A HALF-CENTURY OF MATHEMATICS

HERMANN WEYL, Institute for Advanced Study

1. Introduction. Axiomatics. Mathematics, beside astronomy, is the oldest of all sciences. Without the concepts, methods and results found and developed by previous generations right down to Greek antiquity, one cannot understand either the aims or the achievements of mathematics in the last fifty years. Mathematics has been called the science of the infinite; indeed, the mathematician invents finite constructions by which questions are decided that by their very nature refer to the infinite. That is his glory. Kierkegaard once said religion deals with what concerns man unconditionally. In contrast (but with equal exaggeration) one may say that mathematics talks about the things which are of no concern at all to man. Mathematics has the inhuman quality of starlight, brilliant and sharp, but cold. But it seems an irony of creation that man's mind knows how to handle things the better the farther removed they are from the center of his existence. Thus we are cleverest where knowledge matters least: in mathematics, especially in number theory. There is nothing in any other science that, in subtlety and complexity, could compare even remotely with such mathematical theories as for instance that of algebraic class fields. Whereas physics in its development since the turn of the century resembles a mighty stream rushing on in one direction, mathematics is more like the Nile delta, its waters fanning out in all directions. In view of all this: dependence on a long past, other-worldliness, intricacy, and diversity, it seems an almost hopeless task to give a non-esoteric account of what mathematicians have done during the last fifty years. What I shall try to do here is, first to describe in somewhat vague terms general trends of development, and then in more precise language explain the most outstanding mathematical notions devised, and list some of the more important problems solved, in this period.

One very conspicuous aspect of twentieth century mathematics is the enormously increased role which the axiomatic approach plays. Whereas the axiomatic method was formerly used merely for the purpose of elucidating the foundations on which we build, it has now become a tool for concrete mathematical research. It is perhaps in algebra that it has scored its greatest successes. Take for instance the system of real numbers. It is like a Janus head facing in two directions: on the one side it is the field of the algebraic operations of addition and multiplication; on the other hand it is a continuous manifold, the parts of which are so connected as to defy exact isolation from each other. The one is the algebraic, the other the topological face of numbers. Modern axiomatics, simple-minded as it is (in contrast to modern politics), does not like such ambiguous mixtures of peace and war, and therefore cleanly separated both aspects from each other.

In order to understand a complex mathematical situation it is often convenient to separate in a natural manner the various sides of the subject in question, make each side accessible by a relatively narrow and easily surveyable group of notions and of facts formulated in terms of these notions, and finally return to the whole by uniting the partial results in their proper specialization. The last synthetic act is purely mechanical. The art lies in the first, the analytic act of suitable separation and generalization. Our mathematics of the last decades has wallowed in generalizations and formalizations. But one misunderstands this tendency if one thinks that generality was sought merely for generality's sake. The real aim is simplicity: every natural generalization simplifies since it reduces the assumptions that have to be taken into account. It is not easy to say what constitutes a natural separation and generalization. For this there is ultimately no other criterion but fruitfulness: the success decides. In following this procedure the individual investigator is guided by more or less obvious analogies and by an instinctive discernment of the essential acquired through accumulated previous research experience. When systematized the procedure leads straight to axiomatics. Then the basic notions and facts of which we spoke are changed into undefined terms and into axioms involving them. The body of statements deduced from these hypothetical axioms is at our disposal now, not only for the instance from which the notions and axioms were abstracted, but wherever we come across an interpretation of the basic terms which turns the axioms into true statements. It is a common occurrence that there are several such interpretations with widely different subject matter.

The axiomatic approach has often revealed inner relations between, and has made for unification of methods within, domains that apparently lie far apart. This tendency of several branches of mathematics to coalesce is another conspicuous feature in the modern development of our science, and one that goes side by side with the apparently opposite tendency of axiomatization. It is as if you took a man out of a milieu in which he had lived not because it fitted him but from ingrained habits and prejudices, and then allowed him, after thus setting him free, to form associations in better accordance with his true inner nature.

In stressing the importance of the axiomatic method I do not wish to exaggerate. Without inventing new constructive processes no mathematician will get very far. It is perhaps proper to say that the strength of modern mathematics lies in the interaction between axiomatics and construction. Take algebra as a representative example. It is only in this century that algebra has come into its own by breaking away from the one universal system Ω of numbers which used to form the basis of all mathematical operations as well as all physical measurements. In its newly-acquired freedom algebra envisages an infinite variety of "number fields" each of which may serve as an operational basis; no attempt is made to embed them into the one system Ω. Axioms limit the possibilities for the number concept; constructive processes yield number fields that satisfy the axioms.

In this way algebra has made itself independent of its former master analysis and in some branches has even assumed the dominant role. This development in mathematics is paralleled in physics to a certain degree by the transition from classical to quantum physics, inasmuch as the latter ascribes to each physical structure its own system of observables or quantities. These quantities are subject to the algebraic operations of addition and multiplication; but as their multiplication is non-commutative, they are certainly not reducible to ordinary numbers.

At the International Mathematical Congress in Paris in 1900 David Hilbert, convinced that problems are the life-blood of science, formulated twenty-three unsolved problems which he expected to play an important role in the development of mathematics during the next era. How much better he predicted the future of mathematics than any politician foresaw the gifts of war and terror that the new century was about to lavish upon mankind! We mathematicians have often measured our progress by checking which of Hilbert's questions had been settled in the meantime. It would be tempting to use his list as a guide for a survey like the one attempted here. I have not done so because it would necessitate explanation of too many details. I shall have to tax the reader's patience enough anyhow.

PART I. ALGEBRA. NUMBER THEORY. GROUPS.

2. Rings, Fields, Ideals. Indeed, at this point it seems impossible for me to go on without illustrating the axiomatic approach by some of the simplest algebraic notions. Some of them are as old as Methuselah. For what is older than the sequence of *natural numbers* $1, 2, 3, \cdots$, by which we count? Two such numbers a, b may be added and multiplied ($a + b$ and $a \cdot b$). The next step in the genesis of numbers adds to these positive *integers* the negative ones and zero; in the wider system thus created the operation of addition permits of a unique inversion, subtraction. One does not stop here: the integers in their turn get absorbed into the still wider range of *rational numbers* (fractions). Thereby division, the operation inverse to multiplication, also becomes possible, with one notable exception however: division by zero. (Since $b \cdot 0 = 0$ for every rational number b, there is no inverse b of 0 such that $b \cdot 0 = 1$.) I now formulate the fundamental facts about the operations "plus" and "times" in the form of a table of axioms:

Table **T**

(1) The commutative and associative laws for addition,

$$a + b = b + a. \qquad a + (b + c) = (a + b) + c.$$

(2) The corresponding laws for multiplication.
(3) The distributive law connecting addition with multiplication

$$c \cdot (a + b) = (c \cdot a) + (c \cdot b).$$

(4) The axioms of subtraction: (4_1) There is an element o (0, "zero") such that $a + o = o + a = a$ for every a. (4_2) To every a there is a number $-a$ such that $a + (-a) = (-a) + a = o$.

(5) The axioms of division: (5_1) There is an element e (1, "unity") such that $a \cdot e = e \cdot a = a$ for every a. (5_2) To every $a \neq o$ there is an a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

By means of (4_2) and (5_2) one may introduce the difference $b - a$ and the quotient b/a as $b + (-a)$ and $b \cdot a^{-1}$, respectively.

When the Greeks discovered that the ratio ($\sqrt{2}$) between diagonal and side of a square is not measurable by a rational number, a further extension of the number concept was called for. However, all measurements of continuous quantities are possible only approximately, and always have a certain range of inaccuracy. Hence rational numbers, or even finite decimal fractions, can and do serve the ends of mensuration provided they are interpreted as approximations, and a calculus with approximate numbers seems the adequate numerical instrument for all measuring sciences. But mathematics ought to be prepared for any subsequent refinement of measurements. Hence dealing, say, with electric phenomena, one would be glad if one could consider the approximate values of the charge e of the electron which the experimentalist determines with ever greater accuracy as approximations of one definite *exact* value e. And thus, during more than two millenniums from Plato's time until the end of the nineteenth century, the mathematicians worked out an exact number concept, that of *real numbers*, that underlies all our theories in natural science. Not even to this day are the logical issues involved in that concept completely clarified and settled. The rational numbers are but a small part of the real numbers. The latter satisfy our axioms no less than the rational ones, but their system possesses a certain completeness not enjoyed by the rational numbers, and it is this, their "topological" feature, on which the operations with infinite sums and the like, as well as all continuity arguments, rest. We shall come back to this later.

Finally, during the Renaissance *complex numbers* were introduced. They are essentially pairs $z = (x, y)$ of real numbers x, y, pairs for which addition and multiplication are defined in such a way that all axioms hold. On the ground of these definitions $e = (1, 0)$ turns out to be the unity, while $i = (0, 1)$ satisfies the equation $i \cdot i = -e$. The two members x, y of the pair z are called its real and imaginary parts, and z is usually written in the form $xe + yi$, or simply $x + yi$. The usefulness of the complex numbers rests on the fact that every algebraic equation (with real or even complex coefficients) is solvable in the field of complex numbers. The analytic functions of a complex variable are the subject of a particularly rich and harmonious theory, which is the show-piece of classical nineteenth century analysis.

A set of elements for which the operations $a + b$ and $a \cdot b$ are so defined as to satisfy the axioms (1)–(4) is called a *ring*; it is called a *field* if also the axioms (5) hold. Thus the common integers form a ring I, the rational numbers form a field ω; so do the real numbers (field Ω) and the complex numbers (field Ω^*). But these are by no means the only rings or fields. The polynomials of all possible degrees h,

$$f = f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_hx^h, \tag{1}$$

with coefficients a_i taken from a given ring R (*e.g.* the ring I of integers, or the field ω), called "polynomials over R," form a ring $R[x]$. Here the variable or indeterminate x is to be looked upon as an empty symbol; the polynomial is really nothing but the sequence of its coefficients $a_0, a_1, a_2, \cdots$. But writing it in the customary form (1) suggests the rules for the addition and multiplication of polynomials which I will not repeat here. By substituting for the variable x a definite element ("number") γ of R, or of a ring P containing R as a subring, one projects the elements f of $R[x]$ into elements α of P, $f \to \alpha$: the polynomial $f = f(x)$ goes over into the number $\alpha = f(\gamma)$. This mapping $f \to \alpha$ is *homomorphic, i.e.*, it preserves addition and multiplication. Indeed, if the substitution of γ for x carries the polynomial f into α and the polynomial g into β then it carries $f + g, f \cdot g$ into $\alpha + \beta, \alpha \cdot \beta$, respectively.

If the product of two elements of a ring is never zero unless one of the factors is, one says that the ring is without null-divisor. This is the case for the rings discussed so far. A field is always a ring without null-divisor. The construction by which one rises from the integers to the fractions can be used to show that any ring R with unity and without null-divisor may be imbedded in a field k, the quotient field, such that every element of k is the quotient a/b of two elements a and b of R, the second of which (the denominator) is not zero.

Writing $1a, 2a, 3a, \cdots$, for $a, a + a, a + a + a$, *etc.*, we use the natural numbers $n = 1, 2, 3, \cdots$, as multipliers for the elements a of a ring or a field. Suppose the ring contains the unity e. It may happen that a certain multiple ne of e equals zero; then one readily sees that $na = 0$ for every element a of the ring. If the ring is without null divisors, in particular if it is a field and p is the least natural number for which $pe = 0$, then p is necessarily a prime number like 2 or 3 or 5 or 7 or 11 $\cdots$. One thus distinguishes fields of prime characteristic p from those of characteristic 0 in which no multiple of e is zero.

Plot the integers $\cdots, -2, -1, 0, 1, 2, \cdots$ as equidistant marks on a line. Let n be a natural number $\geqq 2$ and roll this line upon a wheel of circumference n. Then any two marks a, a' coincide, the difference $a - a'$ of which is divisible by n. (The mathematicians write $a \equiv a' \pmod{n}$; they say: a congruent to a' modulo n.) By this identification the ring of integers I goes over into a ring I_n consisting of n elements only (the marks on the wheel), as which one may take the "residues" $0, 1, \cdots, n - 1$. Indeed, congruent numbers give congruent results under both addition and multiplication: $a \equiv a', b \equiv b' \pmod{n}$ imply $a + b \equiv a' + b', a \cdot b \equiv a' \cdot b' \pmod{n}$. For instance, modulo 12 we have $7 + 8 = 3, 5 \cdot 8 = 4$ because 15 leaves the residue 3 and 40 the residue 4 if divided by 12. The ring I_{12} is not without null divisors since $3 \cdot 4$ is divisible by 12, but neither 3 nor 4 is. However, if p is a natural prime number, then I_p has no null divisor and is even a field; for as the ancient Greeks proved by an ingenious procedure (Euclid's algorism), for every integer a not divisible by

p there is one, a', such that $a \cdot a' \equiv 1 \pmod{p}$. This Euclidean theorem is at the basis of the whole of number theory. The example shows that there are fields of any given prime characteristic p.

In any ring R one may introduce the notions of unit and prime element as follows. The ring element a is a unit if it has a reciprocal a' in the ring, such that $a' \cdot a = e$. The element a is composite if it may be decomposed into two factors $a_1 \cdot a_2$, neither of which is a unit. A prime number is one that is neither a unit nor composite. The units of I are the numbers $+1$ and -1. The units of the ring $k[x]$ of polynomials over a field k are the non-vanishing elements of k (polynomials of degree 0). According to the Greek discovery of the irrationality of $\sqrt{2}$ the polynomial $x^2 - 2$ is prime in the ring $\omega[x]$; but, of course, not in $\Omega[x]$, for there it splits into the two linear factors $(x - \sqrt{2})(x + \sqrt{2})$. Euclid's algorism is also applicable to polynomials $f(x)$ of one variable x over any field k. Hence they satisfy Euclid's theorem: Given a prime element $P = P(x)$ in this ring $k[x]$ and an element $f(x)$ of $k[x]$ not divisible by $P(x)$, there exists another polynomial $f'(x)$ over k such that $\{f(x) \cdot f'(x)\} - 1$ is divisible by $P(x)$. Identification of any elements f and g of $k[x]$, the difference of which is divisible by P, therefore changes the ring $k[x]$ into a field, the "residue field κ of $k[x]$ modulo P." Example: $\omega[x]$ mod $x^2 - 2$. (Incidentally the complex numbers may be described as the elements of the residue field of $\Omega[x]$ mod $x^2 + 1$.) Strangely enough, the fundamental Euclidean theorem does not hold for polynomials of two variables x, y. For instance, $P(x, y) = x - y$ is a prime element of $\omega[x, y]$, and $f(x, y) = x$ an element not divisible by $P(x, y)$. But a congruence

$$x \cdot f'(x, y) \equiv 1 \qquad (\text{mod } x - y)$$

is impossible. Indeed, it would imply $-1 + x \cdot f'(x, x) = 0$, contrary to the fact that the polynomial of one indeterminate x,

$$-1 + x \cdot f'(x, x) = -1 + c_1 x + c_2 x^2 + \cdots,$$

is not zero. Thus the ring $\omega[x, y]$ does not obey the simple laws prevailing in I and in $\omega[x]$.

Consider κ, the residue field of $\omega[x]$ mod $x^2 - 2$. Since for any two polynomials $f(x)$, $f'(x)$ which are congruent mod $x^2 - 2$ the numbers $f(\sqrt{2})$, $f'(\sqrt{2})$ coincide, the transition $f(x) \to f(\sqrt{2})$ maps κ into a sub-field $\omega[\sqrt{2}]$ of Ω consisting of the numbers $a + b\sqrt{2}$ with rational a, b. Another such projection would be $f(x) \to f(-\sqrt{2})$. In former times one looked upon κ as the part $\omega[\sqrt{2}]$ of the continuum Ω or Ω^* of all real or all complex numbers; one wished to embed everything into this universe Ω or Ω^* in which analysis and physics operate. But as we have introduced it here, κ is an algebraic entity the elements of which are not numbers in the ordinary sense. It requires for its construction no other numbers but the rational ones. It has nothing to do with Ω, and ought not to be confused with the one or the other of its two projections into Ω. More generally, if $P = P(x)$ is any prime element in $\omega[x]$ we can form the residue field κ_P of $\omega[x]$ modulo P. To be sure, if δ is any of the real or complex roots of the equation $P(x)=0$ in Ω^* then $f(x) \to f(\delta)$ defines a homomorphic projection of κ_P into Ω^*. But the projection is not κ_P itself.

Let us return to the ordinary integers $\cdots, -2, -1, 0, 1, 2, \cdots$, which form the ring I. The multiples of 5, *i.e.*, the integers divisible by 5, clearly form a ring. It is a ring without unity, but it has another important peculiarity: not only does the product of any two of its elements lie in it, but all the integral multiples of an element do. The queer term *ideal* has been introduced for such a set: Given a ring R, an R-ideal $(\mathfrak{a})$ is a set of elements of R such that (1) sum and difference of any two elements of $(\mathfrak{a})$ are in $(\mathfrak{a})$, (2) the product of an element in $(\mathfrak{a})$ by any element of R is in $(\mathfrak{a})$. We may try to describe a divisor $\mathfrak{a}$ by the set of all elements divisible by $\mathfrak{a}$. One would certainly expect this set to be an ideal $(\mathfrak{a})$ in the sense just defined. Given an ideal $(\mathfrak{a})$, there may not exist an actual element a of R such that $(\mathfrak{a})$ consists of all multiples $j = m \cdot a$ of a (m any element in R). But then we would say that $(\mathfrak{a})$ stands for an "*ideal* divisor" $\mathfrak{a}$: the words "the element j of R is divisible by $\mathfrak{a}$" would simply mean: "j belongs to $(\mathfrak{a})$." In the ring I of common integers all divisors are actual.

But this is not so in every ring. An algebraic surface in the three-dimensional Euclidean space with the Cartesian coordinates x, y, z is defined by an equation $F(x, y, z) = 0$ where F is an element of ${}^3\Omega = \Omega[x, y, z]$, *i.e.*, a polynomial of the variables x, y, z with real coefficients. F is zero in all the points of the surface; but the same is true for every multiple $L \cdot F$ of F (L being any element of ${}^3\Omega$), in other words, for every polynomial of the ideal (F) in ${}^3\Omega$. Two simultaneous polynomial equations

$$F_1(x, y, z) = 0, \qquad F_2(x, y, z) = 0$$

will in general define a curve, the intersection of the surface $F_1 = 0$ and the surface $F_2 = 0$. The polynomials $(L_1 \cdot F_1) + (L_2 \cdot F_2)$ formed by arbitrary elements L_1, L_2 of ${}^3\Omega$ form an ideal (F_1, F_2), and all these polynomials vanish on the curve. This ideal will in general not correspond to an actual divisor F, for a curve is not a surface. Examples like this should convince the reader that the study of algebraic manifolds (curves, surfaces, *etc.*, in 2, 3, or any number of dimensions) amounts essentially to a study of polynomial ideals. The field of coefficients is not necessarily Ω or Ω^*, but may be a field of a more general nature.

3. Some achievements of algebra and number theory. I have finally reached a point where I can hint, I hope, with something less than complete obscurity, at some of the accomplishments of algebra and number theory in our century. The most important is probably the freedom with which we have learned to manage these abstract axiomatic concepts, like field, ring, ideal, *etc.* The atmosphere in a book like van der Waerden's *Moderne Algebra*, published about 1930, is completely different from that prevailing, *e.g.*, in the articles on algebra written for the *Mathematical Encyclopaedia* around 1900. More specifically, a general theory of ideals, and in particular of polynomial ideals, was developed. (However, it should be said that the great pioneer of abstract algebra, Richard Dedekind, who first introduced the ideals into number theory, still belonged to the nineteenth century.) Algebraic geometry, before and around 1900 flourishing chiefly in Italy, was at that time a discipline of a type uncommon in the sisterhood of mathematical disciplines: it had powerful methods, plenty of general results, but they were of somewhat doubtful validity. By the abstract algebraic methods of the twentieth century all this was put on a safe basis, and the whole subject received a new impetus. Admission of fields other than Ω^*, as the field of coefficients, opened up a new horizon.

A new technique, the "primadic numbers," was introduced into algebra and number theory by K. Hensel shortly after the turn of the century, and since then has become of ever increasing importance. Hensel shaped this instrument in analogy to the power series which played such an important part in Riemann's and Weierstrass's theory of algebraic functions of one variable and their integrals (Abelian integrals). In this theory, one of the most impressive accomplishments of the previous century, the coefficients were supposed to vary over the field Ω^* of all complex numbers. Without pursuing the analogy, I may illustrate the idea of p-adic numbers by one typical example, that of quadratic norms. Let p be a prime number, and let us first agree that a congruence $a \equiv b$ modulo a power p^h of p for rational numbers a, b has this meaning that $(a - b)/p^h$ equals a fraction whose denominator is not divisible by p;

$$e.g., \frac{39}{4} - \frac{12}{5} \equiv 0 \text{ (mod. } 7^2) \text{ because } \frac{39}{4} - \frac{12}{5} = 7^2 \cdot \frac{3}{20} \cdot$$

Let now a, b be rational numbers, $a \neq 0$, and b not the square of a rational number. In the quadratic field $\omega[\sqrt{b}]$ the number a is a *norm* if there are rational numbers x, y such that

$$a = (x + y\sqrt{b})(x - y\sqrt{b}), \qquad \text{or} \qquad a = x^2 - by^2.$$

Necessary for the solvability of this equation is (1) that for every prime p and every power p^h of p the congruence $a \equiv x^2 - by^2 \pmod{p^h}$ has a solution. This is what we mean by saying the equation has a p-adic solution. Moreover there must exist rational numbers x and y such that $x^2 - by^2$ differs as little as one wants from a. This is what we mean by saying that the equation has an ∞-adic solution. The latter condition is clearly satisfied for every a provided b is positive; however, if b is negative it is satisfied only for positive a. In the first case every a is ∞-adic norm, in the second case only half of the a's are, namely, the positive ones. A similar situation prevails with respect to p-adic norms. One proves that these necessary conditions are also sufficient: if a is a norm locally everywhere, *i.e.*, if $a = x^2 - by^2$ has a p-adic solution for every "finite prime spot p" and also for the "infinite prime spot ∞," then it has a "global" solution, namely an exact solution in rational numbers x, y.

This example, the simplest I could think of, is closely connected with the theory of genera of quadratic forms, a subject that goes back to Gauss' *Disquisitiones arithmeticae*, but in which the twentieth century has made some decisive progress by means of the p-adic technique, and it is also typical for that most fascinating branch of mathematics mentioned in the introduction: class field theory. Around 1900 David Hilbert had formulated a number of interlaced theorems concerning class fields, proved some of them at least in special cases, and left the rest to his twentieth century successors, among whom I name Takagi, Artin and Chevalley. His norm residue symbol paved the way for Artin's general reciprocity law. Hilbert had used the analogy with the Riemann-Weierstrass theory of algebraic functions over Ω^* for his orientation, but the ingenious, partly transcendental methods which he applied had nothing to do with the much simpler ones that had proved effective for the functions. By the primadic technique a rapprochement of methods has occurred, although there is still a considerable gap separating the theory of algebraic functions and the much subtler algebraic numbers.

Hensel and his successors have expressed the p-adic technique in terms of the non-algebraic "topological" notion of ("valuation" or) *convergence*. An infinite sequence of rational numbers $a_1, a_2, \cdots$ is convergent if the difference $a_i - a_j$ tends to zero, $a_i - a_j \to 0$, provided i and j independently of each other tend to infinity; more explicitly, if for every positive rational number ϵ there exists a positive integral N such that $-\epsilon < a_i - a_j < \epsilon$ for all i and $j > N$. The completeness of the real number system is expressed by Cauchy's convergence theorem: To every convergent sequence $a_1, a_2, \cdots$ of rational numbers there exists a *real* number α to which it converges: $a_i - \alpha \to 0$ for $i \to \infty$. With the ∞-adic concept of convergence we have now confronted the p-adic one induced by a prime number p. Here the sequence is considered convergent if for every exponent $h = 1, 2, 3, \cdots$, there is a positive integer N such that $a_i - a_j$ is divisible by p^h as soon as i and $j > N$. By introduction of p-adic numbers one can make the system of rational numbers complete in the p-adic sense as the introduction of real numbers makes them complete in the ∞-adic sense. The rational numbers are embedded in the continuum of all real numbers, but they may be embedded as well in that of all p-adic numbers. Each of these embedments corresponding to a finite or the infinite prime spot p is equally interesting from the arithmetical viewpoint. Now it is more evident than ever how wrong it was to identify an algebraic number field with one of its homomorphic projections into the field Ω of real numbers; along with the (real) infinite prime spots one must pay attention to the finite prime spots which correspond to the various prime ideals of the field. This is a golden rule abstracted from earlier, and then made fruitful for later, arithmetical research; and here is one bridge (others will be pointed out later) joining the two most fascinating branches of modern mathematics: abstract algebra and topology.

Besides the introduction of the primadic treatment and the progress made in the theory of class fields, the most important advances of number theory during the last fifty years seem to lie in those regions where the powerful tool of analytic functions can be brought to bear upon its problems. I mention two such fields of investigation: I. distribution of primes and the zeta function, II. additive number theory.

I. The notion of prime number is of course as old and as primitive as that of the multiplication of natural numbers. Hence it is most surprising to find the distribution of primes among all natural numbers is of such a highly irregular and almost mysterious character. While on the whole the prime numbers thin out the further one gets in the sequence of numbers, wide gaps are always followed again by clusters. An old conjecture of Goldbach's maintains that there even come along again and again pairs of primes of the smallest possible difference 2, like 57 and 59. However, the distribution of primes obeys at least a fairly simple *asymptotic* law: the number $\pi(n)$ of primes among all numbers from 1 to n is asymptotically equal to $n/\log n$. [Here $\log n$ is not the Briggs logarithm which our logarithmic tables give, but the natural logarithm as defined by the integral $\int_1^n dx/x$.] By asymptotic is meant that the quotient between $\pi(n)$ and the approximating function $n/\log n$ tends to 1 as n tends to infinity. In antiquity Eratosthenes had devised a method to sift out the prime numbers. By this sieve method the Russian mathematician Tchebycheff had obtained, during the nineteenth century, the first non-trivial results about the distribution of primes. Riemann used a different approach: his tool is the so-called zeta-function defined by the infinite series

$$\zeta(s) = 1^{-s} + 2^{-s} + 3^{-s} + \cdots. \tag{2}$$

Here s is a complex variable, and the series converges for all values of s, the real part of which is greater than 1, $\Re s > 1$. Already in the eighteenth century the fact that every positive integer can be uniquely factorized into primes had been translated by Euler into the equation

$$1/\zeta(s) = (1 - 2^{-s})(1 - 3^{-s})(1 - 5^{-s}) \cdots$$

where the (infinite) product extends over all primes $2, 3, 5, \cdots$. Riemann showed that the zeta-function has a unique "analytic continuation" to all values of s and that it satisfies a certain functional equation connecting its values for s and $1 - s$. Decisive for the prime number problem are the zeros of the zeta-function, *i.e.*, the values s for which $\zeta(s)=0$. Riemann's equation showed that, except for the "trivial" zeros at $s = -2, -4, -6, \cdots$, all zeros have real parts between 0 and 1. Riemann conjectured that their real parts actually equal $\frac{1}{2}$. His conjecture has remained a challenge to mathematics now for almost a hundred years. However, enough had been learned about these zeros at the close of the nineteenth century to enable mathematicians, by means of some profound and newly-discovered theorems concerning analytic functions, to prove the above-mentioned asymptotic law. This was generally considered a great triumph of mathematics. Since the turn of the century Riemann's functional equation with the attending consequences has been carried over from the "classical" zeta-function (ii) of the field of rational numbers to that of an arbitrary algebraic number field (E. Hecke). For certain fields of prime characteristic one succeeded in confirming Riemann's conjecture, but this provides hardly a clue for the classical case. About the classical zeta-function we know now that it has infinitely many zeros on the critical line $\mathcal{R}s = \frac{1}{2}$, and even that at least a fixed percentage, say 10 per cent, of them lie on it. (What this means is the following: Some percentage of those zeros whose imaginary part lies between arbitrary fixed limits $-T$ and $+T$ will have a real part equal to $\frac{1}{2}$, and this percentage will not sink below a certain positive limit, like 10 per cent, when T tends to infinity.) Finally about two years ago Atle Selberg succeeded, to the astonishment of the mathematical world, in giving an "elementary" proof of the prime number law by an ingenious refinement of old Eratosthenes' sieve method.

II. It has been known for a long time that every natural number n may be written as the sum of at most four square numbers, *e.g.*,

$$7 = 2^2 + 1^2 + 1^2 + 1^2, \qquad 87 = 9^2 + 2^2 + 1^2 + 1^2 = 7^2 + 5^2 + 3^2 + 2^2.$$

The same question arises for cubes, and generally for any k^{th} powers ($k=2, 3, 4, 5, \cdots$). In the eighteenth century Waring had conjectured that every non-negative integer n may be expressed as the sum of a limited number M of k^{th} powers,

$$n = n_1^k + n_2^k + \cdots + n_M^k, \tag{3}$$

where the n_i are also non-negative integers and M is independent of n. The first decade of the twentieth century brought two events: first one found that every n is expressible as the sum of at most 9 cubes (and that, excepting a few comparatively small n, even 8 cubes will do); and shortly afterwards Hilbert proved Waring's general theorem. His method was soon replaced by a different approach, the Hardy-Littlewood circle method, which rests on the use of a certain analytic function of a complex variable and yields asymptotic formulas for the number of different representations of n in the form (3). With some precautions demanded by the nature of the problem, and by overcoming some quite serious obstacles, the result was later carried over to arbitrary algebraic number fields; and by a further refinement of the circle method in a different direction Vinogradoff proved that every sufficiently large n is the sum of at most 3 primes. Is it even true that every even n is the sum of 2 primes? To show this seems to transcend our present mathematical powers as much as Goldbach's conjecture. The prime numbers remain very elusive fellows.

III. Finally, a word ought to be said about investigations concerning the arithmetical nature of numbers originating in analysis. One of the most elementary such constants is π, the area of the circle of radius 1. By proving that π is a transcendental number (not satisfying an algebraic equation with rational coefficients) the age-old problem of "squaring the circle" was settled in 1882 in the negative sense; that is, one cannot square the circle by constructions with ruler and compass. In general it is much harder to establish the transcendency of numbers than of functions. Whereas it is easy to see that the exponential function

$$e^x = 1 + \frac{x}{1} + \frac{x^2}{1\cdot 2} + \frac{x^3}{1\cdot 2\cdot 3} + \cdots$$

is not algebraic, it is quite difficult to prove that its basis e is a transcendental number. C. L. Siegel was the first who succeeded, around 1930, in developing a sort of general method for testing the transcendency of numbers. But the results in this field remain sporadic.

4. Groups, vector spaces and algebras. This ends our report on number theory, but not on algebra. For now we have to introduce the *group* concept, which, since the young genius Evariste Galois blazed the trail in 1830, has penetrated the entire body of mathematics. Without it an understanding of modern mathematics is impossible. Groups first occurred as *groups of transformations*. Transformations may operate in any set of elements, whether it is finite like the integers from 1 to 10, or infinite like the points in space. *Set* is a premathematical concept: whenever we deal with a realm of objects, a set is defined by giving a criterion which decides for any object of the realm whether it belongs to the set or not. Thus we speak of the set of prime numbers, or of the set of all points on a circle, or of all points with rational coordinates in a given coordinate system, or of all people living at this moment in the State of New Jersey. Two sets are considered equal if every element of the one belongs to the other and vice versa. A *mapping* S of a set σ into a set σ' is defined if with every element a of σ there is associated an element a' of σ', $a \to a'$. Here a rule is required which allows one to find the "image" a' for any given element a of σ. This general notion of mapping we may also call of a premathematical nature. Examples: a real-valued function of a real variable is a mapping of the continuum Ω into itself. Perpendicular projection of the space points upon a given plane is a mapping of the space into the plane. Representing every space-point by its three coordinates x, y, z with respect to a given coordinate system is a mapping of space into the continuum of real number triples (x, y, z). If a mapping S, $a \to a'$ of σ into σ', is followed by a mapping S', $a' \to a''$ of σ' into a third set σ'', the result is a mapping SS': $a \to a''$ of σ into σ''. A *one-to-one mapping* between two sets σ, σ' is a pair of mappings, S: $a \to a'$ of σ into σ', and S': $a' \to a$ of σ' into σ, which are inverse to each other. This means that the mapping SS' of σ into σ is the identical mapping E of σ which sends every element a of σ into itself, and that $S'S$ is the identical mapping of σ'. In particular, one is interested in one-to-one mappings of a set σ into itself. For them we shall use the word *transformation*. Permutations are nothing but transformations of a finite set.

The inverse S' of a transformation S, $a \to a'$ of a given set σ, is again a transformation and is usually denoted by S^{-1}. The result ST of any two transformations S and T of σ is again a transformation, and its inverse is $T^{-1}S^{-1}$ (according to the rule of dressing and undressing: if in dressing one begins with the shirt and ends with the jacket, one must in undressing begin with the jacket and end with the shirt. The order of the two "factors" S, T is essential.) A *group of transformations* is a set of transformations of a given manifold which (1) contains the identity E, (2) contains with every transformation S its inverse S^{-1}, and (3) with any two transformations S, T their "product" ST. Example: One could define congruent configurations in space as point sets of which one goes into the other by a congruent transformation of space. The congruent transformations, or "motions," of space form a group; a statement which, according to the above definition of group, is equivalent to the threefold statement that (1) every figure is congruent to itself, (2) if a figure F is congruent to F', then F' is congruent to F, and (3) if F is congruent to F' and F' congruent to F'', then F is congruent to F''. This example at once illuminates the inner significance of the group concept. *Symmetry* of a configuration F in space is described by the group of motions that carry F into itself.

Often manifolds have a structure. For instance, the elements of a field are connected by the two operations of plus and times; or in Euclidean space we have the relationship of congruence between figures. Hence we have the idea of structure-preserving mappings; they are called *homomorphisms*. Thus a homomorphic mapping of a field k into a field k' is a mapping $a \to a'$ of the "numbers" a of k into the numbers a' of k' such that $(a+b)' = a'+b'$ and $(a\cdot b)' = a'\cdot b'$. A homomorphic mapping of space into itself would be one that carries any two congruent figures into two mutually congruent figures. The following terminology (suggestive to him who knows a little Greek) has been agreed upon: homomorphisms which are one-to-one mappings are called isomorphisms; when a homomorphism maps a manifold σ into itself, it is called an endomorphism, and an automorphism when it is both: a one-to-one mapping of σ into itself. Isomorphic systems, *i.e.*, any two systems mapped isomorphically upon each other, have the same structure; indeed nothing can be said about the structure of the one system that is not equally true for the other.

The *automorphisms* of a manifold with a well-defined structure form a *group*. Two sub-sets of the manifold that go over into each other by an automorphism deserve the name of *equivalent*. This is the precise idea at which Leibniz hints when he says that two such sub-sets are "indiscernible when each is considered in itself"; he recognized this general idea as lying behind the specific geometric notion of similitude. The general problem of relativity consists in nothing else but to find the group of automorphisms. Here then is an important lesson the mathematicians learned in the twentieth century: whenever you are concerned with a structured manifold, study its group of automorphisms. Also the inverse problem, which Felix Klein stressed in his famous Erlangen program (1872), deserves attention: Given a group of transformations of a manifold σ, determine such relations or operations as are invariant with respect to the group.

If in studying a group of transformations we ignore the fact that it consists of transformations and look merely at the way in which any two of its transformations S, T give rise to a composite ST, we obtain the abstract composition schema of the group. Hence an *abstract group* is a set of elements (of unknown or irrelevant nature) for which an operation of composition is defined generating an element st from any two elements s, t such that the following axioms hold:

(1) There is a unit element e such that $es=se=s$ for every s.

(2) Every element s has an inverse s^{-1} such that $ss^{-1} = s^{-1}s = e$.

(3) The associative law $(st)u = s(tu)$ holds.

It is perhaps the most astonishing experience of modern mathematics how rich in consequences these three simple axioms are. A realization of an abstract group by transformations of a given manifold σ is obtained by associating with every element s of the group a transformation S of σ, $s \rightarrow S$, such that $s \rightarrow S$, $t \rightarrow T$ imply $st \rightarrow ST$. In general, the commutative law $st = ts$ will not hold. If it does, the group is called commutative or Abelian (after the Norwegian mathematician Niels Henrik Abel). Because composition of group elements in general does not satisfy the commutative law, it has proved convenient to use the term "ring" in the wider sense in which it does not imply the commutative law for multiplication. (However, in speaking of a field one usually assumes this law.)

The simplest mappings are the linear ones. They operate in a vector space. The vectors in our ordinary three-dimensional space are directed segments AB leading from a point A to a point B. The vector AB is considered equal to $A'B'$ if a parallel displacement (translation) carries AB into $A'B'$. In consequence of this convention one can add vectors and one can also multiply a vector by a number (integral, rational or even real). Addition satisfies the same axioms as enumerated for numbers in the table **T**, and it is also easy to formulate the axioms for the second operation. These axioms constitute the general axiomatic notion of vector space, which is therefore an algebraic and not a geometric concept. The numbers which serve as multipliers of the vectors may be the elements of any ring; this generality is actually required in the application of the axiomatic vector concept to topology. However, here we shall assume that they form a field. Then one sees at once that one can ascribe to the vector space a natural number n as its dimensionality in this sense: there exist n vectors $e_1, \cdots, e_n$ such that every vector may be expressed in one and only one way as a linear combination $x_1e_1 + \cdots + x_ne_n$, where the "coordinates" x_i are definite numbers of the field. In our three-dimensional space n equals 3, but mechanics and physics give ample occasion to use the general algebraic notion of an n-dimensional vector space for higher n.

The endomorphisms of a vector space are called its *linear mappings*; as such they allow composition ST (perform first the mapping S, then T), but they also allow addition and multiplication by numbers γ: if S sends the arbitrary vector x into xS, T into xT, then $S + T$, γS are those linear mappings which send x into $(xS) + (xT)$ and $\gamma \cdot xS$, respectively. We must forego to describe how in terms of a vector basis $e_1, \cdots, e_n$ a linear mapping is represented by a square matrix of numbers.

Often rings occur—they are then called *algebras*—which are at the same time vector spaces, *i.e.*, for which three operations, addition of two elements, multiplication of two elements and multiplication of an element by a number, are defined in such manner as to satisfy the characteristic axioms. The linear mappings of an n-dimensional vector space themselves form such an algebra, called the complete matric algebra (in n dimensions). According to quantum mechanics the observables of a physical system form an algebra of special type with a non-commutative multiplication. In the hands of the physicists abstract algebra has thus become a key that unlocked to them the secrets of the atom. A realization of an abstract group by linear transformations of a vector space is called *representation*. One may also speak of representations of a ring or an algebra: in each case the representation can be described as a homomorphic mapping of the group or ring or algebra into the complete matric algebra (which indeed is a group and a ring and an algebra, all in one).

5. Finale. After spending so much time on the explanation of the notions I can be brief in my enumeration of some of the essential achievements for which they provided the tools. If g is a subgroup of the group G, one may identify elements s, t of G that are congruent mod g, *i.e.*, for which st^{-1} is in g; g is a "self-conjugate" subgroup if this process of identification carries G again into a group, the "factor group" G/g. The group-theoretic core of Galois' theory is a theorem due to C. Jordan and O. Hölder which deals with the several ways in which one may break down a given finite group G in steps $G = G_0, G_1, G_2, \cdots$, each G_i being a self-conjugate subgroup of the preceding group G_{i-1}. Under the assumption that this is done in as small steps as possible, the theorem states, the steps (factor groups) G_{i-1}/G_i $(i = 1, 2, \cdots)$ in one such "composition series" are isomorphic to the steps, suitably rearranged, in a second such series. The theorem is very remarkable in itself, but perhaps the more so as its proof rests on the same argument by which one proves what I consider the most fundamental proposition in all mathematics, namely the fact that if you count a finite set of elements in two ways, you end up with the same number n both times. The Jordan-Hölder theorem in recent times received a much more natural and general formulation by (1) abandoning the assumption that the breaking down is done in the smallest possible steps, and (2) by admitting only such subgroups as are invariant with respect to a given set of endomorphic mappings of G. It thus has become applicable to infinite as well as finite groups, and provided a common denominator for quite a number of important algebraic facts.

The theory of representations of finite groups, the most systematic and substantial part of group theory developed shortly before the turn of the century by G. Frobenius, taught us that there are only a few irreducible representations, of which all others are composed. This theory was greatly simplified after 1900 and later carried over, first to continuous groups that have the topological property of compactness, but then also to all infinite groups, with a restrictive imposition (called almost-periodicity) on the representations. With these generalizations one trespasses the limits of algebra, and a few more words will have to be said about it under the title analysis. New phenomena occur if representations of finite groups in fields of prime characteristic are taken into account, and from their investigation profound number-theoretic consequences have been derived. It is easy to embed a finite group into an algebra, and hence facts about representations of a group are best deduced from those of the embedding algebra. At the beginning of the century algebras seemed to be ferocious beasts of unpredictable behavior, but after fifty years of investigation they, or at least the variety called semi-simple, have become remarkably tame; indeed the wild things do not happen in these superstructures, but in the underlying commutative "number" fields. In the nineteenth century geometry seemed to have been reduced to a study of invariants of groups; Felix Klein formulated this standpoint explicitly in his Erlangen program. But the full linear group was practically the only group whose invariants were studied. We have now outgrown this limitation and no longer ignore all the other continuous groups one encounters in algebra, analysis, geometry and physics. Above all we have come to realize that the theory of invariants has to be subsumed under that of representations. Certain infinite discontinuous groups, like the unimodular and the modular groups, which are of special importance to number theory, witness Gauss' class theory of quadratic forms, have been studied with remarkable success and profound results. The macroscopic and microscopic symmetries of crystals are described by discontinuous groups of motions, and it has been proved for n dimensions, what had long been known for 3 dimensions, that in a certain sense there is but a finite number of possibilities for these crystallographic groups. In the nineteenth century Sophus Lie had reduced a continuous group to its "germ" of infinitesimal elements. These elements form a sort of algebra in which the associative law is replaced by a different type of law. A Lie algebra is a purely algebraic structure, especially if the numbers which act as multipliers are taken from an algebraically defined field rather than from the continuum of real numbers Ω. These Lie groups have provided a new playground for our algebraists.

The constructions of the mathematical mind are at the same time free and necessary. The individual mathematician feels free to define his notions and to set up his axioms as he pleases. But the question is, will he get his fellow-mathematicians interested in the constructs of his imagination. We can not help feeling that certain mathematical structures which have evolved through the combined efforts of the mathematical community bear the stamp of a necessity not affected by the accidents of their historical birth. Everybody who looks at the spectacle of modern algebra will be struck by this complementarity of freedom and necessity.

PART II. ANALYSIS. TOPOLOGY. GEOMETRY. FOUNDATIONS.

6. Linear operators and their spectral decomposition. Hilbert space. A mechanical system of n degrees of freedom in stable equilibrium is capable of oscillations deviating "infinitely little" from the state of equilibrium. It is a fact of fundamental significance not only for physics but also for music that all these oscillations are superpositions of n "harmonic" oscillations with definite frequencies. Mathematically the problem of determining the harmonic oscillations amounts to constructing the principal axes of an ellipsoid in an n-dimensional Euclidean space. Representing the vectors x in this space by their coordinates $(x_1, x_2, \cdots, x_n)$ one has to solve an equation

$$x - \lambda \cdot Kx = 0,$$

where K denotes a given linear operator (= linear mapping); λ is the square of the unknown frequency ν of the harmonic oscillation, whereas the "eigen-vector" x characterizes its amplitude. Define the scalar product (x, y) of two vectors x and y by the sum $x_1y_1 + \cdots + x_ny_n$. Our "affine" vector space is made into a metric one by assigning to any vector x the length $\|x\|$ given by $\|x\|^2 = (x, x)$, and this metric is the Euclidean one so familiar to us from the 3-dimensional case and epitomized by the "Pythagoras." The linear operator K is symmetric in the sense that $(x, Ky) = (Kx, y)$. The field of numbers in which we operate here is, of course, the continuum of all real numbers. Determination of the n frequencies ν or rather of the corresponding eigen-values $\lambda = \nu^2$ requires the solution of an algebraic equation of degree n (often known as the secular equation, because it first appeared in the theory of the secular perturbations of the planetary system).

More important in physics than the oscillations of a mechanical system of a finite number of degrees of freedom are the oscillations of continuous media, as the mechanical-acoustical oscillations of a string, a membrane or a 3-dimensional elastic body, and the electromagnetic-optical oscillations of the "ether." Here the vectors with which one has to operate are continuous functions $x(s)$ of a point s with one or several coordinates that vary over a given domain, and consequently K is a linear *integral* operator. Take for instance a straight string of length 1, the points of which are distinguished by a parameter s varying from 0 to 1. Here (x, x) is the integral $\int_0^1 x^2(s) \cdot ds$, and the problem of harmonic oscillations (which first suggested to the early Greeks the idea of a universe ruled by harmonious mathematical laws) takes the form of the integral equation

$$[1] \qquad x(s) - \lambda \int_0^1 K(s, t)x(t)dt = 0, \qquad (0 \leqq s \leqq 1),$$

where

$$[1'] \qquad K(s, t) = \left(\frac{a}{\pi}\right)^2 \cdot \begin{cases} s(1 - t) & \text{for } s \leqq t \\ (1 - s)t & \text{for } s \geqq t \end{cases},$$

and a is a constant determined by the physical conditions of the string. The solutions are

$$\lambda = (na)^2, \qquad x(s) = \sin n\pi s,$$

where n is capable of all positive integral values $1, 2, 3, \cdots$. This fact that the frequencies of a string are integral multiples na of a ground frequency a is the basic law of musical harmony. If one prefers an optical to an acoustic language one speaks of the *spectrum* of eigen-values λ.

After Fredholm at the very close of the 19th century had developed the theory of linear integral equations it was Hilbert who in the next decade established the general *spectral theory of symmetric linear operators* K. Only twenty years earlier it had required the greatest mathematical efforts to prove the existence of the ground frequency for a membrane, and now constructive proofs for the existence of the whole series of harmonic oscillations and their characteristic frequencies were given under very general assumptions concerning the oscillating medium. This was an event of great consequence both in mathematics and theoretical physics. Soon afterwards Hilbert's approach made it possible to establish those asymptotic laws for the distribution of eigen-values the physicists had postulated in their statistical treatment of the thermodynamics of radiation and elastic bodies.

Hilbert observed that an arbitrary continuous function $x(s)$ defined in the interval $0 \leqq s \leqq 1$ may be replaced by the sequence

$$x_n = \sqrt{2} \int_0^1 x(s) \cdot \sin n\pi s \cdot ds, \qquad n = 1, 2, 3, \cdots,$$

of its Fourier coefficients. Thus there is no inner difference between a vector space whose elements are functions $x(s)$ of a continuous variable and one whose elements are infinite sequences of numbers $(x_1, x_2, x_3, \cdots)$. The square of the "length," $\int_0^1 x^2(s) \cdot ds$ equals $x_1^2 + x_2^2 + x_3^2 + \cdots$. Between the two forms in which one may pass from a finite sum to a limit, the infinite sum $a_1 + a_2 + a_3 + \cdots$ and the integral $\int_0^1 a(s) \cdot ds$, there is therefore here no essential difference. Thus an axiomatic formulation is called for. To the axioms for an (affine) vector space one adds the postulate of the existence of a scalar product (x, y) of any two vectors (x, y) with the properties characteristic for Euclidean metric: (x, y) is a number depending linearly on either of the two argument vectors x and y; it is symmetric, $(x, y) = (y, x)$; and $(x, x) = \|x\|^2$ is positive except for $x = 0$. The axiom of finite dimensionality is replaced by a denumerability axiom of more general character. All operations in such a space are greatly facilitated if it is assumed to be complete in the same sense that the system of real numbers is complete; *i.e.*, if the following is true: Given a "convergent" sequence $x', x'', \cdots$ of vectors, namely, one for which $\|x^{(m)} - x^{(n)}\|$ tends to zero with m and n tending to infinity, there exists a vector a toward which this sequence converges, $\|x^{(n)} - a\| \to 0$ for $n \to \infty$. A non-complete vector space can be made complete by the same construction by which the system of rational numbers is completed to form that of real numbers. Later authors have coined the name "Hilbert space" for a vector space satisfying these axioms.

Hilbert himself first tackled only integral operators in the strict sense as exemplified by [1]. But soon he extended his spectral theory to a far wider class, that of bounded (symmetric) linear operators in Hilbert space. Boundedness of the linear operator requires the existence of a constant M such that $\|Kx\|^2 \leqq M\cdot\|x\|^2$ for all vectors x of finite length $\|x\|$. Indeed the restriction to integral operators would be unnatural since the simplest operator, the identity $x \to x$, is not of this type. And now one of those events happened, unforeseeable by the wildest imagination, the like of which could tempt one to believe in a pre-established harmony between physical nature and mathematical mind: Twenty years after Hilbert's investigations *quantum mechanics* found that the observables of a physical system are represented by the linear symmetric operators in a Hilbert space and that the eigen-values and eigen-vectors of that operator which represents *energy* are the energy levels and corresponding stationary quantum states of the system. Of course this quantum-physical interpretation added greatly to the interest in the theory and led to a more scrupulous investigation of it, resulting in various simplifications and extensions.

Oscillations of continua, the boundary value problems of classical physics and the problem of energy levels in quantum physics, are not the only titles for applications of the theory of integral equations and their spectra. One other somewhat isolated application is the solution of *Riemann's monodromy problem* concerning analytic functions of a complex variable z. It concerns the determination of n analytic functions of z which remain regular under analytic continuation along arbitrary paths in the z-plane provided these avoid a finite number of singular points, whereas the functions undergo a given linear transformation with constant coefficients when the path circles one of these points.

Another surprising application is to the establishment of the fundamental facts, in particular of the completeness relation, in the theory of *representations of continuous compact groups*. The simplest such group consists of the rotations of a circle, and in that case the theory of representations is nothing but the theory of the so-called Fourier series, which expresses an arbitrary periodic function $f(s)$ of period 2π in terms of the harmonic oscillations

$$\cos ns, \qquad \sin ns, \qquad\qquad n = 0, 1, 2, \cdots.$$

In Nature functions often occur with hidden non-commensurable periodicities. The mathematician Harald Bohr, the brother of the physicist Niels Bohr, prompted by certain of his investigations concerning the Riemann zeta function, developed the general mathematical theory of such *almost periodic func-*

tions. One may describe his theory as that of almost periodic representations of the simplest continuous group one can imagine, namely, the group of all translations of a straight line. His main results could be carried over to arbitrary groups. No restriction is imposed on the group, but the representations one studies are supposed to be almost-periodic. For a function $x(s)$, the argument s of which runs over the group elements, while its values are real or complex numbers, almost-periodicity amounts to the requirement that the group be compact in a certain topology induced by the function. This relative compactness instead of absolute compactness is sufficient. Even so the restriction is severe. Indeed the most important representations of the classical continuous groups are not almost-periodic. Hence the theory is in need of further extension, which has busied a number of American and Russian mathematicians during the last decade.

7. Lebesgue's integral. Measure theory. Ergodic hypothesis. Before turning to other applications of operators in Hilbert space I must mention the, in all probability final, form given to the idea of integration by Lebesgue at the beginning of our century. Instead of speaking of the area of a piece of the 2-dimensional plane referred to coordinates x, y, or the volume of a piece of the 3-dimensional Euclidean space, we use the neutral term *measure* for all dimensions. The notions of measure and *integral* are interconnected. Any piece of space, any set of space points can be described by its characteristic function $\chi(P)$, which equals 1 or 0 according to whether the point P belongs or does not belong to the set. The measure of the point set is the integral of this characteristic function. Before Lebesgue one first defined the integral for continuous functions; the notion of measure was secondary; it required transition from continuous to such discontinuous functions as $\chi(P)$. Lebesgue goes the opposite and perhaps more natural way: for him measure comes first and the integral second. The one-dimensional space is sufficient for an illustration. Consider a real-valued function $y = f(x)$ of a real variable x which maps the interval $0 \leqq x \leqq 1$ into a finite interval $a \leqq y \leqq b$. Instead of subdividing the interval of the argument x Lebesgue subdivides the interval (a, b) of the dependent variable y into a finite number of small subintervals $a_i \leqq y < a_{i+1}$, say of lengths $< \epsilon$, and then determines the measure m_i of the set S_i on the x-axis, the points of which satisfy the inequality $a_i \leqq f(x) < a_{i+1}$. The integral lies between the two sums $\sum_i a_i m_i$ and $\sum_i a_{i+1} m_i$ which differ by less than ϵ, and thus can be computed with any degree of accuracy. In determining the measure of a point set—and this is the more essential modification—Lebesgue covers the set with infinite sequences, rather than finite ensembles, of intervals. Thus, to the set of rational x in the interval $0 \leqq x \leqq 1$ no measure could be ascribed before Lebesgue. But these rational numbers can be arranged in a denumerable sequence $a_1, a_2, a_3, \cdots$, and, after choosing a positive number ϵ as small as one likes, one can surround the point a_n by an interval of length $\epsilon/2^n$ with the center a_n. Thus the whole set of rational points is enclosed in a sequence of intervals of total length

$$\epsilon(1/2 + 1/2^2 + 1/2^3 + \cdots) = \epsilon;$$

and according to Lebesgue's definition its measure is therefore less than (the arbitrary positive) ϵ and hence zero. The notion of *probability* is tied to that of measure, and for this reason mathematical statisticians are deeply interested in measure theory. Lebesgue's idea has been generalized in several directions. The two fundamental operations one can perform with sets are: forming the intersection and the union of given sets, and thus sets may be considered as elements of a "*Boolean algebra*" with these two operations, the properties of which may be laid down in a number of axioms resembling the arithmetical axioms for addition and multiplication. Hence one of the questions which has occupied the more axiomatically minded among the mathematicians and statisticians is concerned with the introduction of measure in abstract Boolean algebras.

Lebesgue's integral is important in our present context, because those real-valued functions $f(x)$ of a real variable x ranging over the interval $0 \leqq x \leqq 1$, the squares of which are Lebesgue-integrable, form a complete Hilbert space —provided two functions $f(x)$, $g(x)$ are considered equal if those values x for which $f(x) \neq g(x)$ form a set of measure zero (Riesz-Fischer theorem).

The mechanical equations for a system of n degrees of freedom in Hamilton's form uniquely determine the state tP at the moment t if the state P at the moment $t = 0$ is given. Such is the precise formulation of the law of causality in mechanics. The possible states P form the points of a $(2n)$-dimensional phase space, and for a fixed t and an arbitrary P the transition $P \to tP$ is a measure-preserving mapping (t). These transformations form a group: $(t_1)(t_2) = (t_1 + t_2)$. For a given P and a variable t the point tP describes the consecutive states which this system assumes if at the moment $t = 0$ it is in the state P. Considering P as a particle of a $(2n)$-dimensional fluid which fills the phase-space and ascribing to the particle P the position tP at the time t, one obtains the picture of an incompressible fluid in stationary flow. The statistical derivation of the laws of thermodynamics makes use of the so-called *ergodic hypothesis* according to which the path of an arbitrary individual particle P (excepting initial states P which form a set of measure zero) covers the phase-space (or at least that $(2n - 1)$-dimensional sub-space of it where the energy has a given value) everywhere dense, so that in the course of its history the probability of finding it in this or that part of the space is the same for any parts of equal measure. Nineteenth century mathematics seemed to be a long way off from proving this hypothesis with any degree of generality. Strangely enough it was proved shortly after the transition from classical to quantum mechanics had rendered the hypothesis almost valueless, and it was proved by making use of the mathematical apparatus of quantum physics. Under the influence of the mapping (t), $P \to tP$, any function $f(P)$ in phase-space is transformed into the function $f' = U_t f$, defined by the equation $f'(tP) = f(P)$. The U_t form a group of operators in the Hilbert space of arbitrary functions $f(P)$, $U_{t_1}U_{t_2} = U_{t_1+t_2}$, and application of spectral decomposition to this group enabled J. von Neumann to deduce the ergodic hypothesis with two provisos: (1) Convergence of a sequence of functions $f_n(P)$ toward a function $f(P)$, $f_n \to f$, is understood (as it would in quantum mechanics, namely) as convergence in Hilbert space where it means that the total integral of $(f_n - f)^2$ tends to zero with $n \to \infty$; (2) one assumes that there are no subspaces of the phase-space which are invariant under the group of transformations (t) except those spaces that are in Lebesgue's sense equal either to the empty or the total space. Shortly afterwards proofs were also given for other interpretations of the notion of convergence.

The laws of nature can either be formulated as differential equations or as "principles of variation" according to which certain quantities assume extremal values under given conditions. For instance, in an optically homogeneous or non-homogeneous medium the light travels along that road from a given point A to a given point B for which the time of travel assumes minimal value. In potential theory the quantity which assumes a minimum is the so-called Dirichlet integral. Attempts to establish directly the existence of a minimum had been discouraged by Weierstrass' criticism in the 19th century. Our century, however, restored the direct methods of the Calculus of Variation to a position of honor after Hilbert in 1900 gave a direct proof of the Dirichlet principle and later showed how it can be applied not only in establishing the fundamental facts about functions and integrals ("algebraic" functions and "abelian" integrals) on a compact Riemann surface (as Riemann had suggested 50 years earlier) but also for deriving the basic propositions of the *theory of uniformization*. That theory occupies a central position in the theory of functions of one complex variable, and the first decade of the 20th century witnessed the first proofs by P. Koebe and H. Poincaré of these propositions conjectured about 25 years before by Poincaré himself and by Felix Klein. As in an Euclidean vector space of finite dimensionality, so in the Hilbert space of infinitely many dimensions, this fact is true: Given a linear (complete) subspace E, any vector may be split in a uniquely determined manner into a component lying in E (orthogonal projection) and one perpendicular to E. Dirichlet's principle is nothing but a special case of this fact. But since the function-theoretic applications of orthogonal projection in Hilbert space which we alluded to are closely tied up with topology we had better turn first to a discussion of this important branch of modern mathematics: topology.

8. Topology and harmonic integrals. Essential features of the modern approach to *topology* can be brought to light in its connection with the, only recently developed, theory of *harmonic integrals*. Consider a stationary magnetic field h in a domain G which is free from electric currents. At every point of G it satisfies two differential conditions which in the usual notations of vector analysis are written in the form div $h = 0$, rot $h = 0$. A field of this type is called harmonic. The second of these conditions states that the line integral of

h along a closed curve (cycle) C, $\int_C h$, vanishes provided C lies in a sufficiently small neighborhood of an arbitrary point of G. This implies $\int_C h = 0$ for any cycle C in G that is the boundary of a surface in G. However, for an arbitrary cycle C in G the integral is equal to the electric current surrounded by C.

Let the phrase "C homologous to zero," $C \sim 0$, indicate that the cycle C in G bounds a surface in G. One can travel over a cycle C in the opposite sense, thus obtaining $-C$, or travel over it $2, 3, \cdots$ times, thus obtaining $2C, 3C, \cdots$; and cycles may be added and subtracted from each other (if one does not insist that cycles are of one piece). Two cycles C, C' are called homologous, $C \sim C'$, if $C - C' \sim 0$. Note that $C \sim 0$, $C' \sim 0$ imply $-C \sim 0$, $C + C' \sim 0$. Hence the cycles form a commutative group under addition, the "Betti group," if homologous cycles are considered as one and the same group element. These notions of *cycles and their homologies* may be carried over from a three-dimensional domain in Euclidean space to any n-dimensional manifold, in particular to closed (compact) manifolds like the two-dimensional surfaces of the sphere or the torus; and on an n-dimensional manifold we can speak not only of 1-dimensional, but also of 2-, 3-, $\cdots$, n-dimensional cycles. The notion of a harmonic vector field permits a similar generalization, harmonic tensor field (harmonic form) of rank r ($r = 1, 2, \cdots, n$), provided the manifold bears a Riemannian metric, an assumption the meaning of which will be discussed later in the section on geometry. Any tensor field (linear differential form) of rank r may be integrated over an r-dimensional cycle.

The fundamental problem of *homology theory* consists in determining the structure of the Betti group, not only for 1-, but also for 2-, $\cdots$, n-dimensional cycles, in particular in determining the number of linearly independent cycles (Betti number). [ν cycles $C_1, \cdots, C_\nu$ are linearly independent if there exists no homology $k_1C_1 + \cdots + k_\nu C_\nu \sim 0$ with integral coefficients k except $k_1 = \cdots = k_\nu = 0$.] The fundamental theorem for harmonic forms on compact manifolds states that, given ν linearly independent cycles $C_1, \cdots, C_\nu$, there exists a harmonic form h with pre-assigned periods

$$\int_{C_1} h = \pi_1, \cdots, \qquad \int_{C_\nu} h = \pi_\nu.$$

H. Poincaré developed the algebraic apparatus necessary to formulate exactly the notions of cycle and homology. In the course of the twentieth century it turned out that in most problems co-homologies are easier to handle than homologies. I illustrate this for 1-dimensional cycles. A line C_1 leading from a point p_1 to p_2, when followed by a line C_2 leading from p_2 to a third point p_3, gives rise to a line $C_1 + C_2$ leading from p_1 to p_3. The line integral $\int_C h$ of a given vector field h along an arbitrary (closed or open) line C is an additive function $\phi(C)$ of C, $\phi(C_1 + C_2) = \phi(C_1) + \phi(C_2)$. If moreover $\operatorname{rot} h$ vanishes everywhere, then $\phi(C) = 0$ for any closed line C that lies in a sufficiently small neighborhood of a point, whatever this point may be. Any real-valued function ϕ satisfying these two conditions may be called an abstract integral. The co-homology $\phi \sim 0$ means that $\phi(C) = 0$ for any closed line C, and thus it is clear what the co-homology $k_1\phi_1 + \cdots + k_\nu\phi_\nu \sim 0$ with arbitrary real coefficients $k_1, \cdots, k_\nu$ means. The homology $C \sim 0$ could now be defined, not by the condition that the cycle C bounds, but by the requirement that $\phi(C) = 0$ for every abstract integral ϕ. With the convention that any two abstract integrals ϕ, ϕ' are identified if $\phi - \phi' \sim 0$, these integrals form a vector space, and the dimensionality of this vector space is now introduced as the Betti number. And the fundamental theorem for harmonic integrals on a compact manifold now asserts that for any given abstract integral ϕ there exists one and only one harmonic vector field h whose integral is cohomologous to ϕ, $\int_C h = \phi(C)$, for every cycle C (realization of the abstract integral in concreto by a harmonic integral).

J. W. Alexander discovered an important result connecting the Betti numbers of a manifold M that is embedded in the n-dimensional Euclidean space R_n with the Betti numbers of the complement $R_n - M$ (*Alexander's duality theorem*).

The difficulties of topology spring from the double aspect under which one can consider continuous manifolds. Euclid looked upon a figure as an assemblage of a finite number of geometric elements, like points, straight lines, circles, planes, spheres. But after replacing each line or surface by the set of points lying on it one may also adopt the set-theoretic view that there is only one sort of elements, points, and that any (in general infinite) set of points can serve as a figure. This modern standpoint obviously gives geometry far greater generality and freedom. In topology, however, it is not necessary to descend to the points as the ultimate atoms, but one can construct the manifold like a building from "blocks" or cells, and a finite number of such cells serving as units will do, provided the manifold is compact. Thus it is possible here to revert to a treatment in Euclid's "finitistic" style (combinatorial topology).

On the first standpoint, manifold as a point set, the task is to formulate that *continuity* by which a point p approaching a given point p_0 becomes gradually indistinguishable from p_0. This is done by associating with p_0 the *neighborhoods* of p_0, an infinite shrinking sequence of sub-sets $U_1 \supset U_2 \supset U_3 \supset \cdots$, all containing p_0. [$U \supset V$ means: the set U contains V.] For example, in a plane referred to Cartesian coordinates x, y we may choose as the nth neighborhood U_n of a point $p_0 = (x_0, y_0)$ the interior of the circle of radius $1/2^n$ around p_0. The notion of convergence, basic for all continuity considerations, is defined in terms of the sequence of neighborhoods as follows: A sequence of points $p_1, p_2, \cdots$ converges to p_0 if for every natural number n there is an N so that all points p_ν with $\nu > N$ lie in the nth neighborhood U_n of p_0. Of course, the choice of the neighborhoods U_n is arbitrary to a certain extent. For instance, one could also have chosen as the nth neighborhood V_n of (x_0, y_0) the square of side $2/n$ around (x_0, y_0), to which a point (x, y) belongs, if

$$-1/n < x - x_0 < 1/n, \qquad -1/n < y - y_0 < 1/n.$$

However the sequence V_n is equivalent to the sequence U_n in the sense that for every n there is an n' such that $U_{n'} \subset V_n$ (and thus $U_\nu \subset V_n$ for $\nu \geqq n'$), and also for every m an m' such that $V_{m'} \subset U_m$; and consequently the notion of convergence for points is the same, whether based on the one or the other sequence of neighborhoods. It is clear how to define continuity of a mapping of one manifold into another. A one-to-one mapping of two manifolds upon each other is called topological if continuous in both directions, and two manifolds that can be mapped topologically upon each other are topologically equivalent. Topology investigates such properties of manifolds as are invariant with respect to topological mappings (in particular with respect to continuous deformations).

A continuous function $y=f(x)$ may be approximated by piecewise linear functions. The corresponding device in higher dimensions, the method of *simplicial approximations* of a given continuous mapping of one manifold into another, is of great importance in set-theoretic topology. It has served to develop a general *theory of dimensions*, to prove the topological invariance of the Betti groups, to define the decisive notion of the degree of mapping ("Abbildungsgrad," L. E. J. Brouwer) and to prove a number of interesting fixed point theorems. For instance, a continuous mapping of a square into itself has necessarily a fixed point, *i.e.*, a point carried by the mapping into itself. Given two continuous mappings of a (compact) manifold M into another M', one can ask more generally for which points p on M both images on M' coincide. A famous formula by S. Lefschetz relates the "total index" of such points with the homology theory of cycles on M and M'.

Application of fixed point theorems to functional spaces of infinitely many dimensions has proved a powerful method to establish the existence of solutions for non-linear differential equations. This is particularly valuable, because the hydrodynamical and aerodynamical problems are almost all of this type.

Poincaré found that a satisfactory formulation of the homology theory of cycles was possible only from the second standpoint where the n-dimensional manifold is considered as a conglomerate of n-dimensional cells. The boundary of an n-dimensional cell (n-cell) consists of a finite number of $(n-1)$-cells, the boundary of an $(n-1)$-cell consists of a finite number of $(n-2)$-cells, *etc.* The *combinatorial skeleton* of the manifold is obtained by assigning symbols to these cells and then stating in terms of their symbols which $(i-1)$-cells belong to the boundary of any of the occurring i-cells ($i = 1, 2, \cdots, n$). From the cells one descends to the points of the manifold by a repeated process of sub-division which catches the points in an ever finer net. Since this subdivision proceeds according to a fixed combinatorial scheme, the manifold is in topological regard completely fixed by its combinatorial skeleton. And at once the question arises under what circumstances two given combinatorial skeletons represent the same manifold, *i.e.*, lead by iterated sub-division to topologically equivalent manifolds. We are far from being able to solve this fundamental problem. Algebraic topology, which operates with the combinatorial skeletons, is in itself a rich and beautiful theory, linked in various ways with the basic notions and theorems of algebra and group theory.

The connection between algebraic and set-theoretic topology is fraught with serious difficulties which are not yet overcome in a quite satisfactory manner. So much, however, seems clear that one had better start, not with a division into cells, but with a covering by patches which are allowed to overlap. From such a pattern the fundamental topologically invariant concepts are to be developed. The above notion of an abstract integral, which relates homology and co-homology, is an indication; it can indeed be used for a direct proof of the invariance of the first Betti number without the tool of simplicial approximation.

9. Conformal mapping, meromorphic functions, Calculus of Variation in the large. Homology theory, in combination with the Dirichlet principle or the method of orthogonal projection in Hilbert space, leads to the theory of harmonic integrals, in particular for the lowest dimension $n=2$ to the theory of abelian integrals on Riemann surfaces. But for Riemann surfaces the Dirichlet principle also yields the fundamental facts concerning uniformization of analytic functions of one variable if one combines it with the *homotopy* (not homology) *theory* of closed curves. Whereas a cycle is homologous to zero if it bounds, it is homotopic to zero if it can be contracted into a point by continuous deformation. The homotopy theory of 1- and more-dimensional cycles has recently come to the fore as an important branch of topology, and the group-theoretic aspect of homotopy has led to some surprising discoveries in abstract group theory. Homotopy of 1-dimensional cycles is closely related with the idea of the *universal covering manifold* of a given manifold. Given a continuous mapping $p \rightarrow p'$ of one manifold M into another M', the point p' may be considered as the trace or projection in M' of the arbitrary point p on M, and thus M becomes a manifold covering M'. There may be no point or several points p on M which lie over a given point p' of M' (which are mapped into p'). The mapping is without ramifications if for any point p_0 of M it is one-to-one (and continuous both ways) in a sufficiently small neighborhood of p_0. Let p_0 be a point on M, p_0' its trace on M', and C' a curve on M' beginning at p_0'. If M covers M' without ramifications we can follow this curve on M by starting at p_0, at least up to a certain point where we would run against a "boundary of M relative to M'." Of chief interest are those covering manifolds M over a given M' for which this never happens and which therefore cover M' without ramifications and relative boundaries. The best way of defining the central topological notion "simply connected" is by describing a simply connected manifold as one having no other unramified unbounded covering but itself. There is a strongest of all unramified unbounded covering manifolds, the universal covering manifold, which can be described by the statement that on it a curve C is closed only if its trace C' is (closed and) homotopic to zero. The proof of the fundamental theorem on uniformization consists of two parts: (1) constructing the universal covering manifold of the given Riemann surface, (2) constructing by means of the Dirichlet principle a one-to-one conformal mapping of the covering manifold upon the interior of a circle of finite or infinite radius.

All we have discussed so far in our account of analysis, is in some way tied up with operators and projections in Hilbert space, the analogue in infinitely many dimensions of Euclidean space. In H. Minkowski's *Geometry of Numbers* distances $|AB|$, which are different from the Euclidean distance but satisfy the axioms that $|BA| = |AB|$ and that in a triangle ABC the inequality $|AC| \leq |AB| + |BC|$ holds, were used to great advantage for obtaining numerous results concerning the solvability of inequalities by integers. We do not find time here to report on the progress of this attractive branch of number theory during the last fifty years. In infinitely many dimensions spaces endowed with a metric of this sort, of a more general nature than the Euclid-Hilbert metric, have been introduced by Banach, not however for number-theoretic but for purely analytic purposes. Whether the importance of the subject justifies the large number of papers written on *Banach spaces* is perhaps questionable.

The Dirichlet principle is but the simplest example of the direct methods of the Calculus of Variation as they came into use with the turn of the century. It was by these methods that the theory of *minimal surfaces*, so closely related to that of analytic functions, was put on a new footing. What we know about non-linear differential equations has been obtained either by the topological fixed point method (see above) or by the so-called continuity method or by constructing their solutions as extremals of a suitable functional.

A continuous function on an n-dimensional compact manifold assumes somewhere a minimum and somewhere else a maximum value. Interpret the function as altitude. Besides summit (local maximum) and bottom (local minimum) one has the further possibility of a saddle point (pass) as a point of "stationary" altitude. In n dimensions the several possibilities are indicated by an inertial index k which is capable of the values $k = 0, 1, 2, \cdots, n$, the value $k = 0$ a minimum and $k = n$ characterizing a maximum. Marston Morse discovered the inequality $M_k \geqq B_k$ between the number M_k of stationary points of index k and the Betti number B_k of linearly independent homology classes of k-dimensional cycles. In their generalization to functional spaces these relations have opened a line of study adequately described as *Calculus of Variation in the large.*

Development of the theory of uniformization for analytic functions led to a closer investigation of *conformal mapping* of 2-dimensional manifolds in the large, which resulted in a number of theorems of surprising simplicity and beauty. In the same field there is to register an enormous extension of our knowledge of the behavior of *meromorphic functions*, *i.e.*, single-valued analytic functions of the complex variable z which are regular everywhere with the exception of isolated "poles" (points of infinity). Towards the end of the previous century Riemann's zeta function had provided the stimulus for a deeper study of "entire functions" (functions without poles). The greatest stride forward, both in methods and results, was marked by a paper on meromorphic functions published in 1925 by the Finnish mathematician Rolf Nevanlinna. Besides meromorphic functions in the z-plane one can study such functions on a given Riemann surface; and in the way in which the theory of algebraic functions (equal to meromorphic functions on a compact Riemann surface) as a theory of algebraic curves in two complex dimensions may be generalized to any number of dimensions, so one can pass from meromorphic functions to meromorphic curves.

The theory of *analytic functions of several complex variables*, in spite of a number of deep results, is still in its infancy.

10. Geometry. After having dealt at some length with the problems of analysis and topology I must be brief about geometry. Of subjects mentioned before, minimal surfaces, conformal mapping, algebraic manifolds and the whole of topology could be subsumed under the title of geometry. In the domain of *elementary axiomatic geometry* one strange discovery, that of von Neumann's pointless "continuous geometries" stands out, because it is intimately interrelated with quantum mechanics, logic and the general algebraic theory of "lattices." The 1-, 2-, $\cdots$, n-dimensional linear manifolds of an n-dimensional vector space form the 0-, 1-, $\cdots$, $(n-1)$-dimensional linear manifolds in an $(n-1)$-dimensional projective point space. The usual axiomatic foundation of projective geometry uses the points as the primitive elements or atoms of which the higher-than-zero-dimensional manifolds are composed. However, there is possible a treatment where the linear manifolds of all dimensions figure as elements, and the axioms deal with the relation "B contains A" ($A \subset B$) between these elements and the operation of intersection, $A \cap B$, and of union, $A \cup B$, performed on them; the union $A \cup B$ consists of all sums $x + y$ of a vector x in A and a vector y in B. In quantum logic this relation and these operations correspond to the relation of implication ("The statement A implies B") and the operations 'and,' 'or' in classical logic. But whereas in classical logic the distributive law

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

holds, this is not so in quantum logic; it must be replaced by the weaker axiom:

$$\text{If} \quad C \subset A \quad \text{then} \quad A \cap (B \cup C) = (A \cap B) \cup C.$$

On formulating the axioms without the implication of finite dimensionality one will come across several possibilities; one leads to the Hilbert space in which quantum mechanics operates, another to von Neumann's continuous geometry with its continuous scale of dimensions, in which elements of arbitrarily low dimensions exist but none of dimension zero.

The most important development of geometry in the twentieth century took place in differential geometry and was stimulated by general relativity, which showed that the world is a 4-dimensional manifold endowed with a Riemannian metric. A piece of an n-dimensional manifold can be mapped in one-to-one continuous fashion upon a piece of the n-dimensional "arithmetical space" which consists of all n-uples $(x_1, x_2, \cdots, x_n)$ of real numbers x_i. A *Riemann metric* assigns to a line element which leads from the point $P = (x_1, \cdots, x_n)$ to the infinitely near point $P' = (x_1 + dx_1, \cdots, x_n + dx_n)$ a distance ds the square of which is a quadratic form of the relative coordinates dx_i,

$$ds^2 = \sum g_{ij}dx_i dx_j, \qquad (i, j = 1, \cdots, n)$$

with coefficients g_{ij} depending on the point P but not on the line element. This means that, in the infinitely small, Pythagoras' theorem and hence Euclidian geometry are valid, but in general not in a region of finite extension. The line elements at a point may be considered as the infinitesimal vectors of an n-dimensional vector space in P, the tangent space or the compass at P; indeed an arbitrary (differentiable) transformation of the coordinates x_i induces a linear transformation of the components dx_i of any line element at a given point P. As Levi-Civita found in 1915 the development of Riemannian geometry hinges on the fact that a Riemannian metric uniquely determines an infinitesimal parallel displacement of the vector compass at P to any infinitely near point P'. From this a general scheme for differential geometry arose in which each point P of the manifold is associated with a homogeneous space Σ_P described by a definite group of "authomorphisms," this space now taking over the role of the tangent space (whose group of authomorphisms consists of all non-singular linear transformations). One assumes that one knows how this associated space Σ_P is transferred by infinitesimal displacement to the space $\Sigma_{P'}$ associated with any infinitely near point P'. The most fundamental notion of Riemannian geometry, that of curvature, which figures so prominently in Einstein's equations of the gravitational field, can be carried over to this general scheme. Thus one has erected general differential affine, projective, conformal, geometries, *etc.* One has also tried by their structures to account for the other physical fields existing in nature beside the gravitational one, namely the electromagnetic field, the electronic wave-field and further fields corresponding to the several kinds of elementary particles. But it seems to the author that so far all such speculative attempts of building up a unified field theory have failed. There are very good reasons for interpreting gravitation in terms of the basic concepts of differential geometry. But it is probably unsound to try to "geometrize" all physical entities.

Differential geometry in the large is an interesting field of investigation which relates the differential properties of a manifold with its topological structure. The schema of differential geometry explained above with its associated spaces

Σ_P and their displacements has a purely topological kernel which has recently developed under the name of *fibre spaces* into an important topological technique.

Our account of progress made during the last fifty years in analysis, geometry and topology had to touch on many special subjects. It would have failed completely had it not imparted to the reader some feeling of the close relationship connecting all these mathematical endeavors. As the last example of fibre spaces (beside many others) shows, this unity in diversity even makes a clear-cut division into analysis, geometry, topology (and algebra) practically impossible.

11. Foundations. Finally a few words about the *foundations of mathematics.* The nineteenth century had witnessed the critical analysis of all mathematical notions including that of natural numbers to the point where they got reduced to pure logic and the ideas "set" and "mapping." At the end of the century it became clear that the unrestricted formation of sets, sub-sets of sets, sets of sets *etc.*, together with an unimpeded application to them as to the original elements of the logical quantifiers "there exists" and "all" [cf. the sentences: the (natural) number n is even if there exists a number x such that $n = 2x$; it is odd if n is different from $2x$ for all x] inexorably leads to antinomies. The three most characteristic contributions of the twentieth century to the solution of this Gordian knot are connected with the names of L. E. J. Brouwer, David Hilbert and Kurt Gödel. Brouwer's critique of "mathematical existentialism" not only dissolved the antinomies completely but also destroyed a good part of classical mathematics that had heretofore been universally accepted.

If only the historical event that somebody has succeeded in constructing a (natural) number n with the given property P can give a right to the assertion that "there exists a number with that property" then the alternative that there either exists such a number or that all numbers have the opposite property non-P is without foundation. The principle of excluded middle for such sentences may be valid for God who surveys the infinite sequence of all natural numbers, as it were, with one glance, but not for human logic. Since the quantifiers "there is" and "all" are piled upon each other in the most manifold way in the formation of mathematical propositions, Brouwer's critique makes almost all of them meaningless, and therefore Brouwer set out to build up a new mathematics which makes no use of that logical principle. I think that everybody has to accept Brouwer's critique who wants to hold on to the belief that mathematical propositions tell the sheer truth, truth based on evidence. At least Brouwers' opponent, Hilbert, accepted it tacitly. He tried to save classical mathematics by converting it from a system of meaningful propositions into a game of meaningless formulas, and by showing that this game never leads to two formulas, F and non-F, which are inconsistent. Consistency, not truth, is his aim. His attempts at proving consistency revealed the astonishingly complex logical structure of mathematics. The first steps were promising indeed. But then Gödel's discovery cast a deep shadow over Hilbert's enterprise. Consistency itself may be expressed by a formula. What Gödel showed was this: If the game of mathematics is actually consistent then the formula of consistency cannot be proved within this game. How can we then hope to prove it at all?

This is where we stand now. It is pretty clear that our theory of the physical world is not a description of the phenomena as we perceive them, but is a bold symbolic construction. However, one may be surprised to learn that even mathematics shares this character. The success of the anti-phenomenological constructive method is undeniable. And yet the ultimate foundations on which it rests remain a mystery, even in mathematics.

MATHEMATICAL NOTES

EDITED BY F. A. FICKEN, *New York University*

Material for this department should be sent to F. A. Ficken, Institute for Mathematics and Mechanics, New York University, 45 Fourth Ave., New York 3, New York.

ON EVEN NUMBERS m DIVIDING 2^m-2

N. G. W. H. BEEGER, Amsterdam, Netherlands

In a recent paper P. Erdös [1] notes that D. H. Lehmer has recently detected the first case of an even number $m=2.73.1103=161038$ which satisfies the congruence

$$2^m - 2 \equiv 0 \pmod{m}. \tag{1}$$

It is the purpose of this paper to give three more such numbers and to prove that there exists an infinity.

In the first place it is clear from (1) that m is not divisible by 4 so that setting $m=2n$ (n odd), congruence (1) is equivalent to

$$2^{2n-1} - 1 \equiv 0 \pmod{n}. \tag{2}$$

In what follows we denote by e_p the exponent of 2 (mod p), p a prime, that is, the least positive x for which $2^x \equiv 1 \pmod{p}$. It is well known that e_p divides $p-1$ as well as any other x for which $2^x \equiv 1 \pmod{p}$. In particular if p is any prime factor of n in (2) then clearly e_p is odd since it divides $2n-1$.

THEOREM 1. *If* (2) *holds then n has at least two prime factors.*

Proof. If possible let $n=p^k$, then

$$2p^k - 1 = 2(p^k - 1) + 1$$

is divisible by e_p. But e_p divides $p-1$ and hence p^k-1. Therefore $e_p=1$, which is impossible.