THE TEACHING OF MATHEMATICS
2001, Vol. IV, 2, pp. 71–104

SELECTED CHAPTERS FROM ALGEBRA

I. R. Shafarevich

Abstract. This paper is the sixth part of the publication "Selected chapters from algebra", the first five having been published in previous issues of The Teaching of Mathematics, Vol. I (1998), 1–22, Vol. II, 1 (1999), 1–30, Vol. II, 2 (1999), 65–80, Vol. III, 1 (2000), 15–40, Vol. III, 2 (2000), 63–82 and Vol. IV, 1 (2001), 1–34.

AMS Subject Classification: 00 A 35

Key words and phrases: Finite and infinite sets; countable sets, continuum, algebraic and transcendental numbers, thin sets, normal numbers, strong inequality of Chebyshev.

CHAPTER VI. INFINITE SETS

1. Equivalence

In this Chapter we shall deal with infinite sets. Here "infinite" generalizations of some concepts that we introduced in Chapter III appear naturally. For example, let M_1, M_2, M_3, … be an infinite system of subsets of a certain set M. Subset M' of M, containing elements belonging to at least one of the subsets M_i, will be called the *union* of these subsets and denoted in the same way: $M' = M_1 \cup M_2 \cup M_3 \cup \cdots$. We will write

$$M' = \bigcup_{n\geqslant 1} M_n,$$

for short. For example, if M is the set of all natural numbers and M_n contains all numbers k for which $k \leqslant 2^n$, then $\bigcup_{n\geqslant 1} M_n = M$.

In the same way, if $M_1, M_2, \dots, M_n, \dots$ is an infinite system of subsets of a set M, then those elements common to all subsets M_n, $n = 1, 2, \dots$, form their *intersection*. It is denoted by $M_1 \cap M_2 \cap \cdots$ or $\bigcap_{n\geqslant 1} M_n$. For example, if M is the set of all natural numbers and M_n its subset containing all numbers divisible by n, then $\bigcap_{n\geqslant 1} M_n$ is empty.

If the subsets M_n are mutually disjoint (i.e. $M_i \cap M_j = \varnothing$ for $i \neq j$), then their union is called the *sum* and it is denoted by $M_1 + M_2 + \cdots + M_n + \cdots$. For example, if M is the set of all natural numbers and M_n contains all numbers k such that $2^{n-1} < k \leqslant 2^n$, then $M = M_1 + M_2 + \cdots + M_n + \cdots$.

This paper is an English translation of: И. Р. Шафаревич, *Избраные главы алгебры. Глава VI. Бесконечные множества*, Математическое образование, N 3–4(6–7), иль--дек. 1998, Москва, стр. 2--36. In the opinion of the editors, the paper merits wider circulation and we are thankful to the author for his kind permission to let us make this version.

When dealing with infinite sets we immediately encounter the fact that one fundamental notion which we used to formulate all questions and assertions in Chapter III does not exist here—the notion of the number of elements of a set. However, in Chapter III we stated the principle of *equivalence* of two finite sets (i.e. when they have the same number of elements) in another way: *two finite sets are equivalent if and only if there exists a one-to-one correspondence between them.* First of the notions—the number of elements of a set—cannot be applied to infinite sets, but the second—one-to-one correspondence—can be applied. So we can transform the previous principle into the definition of equivalence of two sets, which makes sense for arbitrary sets:

> *Two sets are called equivalent (equipotent) if there exists a one-to-one correspondence between them.*

In this way we can distinguish between finite sets with 1, 2, 3, etc. elements, as well as between infinite sets according to whether they are equivalent to each other. This procedure of dealing with infinite sets was considered by scientists long ago. But there was a seemingly paradoxical phenomenon: a set can be equivalent to its proper subset. For example, the set of all natural numbers is equivalent to the set of even natural numbers. If is enough to notice that for each natural number n there is a corresponding number $2n$; this is obviously a one-to-one correspondence between the sets of natural and even natural numbers. "Paradoxicality" comes from the obvious fact that such a situation cannot arise for finite sets. So it seemed that even the notion of equivalence does not make sense for infinite sets. For example, Galileo in his "Dialogues" gives an example of a one-to-one correspondence between natural numbers and squares of natural numbers where n and n^2 correspond to each other. One of the participants concludes:

> "properties of equalities, and also of inequalities, do not hold when we deal with infinities".

Only much later, in the second half of the XIX century, Dedekind introduced the notion of equivalence as a fundamental notion for dealing with infinite sets. He took a property which was considered "paradoxical" before as a *definition* of an infinite set: a set M is infinite if it is equivalent to its proper subset $M' \subset M$. We shall prove later that this property is in fact equivalent to infinity of the set.

We shall often use the following simple fact:

If the sets A and B are equivalent and B and C are equivalent, then A and C are also equivalent.

Really, since A and B are equivalent, there exists a one-to-one correspondence between them. Let this correspondence map an element $a \in A$ to an element $b \in B$. Analogously, since B and C are equivalent, there exists another one-to-one correspondence between B and C. Let this correspondence map the element b to an element $c \in C$. The correspondence which maps a into c is a one-to-one correspondence between the sets A and C (check it yourself!). Hence, A and C are equivalent.

Using the previous property, if we want to prove equivalence of two sets A and

B we can replace A with an equivalent set A' and then prove equivalence of sets A' and B. Analogously, B can also be replaced by an equivalent set B'. We shall often use this method, even without mentioning it. It is analogous to the following reasoning: in order to prove $a = b$, it is enough to prove $a = a'$ for some a' and then $a' = b$.

Let us first consider some simple infinite sets. The simplest example of an infinite set is the "natural sequence of numbers", i.e. the set of all natural numbers. Each set equivalent to the set of natural numbers will be called *countable*.

Thus, for a countable set M there must exist a one-to-one correspondence between M and the set N of natural numbers. If in such correspondence an element $a \in M$ corresponds to a natural number n, we can say that it is indexed by n and so the whole set M is *numbered*. In other words, the set M is countable if it can be written in the form of an infinite sequence $M = \{a_1, a_2, \dots\}$.

Countable sets are in a certain sense "the smallest" among infinite sets. First of all, *each subset of a countable set is either finite or countable*. Indeed, a countable set M can be numbered: $M = \{a_1, a_2, \dots, a_n \dots\}$. Let M' be its subset. We can number it, calling an element a_k first if k is the smallest index for which a_k belongs to M'; then calling an element a_l second if l is the smallest index for which $l > k$ and a_l belongs to M' and so on. This process will either stop—in which case the subset is finite—or it will continue to give a numbering of all elements of M', since each of them is contained among elements $a_1, a_2, \dots, a_n, \dots$, and will eventually be obtained.

The same property of countable sets as "the smallest" infinite sets can be described in the following way.

Theorem 1. *Each infinite set contains a countable subset.*

Proof. Let M be an infinite set. Choose an arbitrary element a_1 of M. Since M is infinite, it contains other elements as well. Choose from them an element a_2 different from a_1. Since M is infinite, it contains elements different from a_1 and a_2. Choose from them an element a_3. Continuing in this way, if we have already found n distinct elements $a_1, \dots, a_n$ of M, then, since this set is infinite, these elements cannot exhaust it—we can choose again an element a_{n+1} of M from those that are different from all of $a_1, \dots, a_n$. The subset $N = \{a_1, a_2, a_3, \dots\}$ that we obtain in this way consists of distinct elements. Their numbering gives a one-to-one correspondence between N and the set of all natural numbers.

Note that as the first element a_1 in the construction we could use any arbitrary element a of the set M, which means that there exists a countable subset N such that $N \ni a$.

Corollary. *Each infinite set M is equivalent to one of its subsets, different from the whole set M.*

We shall prove this assertion in a more explicit form: for each element a of a given infinite set M, the set $\overline{\{a\}}$ obtained from M by deletion of a, is equivalent to M ($\overline{\{a\}}$ is the complement of the one-element set $\{a\}$ in M). Consider first the case when M is the set of natural numbers N and $N' = \overline{\{a\}}$, where a is an arbitrary natural number. Correspond to each number $n < a$ the number n itself, and to each $n \geqslant a$ the number $n+1$. It is obvious that we have obtained a one-to-one correspondence between N and N'. Hence, this assertion is valid for each countable set.

For an arbitrary infinite set M we shall use Theorem 1. Suppose that M contains a countable subset N. As we have seen, we may suppose that $a \in N$. As we have proved, there exists a one-to-one correspondence between N and N', where N' is obtained by deletion of a from N. Let $\overline{N}$ be the complement of the set N in M, and M' is obtained by deletion of a from M. Then $M = N + \overline{N}$, $M' = N' + \overline{N}$. We can construct a one-to-one correspondence between M and M' extending the already found correspondence between N and N' so that each $b \in \overline{N}$ is mapped onto itself. Thus, we obtain that the sets M and M' are equivalent.

Let us state a few more examples of countable sets.

1. *The set of all integers is countable.*

Correspond the number 0 to number 1, positive integer n to number $2n$ and negative integer $-m$ to number $2m+1$. We obtain a one-to-one correspondence between the set of integers and the set of natural numbers.

Corollary. *The set which is the sum of two countable sets is countable itself.*

Let $A = B + C$. If B and C are countable, then B is equivalent to the set of positive integers, and C is equivalent to the set of negative integers. Hence, A is equivalent to the set of all integers and is therefore countable. (Note that we obtained only integers different from 0. How can this problem be surpassed?)

2. *The set of all positive rational numbers is countable.*

For a positive rational number $\frac{m}{n}$, let us call $m+n$ its height (we consider m and n to be relatively prime). Obviously, there exist only finitely many rational numbers of any given height. Write down first of all the rational numbers of height 2, then of height 3, etc. We obtain an infinite sequence in which each positive rational number appears, sooner or later. If we correspond to each positive rational number its index in this sequence, we obtain a one-to-one correspondence between the set of positive rational numbers and the set of natural numbers. The beginning of our sequence is as follows:

$$1,\ \frac{1}{2},\ 2,\ \frac{1}{3},\ 3,\ \frac{1}{4},\ 4,\ \frac{2}{3},\ \frac{3}{2},\ \dots$$

Here we put $2 = \frac{2}{1}$, $3 = \frac{3}{1}$, $4 = \frac{4}{1}$, ...

Corollary. *The set of all rational numbers is countable.*

We have already established a one-to-one correspondence between the set of positive rational numbers and the set of natural numbers. Analogously, there exists a one-to-one correspondence between the set of negative rational numbers and the set of negative integers. Corresponding zero to zero, we obtain a one-to-one correspondence between all rational numbers and all integers. Since, according to Example 1, the latter set is countable, the former is countable, too.

In Example 2 we represented the set of rational numbers M as a sum of countably many finite subsets M_k, where M_k is the set of rational numbers of height k. Therefore the result of Example 2 follows from the following general result: a countable sum of finite sets is countable. We shall prove even stronger result.

3. *A countable sum of finite or countable sets is countable.*

The proof is based on the same principle we used in Example 2. Let $M = M_1 + M_2 + M_3 + \cdots$. Since the set M_i is finite or countable, its elements can be numbered. We shall assume that all of the sets M_i are really numbered. Define the height of an element a of M. If it belongs to the set M_i and is numbered by the index j in it, its height will be $i + j$. Obviously, there exist only finitely many elements of a given height. Really, if $i + j = n$ is given, then $i < n$, so that an element a of the height n can only belong to one of the sets $M_1, \ldots, M_{n-1}$. If it belongs to M_i, then it has a number $j = n - i < n$ there. There are only finitely many such elements. Therefore, we can list first all the elements of height 2, then of height 3, etc. The principle of numbering the elements of the set M is shown in Fig. 1, where the set M_1 is written in the first row, the set M_2 in the second, etc., and the numbering of elements of M is represented by the zigzag line. It is assumed in Fig. 1 that all of the sets M_i are countable. Try to draw the corresponding figure in which, e.g., the set M_1 is finite and has three elements.

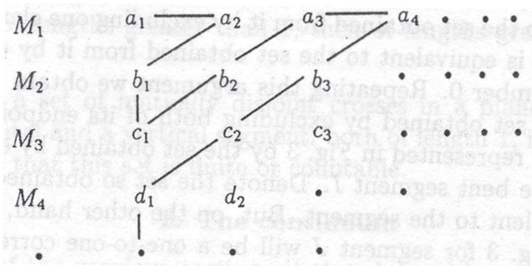


Fig. 1

We have given several examples of countable sets. They are all mutually equivalent. We shall give now some other examples of mutually equivalent sets.

4. *Two arbitrary segments of the real line are equivalent.* We can put our segments $[a, b]$ and $[c, d]$ on two parallel lines and establish a one-to-one correspondence between them as shown in Fig. 2. More precisely, we connect an arbitrary point x of the segment $[a, b]$ with the point P of intersection of the straight lines ac and bd, and we correspond to x the point y of the segment $[c, d]$ which is the point of intersection of the line Px and the line cd containing the segment $[c, d]$.

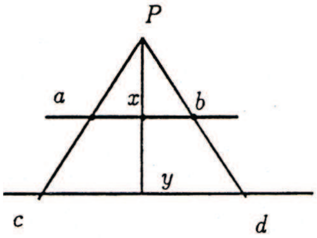


Fig. 2

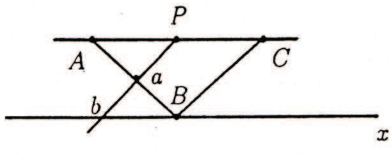


Fig. 3

5. *Every line segment is equivalent to the whole line*, i.e. to the set of all real numbers. Taking into account Example 4, it is enough to consider an arbitrary segment, e.g. $[0, 1]$. Denote it by I. Divide the segment I into two equal parts by the point $1/2$ and, bending it in this point, place it on the plane as shown in Fig. 3: as two equal segments $[A, B]$ and $[B, C]$ of the length $1/2$, making equal angles with the x-axis.

Denote by P the midpoint of the segment AC and make the projection of the bent segment I as in Example 4, i.e. corresponding to the point a the point b of intersection of the line aP with the x-axis. Obviously, the bent segment I is equivalent to the original one. The given correspondence of the bent segment with the line x is one-to-one, with the exception that there is no point of the line x which would correspond to the endpoints A and C, since the lines PA and PC are parallel to this axes and do not intersect it. We shall thus slightly change our construction. Recall that in the proof of the Corollary of Theorem 1 we proved that each infinite set is equivalent to the set obtained from it by excluding one element. In particular, the segment $[0, 1]$ is equivalent to the set obtained from it by excluding one of its endpoints, the number 0. Repeating this argument we obtain that the segment is equivalent to the set obtained by excluding both of its endpoints, the numbers 0 and 1. This set is represented in Fig. 3 by the set obtained by excluding the points A and C from the bent segment I. Denote the set so obtained by J. It is, as we have seen, equivalent to the segment. But, on the other hand, the correspondence represented in Fig. 3 for segment J will be a one-to-one correspondence between this set and the whole x-axis. This proves our assertion.

Problems

1. Prove that the product of two countable sets is countable. The notion of the product of sets was defined in Sec. 1 of Ch. III and it is valid for infinite sets as well as for finite ones.

2. Prove that each circle is equivalent to the segment.

3. Divide the segment $[0, 1]$ into two parts by the number $1/2$, then divide the segment $[1/2, 1]$ into two parts by the number $\frac{1}{2} + \frac{1}{4}$, etc. We obtain numbers $\alpha_n = \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n}$. Prove that the segment $[0, 1]$ is the sum of the intervals $[\alpha_n, \alpha_{n+1})$. Prove, analogously, that the line is a countable sum of the intervals

$[n, n+1)$, where n runs through all integers. Prove that the segments $[\alpha_n, \alpha_{n+1})$ and $[n, n+1)$ are equivalent and deduce again that the segment and the line are equivalent (Example 5).

4. Find explicit formulae for the one-to-one correspondence between the segments $[a, b]$ and $[c, d]$ constructed in Example 4.

5. Prove that there is no one-to-one correspondence between the set of all integers and the set of natural numbers which preserves addition, that is such that if m is mapped onto m' and n is mapped onto n', then $m + n$ is mapped onto $m' + n'$.

6. Prove that there is no one-to-one correspondence between the set of all integers and the set of natural numbers which preserves order, that is such that if m is mapped onto m' and n is mapped onto n', and $m < n$, then $m' < n'$.

7. Define the distance between two points on a circle as the length of the shortest arc of the circle connecting these points. The distance between points A and B on a line segment will, as usual, be the length of the segment AB. Prove that there is no one-to-one correspondence between the set of the points of a circle and the set of the points of an arbitrary segment preserving distances, that is such that if A is mapped onto A' and B is mapped onto B', then the distance between A and B is equal to the distance between A' and B'. Is this assertion valid if we exclude a point from the circle?

8. There is a set of mutually disjoint segments on a line. Prove that the set of these segments is finite or countable. [*Hint.* Prove that the set of segments contained in a given one is finite or countable. In order to do that consider the set of the segments of lengths greater than 1, then of lengths greater than 1/2, 1/3, etc.]

9. There is a set of mutually disjoint crosses in a plane, each of which is made of a horizontal and a vertical segment, both of length 1, intersecting at their midpoints. Prove that this set is finite or countable.

2. The continuum

At the end of the previous section we stated several examples which can be divided into two groups: A—countable sets (all of these are, by definition, mutually equivalent) and B—sets equivalent to a segment (and so also mutually equivalent). A question remained open: are the sets of the first group equivalent to the sets of the second one? The principle of classification of sets depending on their equivalence would probably remain a pure mathematical game if it was not possible to prove that two sets from groups A and B, respectively, are not equivalent. This fact has a fundamental role for the whole mathematics.

Theorem 2. *The set of all points of a segment is not countable.*

We shall give two proofs of this Theorem, using two different properties of segments. As we saw in Section 1, all the segments are equivalent to one of them, e.g., $[0, 1]$, so we shall consider this particular one.

First proof. If the segment $[0,1]$ were countable, then the set obtained from it by deletion of its right endpoint 1 would be countable, too. Write down each number of this set as a decimal expansion $0.a_1a_2\ldots$, where a_i takes values from $\{0,1,\ldots,9\}$. Suppose that all these numbers can be numbered as x_1, x_2, ... , x_n, ... , and write down their decimal representations in the following way:

$$\begin{array}{rl} x_1: & 0.a_1a_2a_3\ldots \\ x_2: & 0.b_1b_2b_3\ldots \\ x_3: & 0.c_1c_2c_3\ldots \\ \cdot & \ldots\ldots\ldots \\ \cdot & \ldots\ldots\ldots \\ \cdot & \ldots\ldots\ldots \end{array} \tag{1}$$

We will derive a contradiction from the assumption that we have numbered *all* of the numbers of the segment by constructing a decimal expansion which does not appear on the list (1). We shall construct it in the form $y = 0.k_1k_2k_3\ldots$. Choose the first digit k_1 so that $k_1 \neq a_1$. Then, for an arbitrary choice of the subsequent digits, $y \neq x_1$. After that, we choose $k_2 \neq b_2$—then for an arbitrary choice of the subsequent digits, $y \neq x_2$. Then we choose $k_3 \neq c_3$ and so on: k_n is chosen to be different from the digit in the n-th place on the n-th row of table (1). Then we are sure that $y \neq x_n$. After choosing all the digits k_n, we find that y does not coincide with any of the x_k's.

One can make the following objection to this reasoning. In Sec. 2 of Chapter V we saw that the correspondence between the numbers of the segment and the decimal expansions is *not* one-to-one—it is violated because of the infinite decimal expansions having 9 as the period. But if we exclude these expansions, then the correspondence will be one-to-one. Therefore, we have to use only expansions that do not have 9 as a period. As a result, each expansion in table (1) will not have 9 as a period. But we have also to ensure that our decimal expansion y does not have 9 as a period. This is definitely possible: when choosing a digit k_n, we have to obey just one condition: k_n has to be distinct from the n-th digit in the n-th row of the table (1). But, since we have 10 possible digits—0, 1, 2, ... , 9—we can choose k_n also different from 9. As a result, the digit 9 will not appear in our expansion y at all. The proof is complete. The process of constructing the expansion y is called the *diagonal process*.

Second proof. In this proof we shall use segments determined by two points a and b, $a \neq b$, where the order $a < b$ or $a > b$ is not given in advance. We shall denote them as $[a,b]$ in both cases, so that if $a > b$, then $[a,b]$ is in fact the segment $[b,a]$. Note that every segment contains points distinct from its endpoints—e.g., the segment $[a,b]$ contains its midpoint $\frac{1}{2}(a+b)$. Applying this reasoning to the segment $[a, \frac{1}{2}(a+b)]$ and repeating it, we deduce that each segment contains infinite number of points.

We come now to the proof of our assertion and we again suppose that the points of the segment $[0, 1]$ are numbered as

$$x_1,\ x_2,\ x_3,\ x_4,\ \dots \tag{2}$$

Since numbering of the segment is, by the assumption, a one-to-one correspondence, the numbers x_m and x_n are different for $m \neq n$. We will prove that the assumption about countability of the segment is contradictory to the Axiom of embedded segments. We first construct a system of embedded segments. We start with the segment $[x_1, x_2]$ and choose only those of the numbers in the sequence (2) which are contained in this segment, not coinciding with the endpoints. As we have seen, there is an infinite number of such numbers and they constitute a new sequence

$$x_p,\ x_q,\ x_r,\ \dots \tag{3}$$

where $1 < 2 < p < q < r < \cdots$. Consider the segment $[x_p, x_q]$ and choose those of the numbers in the sequence (3) which are contained in this segment and do not coincide with the endpoints. We obtain another sequence

$$x_m,\ x_n,\ x_k,\ \dots$$

where $p < q < m < n < k < \cdots$.

This process can be repeated to infinity: we obtain in each step infinitely many numbers from a certain segment, which are contained in sequence (2), and in its part constructed in the previous step. In this way we obtain a countable number of sequences:

$$\begin{gathered} x_p,\ x_q,\ x_r,\ \dots \\ x_m,\ x_n,\ x_k,\ \dots \\ \dots\dots\dots\dots, \end{gathered}$$

where the first sequence contains all of the points of the segment $[x_1, x_2]$, except the endpoints, the second contains all of the points of the segment $[x_p, x_q]$, except the endpoints, etc. By construction, each new sequence starts with a greater index than the previous one and therefore no number from sequence (2) can belong to all of them. But sequences (2), (3), etc., are simply all of the numbers of the segments $[x_1, x_2] \supset [x_p, x_q] \supset [x_m, x_n] \supset \cdots$, except their endpoints. According to the Axiom of embedded segments, there exists a number contained in all of the segments $[x_1, x_2]$, $[x_p, x_q]$, $[x_m, x_n]$, $\dots$. If it belonged, e.g., to the segment $[x_m, x_n]$, it would, a fortiori, belong to the segment $[x_p, x_q]$, and it would not coincide with its endpoints, i.e., it would belong to one of the sequences (2), (3), $\dots$. But we have seen that no number from sequence (2) can belong to each of these sequences, and all of the numbers from the segment $[0, 1]$ are by assumption contained in sequence (2). This contradiction proves the theorem.

The second proof is a bit more complicated than the first one, but it has an advantage that it does not use the representation of numbers in any position system and it proves Theorem 2 directly from the axioms of real numbers.

Both proofs were found by Cantor in the nineteen seventies, and he had found the latter proof before the former (he was troubled by the difficulties connected with expansions having 9 as a period). As we have seen, both arguments are very easy, but the statement of the problem was completely new at the time. Cantor himself, in one of his later articles, said that it took him 8 years to complete the proof of the uncountability of a segment. A very interesting correspondence between Cantor and Dedekind was kept which showed how hard it was to arrive at these new ideas. Cantor wrote that he could not answer the question whether segment was countable or not and asked Dedekind whether he knew the answer. The latter answered that he did not know how to prove it (both of them guessed the answer correctly), but he said that the question was, to his opinion, not worth dealing with, since it was hardly probable that interesting corollaries could be deduced from it.

It is striking that Dedekind did not feel the importance of the question—not least because of the fact that the uncountability of a segment and countability of the set of rational numbers immediately imply the existence of irrational numbers in a completely new way (before that the existence of irrational numbers had been proved only by the argument we followed in Chapter I). It is even more striking that Dedekind himself proved a statement which, together with the uncountability of a segment, implied an even more important consequence.

It is connected with a concept that we have not mentioned before, but which was well known at the time of Dedekind and Cantor. A number α is called *algebraic* if it is a root of a polynomial $a_0 + a_1x + \cdots + a_nx^n$ with rational coefficients a_i. Since the roots of a polynomial do not change when the polynomial is multiplied by a number, we can multiply the polynomial $a_0 + a_1x + \cdots + a_nx^n$ by a common denominator of all the numbers $a_0, \ldots, a_n$, and so we can assume from the beginning that the coefficients $a_0, \ldots, a_n$ are integers. Those numbers that are not algebraic are called *transcendental*.

THEOREM 3. *The set of all algebraic numbers is countable.*

Proof. Let us call the number $n + |a_0| + |a_1| + \cdots + |a_n|$ the *height* of the polynomial $a_0+a_1x+\cdots+a_nx^n$. Obviously, the height of a polynomial is a natural number. It is also obvious that there exist only finitely many polynomials whose height is not greater than a given number m. Indeed, if $n+|a_0|+|a_1|+\cdots+|a_n| \leqslant m$, then $n \leqslant m$ and $|a_i| \leqslant m$ for all $i = 0, 1, \ldots, n$. Hence, for each coefficient a_i there are no more than $2m+1$ possibilities ($-m, -m+1, \ldots, -1, 0, 1, \ldots, m$) and the number of all such polynomials is finite.

Consider now the set of all algebraic numbers which are roots of polynomials with integer coefficients and with height not exceeding a given natural number m. Denote this set by A_m. It is finite: really, the number of polynomials with height not exceeding m is finite, as we have already seen, and each polynomial has a finite number of roots (according to Theorem 3 of Ch. II). The union of all sets A_m for $m = 1, 2, \ldots$ is equal to the set of all algebraic numbers. From Example 3 of Sec. 1 it therefore follows that the set of algebraic numbers is countable.

Since the set of all real numbers is equivalent to the segment (Example 5 of Sec. 1), the existence of transcendental numbers follows from Theorem 3. And that is far from being an easy fact. Although Theorems 2 and 3 imply that there are "a lot more" transcendental numbers than the algebraic ones, it is a very difficult task to construct a single example of a transcendental number and even more difficult to prove transcendence of a certain given number. It was only in the middle of the XIX century that a number was constructed for which it was possible to prove that it was transcendental. The most famous transcendental number is the number π—its transcendence was proved in the nineteen eighties.

The assertion which we called Theorem 3 was proved by Dedekind in a letter to Cantor. It seems that in order to underline the importance of the new ideas, Cantor published a paper titled "On a property of the set of all algebraic real numbers", where he gave proofs of the assertions which we called Theorem 2 and Theorem 3, and deduced the existence of transcendental numbers from them. Dedekind acknowledged afterwards that his statement about the question of uncountability of the segment being not interesting had been "seriously disproved".

But the following discovery was a shock to Cantor himself.

THEOREM 4. *The set of points of a square is equivalent to the set of points of a segment.*

We shall compare the unit square and the segment of length 1. Let us start with a simple technical modification of the problem. Denote the square by K and remove its adjacent sides AB and BC, Fig. 4. Denote the set that remains by P, and the union of the sides AB and BC by L. Then $K = P + L$. Obviously, L is equivalent to the segment (it is a bent segment) and if we prove that P is equivalent to the segment, then K itself will be equivalent to the segment.

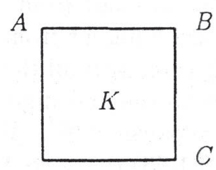


Fig. 6

We have already seen that the segment is equivalent to the set obtained by deleting one of its endpoints. Thus it is sufficient to prove that P is equivalent to the interval $[0, 1)$, with the point 1 deleted. Then, since L is equivalent to the segment $[1, 2]$, K will be equivalent to the segment $[0, 2]$. We need these obvious facts in order to pass from points to numbers. The coordinate method allows us to describe any point of the square P by a pair of numbers (x, y), where $0 \leqslant x < 1$ and $0 \leqslant y < 1$. In the same way, the points of the interval $[0, 1)$ correspond to numbers t with $0 \leqslant t < 1$. Hence, we need to construct a one-to-one correspondence between such pairs of numbers (x, y) and numbers t.

In order to do this, write down all the numbers we need in the form of decimal expansions

$$x = 0.a_1a_2a_3\ldots \tag{4}$$

$$y = 0.b_1b_2b_3\ldots \tag{5}$$

$$t = 0.c_1c_2c_3\ldots, \tag{6}$$

where a_i, b_j, c_k are digits from $\{0, 1, \ldots, 9\}$. All the points (x, y) of the set P and all the numbers t of the interval $[0, 1)$ can be given in this form. Correspond now a number t to the point (x, y) "mixing" expansions (4) and (5), i.e., put $c_1 = a_1$, $c_3 = a_2$, $c_5 = a_3$, $\dots$, $c_2 = b_1$, $c_4 = b_2$, $c_6 = b_3$, $\dots$ This correspondence is one-to-one since expansions (4) and (5) can be reconstructed from the expansion (6): the digits c_i with odd indices form the first expansion, and the digits with even indices form the latter one.

The previous argument has the same problem as our first proof of Theorem 2, namely expansions having 9 as a period. Really, in order that the correspondence between the numbers from a segment and the expansions be one-to-one, we had to exclude expansions which have 9 as a period. But even if expansion (6) does not have 9 as a period, it can happen that one of the generated expansions (4) and (5) still does. For example, if $t = 0.90909\dots$, then $x = 0.999\dots$. This objection was made by Dedekind when Cantor wrote to him about his proof. Cantor was not able to eliminate this defect, and so he soon found a new proof, not using decimal expansions.

As a matter of fact, the proof could be corrected easily. In order to do that, we have to complicate a bit the process of "mixing" expansions (4) and (5), paying special attention to appearance of the digit 9. Namely, we shall mix them as before, taking one digit from the first expansion and one from the second one, as long as they are different from 9. If one of the digits a_k and b_k is equal to 9, we shall take it together with all the 9's which follow it immediately in the respective expansion and with the first digit different from 9—and we shall put the whole group of digits into expansion (6). For example, from the expansions $x = 0.12(995)76\dots$ and $y = 0.4(93)51\dots$ we obtain the expansion $t = 0.142(93)(995)5716\dots$, where the parentheses contain groups of digits taken as a whole. The process of reconstruction of expansions (4) and (5) from expansion (6) also needs to be modified. As before, we put digits of expansion (6) into expansions (4) or (5) as long as they are different from 9. When we encounter a 9, we take it together with all the 9's that follow it and also with the first digit different from 9 that follows them, and put them all together as one group of digits. So within each group of digits that is put into a certain expansion, there is always a digit different from 9, and hence neither of these expansions can have 9 as a period.

This easy argument proves the result which seems contradictory to our geometrical intuition: figures of different dimension, such as a square and a segment, appear to be equivalent! It can also be proved that the cube is equivalent to them (Problem 1). The result shocked Cantor himself. He wrote to Dedekind: "The matter I have reported to you recently was so unexpected to myself, so new, that my mind cannot rest before I hear your opinion, my dear friend. Until I see your justification I can only say" — and there in the letter written in German he unexpectedly switches to French — " I can see but I do not believe" (probably a reference to the Evangelist saying "You believed when you saw me; blessed are those who have not seen but believe!"). It seemed to Cantor that the very mathematical description of our intuition about dimensions needed to be considered again: "The difference that exists between figures of different dimensions needs to be explained in a new way, not using the number of independent coordinates … "

In his reply Dedekind confirmed the validity of the new proof, but expressed his opinion that it does not contradict our belief that the dimension corresponds to the number of independent coordinates. "Authors have always without saying made the natural assumption that for a new definition of a point ... using the new coordinates, and hence the latter must be continuous functions of the old coordinates."

The notion of a continuous function was at that time formulated precisely and well known. We shall not go into the matter in general, but we will consider what can happen in our example of the constructed one-to-one correspondence between points of the square and of the segment. And this will be a consequence of the problems that are caused by digit 9 appearing as a period, and of our method of dealing with this problem. Consider two points (x, y) and (x', y), where $x = 0.10\dots0\dots$, $y = 0.0\dots0$, $x' = 0.09\dots90\dots$ (there are n 9's in x'). Obviously, $y = 0$, $x = \frac{1}{10}$ and $x' = \frac{9}{10^2} + \cdots + \frac{9}{10^{n+1}}$. Then

$$x' = \frac{9}{10^2}\left(1 + \frac{1}{10} + \cdots + \frac{1}{10^{n-1}}\right) = \frac{9}{10^2}\frac{1 - \frac{1}{10^n}}{1 - \frac{1}{10}}$$

(by the formula for the sum of geometric sequence). This number is equal to $\frac{1}{10}\left(1 - \frac{1}{10^n}\right) = \frac{1}{10} - \frac{1}{10^{n+1}}$. Thus, when n increases, x and x' come arbitrarily close to each other.

Consider now which points t and t' are corresponded to our points by the process described in the proof of Theorem 4. To obtain expansion t we just have to "mix" the expansions corresponding to points x and y. After the decimal point, we take 1 from x, then 0 from y, and then only zeros will follow, so that $t = 0.10\dots = \frac{1}{10}$. Consider in more detail the process of constructing the expansion t'. After the decimal point, we have to take 0 from x', then 0 from y, then we come to 9 in x' and we have to take the whole group of 9's together with the following 0. After that digits from y and from x' have to appear, but they are all zeros. As a result we obtain $t' = 0.009\dots90\dots$. In other words, $t' = \frac{9}{10^3} + \cdots + \frac{9}{10^{n+2}}$. As in the case of x' we can calculate:

$$t' = \frac{9}{10^3}\left(1 + \cdots + \frac{1}{10^{n-1}}\right) = \frac{9}{10^3}\frac{1 - \frac{1}{10^n}}{\frac{9}{10}} = \frac{1}{100}\left(1 - \frac{1}{10^n}\right) = \frac{1}{100} - \frac{1}{10^{n+1}}.$$

We have seen that when n grows, x and x' come arbitrarily close to each other. Since y is the same in both pairs, the pairs (x, y) and (x', y) come arbitrarily close to each other, too. But the corresponding points t and t' remain "far" from each other: $t = \frac{1}{10}$, $t' = \frac{1}{100} - \frac{1}{10^{n+1}}$ and $t - t' = \frac{1}{10} - \frac{1}{100} + \frac{1}{10^{n+1}} > \frac{1}{10} - \frac{1}{100} = \frac{9}{100}$. Thus, our correspondence somehow "tears apart" the square—points that are arbitrarily close to each other correspond to points which stay at a distance greater than a certain positive number. The process is similar to the process of tearing apart a sheet of paper.

In another letter to Cantor, Dedekind stated the assumption that if the requirement of continuity was included in the definition of one-to-one correspondence (we skip the precise formulation of that), then it would not be possible to construct a one-to-one correspondence between geometrical figures of different dimension (such as square and segment, or cube and square). He wrote that he had had no time to try to prove that, but he stated it "as his conviction and belief". Later on, Cantor agreed with the Dedekind's point of view and even published a proof of this hypothesis, which turned out to be false. Dedekind's hypothesis was only proved in 1910.

Sets equivalent to the segment are called *continual* or the *continuum*. Hence, Theorem 2 states that *the continuum is uncountable*. Practically all of the infinite sets appearing in mathematics belong to one of the two types—they are either continual or countable. Sets being neither continual nor countable can be constructed (Problem 8) and even an infinite set of infinite sets can be constructed, neither of which is equivalent to either of the others. But such sets are not very important to the rest of the mathematics. Similarly, the equivalence of the square and the segment (Theorem 4) has no important applications we may expect. We have explained the reason for this earlier. Usually sets appearing in mathematics are more specific, for example its elements are linked by certain relationships, or some actions or inequalities or (in geometry) distances are defined on them. In such cases we are interested just in those one-to-one correspondences which preserve these relationships between elements—and there may be a smaller number of them (see Problems 5, 6 and 7 of Sec. 1). Hence Theorem 4, in spite of its striking effect, is not a "working" mathematical result. But Theorem 2 is one of the most important results in mathematics.

Problems

1. Prove that the set of points of the unit cube, containing points (x, y, z), $0 \leqslant x < 1$, $0 \leqslant y < 1$, $0 \leqslant z < 1$ is equivalent to the interval $[0, 1)$.

2. Prove that if M_1 and M_2 are disjoint subsets of a set M and M_1 and M_2 are equivalent, then their complements $\overline{M}_1$ and $\overline{M}_2$ are equivalent. [*Hint.* Consider the special case $M_1 \cup M_2 = M$.]

3. Prove that the set of irrational numbers of the segment $[0, 1]$ is equivalent to the set N of the numbers of the interval not having the form $1/n$. [*Hint.* Compare both sets with the subset N' containing the numbers not having the form $\sqrt{2}/n$, $n > 1$ and apply Problem 2.]

4. Prove that the set of irrational numbers of the segment is continual. [*Hint.* Use Problem 3. It is sufficient to prove that the set N given in that Problem is continual. It divides the segment $[0, 1]$ into the segments $[\frac{1}{n+1}, \frac{1}{n}]$. Map each of these segments onto the segment $[n, n+1]$ contained in the infinite line and prove the equivalence of the set N and the half-line $x \geqslant 1$. Then use the method applied in Problem 5, Sec. 2. Pay attention to the endpoints of the segments!]

5. Prove that the set of all infinite sequences of the form $(a_1, a_2, \dots, a_n, \dots)$, where a_i can take values 0, 1, ..., 9, is continual.

6. A natural number $k > 1$ is given. Prove that the set of sequences $(a_1, a_2, \dots, a_n, \dots)$, where a_i are arbitrary integers, $0 \leqslant a_i < k$, is continual. [*Hint.* Correspond to each such sequence the number x, written in the number system with base k: $x = \frac{a_1}{k} + \frac{a_2}{k^2} + \dots + \frac{a_n}{k^n} + \cdots$. Think how to deal with the problem that this is not a one-to-one correspondence between these sequences and the points of the segment $[0, 1]$.]

7. Let U be the set of all subsets of a set M (when M is finite, we have already dealt with this set in Chapter III). Prove that the sets U and M are not equivalent. [*Hint.* Suppose that a one-to-one correspondence $a \leftrightarrow A$ between the elements and the subsets of the set M can be made, and consider the set B of all elements a which are not contained in the corresponding subset. Let in your correspondence $b \leftrightarrow B$. Consider two possibilities: $b \notin B$ and $b \in B$.]

8. Construct an infinite set which is neither countable nor continual.

3. Thin sets

In this Section we shall consider some specific properties connected with the countability of a set. We shall consider sets contained in the segment $[0, 1]$ and discuss the possibility of measuring the "length" of such sets. Clearly, the length of the whole segment $[0, 1]$ will naturally be taken to be equal to 1. Also, the length of a segment $[a, b]$ contained in $[0, 1]$ will be defined as equal to $b - a$. If a set consists of several disjoint segments, we will define its length to be the sum of the lengths of these segments. For example, the length of the set $M = [0, 1/2] \cup [3/4, 1]$ is equal to $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$. But an arbitrary set does not necessarily split into segments, and so it is not possible to give such an easy definition of its length. How can one define, for example, "the length" of the set of all rational numbers contained in $[0, 1]$? Or the set of all irrational numbers?

There is a theory which enables us to define the length of a wide class, though not of all, subsets of the segment, and this definition possesses all the properties suggested by our intuition. It is called the *Measure Theory.* We shall not deal with this theory in all its aspects, but we shall present the definition of a property of a set which could be considered as having "length zero". In Measure Theory such sets are called *sets of measure zero.* We shall call them *thin sets.*

We start with basic definitions, using geometrical intuition, and formal definitions will be given at the end. We have already defined the length of a segment $[a, b]$ contained in $[0, 1]$, and also of the sum of a finite number of disjoint segments. This is only one step away from a countable sum of segments. Namely, if $M = I_1 + I_2 + \dots + I_n + \cdots$, where I_k are disjoint segments and the length of the segment I_k is equal to α_k, then the segments I_1, I_2, ..., I_n are contained in the segment $[0, 1]$ and they are disjoint, and therefore the sum of their lengths does not exceed 1. In other words, $\alpha_1 + \alpha_2 + \dots + \alpha_n \leqslant 1$ for all $n = 1, 2, \dots$. It follows from the Lemma of Sec. 1, Ch. V that the infinite sum $\alpha_1 + \alpha_2 + \cdots + \alpha_n + \cdots$ exists and also does not exceed 1. This sum will be called the length of the set M. For example, if $I_1 = \left[0, \frac{1}{2}\right]$, $I_k = \left[1 - \frac{1}{2^{2k-2}}, 1 - \frac{1}{2^{2k-1}}\right]$ (Fig. 5), then $\alpha_k = \left(1 - \frac{1}{2^{2k-1}}\right) - \left(1 - \frac{1}{2^{2k-2}}\right) = \frac{1}{2^{2k-2}} - \frac{1}{2^{2k-1}}$, whence $\alpha_k = \frac{1}{2^{2k-1}}$. Hence

$$\alpha_1 + \alpha_2 + \cdots = \frac{1}{2} + \frac{1}{8} + \frac{1}{32} + \cdots = \frac{1}{2}\left(1 + \frac{1}{4} + \left(\frac{1}{4}\right)^2 + \cdots\right) = \frac{1}{2}\frac{1}{1 - \frac{1}{4}} = \frac{2}{3}$$

(according to the formula for infinite geometric series). So we obtain that the length of our set is 2/3.

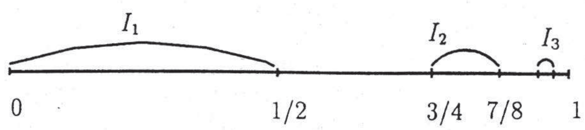


Fig. 5

We shall now make two hypotheses which will allow us to formulate the definition that we need. First of all, consider a modified situation where the set M is the union of segments $I_1, I_2, \ldots, I_n, \ldots$ which may intersect. It is natural to assume that, however we define the length of the set M, it *will not exceed* the sum of the lengths of the segments I_k. Now, of course, we cannot state that the sums $\alpha_1 + \cdots + \alpha_n$ do not exceed 1, where, as before, α_k denote the length of the interval I_k—it can even happen that all the segments I_k coincide. So, our hypothesis makes sense only if the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_n + \cdots$ exists. The second hypothesis is even more intuitive: we shall assume that, however we defined the lengths of sets M_1 and M_2, if $M_1 \subset M_2$ the length of M_1 would not exceed the length of M_2.

The hypotheses that we have made are not sufficient to *measure* the length of an arbitrary set, since it cannot be represented as a union of a countable number of segments. For example, the set of all irrational numbers of the segment $[0, 1]$ (Problem 1) cannot be represented in this way. But, using the second hypothesis, we can *estimate* the length of a set, however it is defined, assuming only that our hypotheses are valid. Assume, for example, that the set M is contained in the union of segments $I_1, I_2, \ldots, I_n, \ldots$. Then its length cannot exceed the sum of the lengths of the segments I_k. We can try to measure the set M by including it in various sets that are unions of countable sequences of segments. If as a result of these "measurements" we obtain that the estimates for the measure of the set M are getting smaller and smaller (closer to 0), then there will be no other possibility than to say that the length of the set M is equal to 0. This brings us to the definition of a thin set.

In the sequel, in order to make formulations shorter, when a set M is contained in the union of sets $M_1, M_2, \dots, M_n, \dots$, we will say that it is *covered* by these sets, and the inclusion

$$M \subset M_1 \cup M_2 \cup \dots \cup M_n \cup \cdots$$

itself will be called the *cover* of M by the sets M_k.

Definition. A set M contained in the segment $[0, 1]$ is called *thin* if for each arbitrarily small positive number ε there exists a cover of the set M by segments $I_1, I_2, \dots, I_n, \dots$, such that the sum of the lengths of the segments I_k does not exceed ε.

We stress once again that our discussion and remarks so far in this Section have not proved anything—they have just been explanations for this definition.

Consider now some examples of thin sets. A set containing just one element x is thin, since for each $\varepsilon > 0$ it has a cover $x \in I_\varepsilon$, where I_ε is the segment $[x-\varepsilon/2, x+\varepsilon/2]$ of the length ε, or, if this segment is not contained in the segment $[0, 1]$, then their intersection, having the length not exceeding ε. In the same manner one can prove that the set containing a finite number of points is thin.

Now we shall show that the notion of a thin set is connected with countability.

Theorem 5. *Each countable subset of the segment* $[0, 1]$ *is thin.*

Let M be a countable set, numbered in some way: $M = \{a_1, a_2, \dots, a_n \dots\}$. We shall construct, for each positive ε, a cover of this set by segments I_1, I_2, $\dots$, I_n, $\dots$ such that the sum of the lengths of these segments does not exceed ε. In order to do that, take for I_1 the segment of the length $\varepsilon/2$ with centre a_1: $I_1 = [a_1-\varepsilon/4, a_1+\varepsilon/4]$, or, if this segment does not lie inside the segment $[0, 1]$, its part which is contained inside $[0, 1]$. Similarly, for each k take for I_k the intersection of the segment $\left[a_k - \frac{\varepsilon}{2^{k+1}}, a_k + \frac{\varepsilon}{2^{k+1}}\right]$ with the segment $[0, 1]$. In each case the length of the segment I_k does not exceed $\varepsilon/2^k$, and the sum of the lengths of all segments I_k does not exceed the sum $\frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \frac{\varepsilon}{8} + \cdots = \varepsilon$ (by the formula for the sum of a geometric series).

It follows, for example, that the set of rational numbers contained in the segment $[0, 1]$ is thin, which is not obvious.

Let us turn now to another property.

Theorem 6. *The union of two thin sets is also a thin set.*

Let M_1 and M_2 be two thin sets and $M = M_1 \cup M_2$. In order to prove that the set M is thin, we have to construct, for each $\varepsilon > 0$, a cover $I_1, I_2, \dots, I_n$, $\dots$ of this set by segments, so that the sum of their lengths does not exceed ε. We shall use the fact that the sets M_1 and M_2 are thin. This means that for each positive number η, M_1 and M_2 can be covered by segments so that the sum of the lengths of segments in each cover does not exceed η. This is valid for every η, and in particular for $\eta = \varepsilon/2$, where ε is the number given in advance. Write down the covers that we have found:

$$M_1 \subset J_1 \cup J_2 \cup \cdots \cup J_n \cup \cdots ,$$
$$M_2 \subset K_1 \cup K_2 \cup \cdots \cup K_n \cup \cdots .$$

Consider the sequence of segments J_1, K_1, J_2, K_2, J_3, K_3, $\ldots$. Their union contains both M_1 and M_2, and so also $M = M_1 \cup M_2$, i.e., it is a cover of the set M by segments. Let us prove that the sum of the lengths of the segments in this cover does not exceed ε. Denote the length of the segment J_m by a_m, and the length of the segment K_m by b_m. Then the sum of the lengths of the segments of the sequence J_1, K_1, J_2, K_2, $\ldots$ is equal to

$$a_1 + b_1 + a_2 + b_2 + \cdots = (a_1 + a_2 + \cdots) + (b_1 + b_2 + \cdots). \tag{7}$$

Since, by the assumption, $a_1 + a_2 + \cdots \leqslant \varepsilon/2$ and $b_1 + b_2 + \cdots \leqslant \varepsilon/2$, the sum on the left-hand side of equation (7) does not exceed $\varepsilon/2 + \varepsilon/2 = \varepsilon$, as we wanted to prove.

This argument needs a clarification, concerning formula (7). If we had been dealing with finite sums, this would have been the assertion that brackets in a sum can be arranged in an arbitrary manner. This is a consequence of commutative and associative laws for addition (axioms I_1 and I_2 from Sec. 1, Ch. V). But we had not given such axioms for infinite sums and so we have to prove equality (7). It is enough to prove slightly less—that the left-hand side of this equality does not exceed the right-hand side. Let $a_1 + a_2 + \cdots = \alpha$, $b_1 + b_2 + \cdots = \beta$. Each finite sum on the left-hand side of equality (7) can be divided into the sum of numbers $a_1, a_2, \ldots , a_n$ and numbers $b_1, b_2, \ldots , b_m$ ($m = n$ or $n-1$, depending on whether we stop the addition in an even or in an odd place). But (using rules for finite sums) this sum is equal to $a_1 + \cdots + a_n + b_1 + \cdots + b_m$. Since $a_1 + \cdots + a_n \leqslant \alpha$, $b_1 + \cdots + b_m \leqslant \beta$, our whole finite sum does not exceed $\alpha + \beta$, which means that the infinite sum on the left-hand side of (7) does not exceed $\alpha + \beta$.

Using induction, we conclude that the union of a finite number of thin sets is also a thin set. But a stronger assertion is valid, and it contains Theorem 6 as a special case.

THEOREM 7. *The union of a countable number of thin sets is also a thin set.*

The proof is very similar to the proof of the previous Theorem, so we shall present it more briefly. Let $M_1, M_2, \ldots , M_n, \ldots$ be a countable set of thin sets and M their union. Let a positive number ε be given. We shall construct a cover of the set M by a countable number of segments, the sum of the lengths of which does not exceed ε—this will prove that M is a thin set. Since each of the sets M_n is thin, by the definition it has a cover formed by a countable number of segments, the sum of their lengths not exceeding $\varepsilon/2^n$. Consider now all the segments contained in any of these covers. Let the cover of the set M_1 be $M_1 \subset I_1 \cup I_2 \cup \cdots$, of the set M_2: $M_2 \subset J_1 \cup J_2 \cup \cdots$, of the set M_3: $M_2 \subset K_1 \cup K_2 \cup \cdots$, and so on for all M_n, $n = 1, 2, 3, \ldots$. We consider now the set of all segments I_r, all segments J_s, all segments K_t and so on. The collection of segments that we obtain is a countable union of countable sets (since each set M_n is covered by a countable number of intervals). By Example 3 of Sec. 1, we obtain a countable set of segments. The sum of their lengths does not exceed $\frac{\varepsilon}{2} + \frac{\varepsilon}{2^2} + \cdots = \varepsilon$. This proves the Theorem.

Note that here we encounter the same question as in the proof of Theorem 6 in connection with equality (7), only in a bit more complicated situation. We have here a countable number of equalities: $a_1 + a_2 + \cdots = \alpha$, $b_1 + b_2 + \cdots = \beta$, $c_1 + c_2 + \cdots = \gamma$ and so on. Then we mix all the numbers a_i, b_j, c_k and so on, renumber them in certain way and consider their sum. It is enough to show that the sum we obtain does not exceed $\alpha + \beta + \gamma + \cdots$. The proof is the same as in Theorem 6, and so we shall skip it.

Finally, we consider a very important property of thin sets. Namely, we have to convince ourselves that the hypotheses we made when defining this notion do not contradict each other. We started from the fact that the length of a segment $[a, b]$ contained in the segment $[0, 1]$ is equal to $b - a$; a thin set has “length 0”, and the “length” of a subset does not exceed the “length” of the set. If the segment $[a, b]$ (with $b \neq a$) turned out to be a thin set, then our theory would be contradictory. We now prove that this is not the case. We will give the first example of a set which is not thin—up to now we have just been proving that certain sets are thin. If in our theory thin sets play the same role as countable sets played in Sec. 2, then the segment plays the role of the continuum, and the Theorem which we now prove is analogous to the uncountability of the continuum (Theorem 2).

THEOREM 8. *No segment is a thin set.*

Let a segment $I = [a, b]$ be given, and assume that, contrary to the assertion of the Theorem, for each $\varepsilon > 0$ there is a cover by segments with the sum of the lengths not exceeding ε. Denote this cover by

$$I \subset I_1 \cup I_2 \cup \cdots$$

and denote by α_k the length of the segment I_k, so that the sum $\alpha_1 + \alpha_2 + \cdots$ does not exceed ε. In what follows we shall see that it is more convenient to deal with *intervals* (a_k, b_k) (i.e., with the sets of x for which $a_k < x < b_k$) instead of segments $[a_k, b_k]$. Denote respective intervals by J_1, J_2, $\ldots$. The length of an interval $J = (c, d)$ is equal to $d - c$. Let us prove that the segment I has a cover by intervals, the sum of whose lengths is arbitrarily small. Let η be an arbitrarily small positive number and include the segment $I_k = [a_k, b_k]$ into the interval $J_k = \left(a_k - \frac{\eta}{2^{k+1}}, b_k + \frac{\eta}{2^{k+1}}\right)$. Its length differs from the length of segment I_k by $\eta/2^k$. Therefore, the sum of their lengths does not exceed

$$\left(a_1 + \frac{\eta}{2}\right) + \left(\alpha_2 + \frac{\eta}{4}\right) + \cdots + \left(\alpha_n + \frac{\eta}{2^n}\right) + \cdots \leqslant \varepsilon + \eta\left(\frac{1}{2} + \frac{1}{4} + \cdots\right) = \varepsilon + \eta.$$

On the other hand, by the construction, $I_k \subset J_k$ and therefore

$$I \subset I_1 \cup I_2 \cup \cdots \subset J_1 \cup J_2 \cup \cdots , \tag{8}$$

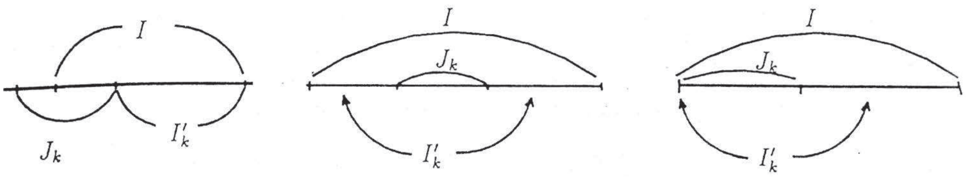
since J_1, J_2, ... is a cover of segment I. Since for ε and η we could take arbitrarily small numbers, intervals J_k can be chosen so that the sum of their lengths is arbitrarily small.

Consider, first of all, an easy case when the number of intervals is finite. Let J_1 be an interval containing at least one number from segment I. If an interval J_k intersects with it, they together form one interval $J_1 \cup J_k$ whose length does not exceed $\alpha_1 + \alpha_k$. If there is an interval J_l intersecting the interval $J_1 \cup J_k$, consider the interval $J_1 \cup J_k \cup J_l$ with the length not exceeding $\alpha_1 + \alpha_k + \alpha_l$. Continuing in this way, we can collect together in an interval J' a group of intervals J_1, J_k, J_l, ... and the remaining intervals will not intersect any of these. Interval J' has to contain the segment I. Indeed, let $J' = (a', b')$. If, for example, $b' \leqslant b$, then b' cannot belong to any of the intervals left out of J': if $b' \in J_r$, $J_r = (a_r, b_r)$, then by assumption $a_r < b'$ (here it is important that we deal with intervals without endpoints), and then intervals J' and J_r would intersect: any of the numbers between a_r and b' would belong to both of them. This contradicts the assumption. Hence, $b' > b$ and analogously $a' < a$, i.e., $I \subset J'$. But, as we have seen, the length of the interval J' does not exceed $\alpha_1 + \alpha_k + \alpha_l + \cdots$ and, a fortiori, it does not exceed the sum $\alpha_1 + \alpha_2 + \cdots$ of the lengths of all intervals J_1, J_2, ... This sum, however, does not exceed $\varepsilon + \eta$, i.e., $b' - a' \leqslant \varepsilon + \eta$. On the other hand, we can choose ε and η arbitrarily small, and, in particular, such that $\varepsilon + \eta < b' - a'$. This is a contradiction and so it proves the Theorem in this case.

Now we come to the more subtle case when the number of intervals is infinite. Considering an interval J_k as a subset of the set of all real numbers, we denote by $\overline{J}_k$ its complement and put $I'_k = \overline{J}_k \cap I$. In other words, I'_k is the set of numbers of the segment I, not belonging to the interval J_k. Relation (8) which we are given is equivalent to

$$I'_1 \cap I'_2 \cap I'_3 \cap \cdots = \emptyset. \tag{9}$$

Really, relation (9) is another way of saying that each number of the interval I belongs to some interval J_k, as in relation (8).



(a) (b) (c)

Fig. 6

The set I'_k is not necessarily a segment: it can be a segment, or two segments (here with endpoints included), or a segment can reduce to a point: $[a, a] = \{a\}$ (Fig. 6).

Put $A_n = I'_1 \cap I'_2 \cap \cdots \cap I'_n$. Relation (9) means that $A_n \supset A_{n+1}$ and

$$A_1 \cap A_2 \cap A_3 \cap \cdots = \emptyset. \tag{10}$$

We obtain a picture very similar to the one we dealt with in the Axiom of embedded segments. If the sets A_n were segments, we could apply this axiom and deduce that there is a number x belonging to all of them. This would be a contradiction with relation (10) and it would prove the Theorem. However, A_n are in general not segments, but a bit more complicated sets.

We now turn to that problem. Since the union of two segments consists of disjoint segments (some of them can be just points), so A_n itself consists of disjoint segments (some of them may be degenerated to points). Denote these segments (or points) by $A_n^{(1)}$, $A_n^{(2)}$, ... , $A_n^{(k)}$. Take A_0 to be the whole segment I. This system of segments is shown in Fig. 7, where each segment $A_n^{(i)}$ is represented by a circle, arranged in the ascending order in n. The circle representing segment $A_n^{(i)}$ is connected to the circle representing $A_{n+1}^{(j)}$ if $A_n^i \supset A_{n+1}^{(j)}$. We say that circle $A_n^{(j)}$ lies below circle A_m^i $(m < n)$ if one can pass from $A_m^{(i)}$ to $A_n^{(j)}$ moving along these connections. This simply means that segment $A_n^{(j)}$ is contained in segment $A_m^{(i)}$. There is no circle below circle $A_n^{(i)}$ if the intersection of the segment $A_n^{(i)}$ with the set I'_{n+1} is empty.

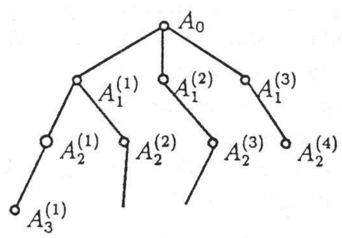


Fig. 7

The picture in Fig. 7 reminds us of a branched root system. It can be of two different types. a) There is only a finite number of circles in the system. If all of them have the form $A_m^{(i)}$ with $m \leqslant n$, then there is no circle lying below any of the circles $A_n^{(i)}$. Hence, $A_n^{(i)} \cap I'_{n+1} = \emptyset$, and since $A_n = I'_1 \cap \cdots \cap I'_n$ and $A_n = \bigcap A_n^{(i)}$, then $I'_1 \cap \cdots \cap I'_{n+1} = \emptyset$. This means that relation (9) is valid for the system of segments $I'_1, \ldots, I'_{n+1}$, and relation (8) is valid for the system of intervals $J_1, \ldots,$ J_{n+1}. But this is the case of a finite number of intervals that we have discussed already. b) The picture in Fig. 7 contains infinitely many circles. If we can find a line that goes down through it without stopping (i.e., a line $A_1^{(i)}$, $A_2^{(j)}$, $A_3^{(k)}$, ... , where $A_2^{(j)}$ is below $A_1^{(i)}$, $A_3^{(k)}$ is below $A_2^{(j)}$, etc.) then we obtain a system of embedded segments $A_1^{(i)} \supset A_2^{(j)} \supset A_3^{(k)} \supset \cdots$. According to Axiom of embedded segments (Axiom VII of Sec. 1, Ch. V), this system of segments has to contain at least one common point x (here it is essential that segments $A_n^{(i)}$ are considered together with their endpoints).

In fact, our situation is a bit more general, since among the segments $A_n^{(i)}$ there may be some degenerate ones of the form $[a_k, b_k]$ with $b_k = a_k$, i.e., points. But in this situation Axiom of embedded segments is also valid: if one segment from an embedded system reduces to a point x, then all segments following it also have to coincide with x. Hence, there always exists a number x belonging to each set A_n, and so $x \in A_1 \cap A_2 \cap A_3 \cap \cdots$, contradicting the condition (10).

We shall check whether such infinitely descending line can always be found. By assumption, the set of all circles in Fig. 7 is infinite. Thus, there are infinitely many circles lying below A_0. It follows that for some i there are infinitely many circles lying below $A_1^{(i)}$. It follows that for some circle $A_2^{(j)}$, lying below $A_1^{(i)}$, there are infinitely many circles lying below $A_2^{(j)}$, etc. Continuing, we obtain an infinite descending line: A_0, $A_1^{(i)}$, $A_2^{(j)}$, $\ldots$. This completes the proof of Theorem 7.

Taking into account Theorem 4, uncountability of the segment (Theorem 2) follows from Theorem 7. Thus this gives us the third proof of Theorem 2.

Now we are for the first time in the position to state that sets that are not thin exist at all. The whole segment is one set of this kind. Moreover, each thin set is so "small" that it cannot contain any segment, of however small length. This justifies our idea of thin sets as sets "infinitely smaller" than intervals. We say that some property is true *for almost all numbers*, if the set of numbers not having this property is thin. For example, almost all numbers are irrational, and almost all numbers are transcendental.

Up to now we have discussed only general properties of thin sets—we have not looked at many examples of such sets. We only know that finite and countable sets are thin. We shall give now one of the most interesting examples of a thin set which is not countable.

This set is connected with the representation of numbers of the segment $[0, 1]$ as decimal expansions. Choose a digit—for example, let it be digit 2. Denote by M the set of all numbers of the segment not containing our digit in their decimal representations. We shall prove that the set M is uncountable and thin. That the set M is uncountable is obvious. It contains the subset M', containing all expansions formed by just two digits, both of them different from 2—e.g., 0 and 1. The set of these expansions is, obviously, equivalent to the set of sequences a_1, a_2, a_3, $\ldots$, where a_i are equal 0 or 1. We know that the set M' is uncountable (Problem 6 in Sec. 2). Since a subset of a countable set is countable, it follows that the set M is uncountable. It is not hard to prove that the set M is continual (Problem 4).

Let us prove now that the set M is thin. Denote by M_n the set of numbers of the segment $[0, 1]$ whose decimal representation does not contain the digit 2 among the first n digits. Hence, decimal representation of an arbitrary number $x \in M_n$ has the form

$$x = 0.a_1 a_2 \ldots a_n \ldots, \tag{11}$$

where $a_1 \neq 2$, $a_2 \neq 2$, $\ldots$, $a_n \neq 2$, and the following digits are arbitrary (chosen from the digits 0, 1, $\ldots$, 9). Obviously, $M_n \supset M$, and we shall construct for each n a cover of the set M_n by segments such that the sum of the lengths of these segments approaches 0 when n increases. Since $M_n \supset M$, the cover of the set M_n will automatically be a cover of the set M and so it will be proved that M is also a thin set.

Fix arbitrary n digits $a_1, a_2, \dots, a_n$ and look at the set of all numbers whose decimal representations has these digits in the first n places. In other words, the numbers from our set have decimal representations of the form (11), where $a_1, a_2, \dots, a_n$ are fixed, and other digits are arbitrary. Put

$$\alpha = 0.a_1a_2\dots a_n00\dots 0, \qquad \beta = 0.00\dots 0a_{n+1}a_{n+2}\dots,$$

where β has the first n digits (after the decimal point) equal to 0, and the rest of the digits are the same as in x. Then $x = \alpha + \beta$, where α is the same for all the numbers from our set, and β runs through all numbers having n zeros after the decimal point. In other words

$$\beta = \frac{a_{n+1}}{10^{n+1}} + \dots = \frac{1}{10^n}\left(\frac{a_{n+1}}{10} + \frac{a_{n+2}}{10^2} + \dots\right).$$

Since the digits $a_{n+1}, a_{n+2}, \dots$ are arbitrary, the expression in the parentheses represents an arbitrary number y, $0 \leqslant y < 1$ and $\beta = \alpha + \frac{1}{10^n}y$, i.e., β (and so our whole set) is contained in the segment $[\alpha, \alpha + \frac{1}{10^n}]$. We have considered numbers with the first n digits fixed. There are 9^n possible choices of these n digits $a_1, \dots, a_n$, because $a_i \neq 2$ (Theorem of Ch. III), since the set of these choices is equivalent to the product of n copies of the set $\{0, 1, 3, 4, 5, 6, 7, 8, 9\}$ of 9 elements (2 is skipped). Hence, our set M_n is covered by 9^n segments of the form $[\alpha, \alpha + \frac{1}{10^n}]$, and each of these segments has the length $\dfrac{1}{10^n}$. The sum of their lengths is equal to $\dfrac{9^n}{10^n} = \left(\dfrac{9}{10}\right)^n$. Since $\dfrac{9}{10} < 1$, according to Lemma 2 of Sec. 1, Ch. V, $\left(\dfrac{9}{10}\right)^n \to 0$ when $n \to \infty$. This proves our assertion.

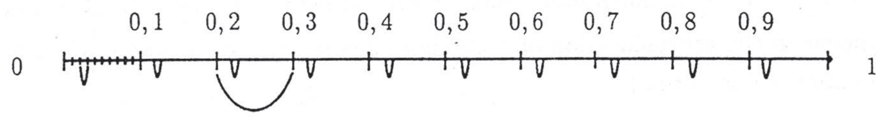


Fig. 8

The cover of the set M_n by 9^n segments of the lengths $1/10^n$ is represented in Fig. 8 for the cases $n = 1$ and $n = 2$. In order to construct a cover of the set M_1 it is enough to remove the interior of the segment $[0.2, 0.3]$ marked by an arc. There remains 9 segments, $[0, 0.1]$, $[0.1, 0.2]$, $[0.3, 0.4]$, ... , $[0.9, 1]$, each having the length $1/10$. In order to construct a cover of the set M_2, one has to remove from each of these 9 segments the interior of one segment more of the length $1/100$. They are noted by smaller arcs. For example, from the segment $[0, 0.1]$ one has to remove the interior of the segment $[0.02, 0.03]$, from $[0.1, 0.2]$ the interior of $[0.12, 0.13]$, etc. In each of the larger segments, there remain 9 segments of the lengths $1/100$, and since there are 9 larger segments, there will remain 9^2 of segments with the sum of lengths equal to $\dfrac{9^2}{10^2}$.

Let g be one of the digits 0, 1, ... , 9. Denote by M_g the set of numbers from the segment $[0, 1]$ whose decimal representations do not contain digit g. We have proved that M_g is a thin set (to be specific, we have considered the set M_2). It follows from Theorem 6 that their union $M_0 \cup M_1 \cup \cdots \cup M_9$ is also a thin set. In other words, almost all decimal expansions (in the segment $[0, 1]$) contain *all* of the digits 0, 1, ... , 9.

This assertion is just a special case of a much more general rule. It appears that in almost all decimal expansions each digit appears "on average" the same number of times. This has the following precise meaning. Choose an arbitrary digit g. For a given number x from the segment $[0, 1]$ denote by k_n the number of times digit g appears among its n first digits. For example, for the number $x = 0.12237152097$ and $g = 2$, $k_1 = 0$, $k_2 = 1$, $k_3 = 2$, $k_4 = 2$, $k_5 = 2$, $k_6 = 2$, $k_7 = 2$, $k_8 = 3$, $k_9 = 3$, $k_{10} = 3$, $k_{11} = 3$. The number k_n depends on the choice of the digit g. For example, for the same number x and $g = 1$ we have $k_1 = 1$, $k_2 = 1$, $k_3 = 1$, $k_4 = 1$, $k_5 = 1$, $k_6 = 2$, $k_7 = 2$, $k_8 = 2$, $k_9 = 2$, $k_{10} = 2$, $k_{11} = 2$. If we add up, for fixed n, all the numbers k_n, calculated for all digits $g = 0, 1, 2, \dots, 9$, the result will be n—the total number of the first n digits. If among the first n digits of number x each digit g appeared the same number of times, then for all the digits the number k_n would be the same, namely equal to $\frac{n}{10}$. In other words, we would have $\frac{k_n}{n} = \frac{1}{10}$. We shall say that all digits g appear in the decimal representation *on average* the same number of times if this relation holds in the limit form, i.e., if $\frac{k_n}{n} \to \frac{1}{10}$ when $n \to \infty$ and this is true for numbers k_n evaluated for arbitrary $g = 0, 1, 2, \dots, 9$. Such numbers are called *normal*. A remarkable theorem states that *almost all numbers are normal*, i.e., the set of numbers that are not normal is thin. This is obviously much more than we proved before. If a certain digit g does not appear in the representation of a number, then all the $k_n = 0$ and $\frac{k_n}{n} \to 0$, so the number is not normal.

The fact that almost all numbers are normal is very striking. It is very easy to construct numbers which are far from being normal—e.g., numbers such that for the given digit g and the respective numbers k_n, we have $\frac{k_n}{n} \to p$, where p is an arbitrary number between 0 and 1; or such that for digit 0 the numbers k_n satisfy $\frac{k_n}{n} \to 0$, and for digit 1, $\frac{k_n}{n} \to 1$; or such that for the given digit g the numbers $\frac{k_n}{n}$ have no limit at all (Problems 6, 7 and 8). It would seem that there is complete chaos in the possible distributions of digits of an arbitrary decimal expansion and only in very special cases there is an easy regularity (i.e., the number is normal). As a matter of fact, the regularity appears almost always, and "chaos" appears only for numbers contained in a thin set.

Proof of the Theorem stating that almost all numbers are normal is based on the same reasoning that we have already met in this Chapter and other parts of the book. However, it is a bit more involved and we shall postpone it until the Appendix.

PROBLEMS

1. Prove that the set of irrational numbers does not contain any segment.

2. Prove that the set of irrational numbers is not thin.

3. Prove the equality

$$a_1 + b_1 + a_2 + b_2 + \cdots = (a_1 + a_2 + \cdots) + (b_1 + b_2 + \cdots)$$

under the assumption that both sums inside parentheses on the right-hand side exist (it was only proved in the text that the left-hand side does not exceed the right-hand side).

4. Prove that the set of numbers from the segment $[0,1]$ not containing digit 2 in their decimal representation is continual. [*Hint.* Use Problem 6 of Sec. 2.]

5. It was proved in the text that the set M_n of numbers from the segment $[0,1]$ not containing digit 2 among the first n digits of the decimal representation, can be covered by 9^n segments of lengths $1/10^n$. Which numbers from these segments are not contained in the set M_n?

6. For an arbitrary real number p, $0 \leqslant p \leqslant 1$, construct a real number x such that the sequence of corresponding numbers k_n evaluated for digit 2 has the property that $\dfrac{k_n}{n} \to p$ when $n \to \infty$.

7. Two nonnegative real numbers p and q are given, such that $p + q \leqslant 1$. Construct a real number x such that the corresponding sequence k_n evaluated for digit 2 has the property that $\dfrac{k_n}{n} \to p$ when $n \to \infty$, and the sequence k'_n, evaluated for digit 3 has the property that $\dfrac{k'_n}{n} \to q$ when $n \to \infty$.

8. Construct a real number x such that the sequence k_n evaluated for digit 2 has the property that $\dfrac{k_n}{n}$ has no limit when $n \to \infty$.

APPENDIX

Normal numbers

We shall consider real numbers x lying between 0 and 1, i.e., belonging to the segment $[0,1]$. Write down such a number as an infinite decimal expansion

$$x = 0.a_1 a_2 \ldots a_n \ldots \tag{1}$$

Recall that number x is called *normal* if each digit r, $0 \leqslant r \leqslant 9$ appears in x "equally frequently". The last expression has the following meaning. Denote by k_n the number of times that digit r appears among the first n digits $a_1, a_2, \ldots, a_n$ of expansion (1). We require that the following relation holds

$$\frac{k_n}{n} \to \frac{1}{10} \quad \text{when} \quad n \to \infty. \tag{2}$$

The number x is called normal if condition (2) holds for each $r = 0, 1, \ldots, 9$. We have to bear in mind that the sequence k_n depends on r. For each r, we can denote by N_r the set of numbers x satisfying condition (2) for the given r (sequence k_n is constructed for this r). Then

(3) $$N = N_0 \cap N_1 \cap \cdots \cap N_9,$$

where N is the set of normal numbers.

This Appendix is devoted to the proof of the following proposition.

THEOREM. *The set of numbers of the segment* $[0, 1]$ *which are not normal is thin.*

Let us, first of all, analyse carefully what we have to prove. The set of numbers which are not normal is, obviously, the set $\overline{N}$, where N is considered as a subset of the segment $[0, 1]$ and $\overline{N}$ is its complement. It follows from (3) that

$$\overline{N} = \overline{N}_0 \cup \overline{N}_1 \cup \cdots \cup \overline{N}_9.$$

Since the union of a finite number of thin sets is a thin set, it is sufficient to prove that each set $\overline{N}_r$ is thin (for $r = 0, 1, \ldots, 9$). Therefore, digit r will in the sequel be fixed and we shall consider the set $\overline{N}_r$ of those numbers of the segment $[0, 1]$ that do not satisfy condition (2), assuming that the sequence k_n of numbers has been constructed for this particular value of r (i.e., it shows how often r appears among the digits $a_1, a_2, \ldots, a_n$).

Denote by U the set $\overline{N}_r$, i.e., the set of numbers x from the segment $[0, 1]$ which do not satisfy relation (2) (for the fixed value of r). Recall the meaning of relation (2): for arbitrary $\varepsilon > 0$, there exists $n(\varepsilon)$, such that

$$\left| \frac{k_n}{n} - \frac{1}{10} \right| < \varepsilon \quad \text{for} \quad n > n(\varepsilon).$$

If x does not possess this property, it means that there is a number ε, such that the inequality $\left| \frac{k_n}{n} - \frac{1}{10} \right| < \varepsilon$ does not hold for some value of n which exceeds an arbitrary value given in advance. In other words, for this x,

(4) $$\left| \frac{k_n}{n} - \frac{1}{10} \right| \geqslant \varepsilon$$

for an infinite number of values of n. Denote the set of such values of x (for the given ε) by $U(\varepsilon)$. Then, for each number $x \in U$, there exists ε, such that $x \in U(\varepsilon)$; in other words, U is the union of all $U(\varepsilon)$. This description can be made a bit simpler. Note that by the definition itself, $U(\varepsilon_1) \supset U(\varepsilon_2)$ if $\varepsilon_1 < \varepsilon_2$. Hence, each set $U(\varepsilon)$ is contained in some $U(\frac{1}{m})$ for m sufficiently large (such that $\varepsilon < \frac{1}{m}$), so that the union of all $U(\varepsilon)$ (for all ε) coincides with the union of all $U(\frac{1}{m})$, i.e., with $\bigcup U(\frac{1}{m})$. We could also use, instead of the sequence $\frac{1}{m}$, an arbitrary sequence ε_m tending to 0. It is important only that the set U is the union of the sets $U(\varepsilon_m)$ for some countable sequence of numbers ε_m: $U = \bigcup U(\varepsilon_m)$. Since the union of a countable number of thin sets is a thin set itself, we only need to prove that each of the sets $U(\varepsilon_m)$ is thin. We shall prove in fact that *the set* $U(\varepsilon)$ *is thin for each* $\varepsilon \geqslant 0$.

Denote by $V(n,\varepsilon)$ the set of numbers satisfying inequality (4) for the given n and ε. Then, $x \in U(\varepsilon)$ means that $x \in V(n_i,\varepsilon)$ for some infinite sequence of natural numbers $n_1 < n_2 < n_3 < \cdots$. That is, however large we chose a natural number N, $x \in V(n,\varepsilon)$ for some $n > N$.

Put

$$U_N(\varepsilon) = V(N,\varepsilon) \cup V(N+1,\varepsilon) \cup V(N+2,\varepsilon) \cup \cdots .$$

This can be written as

$$U_N(\varepsilon) = \bigcup_{n \geqslant N} V(n,\varepsilon). \tag{5}$$

We can therefore say that $x \in U_N(\varepsilon)$ means that

$$U(\varepsilon) \subset U_N(\varepsilon) \tag{6}$$

for all N. We shall prove that, for N sufficiently large, the set $U_N(\varepsilon)$ can be covered by segments whose sum of lengths is arbitrarily small. Taking into account relation (6), this will prove that the set $U(\varepsilon)$ is thin.

All this was in fact only an explanation of what the formulation of the Theorem really means. Now we need to ask which numbers really belong to our sets. The key to our question is the set $V(n,\varepsilon)$, and if we look at it more closely, we shall see that each of these sets is a finite union of segments, similarly to the situation we had with the set of expansions with a missing digit in Sec. 3.

To start with, assume that the first n decimal digits are fixed. Then

$$x = 0.a_1a_2\dots a_nc_{n+1}c_{n+2}\dots,$$

where $a_1, \dots, a_n$ are fixed, and c_i are arbitrary (of course, they have to be digits 0, 1, ..., 9). Put $\alpha = 0.a_1a_2\dots a_n$, $\gamma = 0.0\dots0c_{n+1}c_{n+2}\dots$, where the first n digits in γ are zeros. Then $x = \alpha + \gamma$, where α is fixed, and γ runs through all numbers of the form $\frac{c_{n+1}}{10^{n+1}} + \frac{c_{n+2}}{10^{n+2}} + \cdots$. In other words, $\gamma = \frac{1}{10^n}\beta$, $\beta = 0.c_{n+1}c_{n+2}\dots$, i.e., β is an infinite decimal expansion, defining an arbitrary number from the segment $[0,1]$ different from 1. Thus, $x = \alpha + \frac{1}{10^n}\beta$, α fixed, β arbitrary in $[0,1]$, $\beta \neq 1$. It is clear that these numbers are contained in the segment $\left[\alpha, \alpha + \frac{1}{10^n}\right]$ of the length $1/10^n$. Hence, the set $V(n,\varepsilon)$ can be divided into segments of length $1/10^n$, and the number of segments is equal to the number of sequences $a_1, a_2, \dots, a_n$ (consisting of digits 0, 1, ..., 9), in which the fixed digit r appears k times, and k satisfies relation (4):

$$\left|\frac{k}{n} - \frac{1}{10}\right| \geqslant \varepsilon. \tag{7}$$

Now we have to evaluate the number of sequences in which the digit r appears k times, where k is a given number. If r stands in *fixed* k places, then the remaining $n-k$ places are occupied by arbitrary digits different from r (there are 9 of them).

This means that there will be 9^{n-k} of *such* sequences. (We have used Theorem 1 of Ch. III.) These k possible places among n places in the sequence can be chosen in C_n^k ways (where C_n^k is a binomial coefficient, i.e., the number of subsets of k elements in the set of n elements, as it was shown in Theorem 3 of Ch. III). Thus the number of our sequences will be $C_n^k \cdot 9^{n-k}$. The final answer is the following: the number of sequences $a_1 a_2 \dots a_n$ is equal to $T_n(\varepsilon)$, where

(8) $T_n(\varepsilon)$ is the sum of expressions $C_n^k \cdot 9^{n-k}$ for all numbers k satisfying inequality (7).

It is striking that we have come to almost the same sum which arose in connection with Chebyshev's Theorem concerning the Bernoulli's scheme in the Appendix to Chapter III. To see this connection, divide the sum $T_n(\varepsilon)$ by 10^n. We obtain that $\frac{1}{10^n}T_n(\varepsilon)$ is equal to the sum of expressions $C_n^k\left(\frac{1}{10}\right)^k\left(\frac{9}{10}\right)^{n-k}$ for all values of k satisfying relation (7). Putting here $p = \frac{1}{10}$, $q = \frac{9}{10}$, we obtain the sum S_ε considered in the Appendix to Chapter III.

It is possible to understand why considering of, at the first sight, completely different topics led us to one and the same expression. Namely, the sequences a_1, a_2, ... , a_n can be treated as a Bernoulli's scheme I^n where the probability scheme I is formed of two events: the digit $= r$ with the probability $1/10$ and the digit $\neq r$ with the probability $9/10$. But we will not try to make this connection more precise, since we cannot apply the results proved in the Appendix of Chapter III anyway. The reason is that we need here a more general inequality than the one proved there. We shall formulate and prove it now for the situation considered in Ch. III, when probability p was an arbitrary number between 0 and 1. We will only apply it in the case $p = 1/10$, but it is useful to know it in the more general case.

Strengthened inequality of Chebyshev. *The sum S_ε of all expressions $C_n^k p^k q^{n-k}$ for all k satisfying $0 \leqslant k \leqslant n$ and inequality (7), does not exceed* $\frac{1}{4\varepsilon^4 n^2}$.

We postpone the proof of this inequality for the moment, and we show first of all how the Theorem follows from it. We have seen that the set $V(n,\varepsilon)$ is contained in the union of segments of length $1/10^n$ and the number of segments is equal to $T_n(\varepsilon)$. On the other hand, we have just noted that $\frac{1}{10^n}T_n(\varepsilon) = S_\varepsilon$, hence $T_n(\varepsilon) = 10^n S_\varepsilon$, and since the length of each segment is $1/10^n$, the sum of their lengths is precisely equal to $S_n(\varepsilon)$. According to the strengthened inequality of Chebyshev, $S_\varepsilon \leqslant \frac{1}{4\varepsilon^4 n^2}$. Thus the set $V(n,\varepsilon)$ is the union of a finite number of segments whose sum of their lengths does not exceed $\frac{1}{4\varepsilon^4 n^2}$.

Recall now that according to relation (5), $U_N(\varepsilon)$ is the union of all $V_n(\varepsilon)$ for $n \geqslant N$ and hence the set $U_N(\varepsilon)$ is contained in the union of segments with the sum of lengths not exceeding

$$\frac{1}{4\varepsilon^4}\left(\frac{1}{N^2} + \frac{1}{(N+1)^2} + \cdots\right). \qquad (9)$$

We met this sum in Sec. 2, Ch. V (see the Lemma). We saw there that the boundedness of the sums $\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}$ for all natural n implies that the sum $\frac{1}{N^2} + \frac{1}{(N+1)^2} + \cdots$ is smaller than an arbitrary positive number, if one chooses N large enough. Therefore we can choose N large enough so that the sum (9) will be less than an arbitrary given number $\delta > 0$. It follows that for N large enough the set $U_N(\varepsilon)$ is contained in the union of a countable number of segments with the sum of lengths being less than δ. Finally, recall that according to relation (6), the set $U(\varepsilon)$ is contained in arbitrary $U_N(\varepsilon)$. Therefore, the set $U(\varepsilon)$ has the property that, for arbitrary small number $\delta > 0$, it is contained in the union of a countable number of segments with the sum of lengths smaller than δ . In other words, the set $U(\varepsilon)$ is thin. We showed earlier that the assertion of the Theorem follows from this: the complement $\overline{N}$ of the set of all normal numbers is a thin set.

It remains to prove the strengthened inequality of Chebyshev. For those who solved Problem 5 in the Appendix to Chapter III there is nothing to do—the problem was precisely to prove this inequality. For those who did not solve that Problem, we give here the proof. It might frighten the reader, since it takes more than three pages and there are a lot of long formulae in it, but the idea is very close to the idea of proving the basic Chebyshev's inequality in the mentioned Appendix. It is just the question of removing the parentheses and collecting similar terms.

Consider the sum S_ε, having the summands $C_n^k p^k q^{n-k}$ for which $0 \leqslant k \leqslant n$ and $\left|\frac{k}{n} - p\right| \geqslant \varepsilon$. Following the proof of the Chebyshev's inequality (Appendix to Ch. III) multiply each term $C_n^k p^k q^{n-k}$ in the sum by $\left(\frac{k-np}{n\varepsilon}\right)^4$. This will not decrease the sum, since we consider only summands with values of k satisfying $\left|\frac{k}{n} - p\right| \geqslant \varepsilon$, i.e., $\left|\frac{k-np}{n\varepsilon}\right| \geqslant 1$. Consider after that the sum of *all* terms $\left(\frac{k-np}{n\varepsilon}\right)^4 C_n^k p^k q^{n-k}$ for all $k = 0, 1, \ldots, n$. Since in this manner we include new terms in the sum, the sum itself gets even larger. Denote the obtained sum by $\overline{\overline{S}}_\varepsilon$. As we have seen, $S_\varepsilon \leqslant \overline{\overline{S}}_\varepsilon$. We shall see that the sum $\overline{\overline{S}}_\varepsilon$ may be evaluated explicitly, which will give us the required inequality.

In the sum $\overline{\overline{S}}_\varepsilon$ we can take out of the brackets the common denominator of all terms: $n^4\varepsilon^4$, i.e., $\overline{\overline{S}}_\varepsilon = \frac{1}{n^4\varepsilon^4}P$, where P is the sum of all terms $(k-np)^4 C_n^k p^k q^{n-k}$ for $k = 0, 1, \ldots, n$. Now we expand the expression $(k-np)^4$ using the binomial formula for exponent 4:

$$(k-np)^4 = k^4 - 4k^3np + 6k^2n^2p^2 - 4kn^3p^3 + n^4p^4.$$

We obtain that

$$P = \sigma_4 - 4np\sigma_3 + 6n^2p^2\sigma_2 - 4n^3p^3\sigma_1 + n^4p^4\sigma_0, \tag{10}$$

where for each $r \geqslant 0$, σ_r denotes the sum of all terms $k^r C_n^k p^k q^{n-k}$ for $k = 0, 1, \ldots, n$.

As in the proof of Chebyshev's inequality, we have to find explicit expressions for σ_0, σ_1, σ_2, σ_3 and σ_4.

LEMMA. *Let σ_r denote the sum of terms $k^r C_n^k p^k q^{n-k}$ for $k = 0, 1, \ldots, n$. Then*

$$\sigma_0 = 1, \tag{11}$$

$$\sigma_1 = kp, \tag{12}$$

$$\sigma_2 = n^2p^2 + npq, \tag{13}$$

$$\sigma_3 = n^3p^3 + 3n^2p^2q - npq(2p - 1), \tag{14}$$

$$\sigma_4 = n^4p^4 + 6n^3p^3q - n^2p^2q(11p - 7) + npq(1 - 6pq). \tag{15}$$

The proof consists of several iterations of the steps by which we proved the Lemma in the Appendix to Chapter III.

We introduced there the sums σ_r, formed from terms $k^r C_n^k p^k q^{n-k}$ for $k = 0, \ldots, n$ and we found for them the expression $\sigma_r = q^n f_r(\frac{p}{q})$ (formula (8) of the Appendix to Ch. III), where $f_r(t)$ is the polynomial which is the sum of terms $k^r C_n^k t^k$ for $k = 0, 1, \ldots, n$. Hence our problem reduces to the problem of finding the polynomials $f_r(t)$. They can be found recursively starting from $f_0(t) = (1+t)^n$ and

$$f_{r+1}(t) = f_r'(t)t \tag{16}$$

(see formula (10) of the Appendix to Ch. III). We already found in Ch. III polynomials $f_1(t)$ and $f_2(t)$ (see formulas (12) and (14) of the Appendix to Ch. III). Thus,

$$f_0(t) = (1+t)^n, \quad f_1(t) = n(1+t)^{n-1}t, \quad f_2(t) = n(n-1)(1+t)^{n-2}t^2 + n(1+t)^{n-1}t.$$

Using the last formula and formula (16) we can now find the polynomial $f_3(t)$. Write down $f_2(t)$ in the form $g(t) + h(t)$, where $g(t) = n(n-1)(1+t)^{n-2}t^2$, $h(t) = n(1+t)^{n-1}t$ and apply the derivation rule for sums from Sec. 2 of Ch. II. We obtain

$$f_2'(t) = g'(t) + h'(t). \tag{17}$$

In order to find derivatives of polynomials $g(t)$ and $h(t)$ we have to apply derivation rule for powers from Sec. 2 of Ch. II (we already did this when finding polynomial $f_2(t)$ in the Appendix to Ch. III). We obtain

$$g'(t) = n(n-1)(n-2)(1+t)^{n-3}t^2 + 2n(n-1)(1+t)^{n-2}t,$$
$$h'(t) = n(n-1)(1+t)^{n-2}t + n(1+t)^{n-1}.$$

Substituting these into relation (17), and the result into formula (16) for $r = 2$ and reducing similar terms, we obtain

$$f_3(t) = n(n-1)(n-2)(1+t)^{n-3}t^3 + 3n(n-1)(1+t)^{n-2}t^2 + n(1+t)^{n-1}t. \tag{18}$$

We pass now to the evaluation of the polynomial $f_4(t)$, using formula (16) for $r = 3$. We put again $f_3(t) = u(t) + v(t) + w(t)$, where $u(t) = n(n-1)(n-2) \times (1+t)^{n-3}t^3$, $v(t) = 3n(n-1)(1+t)^{n-2}t^2$, $w(t) = n(1+t)^{n-1}t$. Then

$$f_3'(t) = u'(t) + v'(t) + w'(t). \tag{19}$$

In order to evaluate derivatives $u'(t)$, $v'(t)$ and $w'(t)$, represent each of the polynomials $u(t)$, $v(t)$ and $w(t)$ as the product of a power of $1+t$ and a power of t, and apply then the derivation rule for powers from Sec. 2 of Ch. II and formula (19) from Ch. II. We obtain in this way

$$\begin{aligned} u'(t) &= n(n-1)(n-2)(n-3)(1+t)^{n-4}t^3 + 3n(n-1)(n-2)(1+t)^{n-3}t^2, \\ v'(t) &= 3n(n-1)(n-2)(1+t)^{n-3}t^2 + 6n(n-1)(1+t)^{n-2}t, \\ w'(t) &= n(n-1)(1+t)^{n-2}t + n(1+t)^{n-1}. \end{aligned}$$

It remains to substitute these expression into formula (19) and then use formula (16) for $r = 3$. After reducing similar terms we obtain

(20)
$$\begin{aligned} f_4(t) = n(n-1)(n-2)(n-3)(1+t)^{n-4}t^4 + 6n(n-1)(n-2)(1+t)^{n-3}t^3 \\ + 7n(n-1)(1+t)^{n-2}t^2 + n(1+t)^{n-1}t. \end{aligned}$$

We can now substitute in the expressions (18) and (20) for $f_3(t)$ and $f_4(t)$ the value $t = \dfrac{p}{q}$. We have to bare in mind that $1 + \dfrac{p}{q} = \dfrac{p+q}{q} = \dfrac{1}{q}$, since $p + q = 1$. Using the relation $\sigma_r = q^n f_r(\frac{p}{q})$, we obtain expressions for σ_3 and σ_4. For σ_3 we obtain

$$\sigma_3 = n(n-1)(n-2)p^3 + 3n(n-1)p^2 + np.$$

Here we have to substitute $n(n-1)(n-2) = n^3 - 3n^2 + 2n$ and $n(n-1) = n^2 - n$. Reducing similar terms, we obtain

$$\sigma_3 = n^3p^3 + 3n^2p^2(1-p) + n(2p^3 - 3p^2 + p).$$

Finally, since $2p^3 - 3p^2 + p = p(p-1)(2p-1)$, relation (14) follows.

Let us evaluate now the expression for σ_4. Starting from relation (20), in the same way as for σ_3, we obtain

$$\sigma_4 = n(n-1)(n-2)(n-3)p^4 + 6n(n-1)(n-2)p^3 + 7n(n-1)p^2 + np.$$

Here we have again to remove brackets in the product $n(n-1)(n-2)(n-3)$:

$$n(n-1)(n-2)(n-3) = n^4 - 6n^3 + 11n^2 - 6n$$

(one can also use Viet's formula from Ch. III). The expressions $n(n-1)(n-2)$ and $n(n-1)$ were evaluated earlier. Grouping together terms with the same power of n, we obtain

$$\sigma_4 = n^4p^4 + (-6p^4 + 6p^3)n^3 + (11p^4 - 18p^3 + 7p^2)n^2 + (-6p^4 + 12p^3 - 7p^2 + p)n.$$

It remains to note that

$$-6p^4 + 6p^3 = 6p^3(1-p) = 6p^3 q,$$
$$11p^4 - 18p^3 + 7p^2 = -p^2(1-p)(11p-7) = -p^2 q(11p-7),$$
$$-6p^4 + 12p^3 - 7p^2 + p = p(1-p)(6p^2 - 6p + 1) = pq(1-6pq),$$

and we obtain formula (15). Hence, the Lemma is proved.

We are now ready to complete the proof of the strengthened inequality of Chebyshev. To do this, it remains to substitute expressions (11), (12), (13), (14) and (15) for σ_0, σ_1, σ_2, σ_3 and σ_4 into formula (10) and to reduce similar terms. Let us write down the coefficients of various powers of n:

of n^4: $p^4 - 4p^4 + 6p^4 - 4p^4 + p^4 = 0$.

of n^3: $6p^3q - 12p^3q + 6p^3q = 0$.

of n^2 (only terms from σ_3 and σ_4 contribute):

$$-p^2q(11p-7) + 4p^2q(2p-1) = p^2q(-11p + 7 + 8p - 4) = 3p^2q^2.$$

of n: (only terms from σ_4 contribute): $pq(1-6pq)$.

As a result we obtain that $P = 3p^2q^2n^2 + pq(1-6pq)n$. Since $\overline{\overline{S}}_\varepsilon = \dfrac{1}{n^4\varepsilon^4}P$,

$$\overline{\overline{S}}_\varepsilon = \frac{1}{n^4\varepsilon^4}(3p^2q^2n^2 + pq(1-6pq)n).$$

For the sum S_ε that we are interested in, we showed that $S_\varepsilon \leqslant \overline{\overline{S}}_\varepsilon$ and hence

$$S_\varepsilon \leqslant \frac{1}{n^3\varepsilon^4}(3p^2q^2n + pq(1-6pq)). \tag{21}$$

The expression in the brackets can be estimated as

$$pq(1 + 3(n-2)pq) \leqslant \frac{1}{4}\Big(1 + \frac{3(n-2)}{4}\Big) \leqslant \frac{1}{4}\,n,$$

since we already noted in the Appendix to Ch. III that $pq \leqslant 1/4$. Thus, inequality (21) implies that $S_\varepsilon \leqslant \dfrac{1}{4\varepsilon^4 n^2}$, as we needed to prove.

Therefore the proof of the strengthened inequality of Chebyshev, and so also our Theorem, is complete.

Remark 1. We have proved the strengthened inequality of Chebyshev, where instead of denominator $\varepsilon^2 n$ (from the basic inequality) there is the denominator $(\varepsilon^2 n)^2$. The proof was completely parallel to the proof of the basic inequality, only instead of the factor $\left(\dfrac{k-np}{\varepsilon n}\right)^2$ we used the factor $\left(\dfrac{k-np}{\varepsilon n}\right)^4$. It is natural to ask whether one can make Chebyshev's inequality even stronger by taking factors $\left(\dfrac{k-np}{\varepsilon n}\right)^{2r}$ for some natural exponent r. This is in fact the case. For each specific value of r (e.g., $r = 3$), one would have to make the same transformations as in our proof. But these transformations for higher values of r will be more and more complicated—for example, one has to evaluate $2r+1$ sums σ_k: $\sigma_0, \sigma_1, \ldots, \sigma_{2r}$. As a result, it is possible obtain an inequality with $(\varepsilon^2 n)^r$ as the denominator. We do not need these variants of Chebyshev's inequality, and so we restricted ourselves to the case $r = 2$.

Remark 2. Our calculations are by no means restricted specifically to the decimal number system. In a number system with base g, we call a number x normal if $\frac{k_n}{n} \to \frac{1}{g}$ when $n \to \infty$, where k_n shows how many, among the first n digits of the representation of x in g-number system, are equal to a given digit r. When considering the set of numbers which are not normal, we encounter sums of terms $C_n^k \left(\frac{1}{g}\right)^{n-k} \left(\frac{g-1}{g}\right)^k$, where k satisfies the inequality $\left|\frac{k}{n} - \frac{1}{g}\right| \geqslant \varepsilon$. We considered sums of this kind with $p = \frac{1}{g}$, $q = \frac{g-1}{g}$. Thus, the proof can be completed without any modifications for numbers written in a number system with base g.

There is an interesting application if $g = 100$. A "digit" in the 100-digit system is an arbitrary two-digit number, i.e., an arbitrary combination of two decimal digits. Thus, if k_n counts how many times a given group of two digits (e.g., 13 or 27) appears among the first $2n$ decimal digits of the number x, then $\frac{k_n}{n} \to \frac{1}{100}$ for all x, except for the numbers from a certain thin set. That is, for "almost all" numbers arbitrary combinations of two digits appear equally often—with the "frequency" 1/100. Similarly, we can take $g = 10^l$ for any natural number l and obtain that arbitrary combinations of l decimal digits appear with the equal "frequency" $1/10^l$—for "almost all" numbers x.

Remark 3. We showed that "almost all" numbers x are normal. But proving that a certain particular number x is normal is, usually, a very hard problem. Of course, the number $0.123456789\ldots$, where the digits $1, \ldots, 9$ repeat periodically, is normal (Problem 1). It is much harder to prove that the number $0.123\ldots9101112\ldots$, where all natural numbers are written in order, is normal. This was proved only in the nineteen thirties. Finally, it has not yet been shown whether numbers like $\sqrt{2}$ and π are normal (when we talk about numbers larger than 1, we eliminate the integer part and consider its mantissa). There are, for the time being, no ideas how such problems can be solved.

Problems

1. Consider the number $x = 0.123456789\ldots$, where the digits $1, \ldots, 9$ repeat periodically. Find for each digit $r = 0, 1, \ldots, 9$ the corresponding number k_n and prove that number x is normal.

2. Prove that for an arbitrary rational number x and a given digit $r = 0, 1, \ldots, 9$ the sequence $\frac{k_n}{n}$ tends to a limit. [*Hint.* Recall that the infinite decimal expansion corresponding to a rational number is periodic—Problem 3 of Sec. 3, Ch. V.]

3. What condition does the period of a periodic decimal expansion have to satisfy in order that the corresponding number be normal?

I. R. Shafarevich,
Russian Academy of Sciences,
Moscow, Russia