i \leq 1$ for all i (1)

$$(\tfrac{1}{2}-\varepsilon)m < \sum t_i/r_i < (\tfrac{1}{2}+\varepsilon)m \qquad (2), (3)$$

b) If ϕ is expanded about 0, the coefficients lie in $\mathbb{Z}$ and have absolute values less than $K^{r_1+\dots+r_m}$, where K is a constant depending only on α.

Note that conditions (1) and (3), giving upper bounds, do not depend on the point we are expanding about. They are bounds to the various degrees of ϕ, and we have referred to them in terms of $(\alpha,\dots,\alpha)$ only to get a more compact statement. Condition (2), on the other hand, says that ϕ vanishes to a high (weighted) order at $(\alpha,\dots,\alpha)$.

Behind this lemma is the observation that if we choose m random numbers between 0 and 1, their sum will, on the average, be close to $\frac{1}{2}m$. (In fact, as any statistician can tell us, and as we shall learn in lemma 3.3, p. , it's distance from $\frac{1}{2}m$ will tend to be on the order of $m^{1/2}$.) Hence (2) imposes relatively few conditions compared with the number of variables we have available. It was Schneider who observed that adding condition (3) would also not greatly disturb things, but would cut the contribution of the $q_i^{\sim}$ to the denominator discussed before essentially in half.

Lemma 4 Let m be a positive integer, and ι a positive constant. Then there exist positive constants $C_1 >1$, C_2, and δ with the following properties:

Let $r_1,\dots,r_m$ be positive integers such that $r_i \geq C_1 r_{i+1}$ $(i=1,\dots,m-1)$, and $p_1/q_1,\dots,p_m/q_m$ rational fractions in lowest terms such that $q_1 \geq C_2$, and for all i, $q_i \geq q_1^{r_1/r_i}$. Then there exists no nonzero polynomial $\phi(x_1,\dots,x_m)$ such that:

a) If ϕ is expanded about $(p_1/q_1,\dots,p_m/q_m)$, all terms $(x_1-p_1/q_1)^{t_1}\dots(x_m-p_m/q_m)^{t_m}$ with nonzero coefficients have: $t_i/r_i \leq 1$ (1)

$$\iota < \sum t_i/r_i \qquad (4)$$

b) If ϕ is expanded about 0, the coefficients lie in $\mathbb{Z}$ and are less than or equal to $q_1^{\delta r_1}$.

§4 Proof of the Theorem

Step 1 Reduction to the case where the approximating fractions are in lowest terms, the $q_i^{\sim}$ are of the form $b^{\lambda i}$, and the ratios $\log q_i^{\sim} / \log q_i$ and $\log q_i' / \log q_i$ approach constant values.

The properties of our hypothesis are clearly preserved if we reduce all members of our sequence to lowest terms, and factor our denominators in such a way that the "new" $q_i^{\sim}$ and q_i' respectively divide the "old" factors.

Since $|\varepsilon - p_i/q_i| = oo(q_i^{\sim -1} q_i'^{-2})$ it will also, for sufficiently small ε, be $oo((q_i^{\sim} q_i'^{2})^{-1-\varepsilon})$. Taking such an ε, and assuming the $q_i^{\sim}$ are unbounded, let us apply Lemma 2 to them, getting decompositions $q_i^{\sim} = \bar{q}_i^{\sim} f_i$ where $\bar{q}_i^{\sim}$ is a power of a constant b, for a certain subsequence of the $\bar{q}_i^{\sim}$. Let us also define for the corresponding terms, $\bar{q}_i' = f_i q_i'$, so that $\bar{q}_i^{\sim} \bar{q}_i'$ is just another factorization of q_i. We find that $\bar{q}_i^{\sim} \bar{q}_i'^{2} = q_i^{\sim} f_i q_i'^{2}$, and, using the inequality $f_i \leqslant q_i^{\sim\varepsilon}$, we see that this is $\leqslant (q_i^{\sim} q_i'^{2})^{(1+\varepsilon)}$. It follows that we will have $|\alpha - p_i/q_i| = oo(\bar{q}_i^{\sim -1} \bar{q}_i'^{-2})$. Reindexing our subsequence, and relabeling our $\bar{q}_i^{\sim}$ and $\bar{q}_i'$ as $q_i^{\sim}$ and q_i', we have reduced to the case where the $q_i^{\sim}$ are all powers of a constant b.* If the $q_i^{\sim}$ are bounded, on the other hand, we can take a subsequence on which they have a constant value b.

Finally, let us take a subsequence such that the ratio $\log q_i' / \log q_i$ approaches a limit η. Then $\log q_k^{\sim} / \log q_k$ will approach $1-\eta$.

*This method uses strongly the fact that we are working with a crude type of inequality, our "oo". Actually, lemma 2 is just a convenience, and if we could not afford to introduce factors f_i that are this large, we could be more economical: we would split $q_i^{\sim}$ into prime-power factors $q_i^{(1)}, \ldots, q_i^{(n)}$, and then, in place of the last step on this page, take a subsequence in which $\log q_i^{(1)}, \ldots, \log q_i^{(n)}$ and $\log q_i'$ all approach a constant ratio to $\log q_i$, and then handle each of the $q_i^{(j)}$ in the proof as we here handle $q_i^{\sim}$.

What Lemma 2 does is approximate some cluster point of the ratio of the exponents of the primes in $q_i^{\sim}$ by a rational ratio.

Step 2: We choose a thousand and one items

Assume α is algebraic, of degree s. Let K be the constant of Lemma 3.

Let us choose positive ε, sufficiently small so that $|\alpha - p_i/q_i| < (\tilde{q}_i^{-1} q_i'^{-2})^{\frac{1+16\varepsilon}{1-4\varepsilon}}$ for all but finitely many i. This we can do by our "oo" hypothesis. We can further assume that the given inequality holds for all i, dropping some terms from our sequence if necessary. (We shall not need this unwieldy property of ε till the end of the proof.) Let us also assume $\varepsilon < 1/32$, so that the term $(1+16\varepsilon)/(1-4\varepsilon)$ is $< 1/2$.

Let m be a positive integer such that $2m^{1/2}\varepsilon > 2s+1$ (as in Lemma 3).

Let C_1 and $C_2 \overset{\varepsilon\,\delta}{\wedge}$ be the constants given by Lemma 4, with the above m, and $\iota = \varepsilon m$.

We shall now choose m terms from our series of approximations of α. For convenience of terminology, we shall still call them $p_1/q_1, \dots, p_m/q_m$. We require, first of all, that q_1 be large, namely: $q_1 \geq C_2$, $q_1^{\delta} \geq K^m$, and $q_1^{\varepsilon} \geq 4(1+|\alpha|)K$. Now whatever values we choose for $p_1/q_1, \dots, p_m/q_m$, it is clear that we can choose positive integers $r_1, \dots, r_m$ such that the terms $r_i \log q_i / r_1 \log q_1$ are all greater than 1, but as close to 1 as we wish. Also, if we take our p/q's far enough out in our series, $\log \tilde{q}_i / \log q_i$ and $\log q_i' / \log q_i$ will be as near as we wish to constants, hence with the r_i as above, we will also have $r_i \log \tilde{q}_i / r_1 \log q_1$ and $r_i \log q_i' / r_1 \log q_1$ as near as we wish to constants. In particular, we can assume that they not excede by more than ε, for any i, their value for $i=1$: $(r_i \log \tilde{q}_i - r_1 \log \tilde{q}_1)/r_1 \log q_1 < \varepsilon$, thus $\log \tilde{q}_i - \frac{r_1}{r_i} \log \tilde{q}_1 < \varepsilon \frac{r_1}{r_i} \log q_1$, or, in exponential form:

$$\tilde{q}_i < \tilde{q}_1^{\,r_1/r_i}\, q_1^{\,\varepsilon r_1/r_i} \tag{5}$$

and similarly

$$q_i' < q_1'^{\,r_1/r_i}\, q_1^{\,\varepsilon r_1/r_i} \tag{6}$$

Also recall our original assumption on the r's: $q_i \geq q_1^{r_1/r_i}$. (7)

Finally, since we have chosen the r_i's so that their ratios are very near to the inverse of the ratios of the $\log q_i$'s, it is clear that if we take the q_i's to grow sufficiently rapidly, we can also assume:

$$r_i \geq C_1 r_{i+1} \quad (i=1, \dots, m-1). \tag{8}$$

(From now on it is straight reasoning, with no more details left for the reader to fill in.)

Step 3 Application of Lemmas 3 and 4

By our assumption that α is algebraic of degree s, and our choice of m, we can apply Lemma 3 and get a polynomial $\phi(x_1,\dots,x_m)$ whose terms satisfy (1), (2) and (3) (p.11), and whose coefficients are integers with absolute value less than $K^{r_1+\dots+r_m} \leq K^{mr_1}$. By our choice of q_1, this is $\leq q_1^{\overset{\delta r_1}{\cancel{\varepsilon m}\, r_1}}$. Let us now apply Lemma 4 to this polynomial: we have chosen the r's and q's appropriately, condition (1) holds by lemma 3, and condition (b) holds. ~~because we had set $\delta = \varepsilon m$.~~ Hence (4) must fail: there must be a term $(x_1-p_1/q_1)^{a_1}\dots(x_m-p_m/q_m)^{a_m}$ with nonzero coeffkient such that $\sum a_i/r_i \leq \iota = \varepsilon m$.

Step 4 A new polynomial

$$\text{Let } F(x_1,\dots,x_m) = \frac{1}{a_1!\dots a_m!}\ \frac{\partial^{a_1}}{\partial x_1^{\ a_1}}\dots\frac{\partial^{a_m}}{\partial x_m^{\ a_m}}\ \phi(x_1,\dots,x_m).$$

This polynomial will still have integral coefficients when expanded about 0. Precisely, when the above differential operator is applied to $x_1^{t_1}\dots x_m^{t_m}$, it gives $\binom{t_1}{a_1}\dots\binom{t_m}{a_m}\, x_1^{t_1-a_1}\dots x_m^{t_m-a_m}$. The coefficient in this term is an integer $\leq 2^{t_1}\dots 2^{t_m}$, which in our case makes it $\leq 2^{r_1+\dots+r_m}$; so we can increase our earlier bound on the coefficients of ϕ by this factor to get a bound for those of F.

Now let us consider the magnitudes of the coefficients we get when we expand F about $(\alpha,\dots,\alpha)$. When we expand $x_1^{t_1}\dots x_m^{t_m}$ in powers of $x_1-\alpha,\dots,x_m-\alpha$, the <u>sum</u> of the absolute values of the coefficients is $(1+|\alpha|)^{t_1}\dots(1+|\alpha|)^{t_m} = (1+|\alpha|)^{t_1+\dots+t_m} \leq (1+|\alpha|)^{r_1+\dots+r_m}$. The number of terms in our original polynomial was $\leq (r_1+1)\dots(r_m+m) \leq 2^{r_1}\dots 2^{r_m}$. Combining this with the preceding observations, we see that the sum of the absolute values of the coefficients of F will be at most ~~does not excede the maximum of the coefficients of ϕ by more than a factor~~ ~~of~~ $4^{r_1+\dots+r_m}(1+|\alpha|)^{r_1+\dots+r_m}$ K-times them $<(4(1+|\alpha|)K)^{mr_1}$. By good fortune, we had chosen q_1 so that this will be $\leq q_1^{\varepsilon m r_1}$. ~~This was also our previous estimate on the coefficients of ϕ, so an upper bound on the sum of the coefficients of F, expanded about $(\alpha,\dots,\alpha)$, is $q_1^{2\varepsilon m r_1}$.~~

We also note that the application of our differential operator will not have disturbed conditions (1) and (3) which ϕ satisfied, and cannot have decreased the lower bound (2) by more than $\sum a_i/r_i < \varepsilon m$. So we can conclude: for all terms $(x_1-\alpha)^{t_1}\dots(x_m-\alpha)^{t_m}$ with nonzero coefficient in F, we have

$$t_i/r_i \leq 1 \text{ for all } i, \text{ and } (\tfrac{1}{2}-2\varepsilon) \leq \sum t_i/r_i \leq (\tfrac{1}{2}+\varepsilon)m \qquad (1), (2'), (3).$$

Step 5 The denominator of $F(p_1/q_1,\dots,p_m/q_m)$

We can get an upper bound on the denominator of the nonzero rational number $F(p_1/\tilde{q}_1 q_1',\dots,p_m/\tilde{q}_m q_m')$ by multiplying together the highest powers to which $q_1',\dots,q_m'$ occur, and multiplying this by an upper bound on all products of powers of $\tilde{q}_1,\dots,\tilde{q}_m$ that occur. (Since these are all powers of one integer, least upper bound = least common multiple!)

For the first estimate, we take $\prod q_i'^{r_i}$, and, applying (6), find that it is bounded by $q_1'^{mr_1} q_1^{\varepsilon m r_1}$. For the second, take, over all terms $x_1^{t_1}\dots x_m^{t_m}$ that occur in F, $\sup\prod \tilde{q}_i^{t_i}$. By (6) this is $\leq \sup \prod \tilde{q}_1^{t_i r_1/r_i} q_1^{\varepsilon t_i r_1/r_i}$. In estimating the first term, we recall that $\sum t_i/r_i$ is always $\leq m(\frac{1}{2}+\varepsilon)$. In the second case, we simply use $t_i/r_i \leq 1$. We then get for a bound $\tilde{q}_1^{m(\frac{1}{2}+\varepsilon)r_1} q_1^{\varepsilon m r_1}$.

Bringing these terms together, we see that our denominator will be $\leq q_1'^{mr_1} \tilde{q}_1^{m(\frac{1}{2}+\varepsilon)r_1} q_1^{2\varepsilon m r_1} \leq (\tilde{q}_1 q_1'^2)^{\frac{1}{2}m} q_1^{3\varepsilon r_1}$. [illegible] $\leq (\tilde{q}_1 q_1'^2)^{m(\frac{1}{2}+3\varepsilon)r_1}$.

Step 6 $F(p_1/q_1,\dots,p_m/q_m)$ is too small

Let $(x_1-\alpha)^{t_1}\dots(x_m-\alpha)^{t_m}$ be any term appearing with nonzero coefficient in F, expanded about $(\alpha,\dots,\alpha)$. If we evaluate it at $(p_1/q_1,\dots,p_m/q_m)$, we find

$$|(x_1-\alpha)^{t_1}\dots(x_m-\alpha)^{t_m}|$$

$$\leqslant((q_1^{\sim-1}q_1'^{-2})^{t_1}\dots(q_m^{\sim-1}q_m'^{-2})^{t_m})^{\frac{1+16\varepsilon}{1-4\varepsilon}}$$

by our initial choice of ε!

To estimate this in terms of $q_1^{\sim}$ and q_1', let us square relation (7) (putting $q_i=q_i^{\sim}q_i'$) and divide by (5), getting $q_i^{\sim}q_i'^{2}\geqslant(q_1^{\sim}q_1'^{2})^{r_1/r_i}q_1^{-\varepsilon r_1/r_i}$. Now suppose we substitute this into the above. In the case of the "major" (non-ε) term, we apply the fact that $\sum t_i/r_i$ is at least $m(\frac{1}{2}-2\varepsilon)$, getting a contribution $\lesssim(q_1^{\sim-1}q_1'^{-2})^{m(\frac{1}{2}-2\varepsilon)\frac{1+16\varepsilon}{1-4\varepsilon}r_1}=(q_1^{\sim}q_1'^{2})^{-m(\frac{1}{2}+8\varepsilon)r_1}\leqslant(q_1^{\sim}q_1'^{2})^{-\frac{1}{2}mr_1}q_1^{-8m\varepsilon r_1}$. The "minor" terms we treat much less delicately: we note that raised to the $-t_i$ power, such a term is $\leqslant q_1^{\varepsilon r_1}$, so the total product is $\leqslant q_1^{\varepsilon mr_1}$. The exponent $(1+16\varepsilon)/(1-4\varepsilon)$ is $\leqslant 2$ so this brings it up to no more than $q_1^{2\varepsilon mr_1}$ [illegible]. So our whole term comes to less than or equal to $(q_1^{\sim}q_1'^{2})^{-\frac{1}{2}mr_1}q_1^{-6m\varepsilon r_1}$. Multiplying by the sum of the absolute values of the coefficients of all terms of F, which we had found $\leqslant q_1^{2\varepsilon mr_1}$, we conclude that $|F(p_1/q_1,\dots,p_m/q_m)|\leqslant(q_1^{\sim}q_1^{2})^{-\frac{1}{2}mr_1}q_1^{-4\varepsilon mr_1}$. But this is less than the reciprocal of the bound we obtained for the denominator of this rational number! Contradiction.

So our assumption that α was algebraic is false. |

The reader may prefer the following simplified version of the proof: at the beginning of step 2, we use an exponent $(1+N\varepsilon)/(1-4\varepsilon)$, rather than $(1+16\varepsilon)/(1-4\varepsilon)$, where N is left to be specified. In the course of the proof, we make use of the symbol $A\lesssim B$ to mean $A\leq Bq_1^{n\varepsilon mr_1}$, for some constant n independent of ε, m, etc.. This saves us carrying around all the terms of this sort, and being distracted from the important terms. At the last step, we get $|F|\lesssim|\text{denom. of }F|^{-1}q_1^{N\varepsilon mr_1}$. Thus we know that N can be appropriately selected at the beginning of the proof to get a true inequality here, and a contradiction.

§5 Proof of Lemma 3

The proof is based on a result concerning integral solutions of underdetermined systems of linear equations, of a sort much used in the study of transcendental numbers.

Lemma 3.1 Let $f: \mathbb{R}^N \longrightarrow \mathbb{R}^M$ be a linear function, with $N > M$, given by a matrix whose coefficients have absolute value $\leqslant$ some constant A. Let us norm both $\mathbb{R}^N$ and $\mathbb{R}^M$ by setting $\|(x_i)\| = \sup |x_i|$. Let X be any positive integer. Then there exists nonzero $x \in \mathbb{Z}^N$ with $\|x\| \leqslant X$ such that $\|f(x)\| < NAX^{-\frac{N}{M}+1}$.

Proof Consider points of $\mathbb{R}^N$ having all coordinates in the set $\{-\frac{X}{2}, -\frac{X}{2}+1, \ldots, \frac{X}{2}-1, \frac{X}{2}\}$. There are $(X+1)^N$ of them, and since each satisfies $\|x\| \leqslant X/2$, their images will clearly satisfy $\|f(x)\| \leqslant NAX/2$. If these images are distinct, let ε be the minimal value of $\|f(x)-f(x')\|$ for $x \neq x'$. Let us surround each point $f(x)$ by an open "cube" of radius $\varepsilon/2$ (a "ball" under our metric). These cubes are disjoint by choice of ε, and their union lies within the cube centered at the origin, of radius $(NAX+\varepsilon)/2$. By comparing volumes, we see that:

$$(NAX+\varepsilon)^M \geqslant \varepsilon^M (X+1)^N$$

$$NAX+\varepsilon \geqslant \varepsilon(X+1)^{N/M} > \varepsilon X^{N/M} + \varepsilon \quad \text{(because } N/M > 1\text{)}$$

$$NAX^{-\frac{N}{M}+1} > \varepsilon \,.$$

But recalling that $\varepsilon = \|f(x)-f(x')\| = \|f(x-x')\|$, and noting that $x-x'$ will have integral coordinates, we see that we have obtained the desired result. |

Now let K be a finite algebraic extension of the rationals of degree s. We shall not, for the moment, consider K as a subfield of the complexes, but shall embed it in $\mathbb{R}^s$ as follows: K has s field homomorphisms into the complex numbers. If t of these, $\varphi_1, \ldots, \varphi_t$, have images in $\mathbb{R}$, then let the first n components of our embedding be given by these maps. The remaining homomorphisms will fall into complex conjugate pairs: $\varphi_{t+1}, \varphi_{t+2} = \overline{\varphi_{t+1}}, \ldots, \varphi_{s-1}, \varphi_s = \overline{\varphi_{s-1}}$.

Let us identify the last s-t coordinates of $\mathbb{R}^n$ with $\mathbb{C}^{(s-t)/2}$, and let us map K to these coordinates by $\sqrt{2}\,\varphi_{t+1}, \sqrt{2}\,\varphi_{t+3}, \ldots, \sqrt{2}\,\varphi_{s-1}$.

If we norm $\mathbb{R}^s$ as above, then the induced norm on K relates to the more commonly used function $|\overline{x}| = \sup |\varphi_i(x)|$ by the inequalities $|\overline{x}| \leq \|x\| \leq \sqrt{2}|\overline{x}|$. (Because for any complex number α, $|\alpha| \leq \|\sqrt{2}\alpha\| \leq \sqrt{2}|\alpha|$.) In particular, for α a nonzero integer of K, $\|\alpha\| \geq |\overline{\alpha}| \geq 1$. Note, similarly: $\|\alpha\beta\| \leq \|\alpha\|\ \|\beta\|$.

<u>Lemma 3.2</u> A system of M linear equations in N unknowns:

$$0 = \sum_{j=1}^{N} a_{ij}x_j \quad (i=1,\ldots,M)$$

where the a_{ij} are integers of a field K of degree s over the rationals, with $\|a_{ij}\| \leq A$, and where $N > Ms$, has a nonzero solution $x \in \mathbb{Z}^N$ with $\|x\| \leq (NA)^{Ms/(N-Ms)}$.

<u>Proof</u> The a_{ij} define a map of $\mathbb{R}^N$ into K^M, which we have embedded in $\mathbb{R}^{Ms}$. Clearly A bounds the absolute values of the coefficients. If we set $X = (NA)^{Ms/(N-Ms)} = (NA)^{1/(\frac{N}{Ms}-1)}$, Lemma 3.1 says that for some nonzero $x \in \mathbb{Z}^N$, with $\|x\| \leq X$, $\|f(x)\| < 1$. Since $f(x)$ is an integer of K, it must be 0.| ~~integer of K, must, must be 0.~~

In order to apply this to the coefficients of the polynomial we wish to construct, we need an estimate of the number of terms satisfying conditions (1) and (3), and the number satisfying (1) and (2)-with-inequality reversed. Geometrically, we can see by symmetry that one number can be gotten from the other by subtracting from the total number of lattice points satisfying (1). The problem is essentially that of estimating the volume of the part of the unit n-cube cut off by the hyperplane $\sum x_i = c$. ~~This is not easy. The following substitute,~~

<u>Lemma 3.3</u> Let m and $r_1, \ldots, r_m$ be positive integers, and ε a positive number. Then the number of m-tuples of integers $(t_1, \ldots, t_m)$ satisfying: ~~it goes back to Davenport:~~

$$0 \leq t_i/r_i \leq 1 \quad (i=1,\ldots,m) \tag{1}$$

$$\text{and} \quad \sum t_i/r_i \leq m(\tfrac{1}{2} - \varepsilon) \tag{-2}$$

is less than ~~or equal to~~ $\frac{1}{2}m^{-1/2}\,\varepsilon^{-1}(r_1+1)\ldots(r_m+1)$.

Proof* Let us change variables for more convenient computation: Let $s_i = t_i/r_i - 1/2$. Thus (1) allows s_i to go from $-1/2$ to $+1/2$ by jumps of $1/r_i$, a behavior we shall abbreviate $s_i = -\frac{1}{2}(\frac{1}{r_i})\frac{1}{2}$. Let $\eta = m\varepsilon$. Then (-2) becomes:

$$\sum^{m} s_i < -\eta \qquad (-2')$$

and we wish to show the number of points with this property $\leq \frac{1}{2}m^{\frac{1}{2}}\eta^{-1}(r_1+1)\ldots(r_m+1)$.

By (-2′), at least half the $(r_1+1)\ldots(r_m+1)$ possible points are excluded, so the result will clearly be true whenever $\eta < m^{1/2}$. In the case m=1 this proves our result (and, in fact, for m=2,3,4 as well — for by (-2′), the result is also vacuous for $\eta > m/2$.) So we can assume $\eta \geq m^{1/2}$, and work by induction from m=1.

For each value of $s_m = -\frac{1}{2}(\frac{1}{r_m})\frac{1}{2}$, the number of values of $s_1, \ldots, s_{m-1}$ satisfying (-2′) with the given s_m will, by inductive hypothesis, be $< \frac{1}{2}(m-1)^{\frac{1}{2}}(\eta+s_m)^{-1}(r_1+1)\ldots(r_{m-1}+1)$. (Note that $\eta + s_m > 0$ because $\eta \geq m^{1/2} > 1$.) Hence summing over s_m, the total number of solutions of (-2′) is less than:

$$\frac{1}{2}(m-1)^{1/2}(r_1+1)\ldots(r_{m-1}+1)\sum_{s=-\frac{1}{2}(\frac{1}{r_m})\frac{1}{2}}(\eta+s)^{-1}.$$

To evaluate the sum on the right, we note that by symmetry it equals

$$\frac{1}{2}\sum_{s}(\eta+s)^{-1}+(\eta-s)^{-1} = \frac{1}{2}\sum_{s} 2\eta(\eta^2-s^2)^{-1} = \eta^{-1}\sum_{s}(1-\frac{s^2}{\eta^2})^{-1} \leq \eta^{-1}(r_m+1)(1-\frac{1}{4\eta^2})^{-1}.$$

Now since $\eta \geq m^{1/2}$, we have $(1-\frac{1}{4\eta^2} \geq 1-\frac{1}{4}m^{-1} \geq (1-m^{-1})^{1/2} = (m-1)^{1/2}/m^{1/2}$.

Substituting this into the above, and that into the preceding formula, we get

*Let us compare this result with a rough qualitative analysis of the situation. Take $r_1 = \ldots = r_m = 1$; then we are looking for the number of vertices of our unit cube whose coordinates sum to less than some constant x. The number whose coordinates sum to exactly n is $\binom{m}{n}$. This gives a Gaussian bell. Ignoring the factor $2^m = (r_1+1)\ldots(r_m+1)$, it is given, approximately, by $m^{-\frac{1}{2}}e^{-(x-m/2)^2/m}$. Now Lemma 3.3 appears to correspond to the result of estimating this by the very crude bound $m^{-1/2}/[(x-m/2)^2/m] = m^{1/2}/(x-m/2)^2$. Integrating from $-\infty$ to $m(1/2-\varepsilon)$ gives $m^{-1/2}\varepsilon^{-1}$, which is essentially our formula.

Schneider says that Roth says that the proof of Lemma 3.3 given in the text goes back to Davenport. I have improved his result by a factor of 2. The estimate can, in fact, be further divided by $\sqrt{2}$ without changing the proof: The range of η for which the result is "clear" then becomes $\eta \leq 1/(2\sqrt{2})m^{1/2}$, and at the end of the proof we estimate $1-1/4\eta^2$ by $1-(1/2)m^{-1} > (1-m^{-1})-1/2$.

the bound $(1/2)(m-1)^{1/2}(r_1+1)\dots(r_{m-1}+1)\eta^{-1}(r_m+1)m^{1/2}/(m-1)^{1/2}$, which reduces to $(1/2)m^{1/2}\eta^{-1}(r_1+1)\dots(r_m+1)$. |

We can now prove Lemma 3. Let us first assume α an algebraic integer. Put $K=\mathbb{Q}(\alpha)$.

If we let N be the number of m-tuples $t_1,\dots,t_m$ satisfying (1) and (3), and M the number satisfying (1) and not (2), then we wish to choose N integers, not all zero, to be the coefficients of ϕ expanded about zero, such that the M numbers which are the coefficients, in the expansion about $(\alpha,\dots,\alpha)$, of terms not satisfying (2) are all 0.

When we go from the expansion about 0 to the expansion about $(\alpha,\dots,\alpha)$, the coefficient of $x_1^{t_1}\dots x_m^{t_m}$ appears in that of $(x_1-\alpha)^{t_1'}\dots(x_m-\alpha)^{t_m'}$ with cofactor $\binom{t_1}{t_1'}\dots\binom{t_m}{t_m'}\alpha^{(t_1-t_1')+\dots+(t_m-t_m')}$. If we call this term a, we see that $\|a\|\leqslant 2^{t_1}\dots 2^{t_m}\|\alpha\|^{t_1-t_1'+\dots+t_m-t_m'}\leqslant\|2\alpha\|^{r_1+\dots+r_m}$.

Now by Lemma 3.3, $M<\frac{1}{2}m^{-1/2}\varepsilon^{-1}(r_1+1)\dots(r_m+1)$, and $N>(1-\frac{1}{2}m^{-1/2}\varepsilon^{-1})(r_1+1)\dots(r_m+1)$. Putting $(r_1+1)\dots(r_m+1)=C$, and applying the hypothesis $2m^{1/2}\varepsilon>2s+1$ of Lemma 3, we get $M<C/(2s+1)$, $N>C\cdot 2s/(2s+1)$. So $N>2Ms$, ~~and~~ so $Ms/(N-Ms)<1$.

Applying Lemma 3.3, we see we can get a solution x with $\|x\|<(N\|2a\|^{r_1+\dots+r_m})^1$. Noting that by definition, $N<(r_1+1)\dots(r_m+1)\leqslant 2^{r_1}\dots 2^{r_m}$, we can rewrite this bound as $\|4\alpha\|^{r_1+\dots+r_m}$.

Finally, suppose α is of the form β/n, α an algebraic integer, $n\in\mathbb{Z}$. By the above, we can construct a polynomial ψ satisfying all our conditions with respect to expansion about $(\beta,\dots,\beta)$. Then $\phi=\psi(nx_1,\dots,nx_m)$ satisfies the same conditions at α, and its coefficients are $\leqslant|n|^{r_1+\dots+r_m}$ times those of ψ, hence are bounded by $\|4n\beta\|^{r_1+\dots+r_m}$. |

Incidentally, the reader can easily check that the Lemma also holds with (3) replaced by $\sum t_i/r_i<1/2$ if we merely strengthen the assumption $2m^{1/2}\varepsilon>2s+1$ to $m^{1/2}\varepsilon>2s$. (As a lower bound for N, we use $\frac{1}{2}(r_1+1)\dots(r_m+m)$, while we keep the same upper bound for M.)

§6 Proof of Lemma 4

We stated the Lemma in the operative form we needed for our Theorem. What we shall prove is a more explicit result, a simplified version of Schneider's Hilfsatz 9:

Lemma 4' Let m be a positive integer, and δ a constant with $0 < m\delta < 1$. Let $r_1, \ldots, r_m$ be positive integers such that:

$$\delta r_i \geq r_{i+1} \quad (i=1,\ldots,m-1). \tag{9}$$

Let $p_1/q_1, \ldots, p_m/q_m$ be rational fractions in lowest terms such that:

for all i:

$$q_1^{\delta} \geq 2^{2m^2} \tag{10}$$

$$q_i \geq q_1^{r_i/r_1}. \tag{11}$$

Then there exists no nonzero polynomial $\phi(x_1,\ldots,x_m)$ in m indeterminates such that:

a) If ϕ is expanded about $(p_1/q_1,\ldots,p_m/q_m)$, all terms $(x_1-p_1/q_1)^{t_1}\ldots(x_m-p_m/q_m)^{t_m}$ with nonzero coefficients have: $t_i/r_i \leq 1$ (1)

$$6^m \delta 2^{-m} < \sum t_i/r_i \tag{12}$$

b) If ϕ is expanded about 0, the coefficients lie in $\mathbb{Z}$ and are less than or equal to $q_1^{\delta r_1}$.

Indeed,

Indeed, to prove the original Lemma 4 from this, given m and ε ~~and~~, we choose δ ~~δ~~, sufficiently small so that $6^m \delta 2^{-m} < \varepsilon$., We then take $C_1 = \delta^{-1}$, ~~and~~ $C_2 = 2^{2m^2}\delta^{-1}$. We then clearly get the result originally stated.

Proof of Lemma 4

The situation for polynomials in one indeterminate is quite simple:

Lemma 4.1 If $\phi(x)$ is a nonzero polynomial in one indeterminate, with integral coefficients, which has a zero of order n at a point p/q, p and q relatively prime integers, then the maximum of the absolute values of the coefficients of ϕ is $\geq q^n$.

Proof ϕ must be divisible by $(qx-p)^n$, hence the leading coefficient of ϕ is divisible by q^n.|

Note that we have not had to assume q large, or put any upper bound on the degree of ϕ. In the situation of Lemma 4′ with m=1, without assuming (10) or (1) ((9) and (11) are vacuous for m=1), and weakening the lower bound in (12) to δ, we see that (12) says ϕ has a zero of order $> r_1\delta$ at p/q, whence condition (b) is impossible, and the Lemma holds.

For m>1, bounds on the degree of ϕ are necessary, for polynomials such as $x_1^a - x_2^b$ can have zeroes of high order at points $(p_1/q_1, p_2/q_2)$ with large denominators, without having large coefficients. The proof of the general case is by induction. Though ingenious, it is far from straightforward, and uses some very crude estimations. Perhaps a sharper result and a simpler proof will eventually be found.

One of the tools we shall need is a result on determinants in functions of several variables analogous to the Wronskian determinant:

Let A be the ring of analytic functions on a connected open subset of $\mathbb{C}^n$, and S the set of operators of the form $\frac{\partial^{a_1}}{\partial x_1^{a_1}} \cdots \frac{\partial^{a_n}}{\partial x_n^{a_n}}$ on A. The number $a_1 + \ldots + a_n$ will be called the degree of such an operator:

Lemma 4.2 Let $F_0, \ldots, F_h \in A$ be linearly independent over $\mathbb{C}$. Then there exist $D_0, \ldots, D_h$ in S such that $\det((D_iF_j))$ is not identically 0. These can be chosen such that each D_i is of degree $\leq i$. (The identity operator thus being chosen for D_0).

Proof Clearly, $\det((D_iF_j))$ will be equal to $\det((D_iF_j'))$ if each F_j' is of the form $F_j + \sum_{i<j} c_{ij}F_i$ $(c_{ij} \in \mathbb{C})$. Hence in the course of the proof we may modify any F by a linear combination of the preceding F's.

Let p be any point of our domain. By analyticity, there will exist $D_0 \in S$ such that $D_0F_0(p) \neq 0$. (We put no condition on its degree so far ~~at this point~~.) Now modifying $F_1, \ldots, F_h$ by appropriate multiples of F_0, we can assume $D_0F_1(p) = \ldots = D_0F_h(p) = 0$. The modified F's will still be linearly independent, hence nonzero, hence there will exist $D_1 \in S$ such $D_1F_1(p) \neq 0$. Again, modifying $F_1, \ldots, F_h$ by multiples of F_1 — which will not disturb out previous assumptions about the D_0F_i — we can assume $D_1F_2(p) = \ldots = D_1F_h(p) = 0$. Continuing this process, we get $D_0, \ldots, D_h$ such that, clearly, the function $\det((D_iF_j))$ is nonzero at p.

This shows that the set $SF \subset A^{h+1}$ of vectors $DF = (DF_0, \ldots, DF_h)$ $(D \in S)$ contains a set of h+1 members linearly independent over A.

Now let us pick a new family $D_0, \ldots, D_h$ as follows: Taking d=0,1,..., choose successively as many operators D of each degree d as is possible such that each DF is A-linearly independent of those chosen before (in the same or lower degrees); continuing until we have found h+1 such operators, as we know we can (by uniqueness of basis number of a vector space over A's field of fractions.) Now we claim that until we have obtained our h+1 operators, we will get at least one in every degree. For if all DF with D of degree d, were A-linearly dependent on terms D'F with D' of degree $\leq$ d-1, then, applying to our relation of linear dependence an arbitrary operator E of degree 1, we get a relation of dependence of (ED)F on the elements ED'F, D'F, DF, of degrees $\leq$ d, hence EDF will in fact be dependent on elements of degree $\leq$ d-1. ED is a typical element of S of degree d+1; continuing this process inductively, we see that all elements DF for D of degree $\geq d$ will be linearly dependent on terms with D of degree $<d$. But we know this is impossible if we have not already found our desired h operators in degrees $\leq d$.

Clearly, $D_1, \ldots, D_h$ chosen as above will satisfy our conclusion.|

(This result can be obtained in a more general algebraic context: for the first statement, we take an algebra A without zero-divisors over a field K, with an augmentation $\varepsilon : A \to K$ (corresponding to evaluation at p), and a family S of K-vector-space homomorphisms: $A \to A$ such that $\forall X \in A - \{0\} \; \exists D \in S, \varepsilon(D(X)) \neq 0$. If A is not commutative, we cannot use determinants, and must speak in terms of right linear independence; additional hypotheses are then needed to deduce that linear independence of $\varepsilon(D_1 F), \ldots, \varepsilon(D_h F)$ implies independence of $D_1 F, \ldots, D_h F$.

For the second statement, we need S to be a semigroup under composition, with a generating set S_1, and "degree" defined in terms of minimum number of factors in S_1 needed to represent D. We must also assume S_0 consists of derivations, or at least that its members satisfy some identities that will allow us to go from a dependence relation for DF to one for EDF. However, they need not be commuting derivations, a fact of significance for applications to analytic functions as well.)

Now let m be a positive integer, and S the set of operators of the form $D = \frac{1}{a_1! \ldots a_{m-1}!} \frac{\partial^{a_1}}{\partial x_1^{a_1}} \cdots \frac{\partial^{a_{m-1}}}{\partial x_{m-1}^{a_{m-1}}}$, and C_k $(k=0,1,\ldots)$ the operator $\frac{1}{k!} \frac{\partial^k}{\partial x_m^k}$. All of these send the ring of polynomials in n indeterminates with integral coefficients into itself. The statement of Lemma 4.2 clearly applies to the S just defined, for functions of $x_1, \ldots, x_{m-1}$, since its members differ only by nonzero constant factors from those of the old S. The advantage of this function is, of course, that it is more "conservative" with respect to magnitudes of coefficients.

The following lemma will allow us to make the inductive reduction in the proof of Lemma 4:

Lemma 4.3 Let ϕ be a polynomial in $x_1,\dots,x_m$ with real coefficients, of degree r_m in x_m. Then there exists $h \leq r_m$, and $D_0,\dots,D_h$ in S, with D_i of degree degree $\leq i$, such that $\det((D_i C_k(\phi)))$ $(i,k=0,\dots,h)$ is a nonzero polynomial which can be factored $U(x_1,\dots,x_{m-1})V(x_m)$.

Proof We can decompose the polynomial ϕ as $\sum_0^h P_j(x_1,\dots,x_{m-1})Q_j(x_m)$, where the P's and Q's are polynomials with rational coefficients, and $h \leq r_m$; for instance, by using $Q_j = x^j$. Let us take the decomposition $\sum^h P_j Q_j$ which minimizes h. Then the h+1 polynomials P_j must be linearly independent (over the rationals), for otherwise one, say P_h, could be written as a linear combination of the rest, and we could easily reduce our sum to one using $P_0,\dots,P_{h-1}$. Similarly, the Q_j are independent.

Now let $U(x_1,\dots,x_{m-1}) = \det ((D_i P_j))$, where the $D_i \in S$ are chosen, respectively of degree $\leq i$, so that this determinant is nonzero. By the 1-variable Wronskian result, (contained in our result), we also know that $V(x_m) = \det ((C_k Q_j))$ is nonzero.

Hence $0 \neq UV = \det ((D_i P_j))((C_k Q_j)) = \det ((\sum_{j=0}^h (D_i P_j)(C_k Q_j))) = \det ((D_i C_k \sum P_j Q_j))$ $= \det ((D_i C_k \Phi))$.|

(The general algebraic version of this lemma would concern a tensor product $A \otimes_k A'$ of commutative algebras over a field k, with respective sets, S and S', of k-linear maps satisfying the conclusion of the preceding lemma. In place of the degree of ϕ in x_m, we would in general use the "rank" of ϕ in $A \otimes A'$, that is, the minimal number of terms $P \otimes Q$ needed to represent it. In some cases we could, as above, get a bound based on a "degree" function on A or A'.)

We our now ready to prove the general case of Lemma 4'. Let m>1, and $r_1,\dots,r_m$, $p_1/q_1,\dots,p_m/q_m$, $\phi(x_1,\dots,x_m)$ satisfy all the conditions of the lemma perhaps except (12). Let us designate by θ the infimum, over all nonzero terms $(x_1-p_1/q_1)^{t_1}\dots(x_m-p_m/q_m)^{t_m}$ appearing with nonzero coefficient in Φ, of $\sum t_i/r_i$.

This will be called the index of ϕ with respect to $r_1,\dots,r_m$ at $(p_1/q_1,\dots,p_m/q_m)$. We must prove $\theta \leq 6^m \delta^{2-m}(r_1,\dots,p_m/q_m)$ with respect to $r_1,\dots,r_m$. It is clear that for any point of C^m and any positive constants $r_1,\dots,r_m$, the index at that point with respect to $r_1,\dots,r_m$ constitutes a nonnegative-real-valued valuation of the ring of polynomials in m indeterminates $x_1,\dots,x_m$.

We shall inductively assume Lemma 4′ to hold for m-1.

For our given polynomial ϕ, let us obtain h, $D_0,\dots,D_h$, U, V as in the preceding lemma. U and V can be taken to have integral coefficients because UV does, by its determinant representation. * Now, to work:

Step 1 Estimation of the coefficients of UV, and, by our inductive hypothesis, of the indices of U/q_1, V at $(p_1/q_1,\dots,p_{m-1}/q_{m-1})$ and (p_m/q_m).

When an operator $D_iC_k = \frac{1}{a_1!\dots a_{m-1}!k!}\frac{\partial^{a_1}}{\partial x_1^{a_1}}\dots\frac{\partial^{a_{m-1}}}{\partial x_{m-1}^{a_{m-1}}}\frac{\partial^k}{\partial x_m^k}$ is applied to a term $x_1^{b_1}\dots x_m^{b_m}$, we get $\binom{b_1}{a_1}\dots\binom{b_m}{k}x^{b_1-a_1}\dots x^{b_m-k}$, which is zero if any $a_i>b_i$, but which, in any case, has coefficient $\leq 2^{b_1}\dots 2^{b_m}$. Hence in applying such operators to P, we do not increase the maximum of the coefficients of the terms by more than $2^{r_1+\dots+r_m} \leq 2^{mr_1}$; so for D_iC_kP, this maximum will be $\leq 2^{mr_1}q_1^{\delta r_1}$, and the sum of the absolute values of the coefficients will be $\leq (r_1+1)\dots(r_m+1)2^{mr_1}q_1^{\delta r_1} \leq (r_1+1)^m 2^{mr_1}q_1^{r_1} \leq (2^{r_1})^m 2^{mr_1}q_1^{r_1} \leq (2^{2m}q_1^{\delta})^{r_1}$. (Hence in each of the (h+1)! terms of our expanded determinant, the sum of the absolute values of the coefficients, and thus the maximum of these values will be $\leq (2^{2m}q_1^{\delta})^{r_1(h+1)}$. Multiplying by the number of terms, $(h+1)! \leq (h+1)^{h+1} \leq 2^{r_1(h+1)}$, we see that the maximum of the absolute values of the coefficients of UV, and hence of each of U and V, is $\leq (2^{2m+1}q_1^{\delta})^{r_1(h+1)}$.

Step 2 Estimation of the indices of U and V, by inductive hypothesis.

Now let us define $r_1',\dots,r_{m-1}'$ by $r_i' = (h+1)r_i$, and $\delta' = \frac{m}{m-1}\delta \leq (1+\frac{1}{m})\delta$. We shall apply Lemma 4′ for m-1 to U, using these r′'s and δ',

*In fact, the P's and Q's of the proof of Lemma 4.3 can be chosen to have integral coefficients if ϕ does, though the proof as given does not show this. The fact which must be used is that if $P_0,\dots,P_h$ are a linearly dependent family of polynomials over the integers, there exists an invertible matrix α over the integers such that $(P_0,\dots,P_h)\alpha$ has last component 0. See my major thesis, Theorem 1. Then we can write $\phi = (P)\alpha\cdot\alpha^{-1}(Q)$, which is effectively an h-term representation.

at the point $(p_1/q_1,\dots,p_{m-1}/q_{m-1})$.

All the conditions of the lemma through (11) clearly hold. We see from the determinant expression that U will have degree $\leq (h+1)r_i$ in each x_i, so (1) is satisfied. To prove condition (b) from our above estimate of the coefficients of U, we need to show $(2^{2m+1}q_1^{\delta})^{r_1(h+1)} \leq q_1^{\delta' r_1'}$. Removing the common exponent $r_1' = r_1(h+1)$, and raising to the $m-1$st power, this becomes $2^{(2m+1)(m-1)}q_1^{\delta(m-1)} \leq q_1^{\delta m}$, or $q_1^{\delta} \geq 2^{(2m+1)(m-1)}$, which follows from hypothesis (10)!

Hence looking at condition (12), we conclude that the index of U at our point with respect to $r_1',\dots,r_{m-1}'$ will be $\leq 6^{m-1}\delta'^{2^{-m+1}}$: This means that the index with respect to $r_1,\dots,r_{m-1}$ will be $\leq (h+1)6^{m-1}\delta'^{2^{-m+1}} \leq (h+1)2\cdot 6^{m-1}\delta^{2^{-m+1}}$.

To deal with V, let us use lemma 4.1. Since V's coefficients do not excede $q_1^{\delta' r_1'} \leq q_1^{2\delta r_1(h+1)} \leq q_m^{2\delta r_m(h+1)}$ (using (11)), it cannot have at p_m/q_m a zero of order more than $2\delta r_m(h+1)$. Hence its index with respect to r_m is $\leq 2\delta(h+1)$. So the index of UV is $\leq (h+1)(2\cdot 6^{m-1}\delta^{2^{-m+1}}+2\delta)$.

Step 3 Relation between index of UV and θ=index of ϕ.

TAn operator $\frac{\partial}{\partial x_i}$ will decrease the index of a polynomial by at most $1/r_i$. (It may decrease it by less than this, or even increase it, if some terms go to zero.) In particular, it will decrease it by at most $1/r_{m-1}$ if $i<m$, and hence the operators D_i of our determinant will decrease it by at most $i/r_{m-1} \leq h/r_{m-1} \leq r_m/r_{m-1} \leq \delta$. (Hypothesis (9)). Hence the index of $D_iC_k\phi$ will be at least $\theta - k/r_m - \delta$. The index of any of the $(h+1)!$ terms in our determinant expression for UV will thus be at least $\sum_{k=0}^{h} \theta - k/r_m - \delta$. But we also know that no term $D_iC_k\phi$ can have index less than 0; hence we can improve the above estimate to $\sum_{k=0}^{h}{}_{+}(\theta-k/r_m-\delta)$, where $\sum_+$ means that the sum is taken over those terms which are nonnegative. This, in turn, is $\geq \sum_+(\theta-k/r_m)-(h+1)\delta$.

Step 4 The resulting bound on θ.

Comparing the two above results on the index of UV, we see that $\sum_{0}^{h}{}_{+}(\theta-k/r_m) - (h+1)\delta \leq (h+1)(2\cdot 6^{m-1}\delta^{2^{-m+1}} + 2\delta)$. Hence $\sum_{+}\theta-k/r_m \leq (h+1)(2\cdot 6^{m-1}\delta^{2^{-m+1}} + 3\delta) \leq (h+1)\cdot 3\cdot 6^{m-1}\delta^{2^{-m+1}}$. (Clearly $3\delta \leq 6^{m-1}\delta^{2^{-m+1}}$.)

To evaluate θ from this, we must distinguish between the case where our summation $\sum^{h}_{+}$ actually goes from 0 to h and the case where it has a smaller range:

Case 1 $\theta \geq h/r_m$.

Then our $\sum_{+}$ is the sum of an arithmetic progression of h+1 terms. The average value of the terms is $\geq \frac{1}{2}\theta$, hence the sum is $\geq \frac{1}{2}\theta(h+1)$, so

$$\frac{1}{2}\theta(h+1) \leq (h+1)\cdot 3\cdot 6^{m-1}\delta^{2^{-m+1}}$$

$$\theta \leq 6\cdot 6^{m-1}\delta^{2^{-m+1}} < 6^m\delta^{2^{-m}}. \quad \text{QED}$$

Case 2 $\theta \leq h/r_m$.

Then the sum will run from 0 to the greatest integer contained in θr_m, which is $> \theta r_m - 1$. Hence the number of terms will be $> \theta r_m$, and the sum will be $> \frac{1}{2}\theta\cdot\theta r_m \geq \frac{1}{2}\theta^2 h \geq \frac{1}{4}\theta^2(h+1)$.

$$\frac{1}{4}\theta^2(h+1) \leq (h+1)\cdot 3\cdot 6^{m-1}\delta^{2^{-m+1}}$$

$$\theta \leq \surd(12\cdot 6^{m-1})\surd(\delta^{2^{-m+1}})$$

$$\leq 6^m\delta^{2^{-m}}. \quad \text{QED}$$

(Note on the base "6" occurring in condition (12): in the proof of our theorem, we could use Lemma 4 with any constant in place of 6. We chose 6 as the least value we could get without doing any "arithmetic". It could easily be replaced by 4 if in evaluating the coefficients of U, we bounded $\delta\cdot 2^{-m+1}$ by $\sqrt{2}\cdot\delta^{2^{-m+1}}$ rather than $2\delta^{2^{-m+1}}$, and were similarly careful in our treatment of 3δ at the top of this page. By using different arguments for small and large m, we can probably replace 6^m by a function increasing not much faster than 2^m. The "2" comes from case 1 on this page. Also, in condition (3), δ can be replaced by $\delta^{2^{-i}}$, or even $\inf(1,6^i\delta^{2^{-i}})$) cf. step 3, and the later fate of the δ which there arises.)

§7 Further observations and generalizations

LeVeque |2| generalizes Roth's result to deal with approximation by algebraic numbers in a fixed number field. In place of the magnitude of the denominator, he uses the "height" function: $H(\xi)$ = maximum absolute value of coefficients of minimal polynomial of ξ over $\mathbb{Z}$, and shows that no algebraic number can be approached by a (not eventually constant) sequence $\xi_1, \ldots$ of elements of a fixed finite extension of $\mathbb{Q}$, such that $|\alpha - \xi_i| = oo(H(\xi_i)^{-2})$. Though I have not gone through his proof in full detail, it may be possible to generalize it by Schneider's technique to give the result: if α can be approached by a sequence $\tilde\xi_1\xi_1', \tilde\xi_2\xi_2', \ldots$ of elements of a fixed extension K of $\mathbb{Q}$, where the $\tilde\xi_i$ belong to a fixed finitely generated multiplicative semigroup in K, such that $|\alpha - \tilde\xi_i\xi_i'| = oo(H(\tilde\xi_i)^{-1}H(\xi_i')^{-2})$ then α is transc. The one difficulty may lie in getting an analog to the "reduction to lowest terms" step. This was needed because the hypothesis of Lemma 4 uses lowest-terms denominators. The analogous result we need here appears to be that we can get $H(\xi_i)$ reasonably close to $H(\tilde\xi_i)H(\xi_i')$.

An important class of applications of the Thue-Siegel-Roth theorem is to Diophantine equations. The following result is essentially Theorem 4-18 of |2|, taken in the case where number field K in question is the rationals:

Theorem Let $P(x,y)$ be a polynomial in two indeterminates with integral coefficients, of degree n, such that the "leading form" $U(x,y)$ (homogeneous of degree n) has no multiple factors, and such that P has no terms of degree n-1 or n-2; i.e., $V(x,y) = P(x,y)-U(x,y)$ had degree n-3 or less. Suppose, finally, that P has no homogeneous factors; i.e., that U and V are relatively prime. Then $P(x,y)=0$ has only finitely many integer-valued solutions.

Idea of Proof Suppose we had infinitely many solutions (p_i,q_i) with, say, $q_i>|p_i|$. Now $U(p_i,q_i) = O(q_i^{n-3})$, hence, $V(p_i,q_i)=-U(p_i,q_i)= O(q_i^{n-3})$, hence by homogeneity, $V(p_i/q_i,1) = O(q_i^{-3})$. Take a subsequence of p_i/q_i which converges. Clearly, it must converge to a root of $V(x,1)$, and from the fact that V has no multiple roots, we can deduce that it $O(q^{-3})$-approximates this root. Contradiction.|

One may take as the basic principal in the constructive study of transcendental numbers that any algebraic number, with respect to an arithmetic property, will either behave very specially (e.g., the decimal expansion and approximation properties of a rational number, the continued fraction expansion of a quadratic irrationality), if this is implied by its algebraic equation, or else behave like a typical random number (e.g.g.: apparently, the decimal expansion of an algebraic number of degree >1, and the continued fraction expansion of a number of degree >2.) So far, the only type of arithmetic properties for which we seem to be able to prove such results are approximation-properties. We make a crude estimate of how closely a certain type of expression can approximate an arbitrary number, and prove that any number which can be better approximated must be transcendental. For example: How closely can a number be approximated by an n-place decimal? To within 10^{-n}, certainly. How much better will a random number be approximable, for optimum choice of large n? In other words, (limiting ourselves to approximations from below, for simplicity), what length strings of 0's are liable to occur in a random sequence of 0's, 1's,..., and 9's? In the first N digits, we can expect the longest such sequence to have length about $\log_{10}N$ (for N large). Hence we can expect to find arbitrarily large n such that the n-place expansion of our number is actually its $n+\log_{10}n$-place expansion (more or less), i.e., appraximates it to within $n^{-1}10^{-n}$, and not much better. In other words, a random number is more or less $(q \log_{10}q)^{-1}$ approximable by a decimal fraction, and (once we get this formula exact) we should expect that any better-approximable number is either rational or transcendental. The $oo(q^{-1})$-result given by the Theorem proved above is a weak version of this.

Another natural sort of conjecture is that in the decimal expansion of an irrational algebraic number, each digit should appear with limiting frequency 1/10. This is easily seen to be a property of all real numbers except for a set of measure 0. Similar considerations should be applicable to the continued fraction expansions of algebraic numbers of degree >2. It appears that the integer n should appear in the continued fraction expansion of a random number (any number not in a set of measure 0) with frequency something like $1/n^2$. But the terms in the expansion of e-1 are 1,1,2,1,1,4,1,1,6,1,1,... (see Lang, Intro. to Diophantine Approximations). Thus a result to the effect that algebraic numbers have either terminating, periodic, or "statistical" partial fraction expansions would give a new proof of the transcendence of e.

I am told that someone in the Department of Applied Mathematics here is working on proving that no irrational algebraic number has binary expansion that is is "real-time computable"; that is, that there is no algorithm that will allow one to compute the first n digits in time O(n). Such a statement depends on the type of computing machine one allows. So far, he has proved it only for a very special type of machine, but his results include the transcendence of $\sum 1/2^{2^n}$.

Another line of investigation in this field has been the construction of "transcendence measures", expressing how "badly" a number fails to be algebraic — how hard it is to approximate it by algebraic numbers. Ideally, such a measure would give us a filtration of the complexes by algebraically closed subfields, so that a family of elements, no two of which have the same measure, would be algebraically independent. Theoretical results in this field have been obtained, but it has so far not proved possible to apply them to outstanding questions such as the algebraic independence of π and e.

§8 The analytic theory of transcendental numbers

The main stream of the theory of transcendental numbers has been the problem of proving that various numbers that arise in elementary analysis are transcendental, and, when possible, algebraically independent of one another. The basic principal here is that no number is algebraic — and, more generally, no set of numbers satisfies an algebraic relation — unless they have an obvious reason to.* The main results here are:

(1) Lindemann's Theorem. It is obvious that if real numbers $x_1,\ldots,x_n$ are linearly dependent over the integers, then $e^{x_1},\ldots, e^{x_n}$ will be algebraically dependent over the rationals, satisfying an equation $(e^{x_1})^{a_1}\ldots(e^{x_n})^{a_n}=1$ where the a_i are integers (not necessarily all nonnegative, but not all zero). Lindemann's theorem says that for algebraic exponents, essentially no relations hold but these. That is, if $x_1,\ldots,x_n$ are algebraic numbers linearly independent over the integers, then $e^{x_1},\ldots,e^{x_n}$ are algebraically independent over the rationals. Equivalently, the homomorphism from the group algebra on the additive group of algebraic numbers into the complexes, sending the generator of the group algebra corresponding to x to e^x, is an embedding.

Obvious examples are the transcendence of e, $e^{\sqrt{2}}$, etc.. Turning the theorem around, we see that all numbers whose exponential is algebraic (and which consitute linearly independent singletons — i.e., $\neq 0$) are transcendental. This gives us the natural logarithms of all the integers, and also πi, hence π. But note that we do not get an algebraic independence result for logarithms.

Siegel extended this result to apply to the values of functions satisfying certain differential equations, though they are not so simple as the above. The most notable functions to which they apply are the Weierstraß $\wp$-function, and Bessel functions.

(2) Gelfond showed in 1934 that if a and b are algebraic numbers, with $a\neq 0,1$ and b not rational, then a^b is transcendental. This had been Hilbert's 7th problem. "a^b" here means any expression e^{ub}, where u is a logarithm of a. Taking $a=1$, $u= 2\pi i$, $b= -i/2$, we see that e^π is transcendental.

(3) An outstanding conjecture, proved by Mahler this year (according to a letter from an acquaintance of Oort's) was the transcendentality of the Euler contant γ.

*The algebraicity of $e^{\pi i}$ is not really a counterexample. For though it was for a long time not obvious that one could define complex exponentiation, when it finally was defined, this was one of the most immediate results.

References and other literature

[1] Th.Schneider Einführung in die transzendenten Zahlen Springer, 1957. This includes a rather thorough bibliography to that date.

[2] W.J.LeVeque Topics in Number Theory, Vol.II, Addison-Wesley, 1956

Two important works in the field, covering rather similar ground, are:

C.L.Sigel Transcendental Numbers, Annals of Mathematics studies, 16. Princeton, 1949.

A.O.Gelfond Transcendental and Algebraic Numbers Moscow, 1952. Translation published by Dover, 1960

Some materials not in the bibliography of [1] are:

E. Hille, "Gelfond's solution of Hilbert's seventh problem", Am.Math.Monthly, 49(1942)pp.654-661.

S. Lang "Transzendente Zahlen", Bonner Mathematische Scriften, 21, 1963

S. Lang Introduction to Trasncendental Numbers, Addison Wesley, 1966

Lang's article and book concern themselves entirely with the Analytic theory.