# IV. Supplement

## IVa. Transcendence of the Numbers *e* and *π*

The first topic which I shall discuss will be the numbers $e$ and $\pi$. In particular, I wish to prove that they are transcendental numbers.

### *Historical Aspects*

Interest in the number $\pi$, in geometric form, dates from ancient times. Even then it was usual to distinguish between the problem of its *approximate calculation* and that of its exact *theoretical construction;* and one had certain approaches for the solution of both problems. *Archimedes* made an essential advance, in the first, with his process of *approximating to the circle by means of inscribed and circumscribed polygons*. The second problem soon centred in the question as to whether or not it was possible to *construct $\pi$ with ruler and compass*. This was attempted in all possible ways with never a suspicion that the reason for continued failure was the impossibility of the construction. An account of some of the early attempts has been published by Ferdinand Rudio[167]. The "*quadrature of the circle*" still remains one of the most popular problems, and many persons, as I have already remarked, seek salvation in its solution, without knowing, or believing, that modern science has long since settled the question.

In fact, these *ancient problems are completely solved today*. One is often inclined to doubt whether human knowledge really can advance, and in some fields the doubt may be justified. In mathematics, however, there are indeed advances of which we have here an example.

The *foundations* upon which the modem solution of these problems rests date from the period between Newton and Euler. A valuable tool for the approximate calculation of $\pi$ was supplied by *infinite series*, a tool, which made possible an accuracy adequate for all needs. The most elaborate result obtained was that of the

[167] *Der Bericht des Simplicius über die Quadraturen des Antiphon und Hippokrates.* Leipzig, 1908.



F. Klein, *Elementary Mathematics from a Higher Standpoint*,
DOI 10.1007/978-3-662-49442-4_12

Englishman Shanks, who calculated $\pi$ to 707 places[168]. One can ascribe this feat to
[257] a sportsmanlike interest in making a record, since no applications could ever require such accuracy.

On the *theoretical side*, the *number e*, the *base of the system of natural logarithms*, intervenes into the investigations during the same period. The wonderful relation $e^{i\pi} = -1$ was discovered and a means was developed, within the *integral calculus*, which, as we shall see, was of importance for the final solution of the question as to the quadrature of the circle. The decisive step in the solution of the problem was taken by Charles Hermite[169] in 1873, *when he proved the transcendence of e*. He did not succeed in proving the transcendence of $\pi$. That was done by *Lindemann*[170] in 1882.

These results represent at the same time an *essential generalization of the classical problem*. That was concerned only with the construction of $\pi$ by means of ruler and compass, which amounts, analytically, as we saw (p. [56]) to representing *$\pi$ by a finite succession of square roots and rational numbers*. But the modern results prove not merely the impossibility of this representation; they show far more, namely, that $\pi$ (and likewise $e$) is transcendental, that is, that it satisfies no algebraic relation whatever whose coefficients are integers. In other words, neither $e$ nor $\pi$ can be the root of an algebraic equation with rational integer coefficients:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

no matter how large the integers $a_0, \ldots, a_n$ or the degree $n$. It is essential that the coefficients be *rational integer* numbers[171]. It would suffice however to say *rational*, since we could make them integers by multiplying through by a common denominator.

I pass now to the

## *Proof of the Transcendence of e,*

in which I shall follow the simplified method given by Hilbert in Volume 43[172] of the *Mathematische Annalen* (1893). We shall show that the assumption of an equation

$$(1) \qquad a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0, \quad \text{where } a_0 \neq 0,$$

[168] See Weber-Wellstein, vol. 1, p. 523.

[169] *Comptes Rendus*, vol. 77 (1873), p. 18–24, 74–79, 226–233, 285–293; = Werke III (1912), p. 150.

[170] *Sitzungsberichte der Berliner Akademie*, 1882, p. 679, and *Mathematische Annalen*, vol. 20 (1882), p. 213.

[171] [Transl. note: In number theory, integer numbers are called rational integer numbers, to distinguish them from integer *p*-adic numbers.]

[172] „Über die Transcendenz der Zahlen $e$ und $\pi$“, 216–219.

in which $a_0, \ldots, a_n$ are integers, leads to a contradiction. This will show up by the *simplest properties of integers*. We shall need, namely, from the theory of numbers, only the most elementary theorems on divisibility, in particular, that an *integer can be separated into prime factors in only one way*, and, second, *that the number of primes is infinite*.

The *plan of the proof* is as follows. We shall set up a procedure, which enables one to approximate especially well to $e$ and powers of $e$, by means of rational numbers, so that we have **[258]**

$$(2) \qquad e = \frac{M_1 + \varepsilon_1}{M}, \quad e^2 = \frac{M_2 + \varepsilon_2}{M}, \quad \ldots, \quad e^n = \frac{M_n + \varepsilon_n}{M}$$

where $M, M_1, M_2, \ldots, M_n$ are integers, and $\varepsilon_1/M, \varepsilon_2/M, \ldots, \varepsilon_n/M$ are very small positive fractions. Then the assumed equation (1), after multiplication by $M$, takes the form

$$(3) \quad [a_0 M + a_1 M_1 + a_2 M_2 + \cdots + a_n M_n] + [a_1 \varepsilon_1 + a_2 \varepsilon_2 + \cdots + a_n \varepsilon_n] = 0$$

The *first parenthesis* is an *integer*, and we shall prove that it *with certainty is not zero*. As for the *second parenthesis*, we shall show that $\varepsilon_1, \ldots, \varepsilon_n$ can be made so small that it will be a *positive proper fraction*. Then we shall have the obvious *contradiction* that an *integer* $a_0 M + a_1 M_1 + \cdots + a_n M_n$ *which is not zero, increased by a proper fraction* $a_1 \varepsilon_1 + \cdots + a_n \varepsilon_n$ *should be zero. This will show the impossibility of* (1).

An important application will be made there of the deduction that if an integer is not divisible by a definite number, the integer cannot be zero (for zero is divisible by every number). We shall show, namely, that $M_1, \ldots, M_n$ are divisible by a certain prime number $p$, but that $a_0 M$ with certainty not, and that, therefore, $a_0 M + a_1 M_1 + \cdots + a_n M_n$ is not divisible by $p$, and hence is different from zero.

The principal aid in carrying out the indicated idea of a proof comes from the *use of a certain definite integral* which was devised by Hermite for this purpose and which we shall call Hermite's integral. The key to this proof lies in its structure. This integral, whose value, as we shall see, is an integer and which we shall use to define $M$, is

$$(4) \qquad M = \int_0^\infty \frac{z^{p-1} \left[(z-1)(z-2)\cdots(z-n)\right]^p e^{-z}}{(p-1)!} dz,$$

where $n$ is the degree of the assumed equation (1), and $p$ is an odd prime which we shall determine later. From this integral we shall get the desired approximation (2) to the powers $e^\nu (\nu = 1, 2, \ldots, n)$ by breaking the interval of integration of the integral $M \cdot e^{\nu}$ at the point $\nu$ and setting

(4a) $$M_{\nu} = e^{\nu} \int_{\nu}^{\infty} \frac{z^{p-1}\,[(z-1)\cdots(z-n)]^{p}\,e^{-z}}{(p-1)!}\,dz,$$

(4b) $$\varepsilon_{\nu} = e^{\nu} \int_{0}^{\nu} \frac{z^{p-1}\,[(z-1)\cdots(z-n)]^{p}\,e^{-z}}{(p-1)!}\,dz.$$

[259] Let us now proceed with the proof.

1. We start with the well-known formula from the beginnings of the theory of the gamma function:

$$\int_{0}^{\infty} z^{\varrho-1}e^{-z}\,dz = \Gamma(\varrho),$$

We shall need this formula only for integer values of $\varrho$, in which case $\Gamma(\varrho) = (\varrho-1)!$, and I shall deduce it under this restriction. If we integrate by parts we have, for $\varrho > 1$:

$$\int_{0}^{\infty} z^{\varrho-1}e^{-z}\,dz = \left[-z^{\varrho-1}e^{-z}\right]_{0}^{\infty} + \int_{0}^{\infty} (\varrho-1)\,z^{\varrho-2}e^{-z}\,dz$$
$$= (\varrho-1)\int_{0}^{\infty} z^{\varrho-2}e^{-z}\,dz.$$

The integral on the right is of the same form as the one on the left, except that the exponent of $z$ is reduced. If we apply this process repeatedly we must eventually come to $z^{0}$, since $\varrho$ is an integer; and since $\int_{0}^{\infty} e^{-z}\,dz = 1$, we obtain finally

(5) $$\int_{0}^{\infty} z^{\varrho-1}e^{-z}\,dz = (\varrho-1)\,(\varrho-2)\cdots 3\cdot 2\cdot 1 = (\varrho-1)!$$

Thus for integer $\varrho$ the integral is an integer which increases very rapidly when $\varrho$ increases.

To make this result *geometrically intuitive*, let us draw, on a $z$-axis, the curve $y = z^{\varrho-1}e^{-z}$ for different values of $\varrho$. The value of the integral will then be represented by the area under the curve extending to infinity (see Fig. 115). The larger $\varrho$ is the more closely the curve hugs the $z$-axis at the origin, but the more rapidly it rises beyond $z = 1$. The curve has a maximum at $z = \varrho - 1$, for all values of $\varrho$; in other words the maximum occurs farther and farther to the right as $\varrho$ increases; and its value also increases with $\varrho$. To the right of the maximum, the factor $e^{-z}$ prevails so that the curve falls, and eventually snuggles the $z$-axis intimately. It is thus comprehensible that the area (our integral) always remains finite but increases strongly with $\varrho$.

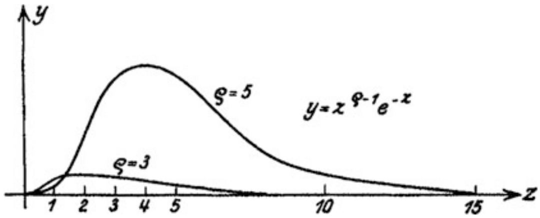



**Figure 115**

2. With this formula we can now easily evaluate our Hermite integral. Expanding the integrand by the polynomial theorem **[260]**

$$[(z-1)(z-2)\cdots(z-n)]^p = [z^n + - \cdots + (-1)^n n!]^p$$
$$= z^{np} + - \cdots + (-1)^n (n!)^p,$$

[where always only the terms involving the highest and the lowest powers of $z$ have to be written down], the integral becomes

$$M = \frac{(-1)^n\,(n!)^p}{(p-1)!}\int_0^\infty z^{p-1}e^{-z}dz + \sum_{\varrho=p+1}^{np+p}\frac{C_\varrho}{(p-1)!}\int_0^\infty z^{\varrho-1}e^{-z}dz.$$

The $C_\varrho$ are *integer* constants, by the polynomial theorem. Now we can apply formula (5) to each of these integrals and obtain

$$M = (-1)^n\,(n!)^p + \sum_{\varrho=p+1}^{np+p} C_\varrho\frac{(\varrho-1)!}{(p-1)!}$$

The summation index $\varrho$ is *always greater than* $p$ and consequently $(\varrho-1)!/(p-1)!$ is an integer and one which contains $p$ as a factor, so that we can take $p$ as a factor out of the entire sum:

$$M = (-1)^n(n!)^p + p[C_{p+1} + C_{p+2}(p+1) + C_{p+3}(p+1)(p+2) + \cdots].$$

Now, so far as divisibility by $p$ is concerned, $M$ must behave like the first summand $(-1)^n(n!)^p$. And since $p$ is a prime number it will not be a divisor of this summand if it is not a divisor of any of its factors $1, 2, \ldots, n$, which will certainly be the case if $p > n$. But this condition can be satisfied in an unlimited number of ways, since the number of primes is infinite. Consequently we can bring it about that $(-1)^n(n!)^p$, and hence *$M$, is with certainty not divisible by $p$.*

Since furthermore $a_0 \neq 0$, we can see to it, at the same time, that $a_0$ *is not divisible by* $p$ by selecting $p$ greater also than $|a_0|$, which is, of course, possible, by what was said above. But *then the product* $a_0 \cdot M$ *will not be divisible by* $p$, and that is what we wished to show.

3. Now we must examine the numbers $M_\nu (\nu = 1, 2, \ldots, n)$, defined in (4a) (p. [258]). Putting the factor $e^\nu$ under the sign of integration and introducing the new variable of integration $\zeta = z - \nu$, which varies from 0 to $\infty$ when $z$ runs from $\nu$ to $\infty$, we have

$$M_\nu = \int_0^\infty \frac{(\zeta + \nu)^{p-1} \left[(\zeta + \nu - 1)(\zeta + \nu - 2) \cdots \zeta \cdots (\zeta + \nu - n)\right]^p e^{-\zeta}}{(p-1)!} d\zeta.$$

**[261]** This expression has a form entirely analogous to the one considered before for $M$ and we can treat it in the same way. If we multiply out the factors of the integrand there will result an aggregate of powers with integer coefficients of which the lowest will be $\zeta^p$. The integral of the numerator will thus be an integer-number combination of the integrals

$$\int_0^\infty \zeta^p e^{-\zeta} d\zeta, \quad \int_0^\infty \zeta^{p+1} e^{-\zeta} d\zeta, \quad \ldots, \quad \int_0^\infty \zeta^{(n+1)p-1} e^{-\zeta} d\zeta,$$

and since these are, by (5), equal to $p!, (p+1)!, \ldots$ the numerator will be $p!$ multiplied by an integer number $A$, thus each one is:

$$M_\nu = \frac{p! A_\nu}{(p-1)!} = p \cdot A_\nu, \quad (\nu = 1, 2, \ldots, n).$$

In other words, every $M^\nu$ is an integer number, which is divisible by $p$.

This, combined with the result of No. 2, proves the statement made on p. [258] et seq. that $a_0 M + a_1 M_1 + \cdots + a_n M_n$ *is clearly not divisible by* $p$ *and is therefore different from zero*.

4. The second part of the proof has to do with the sum $a_1 \varepsilon_1 + \cdots + a_n \varepsilon_n$, where, by (4b),

$$\varepsilon_\nu = \int_0^\nu \frac{z^{p-1} \left[(z-1)(z-2) \cdots (z-n)\right]^p e^{-z+\nu}}{(p-1)!} dz.$$

We must show that these $\varepsilon_\nu$ can be made sufficiently small by an appropriate choice of $p$. To this end we use the fact that we can make *$p$ as large as we chose;* for the only conditions thus far imposed upon $p$ are that it should be a prime number greater than $n$ and also greater than $|a_0|$, and these can be still satisfied by arbitrarily large prime numbers.

Let us study a geometrical image of the shape of the integrand. At $z = 0$ it will be tangent to the $z$-axis, but at $z = 1, 2, \ldots, n$ (in Fig. 116, $n = 3$) it will be tangent to the $z$-axis and also cut it, since $p$ is odd. As we shall see soon, the presence in the denominator of $(p-1)!$ brings it about that for large $p$ the curve departs but little

from the $z$-axis in the interval $(0, n)$, so that it seems plausible that the integrals $\varepsilon_\nu$ should be very small. For $z > n$ the curve rises and proceeds asymptotically like the former curve $z^{\varrho-1}e^{-z}$ [for $\varrho = (n+1)p$] and finally approaches indefinitely [262]
the $z$-axis. It was for this reason that the value $M$ of the integral (when the interval of integration was from 0 to $\infty$) increased so rapidly with $p$.

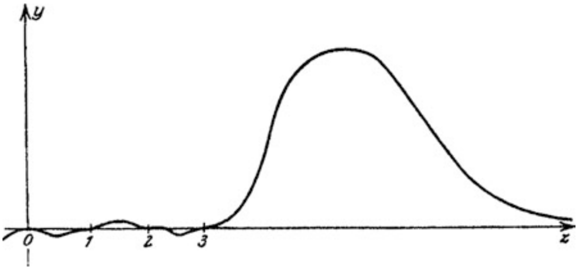



**Figure 116**

In actually estimating the integrals we can be satisfied with a quite rough approximation. Let $G$ and $g_\nu$ be the maxima of the absolute values of the functions $z(z-1)\dots(z-n)$ and $(z-1)(z-2)\dots(z-n)e^{-z+\nu}$ respectively in the interval $(0, n)$:

$$\left.\begin{array}{l} |z\,(z-1)\dots(z-n)\,| \leqq G \\ |\,(z-1)\,(z-2)\dots(z-n)\,e^{-z+\nu}| \leqq g_\nu \end{array}\right\} \quad \text{for } 0 \leqq z \leqq n.$$

Since the integral of a function, taken absolutely, is never greater than the integral of its absolute value, we have, for each $\varepsilon_r$

$$(6) \qquad |\varepsilon_\nu| \leqq \left\{ \int\limits_0^\nu \frac{G^{p-1} g_\nu}{(p-1)!} dz = \frac{G^{p-1} g_\nu \cdot \nu}{(p-1)!} \right\}.$$

Now $G$, $g_\nu$, and $\nu$ are fixed numbers independent of $p$, but the number $(p-1)!$ in the denominator increases ultimately more rapidly than the power $G^{p-1}$, or, more exactly, the fraction $G^{p-1}/(p-1)!$ becomes, for sufficiently large $p$, smaller than any pre-assigned number, however small. Thus, because of (6), we can actually make each of the $n$ numbers $\varepsilon_\nu$ *arbitrarily small* by choosing $p$ sufficiently large.

It follows immediately from this that we can also make the sum of $n$ terms $a_1\varepsilon_1 + \dots + a_n\varepsilon_n$ arbitrarily small. We have, in fact

$$|a_1\varepsilon_1 + a_2\varepsilon_2 + \dots + a_n\varepsilon_n| \leqq |a_1|\,|\varepsilon_1| + |a_2|\,|\varepsilon_2| + \dots + |a_n|\,|\varepsilon_n|$$

and by (6)

$$\leqq (|a_1| \cdot 1 \cdot g_1 + |a_2| \cdot 2 \cdot g_2 + \dots + |a_n| \cdot n \cdot g_n) \cdot \frac{G^{p-1}}{(p-1)!}.$$

Since the parenthesis has a value which is independent of $p$, we can, by virtue of the factor $G^{p-1}/(p-1)!$, make the entire right hand side, and *hence also* $a_1\varepsilon_1 + a_2\varepsilon_2 + \cdots + a_n\varepsilon_n$, *as small as we choose, and, in particular, smaller than unity*.

With this we have shown, as we agreed to do (p. [258]), that the assumption of the equation (3)

$$[a_0 M + a_1 M_1 + \cdots + a_n M_n] + [a_1\varepsilon_1 + \cdots + a_n\varepsilon_n] = 0$$

leads to a contradiction, namely that a non-vanishing integer increased by a proper fraction should give zero. *And since this equation cannot exist the transcendence of*
**[263]** *e is proved.*

## *Proof of the Transcendence of π*

We turn now to the proof of the transcendence of the number $\pi$. This proof is somewhat more difficult than the foregoing, but it is still fairly easy. It is only necessary to begin at the right end, which is indeed the art of all mathematical discovery.

The problem, as *Ferdinand Lindemann* considered it, was the following: It has been shown thus far that an equation $\sum_{\nu=0}^{n} a_\nu e^\nu = 0$ cannot exist if the coefficients $a_\nu$ and the exponents $\nu$ of $e$ are ordinary rational integer numbers. Would it not be possible to prove a similar thing where $a_\nu$ and $\nu$ are arbitrary *algebraic* numbers? He succeeded in doing this; in fact, his most general theorem concerning the *exponential function* is as follows: *An equation* $\sum_{\nu=1}^{n} a_\nu e^{b_\nu} = 0$ *cannot exist if the* $a_r$, $b_\nu$ *are algebraic numbers, whereby the* $a_\nu$ *are arbitrary, the* $b_\nu$ *different from one another.* The *transcendence of* $\pi$ *is then only a corollary* to this theorem. For, as is well known, $1 + e^{i\pi} = 0$; and if $\pi$ were an algebraic number, $i\pi$ would be also, and the existence of this equation would contradict the above theorem of Lindemann.

I shall now prove in detail only a *certain special case of Lindemann's theorem*, one *which carries with it, however, the transcendence of* $\pi$. I shall follow again, in the main, Hilbert's proof in Volume 43 of the *Mathematische Annalen*, which is essentially simpler than Lindemann's, and which is an exact generalization of the discussion, which we have given for $e$.

The starting point is the relation

$$(1) \qquad 1 + e^{i\pi} = 0.$$

If, now, $\pi$ satisfies any algebraic equation with rational integer coefficients then $i\pi$ also satisfies such an equation. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be *all* the roots, including $i\pi$ itself, of this last equation. Then we must also have, because of (1):

$$(1 + e^{\alpha_1})(1 + e^{\alpha_2}) \cdots (1 + e^{\alpha_n}) = 0.$$

Multiplying out we obtain

$$(2) \qquad \begin{cases} 1 + \left(e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_n}\right) + \left(e^{\alpha_1+\alpha_2} + e^{\alpha_1+\alpha_3} + \cdots + e^{\alpha_{n-1}+\alpha_n}\right) \\ \qquad + \cdots + \left(e^{\alpha_1+\alpha_2+\cdots+\alpha_n}\right) = 0. \end{cases}$$

Now some of the exponents, which appear here might, by chance, be zero. Every time that this occurs the left hand sum has a positive summand 1, and we combine these, together with the 1 that appears formally, into a positive integer $a_0$, which is certainly different from zero. The remaining exponents, all different from zero, we **[264]** denote by $\beta_1, \beta_2, \ldots, \beta_N$ and we write, accordingly, instead of (2),

$$(3) \qquad a_0 + e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_N} = 0, \quad \text{where } a_0 > 0.$$

Now $\beta_1, \ldots, \beta_N$ are the *roots of an algebraic equation with integer coefficients*. For, from the equation whose roots are $\alpha_1, \ldots, \alpha_n$ we can construct one of the same character whose roots are the two-term sums $\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \ldots$, then another for the three-term sums $\alpha_1 + \alpha_2 + \alpha_3$, $\alpha_1 + \alpha_2 + \alpha_4, \ldots$ and so on; finally, $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ is itself rational and satisfies therefore a linear integer equation. By multiplying together all these equations, we obtain again an equation with rational integer coefficients, which might have some zero roots, and whose remaining roots are the $\beta_1, \ldots, \beta_N$. Omitting the power of the unknown, which corresponds to the zero roots, there will remain *for the N quantities $\beta$ an algebraic equation of degree N with integer coefficients* and absolute term different from zero

$$(4) \qquad b_0 + b_1 z + b_2 z^2 + \cdots + b_N z^N = 0, \quad \text{where } b_0, b_N \neq 0.$$

We now have to prove the following special case of Lindemann's theorem. *An equation of the form* (3), *with integer non-vanishing $a_0$, cannot exist if $\beta_1, \ldots, \beta_N$ are the roots of an algebraic equation of degree N, with integer coefficients.* This theorem includes the transcendence of $\pi$.

The proof involves the same steps as the one already given for the transcendence of $e$. Just as we could there approximate closely to the powers $e^1, e^2, \ldots, e^n$ by means of rational numbers, so we shall be concerned here with the *best possible approximation to the powers of e* which appear in (3), and we shall write, in the old notation,

$$(5) \qquad e^{\beta_1} = \frac{M_1 + \varepsilon_1}{M}, \quad e^{\beta_2} = \frac{M_2 + \varepsilon_2}{M}, \cdots, e^{\beta_N} = \frac{M_N + \varepsilon_N}{M};$$

where the denominator $M$ is again an *ordinary rational integer number, but the $M_1, \ldots, M_N$ are no longer rational integer numbers as formerly, but are integer a l g e b r a i c numbers, and the $\beta_1, \ldots, \beta_N$, which in general can now be complex, are in absolute value very small.* It is here that the difficulty in this proof lies, as compared to the earlier one. The *sum of all the $M_1, \ldots, M_N$ will again, however, be an rational integer number*, and we shall be able to arrange it so that the *first summand* in the equation:

$$(6) \qquad [a_0 M + M_1 + M_2 + \cdots + M_N] + [\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_N] = 0.$$

**[265]** into which (3) goes over when we multiply by $M$ and use (5)] will be a *non-vanishing rational integer number*, while the *second summand* will be, in absolute value, *smaller than unity*. *Essentially, this will be the same type of contradiction, which we used before. It will show the impossibility of* (6) *and* (3) *and so complete our proof.* As to detail, we shall again show that $M_1 + M_2 + \cdots + M_N$ is divisible by a certain prime number $p$, but that $a_0 M$ is not, which will show that the first summand in (6) cannot vanish; then we shall choose $p$ so large that the second summand will be arbitrarily small.

1. Our first concern is to define $M$ by a *suitable generalization of Hermite's integral.* A hint here lies in the fact that the zeros of the factor $(z-1)(z-2)\ldots(z-n)$ in Hermite's integral were the exponents in the powers of $e$ in the hypothetical algebraic equation. Hence we now replace that factor by the product made by using the exponents in (3), i.e., the solutions in (4):

$$(7) \qquad (z-\beta_1)(z-\beta_2)\ldots(z-\beta_N) = \frac{1}{b_N}\left[b_0 + b_1 z + \cdots + b_N z^N\right].$$

It turns out to be essential here *to put in a suitable power of* $b_N$ *as factor*, which was unnecessary before because $(z-1)\ldots(z-n)$ was integer. We set then finally

$$(8) \qquad M = \int_0^\infty \frac{e^{-z} z^{p-1} dz}{(p-1)!}\left[b_0 + b_1 z + \cdots + b_N z^N\right]^p b_N^{(N-1)p-1}.$$

2. Just as before, we now expand the integrand of $M$ according to powers of $z$. The lowest power, that belonging to $z^{p-1}$, gives then:

$$\int_0^\infty \frac{e^{-z} z^{p-1} dz}{(p-1)!} b_0^p b_N^{(N-1)p-1} = b_0^p b_N^{(N-1)p-1},$$

where the integral has been evaluated by means of the gamma-formula (p. [239]). The remaining summands in the integrand contain either $z^p$ or still higher powers, so that the integrals contain the factor $p!/(p-1)!$, multiplied by integers, and are thus all divisible by $p$. *Consequently M is an integer which is certainly not divisible by p,* i.e., provided the prime number $p$ is not a divisor of either $b_0$ or $b_N$. But since these two numbers are both different from zero, we can bring this about by choosing $p$ so that $p > |b_0|$ and also $p > |b_N|$.

**[266]** Since $a_0 > 0$ it follows that $a_0 M$ is *not divisible by p* if we impose the additional condition $p > a_0$. Inasmuch as the number of primes is infinite we can satisfy all these conditions in an unlimited number of ways.

3. We must now approach to construct $M_\nu$ and $e_\nu$. Here we must *modify our earlier plan* because the $\beta_\nu$ which now take the place of the former $\nu$, can be *complex;* in fact one of them is $i\pi$. If we are to split the integer $M$ as we did before we must first determine the *path of integration in the complex plane*. Fortunately the *integrand of our integral is a finite univocal function of the integration variable z,*

regular everywhere except at $z = \infty$, where it has an *essential singularity*. Instead of integrating from 0 to $\infty$ along the real axis we can choose any other path from 0 to $\infty$, provided it ultimately runs asymptotically parallel to the positive real half-axis. This is necessary if the integral is to have a meaning at all, in view of the behaviour of $e^{-z}$ in the complex plane.

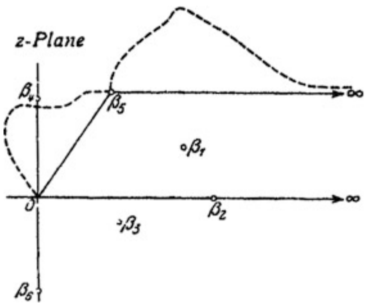



**Figure 117**

Let us now mark the $N$ points $\beta_1, \beta_2, \ldots, \beta_N$ in the plane and recall that we shall obtain the same value for $M$ if we first integrate rectilinearly from 0 to one of the points $\beta_N$ and then to $\infty$ along a parallel to the real axis (see Fig. 117). Along this path we can separate $M$ into the two characteristic parts: *The rectilinear path from 0 to $\beta_N$ supplies the $\varepsilon_\nu$ which will become arbitrarily small with increasing p; the parallel from $\beta_N$ to $\infty$ will supply the integral algebraic number $M_N$*:

$$\text{(8a)}\quad \varepsilon_\nu = e^{\beta_\nu} \int_0^{\beta_\nu} \frac{e^{-z} z^{p-1} dz}{(p-1)!} \left[b_0 + b_1 z + \cdots + b_N z^N\right]^p b_N^{(N-1)p-1}, \qquad (\nu = l, 2, \ldots, N),$$

(8b)

$$M_\nu = e^{\beta_\nu} \int_{\beta_\nu}^{\infty} \frac{e^{-z} z^{p-1} dz}{(p-1)!} \left[b_0 + b_1 z + \cdots + b_N z^N\right]^p b_N^{(N-1)p-1}.$$

These assumptions satisfy (5). Our choice of a *rectilinear path* of integration was made solely for convenience; any curvilinear path from 0 to $\beta_\nu$ would, of course, yield the same value for $\varepsilon_\nu$, but one achieves the best estimation for the integral when the path is straight. Similarly, we might choose, instead of the horizontal path **[267]** from $\beta_\nu$ to $\infty$, an arbitrary curve provided only that it approached the horizontal asymptotically; but that would be unnecessarily inconvenient.

4. I will discuss first the estimation of the $e_\nu$, because this involves nothing new if we only recall that the absolute value of a complex integral cannot be larger than the maximum of the absolute value of the integrand, multiplied by the length of the path of integration, which, in our case, is $|\beta_\nu|$. The upper limit for $\varepsilon_\nu$ would be,

then, the product of $G^{p-1}/(p-1)!$ by factors which are independent of $p$, where $G$ denotes the maximum of $\left|z\left(b_0+b_1z+\cdots+b_Nz^N\right)b_N^{N-1}\right|$ in a region which contains all the segments joining 0 with the points $\beta_\nu$. From this one may infer, as we did before, (p. [262]), that, *by sufficiently increasing p, the value of each $\varepsilon_\nu$ and, therefore, the value of $\varepsilon_1+\cdots+\varepsilon_N$ can be made as small as we please and, in particular, smaller than unity*.

5. It is only in the *investigation of the $M_\nu$* that essentially new considerations are necessary, and these are, to be sure, only generalisations of our former reasoning, due to the fact that *integer algebraic numbers* take the place now of what were then *rational integer numbers*. We shall consider, as a whole, the sum:

$$\sum_{\nu=1}^{N} M_\nu = \sum_{\nu=1}^{N} e^{\beta_\nu} \int_{\beta_\nu}^{\infty} \frac{e^{-z}z^{p-1}dz}{(p-1)!}\left[b_0+b_1z+\cdots+b_Nz^N\right]^p b_N^{(N-1)p-1}.$$

If we make use of (7) (p. [265]) and replace, in each summand of the above summation, the polynomial in $z$ by the product of the factors $(z-\beta_1)\cdots(z-\beta_N)$ and introduce the new variable of integration $\zeta=z-\beta_\nu$, which will run through real values from 0 to $\infty$, we obtain

(9)
$$\begin{cases} \sum_{\nu=1}^{N} M_\nu = \sum_{\nu=1}^{N} \int_0^\infty \frac{e^{-\zeta}d\zeta}{(p-1)!}(\zeta+\beta_\nu)^{p-1}(\zeta+\beta_\nu-\beta_1)^p\cdots\zeta^p\cdots(\zeta+\beta_\nu-\beta_N)^p\, b_N^{Np-1} \\ \text{which may be written} = \displaystyle\int_0^\infty \frac{e^{-\zeta}d\zeta}{(p-1)!}\zeta^p\cdot\Phi(\zeta) \end{cases},$$

where we use the abbreviation

$$(9')\qquad \begin{cases} \Phi(\zeta) = \sum_{\nu=1}^{N} b_N^{Np-1}(\zeta+\beta_\nu)^{p-1}(\zeta+\beta_\nu-\beta_1)^p\cdots \\ \qquad (\zeta+\beta_\nu-\beta_{\nu-1})^p(\zeta+\beta_\nu-\beta_{\nu+1})^p\cdots(\zeta+\beta_\nu-\beta_N)^p \end{cases}.$$

This sum $\Phi(\zeta)$, like each of its $N$ summands, is a polynomial in $\zeta$. In each of the summands, one of the $N$ quantities $\beta_1,\ldots,\beta_N$ plays a marked role; but if we con-
[268] sider the polynomial in $\zeta$ obtained by multiplying out in $\Phi(\zeta)$, we see that these $N$ quantities appear, without preference, in the coefficients of the different powers of $\zeta$. In other words, each of these coefficients is a *symmetric function of* $\beta_1,\ldots,\beta_N$. The multiplying out of the individual factors by the multinomial theorem permits the further inference that these functions $\beta_1,\ldots,\beta_N$ are *rational integer functions with rational integer coefficients*. But according to a well-known theorem in algebra, *rational symmetric functions, with rational coefficients of all the roots of a rational integer equation are always rational numbers;* and since the $\beta_1,\ldots,\beta_N$ are all the roots of equation (4), *the coefficients of $\Phi(\zeta)$ are actually rational numbers*.

But, more than this, we need rational integer numbers. These are supplied by the power of $b_N$ which occurs as a factor of $\Phi(\zeta)$. We can, in fact, distribute this power among all the linear factors, which occur there and write

(9′)

$$\begin{cases} \Phi(\zeta) = \sum_{\nu=1}^{N} (b_N\zeta + b_N\beta_\nu)^{p-1}(b_N\zeta + b_N\beta_\nu - b_N\beta_1)^p \cdots (b_N\zeta + b_N\beta_\nu - b_N\beta_{\nu-1})^p \\ \qquad (b_N\zeta + b_N\beta_\nu - b_N\beta_{\nu+1})^p \cdots (b_N\zeta + b_N\beta_\nu - b_N\beta_N)^p \end{cases}$$

In analogy with what we had earlier, the coefficients of $\zeta$, when this polynomial is calculated, are *rational integer symmetric functions of the products* $b_N\beta_1, b_N\beta_2, \ldots, b_N\beta_N$, *with rational integer coefficients*. But these $N$ products are roots of the equation into which (4) transforms if we replace $z$ by $z/b_N$:

$$b_0 + b_1\frac{z}{b_N} + \cdots + b_{N-1}\left(\frac{z}{b_N}\right)^{N-1} + b_N\left(\frac{z}{b_N}\right)^N = 0.$$

If we multiply through by $b_N^{N-1}$ this equation goes over into:

$$(10) \qquad b_0 b_N^{N-1} + b_1 b_N^{N-2}\cdot z + \cdots + b_{N-2}b_N z^{N-2} + b_{N-1}z^{N-1} + z^N = 0,$$

that is, an equation with integral coefficients throughout and where the coefficient of the highest power is unity. Algebraic numbers which satisfy such an equation are called *integer algebraic numbers*, and we have the following refinement of the theorem mentioned above: *Rational integer symmetric functions, with rational integer coefficients of all the roots of an integer equation whose highest coefficient is unity* (*i.e., of integer algebraic numbers*) *are themselves rational integer numbers.* You will find this theorem in textbooks on algebra; and if it is not always enunciated in this precise form you can, nevertheless, by following the proof, convince yourselves of its correctness.

Now the coefficients of the polynomial $\Phi(\zeta)$ actually satisfied the assumptions **[269]** of this theorem so that they are rational integer numbers, which we shall denote by $A_0, A_1, \ldots, A_{Np-1}$. We have, then according to (9),

$$\sum_{\nu=1}^{N} M_\nu = \int_0^\infty \frac{e^{-\zeta}\zeta^p d\zeta}{(p-1)!}\left(A_0 + A_1\zeta + \cdots + A_{Np-1}\zeta^{Np-1}\right).$$

With this we have essentially reached our goal. For, if we carry out the integrations in the numerator, using our gamma formula (p. [259]), we obtain factors $p!, (p+1)!, (p+2)!\ldots$, since each term contains as factor a power of $\zeta$ of degree $p$ or higher; and after division by $(p-1)!$ *there remains everywhere a factor* $p$, while the other factors are *rational* integer numbers (the $A_0, A_1, A_2, \ldots$). *Thus* $\sum_{\nu=1}^{N} M_\nu$ *is certainly a rational integer number divisible by* $p$.

We saw (p. [266]) that $a_0 \cdot M$ was not divisible by $p$, so that

$$a_0 M + \sum_{\nu=1}^{N} M_\nu$$

is necessarily a rational integer number which is not divisible by $p$ and hence, in particular, different from zero. Therefore the equation (6):

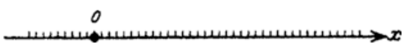
$$\left\{ a_0 M + \sum_{\nu=1}^{N} M_\nu \right\} + \left\{ \sum_{\nu=1}^{N} \varepsilon_\nu \right\} = 0$$

cannot exist, for a non-vanishing integer added to $\sum_{\nu=1}^{N} \varepsilon_\nu$, which was shown in No. 4 (p. [267]) to be smaller than unity in absolute value, cannot yield zero. *But this proves the special case of Lindemann's theorem which we enunciated above (p. [264]) and which carries with it the transcendence of* $\pi$.

## *More on Transcendent and Algebraic Numbers*

I should like to emphasise here *another interesting special case of the general Lindemann theorem*, namely, that in the equation $e^\beta = b$ the numbers $b, \beta$ cannot both be algebraic, with the trivial exception $\beta = 0$, $b = 1$. In other words, the exponential function of an algebraic argument $\beta$ as well as the natural logarithm of an algebraic number $b$ is, with this one exception, always transcendental. This statement includes the transcendence of both $e$ and $\pi$, the former for $\beta = 1$; the latter for $b = -1$ (because $e^{i\pi} = -1$). The proof of this theorem can be effected by an exact generalisation of the last discussion. One would start from $b - e^\beta$ instead of from $1 + e^\alpha$ as before. It would be necessary to take into account not only all the roots of the algebraic equation for $\beta$, but also all the roots of the equation for $b$, in order to arrive at an equation analogous to (3), so that one would need more
[270] notation and the proof would be apparently less perspicuous; but it would require no essentially new ideas. The *proof of the most general Lindemann theorem* can be realised in an entirely analogous manner.

I shall not go farther into these proofs, but I should like to make you appreciate the significance of the *last theorem concerning the exponential function* as intuitively as possible. Let us think of all points with an algebraic abscissa as marked off on the $x$-axis.




We know that even the rational numbers, and hence, with greater reason, the algebraic numbers lie everywhere dense on the $x$-axis. One might think at first that at least the algebraic numbers would exhaust all the real numbers. But our theorem yields that this is not the case; *that between the algebraic numbers on the x-axis there are infinitely many other numbers, viz. the transcendental numbers;* and that we have examples of them in unlimited quantity in $e^{\text{algbr. no.}}$, in log(*algebr. no.*), and in every algebraic function of these transcendental numbers. It will even be more obvious, perhaps, if we write the equation in the form $y = e^x$ and interpret it as *curve* in an $x$-$y$-plane (see Fig. 118). If we now mark all the algebraic numbers on the $x$-axis and on the $y$-axis and consider all the points in the plane that have both an algebraic $x$ and an algebraic $y$, the $x$-$y$-plane will be densely covered with these "*algebraic* points". *In spite of this dense distribution, the exponential curve y = e^x does not contain a single algebraic point except the one* $x = 0$, $y = 1$. Of all the other number pairs $x$, $y$ which satisfy $y = e^x$, one, at least, is transcendental. This shape of the exponential curve is certainly a most remarkable fact!

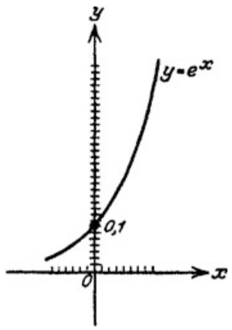



**Figure 118**

The theoretical significance of these theorems which reveal the existence in great quantity of numbers which are not only not rational but which cannot be represented by algebraic operations upon numbers representable by integer numbers – their significance for our *representations of the number continuum is tremendous.* What would Pythagoras have sacrificed after such a discovery if the irrational seemed to him to merit a hecatomb!

It is remarkable how little in general these questions of transcendence are grasped and assimilated, although they are so simple when one has once thought them through. I continually have the experience, in an examination, that the candidate cannot even explain the notion "transcendence". I often get the answer that a transcendental number satisfies no algebraic equation, which, of course, is entirely false, as the example $x - e = 0$ shows. The essential thing, that the coefficients in **[271]** the equation must be rational, is overlooked.

If you will think our transcendence proofs through again you will be able to grasp these simple elementary steps as a whole, and to make them permanently your own. You need to impress upon your memory only the Hermite integral; then everything develops itself naturally. I should like to emphasise the fact that in these proofs we have used the *integral concept* (or, speaking geometrically, the idea of *area*) as something in its essence thoroughly elementary, and I believe that this has contributed markedly to the clearness of the proof. Compare in this respect, the presentation in Volume I of Weber-Wellstein, or in my own little book, *Vorträge über ausgewählte Fragen der Elementargeometrie*[173], where, as in the older school-books, the integral sign is avoided and its use replaced by approximate calculation of series developments. I think that you will admit that the proofs there are far less clear and easy to grasp.

These discussions concerning the distribution of the algebraic numbers within the realm of real numbers lead us naturally to that *second modern field* to which I have already often referred during these lectures, and which I shall now consider in some detail.

## IVb. Set Theory

The investigations of George Cantor, the founder of this theory, had their beginning precisely in considerations concerning the existence of transcendental numbers[174]. They permit one to view this matter in an entirely new light.

If the brief survey of set theory, which I shall give you, has any special character, it is this, that I shall bring the treatment of concrete examples more into the foreground than is usually done in those very general abstract presentations, which too often give this subject a form that is hard to grasp and even discouraging.

### *1. The Potency of Sets*

With this end in view, let me remind you that in our earlier discussions we have often had to do with *different characteristic totalities of numbers*, which we can **[272]** now call sets of numbers. If I confine myself to real numbers, these assemblages are

1. The positive integers.
2. The rational numbers.
3. The algebraic numbers.
4. All real numbers.

Each of these sets contains *infinitely many numbers*. Our first question is whether, in spite of this, we cannot compare the magnitude or the range of these sets in a definite sense, i.e., whether we cannot call the "*infinity*" of one *greater than, equal to,* or *less than* that of another. It is the great achievement of Cantor to have cleared up and answered this at first quite indefinite question, by setting

[173] Referred to p. [135].

[174] See: „Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen.“, *Journal für reine und angewandte Mathematik*, vol. 77 (1873). p. 258.

up precise concepts. Above all we have to consider his concept of *"potency"* or *"cardinal number"*: *Two sets have "equal potency" (are "equivalent") when their elements can be put into one-to-one correspondence, i.e., when the two sets can be so related to each other that to each element of the one there corresponds one element of the other, and conversely.* If such a mutual correspondence is not possible the two assemblages are of "*different potency";* if it turns out that, no matter how one tries to set up a correspondence, there are always elements of one of the sets left over, this one has the "*greater potency*".

Let us now apply this principle to the four examples given above. It might seem, at first, that the potency of the integers would be smaller than that of the rational numbers, the potency of these smaller than that of the algebraic numbers, and this finally smaller than that of all real numbers; for each of these sets arises from the preceding by the addition of new elements. But such a conclusion would be too hasty. For although *the potency of a finite set is always greater than the potency of a part of it*, this theorem is *by no means transferable to infinite sets*. This discrepancy, after all, need not cause surprise, since we are concerned in the two cases with entirely different fields. Let us examine a simple *example*, which will show clearly that an infinite set and a part of it can actually have the same potency, the set, namely, of all positive integers and that of all positive even integers

$$\begin{array}{cccccccc} 1, & 2, & 3, & 4, & 5, & 6, & \ldots, \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 2, & 4, & 6, & 8, & 10, & 12, & \ldots. \end{array}$$

The correspondence indicated by the double arrows is obviously of the sort prescribed above, in that each element of one set corresponds to one and only one of the other. Therefore, by Cantor's definition, the set of the positive integers and its **[273]**
subset of the even integers have the same potency.

### Denumerability of Rational and Algebraic Numbers

You see that the question as to the potencies of our four sets is not so easily disposed of. The simple answer, which then appears the more remarkable, consists in Cantor's great discovery of 1873: *The three sets, the positive integers, the rational, and the algebraic numbers, have the same potencies; but the set of all real numbers has another, namely, a larger potency.* A set whose elements can be put into one-to-one correspondence with the series of positive integers (which has therefore the same potency) is called *denumerable*. The above theorem can therefore be stated as follows: *The set of the rational as well as of the algebraic numbers is denumerable; that of all real numbers is not denumerable.*

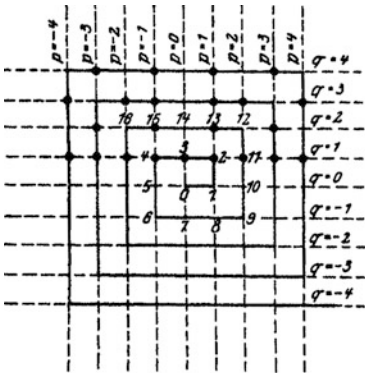


**Figure 119**

Let us first give the *proof for rational numbers*, which is no doubt familiar to some of you. Every rational number (we shall include the negative ones) can be expressed uniquely in the form $p/q$, where $p$ and $q$ are integers without a common divisor, where, say, $q$ is positive, while $p$ may also be zero or negative. In order to bring all these fractions $p/q$ into a single series, let us mark in a $p$-$q$-plane all points with integer coordinates $(p, q)$, so that they appear as points on a spiral path as shown in Fig. 119. Then we can number all these pairs ($p$, $q$) so that only one number will be assigned to each and all integers will be used (see Fig. 119). Now delete from this succession all the pairs $(p, q)$, which do not satisfy the above prescription ($p$ prime to $q$ and $q > 0$) and number anew only those, which remain (indicated in the figure by heavy points). We get thus a series, which begins as follows:

$$\begin{array}{ccccccccccc} \underbrace{1} & \underbrace{2} & \underbrace{3} & \underbrace{4} & \underbrace{5} & \underbrace{6} & \underbrace{7} & \underbrace{8} & \underbrace{9} & \underbrace{10} & \underbrace{11} \\ 1 & 0 & -1 & 2 & \frac{1}{2} & -\frac{1}{2} & -2 & 3 & \frac{3}{2} & \frac{2}{3} & \frac{1}{3} \end{array} \quad \ldots,$$

*one in which a positive integer is assigned to each rational number and a rational number to each positive integer. This shows that the rational numbers are denumerable. This arrangement of the rational numbers*

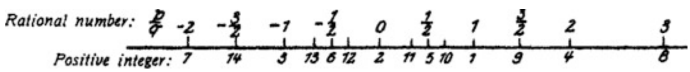



**Figure 120**

*into a denumerable series requires, of course, a complete dislocation of their rank*
[274] *as to size*, as is indicated in Fig. 120, where the rational points, laid off on the axis of abscissas, are marked with the order of their appearance in the artificial series.

We come, secondly, to the *algebraic numbers*. I shall confine myself here to real numbers, although the inclusion of complex numbers would not make the discussion essentially more difficult. Every real algebraic number satisfies a real integer equation

$$a_0\omega^n + a_1\omega^{n-1} + \cdots + a_{n-1}\omega + a_n = 0,$$

which we shall assume to be *irreducible*, i.e., we shall omit any rational detachable factor of the left-hand member, and also any possible common divisors of $a_1, a_2, \ldots, a_n$. We assume also that $a_0$ is always positive. *Then, as is well known, every algebraic $\omega$ satisfies but one irreducible equation with integer coefficients, in this normal form; and conversely, every such equation has as roots at most n real algebraic numbers, but perhaps fewer, or none at all. If, now, we could bring all these algebraic equations into a denumerable series* we could obviously infer that their roots and hence all real algebraic numbers are denumerable.

Cantor succeeded in doing this by assigning to each equation a definite number, its "index",

$$N = n - 1 + a_0 + |a_1| + \cdots + |a_{n-1}| + |a_n|,$$

and by separating all such equations into a denumerable succession of classes, according as the index $N = 1, 2, 3, \ldots$ In no one of these equations can either the degree $n$ or the absolute value of any coefficient exceed the finite limit $N$, *so that, in every class, there can be only a finite number of equations, and hence, in particular, only a finite number of irreducible equations.* One can easily determine the coefficients by trying out all possible solutions for a given $N$ and can, in fact, write down at once the beginning of the series of equations for small values of $N$.

Now let us consider that, for each value of the index $N$, the real roots of the finite number of corresponding irreducible equations have been determined, and arranged according to size. Take first the roots, thus ordered, belonging to index one, then those belonging to index two, and so on, and number them in that order. *In this way we shall have shown, in fact, that the set of real algebraic numbers is denumerable,* for we come in this way to every real algebraic number and, on the other hand, we use all the positive integers. In fact one could, with sufficient patience, determine **[275]** say the 7563-rd algebraic number of the scheme, or the position of a given algebraic number, however complicated.

Here, again, our "denumeration" disturbs completely the natural order of the algebraic numbers, although that order is preserved among the numbers of like index. For example, two algebraic numbers so nearly equal as $2/5$ and $2001/5000$ have the widely separated indices 7 and 7001 respectively; whereas $\sqrt{5}$, as root of $x^2 - 5 = 0$, has the same index, 7, as $2/5$.

Before we go over to the last example, I should like to give you a small lemma, which will supply us with another denumerable set, as well as with a method of proof that will be useful to us later on. If we have *two* denumerable sets

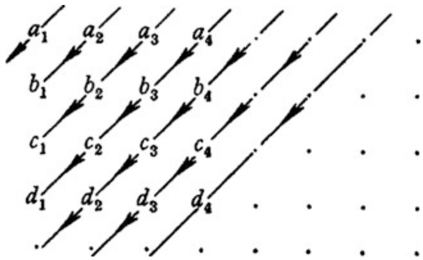
$$a_1, a_2, a_3, \ldots \quad \text{and} \quad b_1, b_2, b_3, \ldots,$$

then the set of all $a$ and all $b$ which arises by combining these two is also denumerable. For one can write this set as follows:

$$a_1, b_1, a_2, b_2, a_3, b_3, \ldots,$$

and we can at once set this into a one-to-one relation with the series of positive integers. *Similarly, if we combine 3, 4, ..., or any finite number of denumerable assemblages, we obtain likewise a denumerable set.*

But it does not seem quite so obvious, and this is to be our lemma, that *the combination of a denumerable infinity of denumerable assemblages yields also a denumerable assemblage.* To prove this, let us denote the elements of the first assemblage by $a_1, a_2, a_3, \ldots$, those of the second by $b_1, b_2, b_3, \ldots$, those of the third by $c_1, c_2, c_3, \ldots$, and so on, and let us imagine these set written under one another. Then we need only represent all the elements in the order as indicated by the successive diagonals, as indicated in the following scheme:




The resulting arrangement

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_1$ | $a_2$ | $b_1$ | $a_3$ | $b_2$ | $c_1$ | $a_4$ | $b_3$ | $c_2$ | $d_1$ | $a_5$ | ... |

**[276]** reaches ultimately every one of the numbers $a, b, c, \ldots$ and brings it into correspondence with just one definite positive integer, which proves the theorem. In view of this scheme one could call the process a "counting by diagonals".

## The Continuum Not Being Denumerable

The large variety of denumerable sets, which has thus been brought to our knowledge, might incline us to the belief that all infinite sets are denumerable. To show that this is not true we shall prove the second part of Cantor's theorem, namely, *that the continuum of all real numbers is certainly not denumerable*. We shall denote it by $\mathfrak{C}_1$ because we shall have occasion later to speak of multi-dimensional continua.

$\mathfrak{C}_1$ is defined as the *totality of all finite real values x*, where we may think of $x$ as an abscissa on a horizontal axis. We shall first show that the set of all inner points on the unit segment $0 < x < 1$ has the same power as $\mathfrak{C}_1$. If we represent the first set on the $x$-axis and the second on the $y$-axis, at right angles to it, then a one-to-one correspondence between them will be established by a rising monotone curve of the sort sketched in Fig. 121 (e.g., a branch of the curve $y = -(1/\pi) \cdot \tan^{-1} x$). It is permissible, therefore, to think of the assemblage of all real numbers between 0 and 1 as standing for $\mathfrak{C}_1$ and we shall do this from now on.

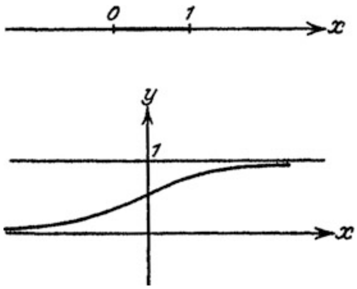
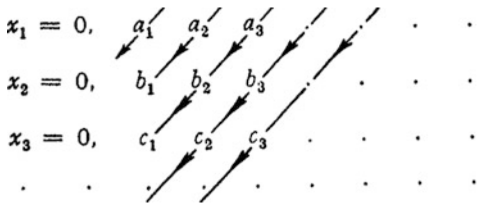



**Figure 121**

The proof by which I shall show you that $\mathfrak{C}_1$ is not denumerable is the one which Cantor gave in 1891 at the meeting of the natural scientists in Halle. It is clearer and more susceptible of generalization than the one, which he published in 1873. The essential thing in it is the so-called "diagonal process", by which a real number is disclosed that cannot possibly be contained in any assumed denumerable arrangement of all real numbers. This is a contradiction, and $\mathfrak{C}_1$ cannot, therefore, be denumerable.

We write all our numbers $0 < x < 1$ of $\mathfrak{C}_1$ as decimal fractions and think of them as forming a denumerable sequence




where $a, b, c$ are the digits $0, 1, \ldots, 9$ in every possible choice and arrangement. **[277]**
Now we must not forget that our decimal notation is not uniquely definite. In fact according to our definition of equality we have $0{,}999\ldots = 1{,}000\ldots$, and we could write every terminating decimal as a non-terminating one in which all the digits, after a certain one, would be nines. This is one of the first assumptions in calculating with decimal fractions (see p. [37]). In order, then, to have a unique notation, let us assume that we are employing only infinite, non-terminating decimal fractions; that all terminating ones have been converted into such as have an endless succession of nines; and that only infinite decimal fractions appear in our scheme above.

In order now to write down a decimal fraction $x'$ which shall be different from every real number in the table, we fix our attention on the digits $a_1, b_2, c_3, \ldots$ in the diagonal of the table (hence the name of the procedure). For the first decimal place of $x'$ we select a digit $a_1'$ different from $a_1$; for the second place a digit $b_2'$ different from $b_2$; for the third place a digit $c_3'$ different from $c_3$; and so on:

$$x' = 0,\ a_1'\, b_2'\, c_3' \ldots .$$

These conditions for $a_1', b_2', c_3', \ldots$ allow sufficient freedom to insure *that $x'$ is actually a proper decimal fraction, not, e.g., 0,999... = 1, and that it shall not terminate after a finite number of digits;* in fact, we can even select $a_1', b_2', c_3', \ldots$ always different from 9 and 0. Then $x'$ is *certainly different from* $x_1$ since they are unlike in the first decimal place/figure?, and two infinite decimal fractions can be equal only when they coincide in every decimal place?. Similarly $x' \neq x_2$, on account of the second place; $x' \neq x_3$ because of the third place; etc. *That is, $x'$ – a proper decimal fraction – is different from all the numbers $x_1, x_2, x_3, \ldots$ of the denumerable tabulation*. Thus the promised contradiction is achieved and we have *proved that the continuum $\mathfrak{C}_1$ is not denumerable*.

This theorem *assures us, a priori, the existence of transcendental numbers;* for the totality of algebraic numbers was denumerable and could therefore not exhaust the non-denumerable continuum of all real numbers. But, whereas all the earlier discussions exhibited only a *denumerable infinity of transcendental numbers*, it follows here that the potency of this set is actually greater, so that it is only now that we get the correct general understanding. To be sure, those special examples are of
**[278]** service in giving life to an otherwise somewhat abstract picture[175].

**Potency of Continua of More Dimensions**

Now that we have disposed of the one-dimensional continuum it is very natural to inquire about the *two-dimensional* continuum. Everybody had supposed that there were more points in the plane than in the straight line, and it attracted therefore much attention when Cantor showed[176] that the potency of the two-dimensional continuum $\mathfrak{C}_2$ was exactly the same as that of the one-dimensional $\mathfrak{C}_1$. Let us take for $\mathfrak{C}_2$ the square with side of unit length, and for $\mathfrak{C}_1$ the unit segment (see Fig. 122). We shall show that the points of these two figures can be put into a one-to-one relation. The fact that this statement seems so paradoxical depends probably on our difficulty in freeing our mental picture of a *certain continuity in the correspondence*. But the relation, which we shall establish, will be as *discontinuous* or, if you please, *as inorganic as it is possible to be*. It will disturb everything which one thinks of as characteristic for the plane and the linear manifold as such, with the exception of the "potency". It will be as though one put all the points of the square into a sack and shook them up thoroughly.

---

175 [The existence of transcendental numbers was first proved by Joseph Liouville; in an article which appeared in 1851 in vol. 16, series 1, of the *Journal des mathématiques pures et appliquées*, he gave entirely elementary methods for constructing such numbers.]

176 „Ein Beitrag zur Mannigfaltigkeitslehre", *Journal für reine und angewandte Mathematik*, vol. 84 (1878), 242-.258.

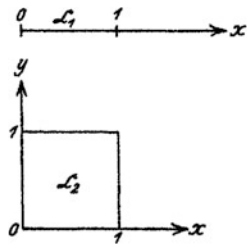


**Figure 122**

The set of the points of the square coincides with *that of all pairs of decimal fractions*

$$x = 0, a_1 a_2 a_3 \ldots, \quad y = 0, b_1 b_2 b_3 \ldots,$$

*all of which we shall suppose to be non-terminating.* We exclude points on the boundary for which one of the coordinates $(x, y)$ vanishes, i.e., we exclude the two sides, which meet at the origin, but we include the other two sides. It is easy to show that this has no effect on the potency. The fundamental idea of the Cantor proof is to combine these two decimal fractions into a new decimal fraction $z$ from which one can obtain $(x, y)$ again uniquely and which will take just once all the values $0 < z \leqq 1$ when the point $(x, y)$ traverses the square once. If we then think of $z$ as an abscissa, we have the desired one-to-one correspondence between the square $\mathfrak{C}_2$ and the segment $\mathfrak{C}_1$, whereby the agreement concerning the square carries with it the inclusion of its end point $z = 1$ of the segment.

One might try to effect this combination by setting

$$z = 0, a_1 b_1 a_2 b_2 a_3 b_3 \ldots,$$

from which one could in fact determine $(x, y)$ uniquely by detaching the odd and even decimal places respectively. But there is an *objection to this, due to the ambiguous notation for decimal fractions.* This $z$, namely, would not traverse the *whole* of $\mathfrak{C}_1$ when we chose for $(x, y)$ all possible pairs of non-terminating decimal fractions, that is, when we traversed all the points of $\mathfrak{C}_2$. For, although $z$ is, to be sure, always non-terminating, there can be non-terminating values of $z$, such as **[279]**

$$z = 0, c_1 c_2 0 c_4 0 c_6 0 c_8 \ldots,$$

which correspond only to a terminating $x$ or $y$, in the present case to the values

$$x = 0, c_1 000 \ldots, \quad y = 0, c_2 c_4 c_6 c_8 \ldots$$

This difficulty is best overcome by means of a device suggested by Julius König of Budapest. He thinks of the $a, b, c$ not as individual digits but as *complexes of digits* – one might call them *"molecules" of the decimal fraction.* A "molecule" *consists of a single digit, different from zero, together with all the zeros, which immediately precede it.* Thus every non-terminating decimal must contain an *infinity* *of molecules*, since digits different from zero must always recur; and conversely. As an example, in

$$x = 0{,}320\,8007\,000\,302\,405\ldots$$

we should take as molecules $a_1 = [3]$, $a_2 = [2]$, $a_3 = [08]$, $a_4 = [007]$, $a_5 = [0003]$, $a_6 = [02]$, $a_7 = [4], \ldots$

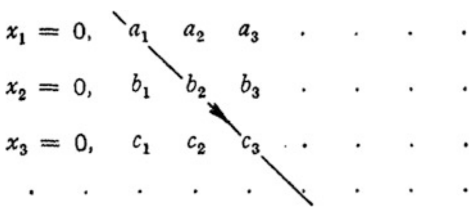
Now let us suppose, in the above rule for the relation between $x$, $y$ and $z$, that the $a, b, c$ *stand for such molecules*. Then there will correspond uniquely to every pair $(x, y)$ a non-terminating $z$ which would, in its turn, determine $x$ and $y$. But now every $z$ breaks up into an $x$ and a $y$ each with infinity of molecules, and each $z$ appears therefore just once when $(x, y)$ run through all possible pairs of non-terminating decimal fractions. This means, however, that the *unit segment and the square have been put into one-to-one correspondence, i.e., they have the same potency.*

In an analogous way, of course, it can be shown *that also the continuum of 3, 4, ... dimensions has the same potency as the one-dimensional segment.* It is more remarkable, however, that the continuum $\mathfrak{C}_\infty$, of infinitely many dimensions, or more exactly, of infinitely denumerable dimensions, has also the same potency. This infinite-dimensional space is defined as the totality of the systems of values, which can be assumed by the denumerable infinity of variables

$$x_1, x_2, \ldots, x_n, \ldots$$

when each, independently of the others, takes on all real values. This is really only a new form of expression for a concept that has long been in use in mathematics. When we talk of the totality of all power series or of all trigonometric series, we
**[280]** have, in the denumerable infinity of coefficients, really nothing but so many independent variables, which, to be sure, are for purposes of calculation restricted by certain requirements to ensure convergence.

Let us again confine ourselves to the "*unit cube*" of the $\mathfrak{C}_\infty$, i.e., to the totality of points, which are subject to the condition $0 < x_n \leqq 1$, and show that they can be put into one-to-one relation with the points of the unit segment $0 < z \leqq 1$ of $\mathfrak{C}_1$. For convenience, we exclude again all boundary points for which one of the coordinates $x_n$ vanishes, as well as the end point $z = 0$, but admit the others. As before we start with the decimal fractional representation of the coordinates in $\mathfrak{C}_\infty$:




where we assume that the decimal fractions are all written *in non-terminating form*, and furthermore that the $a$, $b$, $c$, ... are "*decimal fraction molecules*" in the sense indicated above, i.e., digit complexes which end with a digit, which is different from zero, but which is preceded exclusively by zeros. Now we must combine all these infinitely many decimal fractions into a new one, which will permit recognition of its components; or, if we keep to the chemical figure, we wish to form such a loose alloy of these molecular aggregates that we can easily separate out the components. This is possible by means of the "*diagonal process*" which we applied before (p. [275] et seq.). From the above table we get, according to that plan

$$z = 0,\ a_1 a_2 b_1 a_3 b_2 c_1 a_4 b_3 c_2 d_1 a_5 \ldots,$$

which relates uniquely a point of $\mathfrak{C}_1$ to each point of $\mathfrak{C}_\infty$. Conversely we get in this way *every* point $z$ of $\mathfrak{C}_1$ for from the non terminating decimal fraction for a given $z$ we can derive, according to the above given scheme, an infinity of non-terminating decimals $x_1, x_2, x_3, \ldots,$ out of which this $z$ would arise by the method indicated. *We have succeeded therefore in setting up a one-to-one correspondence between the unit cube in* $\mathfrak{C}_\infty$ *and the unit segment in* $\mathfrak{C}_1$.

Our results thus far show that *there are at least two different potencies*:

1. That of the denumerable sets.
2. That of all continua ($\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3, \ldots,$ including $\mathfrak{C}_\infty$. **[281]**

## Sets with Higher Potencies

The question naturally arises whether there are still *larger potencies*. The answer is that one can exhibit a still higher potency, not merely as a result of abstract reasoning, but one lying quite within the range of concepts, which one is anyway using in mathematics. This set is, namely:

3. that of all possible real functions $f(x)$ of a real variable $x$.

It will be sufficient for our purpose to restrict the variable to the interval $0 < x < 1$. It is natural to think first of the set of *continuous* functions $f(x)$, but there is a remarkable theorem, which states *that the totality of all continuous functions has the same potency as the continuum, and belongs therefore in group* 2. We can reach a new, a higher potency, only by admitting discontinuous functions of the most general kind imaginable, i.e., where the function value at any place $x$ is entirely arbitrary and has no relation to neighbouring values.

I shall first prove the *claim concerning the set of continuous functions*. This will involve a repetition and a refinement of the considerations, which we adduced (p. [222]) in order to make plausible the possibility of expanding "arbitrary" functions into trigonometric series. At that time I remarked:

a) *A continuous function* $f(x)$ *is determined if one knows the values* $f(r)$ *at all rational values of* $r$.

b) We know now that *all rational values* $r$ *can be brought into a denumerable series* $r_1, r_2, r_3, \ldots$

c) Consequently $f(x)$ is determined when one knows the denumerable infinity of quantities $f(r_1), f(r_2), f(r_3), \ldots$ Moreover, these values cannot, of course, be assumed arbitrarily if we are to have a univocal continuous function. *The set then of* *all possible systems of values $f(r_1), f(r_2), \ldots$ must contain a subset whose potency is the same as that of the set of all continuous functions* (see Fig. 123).

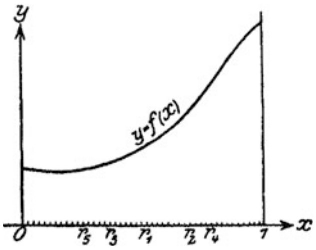



**Figure 123**

d) Now the magnitudes $f_1 = f(r_1), f_2 = f(r_2), \ldots$ can be considered as the coordinates of a $\mathfrak{C}_\infty$, since they make up a denumerable infinity of continuously varying magnitudes. Hence, in view of the theorem already proved, the *totality of all their possible systems of values has the potency of the continuum.*

e) As a subset of this set, which can be mapped one-to-one to the continuum, the set of all continuous functions can be mapped to a subset of the continuum.

f) *But it is not hard to see that, conversely, the entire continuum can be put*
**[282]** *into one-to-one correspondence with a subset of all continuous functions*. For this purpose, we need to consider only the functions defined by $f(x) = k =$ const., where $k$ is a real parameter. If $k$ traverses the continuum $\mathfrak{C}_1$ then $f(x)$ will traverse a subset of all continuous functions, which is in one-to-one correspondence with $\mathfrak{C}_1$.

g) Now we must make use of an important general theorem of set theory, the so-called *theorem of equivalence*, due to *Felix Bernstein*[177]: *If each of two sets is equivalent to a subset of the other then the two sets are equivalent.* This theorem is very plausible. The proof of it would take us too far afield.

h) According to e) and f) the continuum $\mathfrak{C}_1$ and the set of all continuous functions satisfy the conditions of the theorem of equivalence. They are therefore of like potency, and our theorem is proved.

Let us now go over to the proof of our first claim, that the set of all possible functions that are really "*entirely arbitrary*" has a potency higher than that of the continuum. The proof is an immediate application of Cantor's diagonal procedure:

a) Assume *our claim to be false*, i.e., that the set of all functions can be put into one-to-one correspondence with the continuum $\mathfrak{C}_1$. Suppose now, in this one-to-one relation, that the *function $f(x, v)$ of $x$ corresponds to each point $x = v$ in* $\mathfrak{C}_1$, so that, while $v$ traverses the continuum $\mathfrak{C}_1$, $f(x, v)$ represents all possible

---

[177] First published in: Émile Borel, *Leçons sur la Théorie des Fonctions,* Paris, 1898, p. 103 et seq.

functions of $x$. We shall reduce this supposition to an absurdity by actually setting up a *function $F(x)$, which is different from all such functions $f(x, v)$*.

b) For this purpose we construct the "*diagonal function*" of the tabulation of the $f(x, v)$, i.e., that function which, for every value $x = x_0$, has that value which the assumed correspondence imposes upon $f(x, v)$ when the parameter $v$ also has the value $v = x_0$, namely $f(x_0, x_0)$. Written as a function of $x$, this is simply the function $f(x, x)$.

c) Now we construct a *function F(x) which for every x is different from this $f(x, x)$*:

$$F(x) \neq f(x, x) \quad \text{for every } x.$$

We can do this in the greatest variety of ways, since we definitely admit discontinuous functions, whose value at any point can be arbitrarily determined. We might, for *example*, put

$$F(x) = f(x, x) + 1.$$

d) *This $F(x)$ is actually different from every one of the functions $f(x, v)$*. For, if $F(x) = f(x, v_0)$ for some $v = v_0$, the equality would hold also for $x = v_0$; **[283]** that is, we should have $F(v_0) = f(v_0, v_0)$, which contradicts the assumption in c) concerning $F(x)$.

The assumption a) that the functions $f(x, v)$ could exhaust all functions is thus overthrown, and *our claim is proved*.

It is interesting to compare this proof with the analogous one for the non-denumerability of the continuum. There we assumed the totality of decimal fractions arranged in a denumerable schema; here we consider the function scheme $f(x, v)$. The singling out there of the diagonal elements corresponds to the construction here of the diagonal function $f(x, x)$; and in both cases the application was the same, namely the setting up of something new, i.e., not contained in the schema – in the one case a decimal fraction, in the other a function.

You can readily imagine that *similar considerations could lead us to sets of ever increasing potency* – beyond the three, which we have already discussed. The most noteworthy thing in all these results is that there *remain any abiding distinctions and gradations at all in the different infinite sets*, notwithstanding our having subjected them to the most drastic treatment imaginable; treatment which deleted all their special properties, such as order, and permitted only the ultimate elements, quasi their atoms, to retain an independent existence as things, which could be tossed about in the most arbitrary manner. And it is worth noting that *three of these gradations*, which we did establish, *were among concepts, which have long been familiar in mathematics* – integers, continua, and functions.

With this I shall close this first part of my set-theoretic discussion, which has been devoted mainly to the concept of potency. In a similar concrete manner, but with still greater brevity, I shall now tell you something about a *farther section of this theory*.

## *2. Arrangement of the Elements of a Set*

We shall now bring to the front just that thing which we have heretofore purposely neglected, the question, namely, *how individual sets of the same potency differ from one another* by virtue of those relations as to the arrangement of the elements which are intrinsic to each set. The most general one-to-one representations, which we have admitted thus far deleted all these relations – think only of the representation of the square upon the segment. I desire to emphasise, especially, the *significance of precisely this chapter of set theory*. It cannot possibly be the purpose of set theory to banish the differences, which have long been so familiar in mathematics,
**[284]** by introducing new concepts of a most general kind. On the contrary, this theory can and should aid us to understand those differences in their deepest essence, by focussing on their properties from a more general standpoint.

### Types of Arrangement of Denumerable Sets

We shall try to make clear the *different possible arrangements*, by considering definite familiar examples. Beginning with denumerable sets, we note *three forms of fundamentally different arrangement*, so different that the equivalence of their potencies was, as we saw, the result of a special and by no means obvious theorem. These examples are:

1. The set of all positive integers.
2. The set of all (negative and positive) integers.
3. The set of all rational numbers and that of all algebraic numbers.

All these sets have at first the one common property in the arrangement of their elements, which finds expression in the designation *simply ordered*, i. e., *of two given elements, it is always known, which precedes the other*, or, put algebraically, which is the smaller and which the greater. Further, if three elements $a, b, c$ are given, then, if $a$ precedes $b$ and $b$ precedes $c$, $a$ precedes $c$ (if $a < b$ and $b < c$ then $a < c$).

But now as to the *characteristic differences.* In (1), there is a *first element* (one) which precedes all the others, but no last, which follows all the others; in (2), there is *neither a first nor a last element*. Both (1) and (2) have this in common, that *every element is followed by another definite one, and also that every element* [*except the first in* (1)] *is preceded by another definite one*. In contrast with this, we find in (3) (as we saw p. [33]) that *between any two elements there are always infinitely many others* – the elements are "*everywhere dense*", so that *among the rational or the algebraic numbers lying between a and b* (*a* and *b* themselves not counted) *there is neither a smallest nor a largest*. The manner of arrangement in these three examples, the *type of arrangement* (Cantor's term *type of order* seems to me less expressive) is different, although the potency is the same. One could raise *the question here as to all the types of arrangement that are possible in denumerable sets,* and that is what researchers on set theory actually do.

Let us now consider sets having the potency of the continuum. We know a simply ordered set, namely the continuum $\mathfrak{C}_1$ of all real numbers. but in the multi-dimensional types $\mathfrak{C}_2, \mathfrak{C}_3, \ldots$ we have examples of an order no longer simple. In the case of $\mathfrak{C}_2$, for instance, two relations are necessary, instead of one, to determine the mutual position of two points.

## The Continuity of the Continuum [285]

The most important thing here is to analyse the *concept of continuity for the one-dimensional continuum.* The recognition of the fact that continuity here depends on simple properties of the arrangement which is peculiar to $\mathfrak{C}_1$, is the first great achievement of set theory toward the clarifying of the traditional mathematical concepts. It was found, namely, that all the continuity properties of the ordinary continuum flow from its being a simply-ordered set with the following two properties:

1. *If we separate the set into two parts A, B such that every element belongs to one of the two parts and all the elements of A precede all those of B, then either A has a last element or B a first element.* If we recall Dedekind's definition of irrational number (see p. [36] et seq.) we can express this by saying that every "cut" in our set is produced by an actual element of the set.

2. *Between any two elements of the set there are always infinitely many others.*

This second property is common to the continuum and the denumerable set of all rational numbers. It is the first property however that marks the distinction between the two. In set theory it is customary to call all simply-ordered sets *continuous* if they possess the two preceding properties, for it is actually possible to prove for them all the theorems which hold for the continuum by virtue of its continuity.

Let me remind you that these properties of continuity can be formulated somewhat differently in terms of *Cantor's fundamental series.* A fundamental series is a simply-ordered denumerable series of elements $a_1, a_2, a_3, \ldots$ of a set such that each element of the series precedes the following or each succeeds it:

$$a_1 < a_2 < a_3 < \ldots \quad \text{or} \quad a_1 > a_2 > a_3 > \ldots$$

An element $a$ of the set is called a *limit element of the fundamental series if* (*in the first sort*) *every element, which precedes a, but no element which follows a is ultimately passed by elements of the fundamental series;* and similarly for the second sort. Now if every fundamental series in a set has a limit element, the set is called *closed;* if, conversely, every element of the set is a limit element of a fundamental series, the set is said to be *dense in itself.* Now continuity, in the case of sets having the potency of the continuum, consists essentially in the union of these two properties.

Let me remind you incidentally that when we were discussing the foundations of the calculus we spoke also of another continuum, the *continuum of Veronese*, which arose from the usual one by the addition of actually infinitely small quantities. This [286] continuum constitutes a simply-ordered set in as much as the succession of any two elements is determinate, but it has a type of arrangement entirely different from that of the customary $\mathfrak{C}_1$; even the theorem that every fundamental series has a limit element no longer holds in it.

### Invariance of Dimension for Continuous One-to-One Representations

We come now to the important question as to what representations preserve the distinctions among the continua $\mathfrak{C}_1, \mathfrak{C}_2, \ldots$ of different dimensions. We know, indeed, that the most general one-to-one representation obliterates every distinction. We have here the important theorem that *the dimension of the continuum is invariant with respect to every continuous one-to-one representation, i.e., that it is impossible to effect a reversibly unique and continuous mapping of a* $\mathfrak{C}_m$ *upon a* $\mathfrak{C}_n$ *where* $m \neq n$. One might be inclined to accept this theorem, without further ado, as self evident; but we must recall that naïve intuition seemed to exclude the possibility of a reversibly unique mapping of $\mathfrak{C}_2$ upon $\mathfrak{C}_1$, and this should dispose us to caution in accepting its conclusions.

I shall discuss in detail only the simplest case[178], which concerns the relation between the one-dimensional and the two-dimensional continuum and I shall then indicate the difficulties in the way of an extension to the most general case. We shall prove, then, that *a reversibly unique, continuous relation between* $\mathfrak{C}_1$ *and* $\mathfrak{C}_2$ *is not possible.* Every word here is essential. We have seen, indeed, that we may not omit continuity; and that reversible uniqueness may not be omitted is shown by the example of the "Peano curve" which is doubtless familiar to some of you.

We shall need the following lemma: *Given two one-dimensional continua* $\mathfrak{C}_1, \mathfrak{C}_1'$ *which are mapped continuously upon each other so that to every element of* $\mathfrak{C}_1'$ *there corresponds one and but one element of* $\mathfrak{C}_1$ *and to every element of* $\mathfrak{C}_1$ *there corresponds at most one element of* $\mathfrak{C}_1'$; if, then, $a, b$ are two elements of $\mathfrak{C}_1$ to which two elements $a', b'$ in $\mathfrak{C}_1$ actually correspond, respectively, it follows that to every element $c$ of $\mathfrak{C}_1$ lying between $a$ and $b$ there will correspond an element $c'$ of $\mathfrak{C}_1'$ which lies between $a'$ and $b'$ (see Fig. 124). This claim is analogous to the familiar theorem that a continuous function $f(x)$ which takes two values $a$, $b$ at the points $x = a', b'$ must take a value $c$, chosen arbitrarily between $a$ and $b$, at some value $c'$ between $a'$ and $b'$; and it could be proved as an exact generalisation of this theorem, by using only the above definition of continuity. This would require one also to explain continuous mapping of continuous sets in a manner analogous to
**[287]** the usual definition of continuous functions, and it can be done with the aid of the concept of arrangement. But this is not the place to amplify these hints.

[178] Luitzen Egbertus Jan Brouwer gave a proof for the general case in 1911, in volume 71, of the general case: "Über Abbildung von Mannigfaltigkeiten", 97–115.

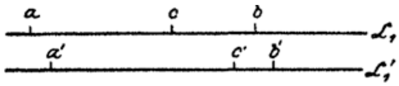



**Figure 124**

We shall give *our* proof as follows. We assume that a continuous reversibly unique mapping of the one-dimensional segment $\mathfrak{C}_1$ upon the square $\mathfrak{C}_2$ has been effected (see Fig. 125). Hence two elements $a, b$ on $\mathfrak{C}_1$ should correspond to the elements $A, B$, respectively, of $\mathfrak{C}_2$. Now we can join these elements $A, B$ by two different paths within $\mathfrak{C}_1$, e.g., by the stepped path $\mathfrak{C}_1', \overline{\mathfrak{C}_1'}$ drawn in the figure. To do this, it is not necessary to presuppose any special properties of $\mathfrak{C}_2$, such as the determination of a coordinate system; we need merely use the concept of double order. Each of the paths $\mathfrak{C}_1'$ and $\overline{\mathfrak{C}_1'}$ will be a simply-ordered one-dimensional continuum like $\mathfrak{C}_1$, and because of the continuous reversibly unique relation between $\mathfrak{C}_1$ and $\mathfrak{C}_2$ there must correspond just one point on $\mathfrak{C}_1$ to each element of $\mathfrak{C}_1'$ and $\overline{\mathfrak{C}_1'}$; but to-each element of $\mathfrak{C}_1$ there must correspond at most one on $\mathfrak{C}_1'$ or $\overline{\mathfrak{C}_1'}$. In other words, we have precisely the conditions of the above lemma, and it follows that to every point $c$ in $\mathfrak{C}_1$ between $a$ and $b$ there corresponds not only a point $c'$ of $\mathfrak{C}_1$ but also a point $\overline{c'}$ of $\overline{\mathfrak{C}_1'}$. But this contradicts the assumed reversible uniqueness of the mapping from $\mathfrak{C}_1$ to $\mathfrak{C}_2$. *Consequently this mapping is not possible and the theorem is proved.*

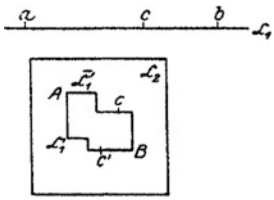



**Figure 125**

If one wished to extend these considerations to two arbitrary continua $\mathfrak{C}_m, \mathfrak{C}_n$, it would be necessary to know in advance something about the constitution of continua of general nature and of dimension $1, 2, 3, \ldots, m-1$, which can be embedded in $\mathfrak{C}_m$. As soon as $m, n \geqq 2$, one cannot get along merely with the concept "between" as we could in the simplest case above. On the contrary, one is led to very difficult investigations, which include, among the earliest cases, the overly difficult questions, fundamental for geometry, concerning the most general continuous one-dimensional points sets in the plane, questions which only recently have been somewhat cleared up. One of these interesting questions is as to when such a point set should be considered as a *curve*.

## *Closing Remarks*

### Importance and Goals of Set Theory

I shall close with this my very special discussion of set theory, in order to add *a few remarks of a general nature*. First, a word as to the general notions, which Cantor had developed concerning the *position of set theory with reference to geometry and analysis*. These notions exhibit set theory in a special light. The difference between the *discrete magnitudes of arithmetic and the continuous magnitudes of geometry* **[288]** has always had a prominent place in history and in philosophical speculations. *In recent times the discrete magnitude, as conceptually the easiest to be grasped, has come into the foreground*. According to this tendency we look upon natural numbers, integers, as the simplest given concepts; we derive from them in the familiar way, rational and irrational numbers, and we construct the complete apparatus for the control of geometry by means of analysis, namely, analytic geometry. This tendency of modern development can be called that of *arithmetising geometry*. *The geometric idea of continuity is reduced to the idea of whole numbers*. This lecture course has, in the main, held to this direction.

Now, as opposed to this one-sided preference for integers, Cantor would (as he himself told me in 1903 at the meeting of the natural scientists in Cassel) achieve, *by set theory, "the genuine fusion of arithmetic and geometry"*. Thus the theory of integer numbers, on one hand, as well as the theory of different point continua, on the other, and much more, would constitute parallel chapters on an equal footing of a general theory of sets.

I shall add a few general remarks concerning the relation of set theory to geometry. In our discussion of set theory we have considered:

1. The *potency of a set* as something that is unchanged by any reversibly unique mapping.

2. *Types of order of sets*, which take account of the relations among the elements as to order. We were able here to characterise the concept of continuity, the different multiple arrangements or multidimensional continua, etc., so that the *invariants of continuous mappings* found their place here. When carried over to geometry, this gives the branch which, since Riemann, has been called *analysis situs*, that most abstract chapter of geometry, which treats those properties of geometric configurations, which are invariant under the most general reversibly unique continuous mappings. Riemann had used the word manifold (*Mannigfaltigkeit*) in a very general sense. Cantor used it also, at first, but replaced it later by the more convenient word set (*Menge*).

3. If we go over to *concrete geometry* we come to such differences as that between *metric* and *projective* geometry. It is not enough here to know, say, that the straight line is one-dimensional and the plane two-dimensional. We desire rather to *construct or to compare figures*, for which we have to dispose of a fixed *unit of* **[289]** *measure* or at least construct a *line in the plane, or a plane in space*. In each of these concrete domains it is necessary, of course, to add a *special axiomatics to the*

*general properties of arrangement*. This implies, of course, a further development of the theory of simply-ordered, doubly-ordered, .... *n*-tuply-ordered, continuous sets.

This is not the place for me to go into these things in detail, especially since they must be taken up anyway in the following volumes of the present work.[179] I shall merely mention literature in which you can inform yourselves farther. Here, above all, I should speak of the reports in the *Mathematische Enzyklopädie*: Federico Enriques, *Prinzipien der Geometrie* (III. A. B. 1) and Hans von Mangoldt, *Die Begriffe „Linie" und „Fläche"* (III. A. B. 2), which treat mainly the subject of axioms; also Max Dehn-Poul Heegaard, *Analysis situs* (III. A. B. 3). The last article is written in rather abstract form. It begins with the most general formulation of the concepts and fundamental facts of analysis situs, as these were set up by Dehn himself, from which everything else is deduced then by pure logic. This is in direct opposition to the inductive method of presentation, which I always recommend. The article can be fully understood only by an advanced reader who has already thoroughly worked the subject through inductively.

As to literature concerning set theory, I should mention, first of all, the report made by Arthur Schoenflies to the Deutsche Mathematikervereinigung, entitled: *Die Entwickelung der Lehre von den Punktmannigfaltigkeiten*[180]. The first part appeared in volume 8 of the *Jahresbericht der deutschen Mathematikervereinigung;* the second appeared recently as a second supplementary volume to the *Jahresbericht*. This work is really a report on the entire set theory, in which you will find information concerning numerous details. Alongside of this, I would mention the first systematic textbook on set theory: *The Theory of Sets of Points*, by William Henry Young and his wife, Grace Chisholm Young (whom we mentioned p. [194]).

In concluding this discussion of the theory of assemblages we must again put the question, which accompanies our entire lecture course: *What of this can one use in the schools?* From the standpoint of mathematical pedagogy, we must of course protest against putting such abstract and difficult things before the pupils too early.[181] In order to give precise expression to my own view on this point,

---

[179] [Transl. note: The following two paragraphs are contained in the thirs edition of 1924 but no longer in the fourth of 1933. It is reasonable to maintain these two paragraphs, which had been included in the American translation.]

[180] 2 parts, Leipzig 1900 and 1908, A revision of the first half appeared in 1913 under the title: *Entwickelung der Mengenlehre und ihrer Anwendungen;* as a continuation of this, see H. Hahn: *Theorie der reellen Funktionen,* vol. I, Berlin, 1921.

[181] [Translator's note: Klein changed this part considerably over the various editions. In the first edition, of 1908, Klein had sharply criticised the first schoolbook ever published including set theory: it was „Elemente der Arithmetik and Algebra", by Friedrich Meyer, published in Halle in 1885, even before Cantor's complete publication of his new theory. Meyer, a friend of Cantor and teacher at a Gymnasium in Halle, was criticised for developing school mathematics deductively, and for starting from set theory, and arriving at the first concrete mathematical issues, only after many pages of deductive reasoning, (Klein 1908, 599). Since various readers had protested against Klein's verdict on Meyer – in particular Wilhelm Lorey who cooperated strongly with Klein – Klein introduced an addendum in the second edition: he gave credit to the high teaching qualities of Meyer as had been reported to him (Klein 1911, p. 613 et seq.). See: Gert Schubring,

I should like to bring forward the *biogenetic fundamental law*, according to which the individual in his development goes through, in an abridged series, all the stages in the development of the species. Such thoughts have become today part and parcel
[290] of the general culture of everybody. Now, I think that instruction in mathematics, as well as in everything else, should follow this law, at least in general. *Taking into account the native ability of youth, instruction should guide it slowly to higher things, and finally to abstract formulations; and in doing this it should follow the same road along which the human race has striven from its naïve original state to higher forms of knowledge*. It is necessary to formulate this principle frequently, for there are always people who, after the fashion of the mediaeval scholastics, begin their instruction with the most general ideas, defending this method as the "only scientific one". And yet this justification is based on anything but truth. *To instruct scientifically can only mean to induce the person to think scientifically, but by no means to confront him, from the beginning, with cold, scientifically polished systematics*.

An essential obstacle to the spreading of such a natural and truly scientific method of teaching is the *lack of historical knowledge*, which so often makes itself felt. In order to combat this, I have made a point of introducing historical remarks into my presentation. By doing this I trust I have made it clear to you how slowly all mathematical ideas have come into being; how they have nearly always appeared first in rather prophetic form, and only after long development have crystallized into the rigid form so familiar in systematic presentation! It is my earnest hope that this knowledge („*Erkenntnis*") may exert a lasting influence upon the character of your own teaching.

---

„Historische Begriffsentwicklung und Lernprozeß aus der Sicht neuerer mathematik-didaktischer Konzeptionen (Fehler, "Obstacles", Transposition)", *Zentralblatt für Didaktik der Mathematik*, 1988, *20*, 138–148. In the third edition however, Klein had deleted the names and publications mentioning the position he had criticised.]