Department of Mathematics, The University of Pennsylvania, Philadelphia, PA 19104-6395 *E-mail address: kirillov@math.upenn.edu*

Math480/540, TOPICS IN MODERN MATH.
What are numbers?

A.A.Kirillov

Dec. 2007

The aim of this course is to show, what meaning has the notion of number in modern mathematics; tell about the problems arising in connection with different understanding of numbers and how these problems are being solved. Of course, I can explain only first steps of corresponding theories. For those who want to know more, I indicate the appropriate literature.

0.1 Preface

> The "muzhiks" near Vyatka lived badly. But they did not know it and believed that they live well, not worse than the others
>
> A.Krupin, *"The live water."*

When a school student first meet mathematics, (s)he is told that it is a science which studies numbers and figures. Later, in a college, (s)he learns analytic geometry which express geometric notions using numbers. So, it seems that numbers is the only object of study in mathematics.

True, if you open a modern mathematical journal and try to read any article, it is very probable that you will see no numbers at all. Instead, authors speak about sets, functions, operators, groups, manifolds, categories, etc.

Nevertheless, all these notions in one way or another are based on numbers and the final result of any mathematical theory usually is expressed by a number.

So, I think it is useful to discuss with math major students the question posed in the title. I want to show, what meaning can have the term "number" in modern mathematics, speak of some problems arising in this connection and of their solutions.

I hope, this will help novices to orient themselves in the reach, beautiful and complicated world of mathematics.

Chapter 1

The chain $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$

This chain of subsequent extensions of the notion of number (or at least first 4-6 members of it) you must already know. The symbols occurring here are now the standard notations for the sets of natural, integer, rational, real or complex numbers, quaternions and octonions. (The latter are also known as octaves and Cayley numbers).

I want to discuss here the transition from one link of the chain to the next one and show that the ideas used in these transitions are working in other, sometimes unexpected and beautiful theories.

1.1 From $\mathbb{N}$ to $\mathbb{Z}$ and from $\mathbb{Z}$ to $\mathbb{Q}$: the Grothendieck group, the Lie fields and derived categories

> We pull ourselves to the sky by the shoe laces.
>
> J.-P. Serre, *"Local algebra and multiplicity theory".*

We can add natural numbers but not always to subtract them; the integers can be multiplied but not always divide. The wish to circumvent this inconvenience actually provoked the transition from natural numbers to integers and from integers to rationals.

Recall how these transitions are made. If we want to subtract a natural number m from a natural number n, then, in case $m \geq n$ the answer can

not be a natural number. Let us denote it temporally by $n \ominus m$. If we want that in the extended set of numbers the habitual rules were verified, we have to identify $n \ominus m$ with all expressions of the form $(n+k) \ominus (m+k)$, $k \in \mathbb{N}$ and also with expressions $(n-k) \ominus (m-k)$, $1 \leq k \leq \min(m, n)$.

In other words, the symbols $n_1 \ominus m_1$ and $n_2 \ominus m_2$ are identified if $n_1 + m_2 = n_2 + m_1$.

Consider now all expressions of the form $n \ominus m$, $n, m \in \mathbb{N}$. We can not only add them (componentwise) but also subtract according to the rule

$$n_1 \ominus m_1 - n_2 \ominus m_2 = (n_1 + m_2) \ominus (n_2 + m_1). \tag{1.1}$$

E.g., we have $0 \ominus 0 - m \ominus n = n \ominus m$. One can check that equivalence classes form an additive group. Do it yourself (This exercise is for those who only start to study the group theory).

It is rater easy to establish that the group in questin is isomorphic to $\mathbb{Z}$. Indeed, for $m > n$ all symbols of the form $(m+k) \ominus (n+k)$ are identified with the natural number $m - n$, for $m = n$ they are identified with zero, and for $m < n$ with the negative number $m - n$.

The procedure of constructing of multiplicative group $\mathbb{Q}^*$ consisting of non-zero rational numbers from the semigroup $\mathbb{Z}\backslash\{0\}$ is completely analogous. Namely, we consider the formal symbols $m : n$ where m, $n \in \mathbb{Z}\backslash\{)\}$ and identify $m_1 : n_1$ with $m_2 : n_2$ if $m_1 n_2 = m_2 n_1$. It is clear that the equivalence class of the symbol $m : n$ can be identified with the rational number $f = \frac{m}{n}$.

More interesting example. Consider the collection of all finite groups Γ. In case, when Γ_1 is a normal subgroup in Γ and Γ_2 is the quotient group Γ/Γ_1, it is natural to say that Γ is divisible by Γ_1 and the quotient is equal to Γ_2. We denote by $[\Gamma]$ the class of all finite groups isomorphic to Γ.

Define a new group $\mathfrak{G}$ as follows. By definition, $\mathfrak{G}$ is the abelian group generated by all symbols $[\Gamma]$ with the relations

$$[\Gamma] = [\Gamma_1] + [\Gamma_2] \tag{1.2}$$

if Γ_1 is a normal subgroup in Γ and $\Gamma_2 = \Gamma/\Gamma_1$.

One can check that any element of $\mathfrak{G}$ has the form

$$g = n_1 \cdot [\Gamma_1] + \cdots + n_k \cdot [\Gamma_k] \tag{1.3}$$

where $\Gamma_1, \ldots \Gamma_k$ are finite groups.

Theorem 1 *The group $\mathfrak{G}$ is a free abelian group with countable set of generators. As generators one can take the symbols $[\Gamma]$ where Γ is a cyclic group Z_p of a prime order p, or a simple non-abelian finite group.*

So, an element $g \in \mathfrak{G}$ can be uniquely written in the form (1.3) where Γ_i belong to the list of groups pointed out in the theorem.

Exercise 1 *Show that in the group $\mathfrak{G}$ the classes $[Z_6]$ and $[S_3]$ define the same element $[Z_2] + [Z_3]$, though Z_6 and S_3 are not isomorphic.*

Exercise 2 *Express in terms of generators the following elements of $\mathfrak{G}$:*

a) $[\mathbb{Z}_n$, n is not a prime.

b) $[S_n]$ where S_n is the group of permutations of n objects.

c) $[T_n(\mathbf{F}_q)]$ where $T_n(\mathbf{F}_q)$ is the group of all invertible upper triangular matrices of order n with entries from a finite field with $q = p^k$ elements (p is prime).

In all cases considered above we construct a group using the same method: by introducing new elements (negative numbers, fractions, formal linear combinations etc) and by splitting a set into equivalence classes. The most general form of this method until recently was the notion of so-called Grothendieck group $\mathfrak{G}(\mathcal{C})$ of a small additive category $\mathcal{C}$ (see [21])[1]

This group by definition, is commutative and generated by equivalence classes of objects of $\mathcal{C}$ with relations

$$[A] = [B] + [C] \tag{1.4}$$

where B is a subobject of A and C is the corresponding quotient object A/B. For instance, the group $\mathfrak{G}$ above is the Grothendieck group of the category of finite groups.

Exercise 3 *Show that for the category $\mathcal{A}$ of all abelian groups with finite number of generators the group $\mathfrak{G}(\mathcal{A})$ is isomorphic to $\mathbb{Z}$.*

One of the most brilliant applications of this construction is the so-called K-theory, where the initial material is the collection of vector bundles over a given smooth manifold. The detailed exposition of this young but already very famous theory one can find in [1, 5].

A further generalization is possible when the operation in question is non-commutative.

[1] Unfortunately, the notion of a category is not in the curriculum of any undergraduate course, though in the modern mathematics it plays the role comparable with the notions of a set and a function. The initial material about categories is given in [11, 12] and more detailed information one can find in [6, **?**, 9].

Example 1 *Let A denote an algebra with a unit over $\mathbb{C}$ generated by elements p and q with relations*

$$pq - qp = 1. \tag{1.5}$$

This algebra has a convenient realization as an algebra of differential operators on the real line with polynomial coefficients. The generators have the form

$$p = \frac{d}{dx} \quad \textit{(differentiation)}, \qquad q = x \quad \textit{(multiplication by } x\textit{)}.$$

Exercise 4 *Show that A has no zero divisors, i.e. if $ab = 0$, then $a = 0$ or $b = 0$.*

Let us call a *right fraction* the expression ab^{-1} where a, $b \in A$ and $b \neq 0$. Analogously, a *left fraction* is an expression $b^{-1}a$.

We say that a left fraction $c^{-1}d$ is equivalent to a right fraction ab^{-1} if $ca = db$. Two left (respectfully, right) fractions we consider as equivalent if they are equivalent to the same right (resp., left) fraction. The following remarkable fact takes place.

Theorem 2 *In any equivalence class there are both left and right fractions.*

In any two classes there are left (resp., right) fractions with a common denominator.

The theorem follows rather easily from the following important

Lemma 1 *For any two non-zero elements of A there exists a common right (resp., left) multiple.*

Proof of the Theorem. Let $A^{(n)}$ denote the subspace in A consisting of all elements which can be written as polynomials of degree $\leq n$ in generators p, q. Check yourself that $\dim A^{(n)} = \frac{1}{2}(n+1)(n+2)$.

Assume now that that a, b are non-zero elements of A. They belong to A_m for some m. Consider the spaces[2] $a \cdot A^{(n)}$ and $b \cdot A^{(n)}$. It is clear that both spaces are contained in $A^{(m+n)}$. On the other hand, for n big enough, we have

$$2 \dim A^{(n)} = (n+1)(n+2) > \frac{1}{2}(n+m+1)(n+m+2) = \dim A^{(n+m)}.$$

[2]We denote by $a \cdot A^{(n)}$ the set of all elements of the form ax, $x \in A.n$ In general, if A and B are some sets and $*$ is an algebraic operation applicable to their elements, then the symbol $A * B$ denote the set of all $a * b$ where $a \in A$, $b \in B$.

Therefore, $a \cdot A^{(n)}$ and $b \cdot A^{(n)}$ have a common non-zero element which is a desired common right multiple of a and b.

□

Exercise 5 *Find a common right multiple of p^n and q^n.*

Using Theorem 2, we can define the quotient skew field D for the algebra A. Namely, we cal take the equivalence classes of fractions as elements of D and define addition, subtraction and division by the rules:

$$ac^{-1} \pm bc^{-1} := (a \pm b)c^{-1}, \qquad ac^{-1} : bc^{-1} := ab^{-1}. \tag{1.6}$$

The multiplication by ab^{-1} can be defined as the division by the inverse fraction ba^{-1}. Of course, we have to check the correctness of all these definitions (i.e. independence of the result from the choice of representatives) and also all the ordinary laws (commutativity of addition, distributivity of multiplication and associativity of both laws). All this traditionally is left to the reader.

The skew field D is a very interesting object. Many of its properties are still not known. We recommend [10] to the interested reader.

The construction of the skew field D can be generalized. First of all, we can start with several pairs of generators p_i, q_i, $1 \le i \le n$ and relations

$$p_i p_j = p_j p_i, \quad q_i q_j = q_j q_i, \quad p_i q_j - q_j p_i = \delta_{ij}. \tag{1.7}$$

More essential and more interesting generalization we obtain by considering an associative algebra with generators $x_1, \ldots, x_n$ and relations of a special form:

$$x_i x_j - x_j x_i = \sum_{k=1}^{n} c_{ij}^k x_k, \quad 1 \le i, j \le n \tag{1.8}$$

where c_{ij}^k are some constants. The left hand side of (1.8) is called a *commutator* of x_i and x_j. It is usually denoted by $[x_i, x_j]$.

Exercise 6 *Show that in any associative algebra the operation "commutator" satisfies the so-called Jacobi identity:*

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0. \tag{1.9}$$

It is worth to mention (or recall) here that a vector space with a bilinear skew-symmetric operation satisfying (1.9) is called a *Lie algebra*. This name is related to Lie groups which we shall discuss later.

Come back to our associative algebra. We assume that the generators x_i are linearly independent. Then from exercise 6 it follows that the constants c_{ij}^k satisfy the equation

$$\sum_{s=1}^{n}(c_{ij}^s c_{sk}^m + c_{jk}^s c_{ki}^m + c_{ki}^s c_{sj}^m) = 0 \tag{1.10}$$

for all i, j, k, m.

In this case the linear span of $x_1, \ldots, x_n$ is a Lie algebra L and our associative algebra is denoted by $U(L)$ and is called a *universal enveloping algebra* for L.

It is remarkable that the statements of the lemma and of the theorem 2 remain valid for the algebra $U(L)$. Therefore, for any Lie algebra L a skew field $D(L)$ is defined as a quotient field of $U(L)$. The study of skew fields D_n and $D(L)$ is one of most interesting parts of a new direction in mathematics called *non-commutative algebraic geometry* (see [11, 8]).

In conclusion of this section we propose two simply formulated questions which are still unsolved.

1. Does the Fermat equation

$$X^k + Y^k = Z^k \tag{1.11}$$

has a non-trivial solution ($XYZ \neq$ const) in the algebras A, $A_n, U(L)$?

It is known that in the polynomial algebra $\mathbb{C}[p, q]$ all solutions are trivial for $k > 2$. In [10] a non-trivial solution of (1.11) is found for $k = 3$.

Exercise 7 *Find the general solution to* (1.11) *in the algebra* $\mathbb{C}[x, y]$.

2. Let $P, Q \in A$ have the property

$$PQ - QP = 1.$$

Then the map $\varphi : \ p \mapsto P, \ q \mapsto Q$ defines an endomorphism of the algebra A into itself. Is it true that φ is actually an isomorphism?

In other words: is φ always invertible?

Or, does A contain a proper subalgebra isomorphic to A?

The commutative analogue of this problem is also non-solved. This is so-called *Jacobian problem*. The exact formulation is

Let $P, Q \in \mathbb{C}[x, y)$ satisfy

$$\begin{bmatrix} \frac{\partial P}{\partial x} & \frac{\partial Q}{\partial x} \\ \frac{\partial P}{\partial y} & \frac{\partial Q}{\partial y} \end{bmatrix} = 1 \tag{1.12}$$

Is it true that the polynomial map

$$\varphi:\ (x,y)\mapsto \big(P(x,y),\, Q(x,y)\big)$$

has a polynomial inverse map?

In the same circle of ideas is the notion of a *derived category* which unexpectedly turned out to be a very effective method of solution of many difficult algebraic and geometric problems. The idea of construction of a derived category is rather simple and recall simultaneously the construction of the Grothendick group and the construction of the quotient skew field. View to the lack of time, place and competence, I refer to the book [9] for the further information.

Answers and hints to the problems.

1. In both groups there is a normal subgroup isomorphic to Z_3.

2. a) $[\mathbb{Z}_n] = \sum_k a_k[\mathbb{Z}_{p_k}]$, if $n = \prod_k p_k^{a_k}$ is the decomposition of n in prime powers.

b) $[S_2] = [Z_2],\ [S_3] = [Z_2] + [Z_3],\ [S_4] = 3[Z_2] + [Z_3],\ [S_n] = [Z_2] + [A_n]$ for $n \geq 5$ Here A_n is a simple group of order $\frac{n!}{2}$ consisting of all even permutations in S_n.

c) If $q = p^k,\ p$ prime and $q - 1 = \prod_k p_k^{a_k}$ is the decomposition in prime powers, then $[T_n(\mathbf{F}_q)] = \frac{1}{2}mn(n-1)[Z_p] + \sum_k a_k[Z_{p_k}]$.

3. Take $[\mathbb{Z}]$ as generator of $\mathfrak{G}$. Use the fact that for any n we have $\mathbb{Z}/n\mathbb{Z} \simeq Z_n$.

4. Introduce the notion of a *leading term* for elements of A, so that the leading term of $a \in A^{(n)}\backslash A^{(n-1)}$ is $[a] \in \mathbb{C}^n[p,\, q]$. Then check that $[ab] = [a]\,[b]$.

5. $\frac{p^{2n}q^n}{(2n)!n!} = \sum_{k=0}^{n} \frac{q^k p^k}{k!(n-k)!(n+k)!}p^n$

7. One of the possibilities: $X = (A^2 - B^2)C,\ Y = 2ABC,\ Z = (A^2 + B^2)C$ where A, B, C are arbitrary polynomials.

1.2 From $\mathbb{Q}$ to $\mathbb{R}$: the idea of completion. p-adic numbers and adeles

> In a domain without center,
> when center can be any
> random point...
>
> A.K. Tolstoj, *"Don Juan"*

1.2.1 p-adic numbers

The real numbers are obtained from rational ones by the procedure of *completion*. This procedure can be applied to any *metric space*, i.e. a set where a distance is defined for any pair of points. You can find a rigorous definition and basic theorems in any textbook in advanced calculus (e.g. [KG] or [KF]).

Instead, we ask a seditious question: how natural is the ordinary definition of a distance between rational numbers:

$$d(r_1,\, r_2) = |r_1 - r_2|; \tag{1.13}$$

is there an other way to describe the proximity between them? It turns out that such a way exists. Here is an example. Let us choose a prime number p. Any rational number r can be uniquely written in the form $r = p^k \cdot \frac{m}{n}$ where $k \in \mathbb{Z}$ and $\frac{m}{n}$ is an irreducible fraction whose numerator and denominator are relatively prime to p. The quantity p^{-k} is called the *p-adic norm* of r and is denoted by $||r||_p$. One can check that the distance

$$d_p(r_1,\, r_2) = ||r_1 - r_2||_p \tag{1.14}$$

has many properties of an ordinary distance (1.13) . For example, it satisfies the Triangle inequality:

$$d_p(r_1,\, r_2) \leq d_p(r_1,\, r_3) \geq d_p(r_2,\, r_3). \tag{1.15}$$

In the same time there are differences. E.g., with respect to the distance (1.14) all triangles are isosceles and, moreover, the equal sides are not shorter than the third side. The metric spaces with this property are called *ultrametric*. The Triangle inequality takes here a stronger form:

$$d_p(r_1,\, r_2) \leq \max\{d_p(r_1,\, r_3),\ d_p(r_2,\, r_3)\}. \tag{1.16}$$

Exercise 8 *Show that in an ultrametric space the following simple criterion takes place*

A series $\sum_{k=1}^{\infty} x_n$ converges iff x_n tends to 0 when $n \to \infty$.

Another remarkable property of the p-adic distance is that all integers form a bounded set of diameter 1. If we apply to this set the completion procedure, we get a compact set $\mathbf{O}_p$ whose elements are called *p-adic integers*. They can be conveniently written in the form of infinite-digit numbers

in a p-adic numerical system. Namely, every $a \in \mathbf{O}_p$ can be uniquely written as

$$a = \dots a_n \dots a_2 a_1 a_0, \qquad 0 \le a_i \le p-1. \tag{1.17}$$

It can be understood as a sum of the series

$$a = \sum_{k=0}^{\infty} a_k p^k. \tag{1.18}$$

Indeed, $||a_k p^k|| \le p^{-k}$, so that terms of the series tend to 0 and the series is convergent. By definition, a is the sum.

Exercise 9 *Construct a bicontinuous bijection of $\mathbf{O}_p$ to the Cantor set. (It is especially simple for $p = 2$ and slightly more complicated for general p.)*

The p-adic numbers form a ring: we can add them, subtract and multiply. It is also convenient to write a mixed-periodic p-adic number $\dots AAAB$ in the form $(A)B$.

Exercise 10 *Compute the following quantities in $\mathbf{O}_5$:*

a) $(4) + (0)1$, b) $\dots (0) - (0)1$, c) $(1) \times (4)$.

However, the set $\mathbf{O}_p$, unlike $\mathbb{Z}$, has no natural order. Hence, there are no positive and negative numbers. Indeed, the set $\mathbb{N}$ of natural numbers is dense in $\mathbf{O}_p$ (for instance, $-1 = \lim_{n\to\infty} p^n - 1$).

Nevertheless, for p-adic numbers we can define an analogue of the function "signum", which takes p different values.

We recall that the ordinary signum

$$\operatorname{sgn} x = \begin{cases} 1, & \text{if} \quad x > 0, \\ 0, & \text{if} \quad x = 0, \\ -1, & \text{if} \quad x < 0 \end{cases}$$

can be approximated on the segment $[-1, 1]$ by the function x^ϵ where ϵ is a small rational number $\frac{1}{n}$ (with an odd denominator n to make sense for negative x). In the p-adic situation the role of $\epsilon = \frac{1}{n}$ is played by p^n.

Theorem 3 *t:sgn For any $a \in \mathbf{O}_p$ there exists a limit*

$$\lim a^{p^n} \quad \text{for} \quad n \to \infty. \tag{1.19}$$

It is denoted by $sgn_p(a)$ and has the properties

a) $sgn_p(ab) = sgn_p(a) \cdot sgn_p(b)$

b) $sgn_p(a)$ depends only on the digit a_0 of number a.

c) $sgn_p(a) = 0$ if $a_0 = 0$ and is a root of degree $p-1$ from 1 if $a_0 \neq 0$.

Thus, the p-adic line has $p-1$ different "directions".

For the proof of the theorem the following result is useful.

Lemma 2 *If* $0 < d_p(a,\, b) < 1$, *then* $d_p(a^p,\, b^p) < d_p(a,\, b)$.

Unlike ordinary integers, many p-adic integers are invertible. Namely, if $a \in \mathbf{O}_p$ and $\mathrm{sgn}(a) \neq 0$, then a^{-1} is also a p-adic integer. In particular, all rational numbers with denominator relatively prime to p are p-adic integers.

Exercise 11 *Show that the number a of the form* (1.17) *is rational if and only if the sequence $\{a_n\}$ is eventually periodic (i.e. periodic starting with some place.)*

If we apply the completion procedure with respect to the distance (1.14) not to $\mathbb{Z}$ but to $\mathbb{Q}$, we get the set of all p-adic numbers, not necessary integers. This set is denoted by $\mathbf{Q}_p$. Its elements are conveniently written as mixed p-adic fractions of the form

$$a \;=\; \ldots\, a_n \,\ldots\, a_2 a_1 a_0 . a_{-1} \,\ldots\, a_{-k} \tag{1.20}$$

In particular, every p-adic number has the form $a \cdot p^{-k}$ where $a \in \mathbf{O}_p$.

The rules of arithmetic operations on p-adic numbers are very similar to the rules of operations on usual decimal fractions but with one additional principle: all computations one must start with the last digit.

Here is an example of such computation in $\mathbf{O}_5$:

(123)	$\ldots$ (123)	(123)
$+$(10).1	(10).1	(10).1
$=$(224133).1	(302211)2.4	(312).3
		(123)0.
		(123)000.
		(123)00000.
		$\ldots$ .....
		$\ldots$ 210022042.3

Actually, here some relations between rational numbers are written. Can you tell which ones?

Here is a little more complicated example.

$$\sqrt{-1} \;=\; \sqrt{\ldots\, 4444} \,=\, \mathrm{sgn}\, 2 \;=\; \lim_{n\to\infty} 2^{5^n} \;=\; \ldots\, 212.$$

Exercise 12 *How, knowing a p-adic form of a rational number r to tell is it positive or negative?*

1.2.2 p-adic analysis

In the set $\mathbf{Q}_p$ of p-adic numbers all operations of analysis are defined: four arithmetic operations and the limit of a sequence. So, we can transfer to the p-adic case almost all material of an advanced calculus which is studied in the undergraduate school. Some theorem are true literally, the other need some corrections and some are replaced by completely different (or even opposite) statements.

For example, for the segment [0, 1], the favorite object of real analysis, a natural p-adic analogue is the set $\mathbf{O}_p$ of p-adic integers. This p-adic segment, as well as the real one, is a ball.

Recall that in any metric space X a *ball* B, or, more precisely, a *ball* $B_r(a)$ with a *center* a and a *radius* r is defined as a subset of the form

$$B_r(a) = \{x \in X \mid d(x, a) \leq r\}.$$

In our case $X = \mathbf{Q}_p,\ B = \mathbf{O}_p$. Here we have $r = 1$, but, unlike the usual ball, the role of a center can be played by arbitrary point $a \in \mathbf{O}_p$[3].

Moreover, $\mathbf{O}_p$ is a compact set, hence has all the properties of the segment [0, 1] which follow from its compactness.

Exercise 13 *Prove that any continuous function on $\mathbf{O}_p$ with values in $\mathbf{O}_p$ can be uniformly approximated by polynomials with coefficients in $\mathbf{O}_p$*

Exercise 14 *Consider the map $s:\ \mathbf{Q}_p \to \mathbb{R}$ which sends a p-adic number a of the form (1.20) to the real number $s(a) = \sum_k a_k p^{-k}$.*

(In other words, the p-adic form of $s(a)$ is obtained from the p-adic form of a by the "reflection in the point".)

Show that s is continuous and maps $\mathbf{Q}_p$ onto $\mathbb{R}_+$ and $\mathbf{O}_p$ onto [0, 1].

You might think that s is bijective and bicontinuous, but it is not so. The reason is that the p-adic form of a real number is not unique. Note also that in the case $p = 2$ the restriction of s to $\mathbf{O}_2$ is related to the so-called "Cantor ladder" (or, in other terminology, "devil ladder").

To those, who became interested in p-adic analysis I recommend the following problems for the independent study:

What is a p-adic analogue of

[3]May be, A.K.Tolstoj had in mind exactly this?

a) the signature of a quadratic form;
b) exponential and logarithmic functions;
c) the Fourier transform;
d) Γ-function and B-function of Euler?
An additional material you can find in [11, 12, 14].

1.2.3 Adeles

The main application of p-adic analysis until now were in the number theory. In this language it is convenient to formulate different questions of divisibility and residues modulo an integer. Last time, however there were many attempts to use the p-adic analysis in mathematical physics. Some of these attempts based only on the belief that any mathematical construction must have a physical meaning (and the simpler and more beautiful the construction is, the more fundamental it meaning is.) Other attempts are, essentially, *ad absurdum*: if the usual analysis is not enough, let us try the p-adic one. Finally, there is one more important fact for which one can look a physical explanation. The point is that the usual real field $\mathbb{R}$ can be united with all p-adic fields $\mathbf{Q}_p$ in one beautiful object: the ring $\mathbf{A}$ of *adeles*.

An adele $a \in \mathbf{A}$ is by definition a sequence

$$a \;=\; (a_\infty,\, a_2,\, a_3,\, a_5,\, \dots, a_p,\, \dots) \tag{1.21}$$

where $a_\infty \in \mathbb{R}$, $a_p \in \mathbf{Q}_p$, and for almost all p (i.e. for all but a finite number of them) $a_p \in \mathbf{O}_p$.

The arithmetic operations and limits for adeles are defined componentwise. The invertible adeles are called *ideles*[4] The set of ideles is denoted by $\mathbf{A}^\times$. For an idele a we can define its *norm* by the formula

$$||a|| = |a_\infty| \cdot \prod_p ||a_p||_p. \tag{1.22}$$

This infinite product make sense, because almost all factors are equal to 1. Note now, that the field $\mathbb{Q}$ of rational numbers can be embedded into $\mathbf{A}^\times$, namely a rational number r can be considered as adele

$$\underline{r} \;=\; (r,\, r,\, r, \dots,\, r,\, \dots)$$

where the first r is considered as a real number, the second one as a 2-adic number, the third one as a 3-adic number etc. The adeles of this form are called *principal adeles*. It is clear that any principal adele is actually an idele. Moreover, the following is true

[4] Actually, ideles appeared first and provoked the invention of adeles as *additive ideles*.

Exercise 15 *Show that*

$$||\underline{r}|| = 1 \quad \textit{for all } r \in \mathbb{Q}. \tag{1.23}$$

The map $r \mapsto \underline{r}$ defines an embedding of $\mathbb{Q}$ into $\mathbf{A}$, so from now on we shall not distinguish r and $\underline{r}$.

Let now M be an algebraic manifold defined over the field of rational numbers. (I.e., a system of algebraic equations with coefficients in $\mathbb{Q}$). Then we can consider the sets M_K of solutions of this system over any $\mathbb{Q}$-algebra K. For $K = \mathbb{R}$ we get an ordinary real algebraic manifold and for $K = \mathbf{A}$ it is an *adelic manifold*.

We come in this way to the so-called *adelic* analysis. It is remarkable, that the adelic theorems relate together the real and p-adic facts. For example many elementary and special (higher transcendental) functions have nice p-adic and adelic analogues. Here I consider only two examples of these analogues.

1.2.4 Tamagawa numbers

If M is a real algebraic manifold, then to any differential form ω of top degree on M we can associate a measure $\mu = |\omega|$ on M. Assume that M is defined over $\mathbb{Q}$ and in appropriate local coordinates ω has rational coefficients. When ω is multiplied by a rational number r, the measure $|\omega|$ is multiplied by $|r|$.

It turns out that the set $M_{\mathbf{Q}_p}$ of all points of M over $\mathbf{Q}_p$ also has a canonical measure $\mu_p = ||\omega||_p$ and the the replacement of *omega* by $r \cdot \omega$ leads to the multiplication of μ_p by $||r||_p$.

Finally, we can define an adelic manifold $M_{\mathbf{A}}$ and a measure $\mu_{\mathbf{A}}$ corresponding to the initial differential form ω. But now, the replacement of *omega* by $r \cdot \omega$ does not change the measure $\mu_{\mathbf{A}}$, since the adelic norm of r is 1. Hence, the integral

$$I(M, \omega) = \int_{M_{\mathbf{A}}} \mu_{\mathbf{A}} \tag{1.24}$$

depends only on M and ω modulo multiplication on a rational number.

There is one case when such an equivalence class is naturally defined: suppose that M is an homogeneous manifold with respect to some algebraic group G acting rationally on M. When, a G-invariant differential form of top degree, if it exists, is uniquely defined up to constant factor. The

simplest example is the homogeneous space $M = G_{\mathbf{A}}/G_{\mathbb{Q}}$. In this case $I(M, \omega)$ is called the *Tamagawa number* of the group G and is denoted by $\tau(G)$. For many classes of groups this number is the product of the real volume of the manifold $G_{\mathbb{R}}/G_{\mathbb{Z}}$ and p-adic volumes of $G_{\mathbf{O}_p}$ for all primes p. It is astonishing that $\tau(G)$ is often a very simple number, e.g. 1!

Consider in details two particular cases where G is an additive group of the basic field $\mathbb{Q}$ or the unit circle on plane.

1. *Additive group*

In this case $G_K = K$ and the manifold M is $\mathbf{A}/\mathbb{Q}$. The differential form in question is $\omega = dx$. It defines the ordinary Lebesgue measure μ on $\mathbb{R}$ and the Haar measure μ_p on $\mathbf{Q}_p$, normalized by the condition $\mu_p(\mathbf{O}_p) = 1$ (i.e. the measure of a unit ball is equal to 1).

Exercise 16 *Show that* $\mathbf{A}/\mathbb{Q}$ *is in a natural bijection with* $\mathbb{R}/\mathbb{Z} \times \prod_{p \ prime} \mathbf{O}_p$.

We see that in this case $\tau(G) = vol_{\mathbb{R}}(\mathbb{R}/\mathbb{Z}) \times \prod_{p \ prime} vol_p(\mathbf{O}_p) = 1$.

2. *Circle group*

Here G is an algebraic manifold given by equation $x^2 + y^2 = 1$. The group law is inspired by multiplication of complex numbers and is defined by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1).$$

We choose the form $\omega = \frac{dx}{y} = -\frac{dy}{x}$ as the top degree form on G with rational coefficients.

Consider the group $G_{\mathbb{Q}}$ of rational points of G. Let us suppose first that $(x, y) \neq (-1, 0)$ and rewrite the initial equation in the form

$$y^2 = (1 - x)(1 + x), \quad \text{or} \quad \frac{y}{1 + x} = \frac{1 - x}{y}.$$

The common value of last two fractions is a rational number which we denote by r. Then we have a system of linear equation for (x, y):

$$y = r(1 + x) \qquad 1 - x = ry$$

with the solution

$$x = \frac{1 - r^2}{1 + r^2}, \qquad y = \frac{2r}{1 + r^2}. \tag{1.25}$$

When r run through the set $\mathbb{Q}$ of all rationals, (x, y) runs through $G_{\mathbb{Q}}$ with the point $(-1, 0)$ deleted.

Actually, we can make r run through the set $\overline{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ and obtain the whole set of solutions, including $(-1, 0)$.

In terms of parameter r the group multiplication law looks like

$$r_1 * r_2 = \frac{r_1 + r_2}{1 - r_1 r_2}. \tag{1.26}$$

Now, let us try the same approach to study the group $G_{\mathbf{Q}_p}$. Namely, assume that $(x, y) \neq (-1, 0)$ and denote by λ the common value of fractions $\frac{y}{1+x} = \frac{1-x}{y}$. Then we obtain the system of linear equations

$$y = \lambda(1 + x) \qquad 1 - x = \lambda y$$

with determinant $1 + \lambda^2$. For some p the expression $1 + \lambda^2$ never vanishes for $\lambda \in \mathbf{Q}_p$.

Exercise 17 *Prove that for $p = 2$ and for a prime p of the form $4k - 1$ the equation*

$$1 + \lambda^2 = 0$$

has no solutions in $\mathbf{Q}_p$.

So, for this kind of primes we can parametrize the p-adic circle by the points $\lambda \in \overline{\mathbf{Q}_p} = \mathbf{Q}_p \cup \{\infty\}$:

$$x = \frac{1 - \lambda^2}{1 + \lambda^2}, \qquad y = \frac{2\lambda}{1 + \lambda^2}. \tag{1.27}$$

But if $p = 4k+1$ the situation is different. Recall that the non-zero values of the function $\operatorname{sgn} x$ are roots of degree $p-1$ from -1. When $p = 4k+1$, two of these values are square root from -1. Denote by $\pm i$ the corresponding points in $\mathbf{Q}_p$. The initial equation can be rewritten as

$$(x + iy)(x - iy) = 1.$$

So, in this case the group $G_{\mathbf{Q}_p}$ is isomorphic to the multiplicative group $\mathbf{Q}_p^\times$ of the field $\mathbf{Q}_p$. The corresponding parametrization looks like

$$x = \frac{\lambda + \lambda^{-1}}{2}, \qquad y = \frac{\lambda - \lambda^{-1}}{2i}. \tag{1.28}$$

It turns out that the shape of the set $G_{\mathbf{Q}_p}$, the p-adic circle, depends on the residue $p \mod 4$.

Theorem 4 *The p-adic circle $G_{\mathbb{Q}_p}$ consists of:*
a) four disjoint balls of radius $\frac{1}{4}$ if $p = 2$;
b) $p - 1$ disjoint balls of radius $\frac{1}{p}$ if $p \equiv 1 \mod 4$;
c) $p + 1$ disjoint balls of radius $\frac{1}{p}$ if $p \equiv -1 \mod 4$;

So, we have

$$\begin{gathered} vol(G_{\mathbf{O}_2}) = \frac{1}{2}, \qquad vol(G_{\mathbf{O}_p}) = \frac{p-1}{p} \quad \text{for} \quad p = 4k-1, \\ vol(G_{\mathbf{O}_p}) = \frac{p+1}{p} \quad \text{for} \quad p = 4k+1. \end{gathered} \tag{1.29}$$

Finally, observe that $G_{\mathbb{Z}}$ consists of four points: $\{(\pm 1, 0),\ (0, \pm 1)\}$. Thus, the set $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is a quarter of a unit circle and has the length $\frac{\pi}{2}$.

Collecting all this together we obtain for the Tamagawa number of the group G the value

$$\tau(G) = \frac{\pi}{2} \cdot \prod_{\substack{p \ prime, \\ p=4k+1}} \frac{p-1}{p} \cdot \prod_{\substack{q \ prime, \\ q=4k-1}} \frac{q+1}{q}. \tag{1.30}$$

Note, that the both infinite products in this formula are actually divergent – the first goes to 0, the second to ∞. But we can make sense of the whole product, rewriting it in the form of a conditionally convergent series.

For this end we use the equalities

$$\frac{p-1}{p} = \left(\sum_{k \geq 0} p^{-k} \right)^{-1}, \qquad \frac{q+1}{q} = \left(\sum_{k \geq 0} (-q)^{-k} \right)^{-1}.$$

and

$$\prod_{\substack{p \ prime, \\ p=4k+1}} \prod_{\substack{q \ prime, \\ q=4k-1}} \sum_{k \geq 0} p^{-k} \cdot \sum_{k \geq 0} (-q)^{-k} = \sum_{k \geq 0} \frac{(-1)^k}{2k+1} = \frac{\pi}{4}.$$

(The last equality is the famous result of Leibniz and also the Taylor series for $\arctan 1$).

The final result is: $\tau(G) = 1$.

Exercise 18 *The well prepared readers can try to find the Tamagawa number for some more complicated groups. The most appropriate examples are the group $SO(3, \mathbb{R})$ of all real orthogonal matrices of order three and the group $SU(2, \mathbb{C}) \simeq U(1, \mathbb{H})$ of unit quaternions.*

1.2.5 p-adic ζ-function

The classical ζ-function of Riemann is defined as a sum of the series

$$\zeta(s) = \sum_{n\geq 1} n^{-s}, \tag{1.31}$$

which is convergent for $\Re(s) > 1$. We shall see in a moment that this function can be analytically extended to the whole complex plane $\mathbb{C}$ with the origin deleted. Moreover, the values of $\zeta(s)$ at negative integer points have very interesting arithmetic properties.

For this we need some elementary facts from the complex analysis: The notion of a holomorphic function and its analytic continuation, the Cauchy residue theorem and some properties of elementary functions.

Consider the integral

$$I(s) = \oint \frac{z^s}{e^z - 1} \cdot \frac{dz}{z} \tag{1.32}$$

over the contour C starting at ∞, going along real axis from below, then along small circle surrounding clockwise the origin and going back along real axis from above to ∞. Here the expression z^s is understood as $e^{s(\log|z| + i\arg z}$ and $0 \leq \arg z \leq 2\pi$ on the contour C. So, the integrand is holomorphic in s and the integral converges for every $s \in \mathbb{C}$. Therefore, its value $I(s)$ is a holomorphic function on $\mathbb{C}$.

We compute this integral in two different ways. First, assuming $\Re(s) > 1$ and contracting our contour C to the twice passed ray $[0, \infty)$, we get

$$I(s) = (1 - e^{2\pi i s}) \int_0^\infty \frac{x^s}{e^x - 1} \frac{ds}{s}.$$

Further, since

$$\frac{1}{e^x - 1} = \sum_{n=1}^{\infty} e^{-nx} \quad \text{(sum of a geometric progression)}$$

and

$$\int_0^\infty x^{s-1} e^{-nx} dx = n^{-s}\Gamma(s)$$

(by the substitution $y = nx$ this integral is reduced to the definition of the Γ-function), we obtain

$$I(s) = (1 - e^{2\pi i s})\Gamma(s)\zeta(s) = -2i\sin(\pi s)e^{\pi i s}\Gamma(s)\zeta(s) \quad \text{for } \Re(s) > 1. \tag{1.33}$$

This equality shows that $\zeta(s)$ can be analytically extended to $\mathbb{C}\backslash\{1\}$.

Second, for $\Re(s) < 0$ the value of the integrand on a big circle C_R of radius R is $o(R^{\Re(s)-1}$, so the integral over C_R tends to 0 when $R \to \infty$. If we complete the contour C by C_R, we can compute the new integral $I^R(s)$ by the Cauchy residue formula. The integrand has poles at the points $\pm 2n\pi i$ and we get the result

$$I_R(s) = 2\pi i \sum_{\substack{|n|<\frac{R}{2\pi} \\ n\neq 0}} (2\pi i n)^{s-1}.$$

When $R \to \infty$, we get in the limit

$$I(s) = 2\pi i \sum_{n\neq 0} (2\pi i n)^{s-1}.$$

The sum over positive n gives

$$\sum_{n\geq 1} (2\pi i)(2\pi i n)^{s-1} = (2\pi)^s e^{\frac{\pi i s}{2}} \cdot \Gamma(1-s)$$

The sum over negative n gives

$$\sum_{n\geq 1} (2\pi i)(-2\pi i n)^{s-1} = -(2\pi)^s e^{\frac{3\pi i s}{2}} \cdot \Gamma(1-s)$$

So, together we have

$$I(s) = (2\pi)^s (e^{\frac{\pi i s}{2}} - e^{\frac{3\pi i s}{2}})\zeta(1-s) = -2i \sin\frac{\pi s}{2} (2\pi)^s e^{\pi i s}\zeta(1-s). \quad (1.34)$$

Comparing (1.33) and (1.34), we get the famous *Riemann functional equation* for $\zeta(s)$:

$$\zeta(s) = \frac{(2\pi)^s}{2\cos\left(\frac{\pi s}{2}\right)\Gamma(s)}\zeta(1-s). \quad (1.35)$$

We mention some corollaries from this equation. First of all, replasing in (1.35) s by $1-s$ and comparing the two expressions, we come to the *Euler identity*:

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

Second, for $s = 2k$, $k \in \mathbb{N}$, we get

$$\zeta(2k) = \frac{(2\pi)^{2k}\zeta(1-2k)}{2\cos(\pi k)\Gamma(2k)} = (-1)^k \frac{2^{2k-1}\pi^{2k}}{(2k-1)!}\zeta(1-2k). \quad (1.36)$$

On the other hand, it is well-known that The value $\frac{\zeta(2k)}{2\pi^{2k}}$ is a rational number. To show it, consider the sequence of functions

$$f_k(x) = \sum_{n\neq 0} \frac{e^{2\pi inx}}{(2\pi in)^k}. \tag{1.37}$$

This series is convergent absolutely for $k \geq 2$ and conditionally for $k = 1$ and $x \notin \mathbb{Z}$. The sum is, evidently a periodic function: $f(x + 1) = f(x)$. It turns out that on the interval (0, 1) this function coinsides with a certain polynomial of degree k, namely

$$f_k(x) = -B_k(x)/k!. \tag{1.38}$$

The polynomials B_k are called *Bernoulli polynomials*. They can be uniquely determined by the properties:

a) $B_0(x) = 1$;
b) $B'_k(x) = kB_{k-1}(x)$;
c) $\int_0^1 B_k(x)dx = 0 \quad \text{for} \quad k \geq 1$.

The constant terms $B_k(0)$ are denoted by B_k and are called *Bernoulli numbers*. It is easy to see that they are rational and that $B_{2k+1} = 0$ except $k = 0$.

From (1.37) and (1.38) follows that

$$\zeta(2k) = (2\pi i)^{2k} f_{2k}(0) = -(2\pi i)^{2k} B_{2k}/(2k)!$$

and, using (1.36), we get

$$\zeta(1 - 2k) = -B_{2k}/(2k). \tag{1.39}$$

The following arithmetic properties of Bernoulli numbers were discovered by E.Kummer.

Theorem 5 (Kummer congruences) *If $p - 1$ is not a divisor of k, then*
a) $||B_k||_p \leq 1$;
b) if $k \equiv m \mod (p - 1)p^N$, then

$$(1 - p^k)B_k/k \equiv (1 - p^m)B_m/m \mod p^{N+1}.$$

□

Let us define the p-adic ζ-function by the formula

$$\zeta_p(k) = (1 - p^{k-1})\zeta(1 - k). \tag{1.40}$$

From the Kummer congruences it follows, that $\zeta_p(k)$ is uniformly continuous on every set M_a of the form $a + (p-1)\mathbb{N},\ a = 1, 2, \ldots, p-2$. Therefore, it can be extended to the closure of M_a in $\mathbf{Q}_p$ which coincides with $\mathbf{O}_p$. The culmination of these beautiful theory is the formula of Kubota-Leopold which gives an integral presentation

$$\zeta_p(k) = \int_{\mathbf{O}_p} x^{-k} d\mu_a(x) \quad \text{for} \quad k \equiv a \mod (p-1),$$

where μ_a is a measure on $\mathbf{O}_p$ with support on $\mathbf{O}_p^\times$. The details one can find in [14].

Besides number-theoretic and probable physical applications, the existence of fields $\mathbf{Q}_p$ essentially enlarges the horizon and the intuition of mathematicians. For any definition, theorem, formula one can ask: what is its p-adic analogue? Sometimes the very possibility of such question can help better understand the situation.

Here I stop the excursus into p-adic analysis and address the interested readers to [14, 7, 22] (see also some exercises in [11, 12]).

Answers and hints to the problems.

8. Follows from the inequality $||a_1 + a_2 + \cdots + a_n||_p \le \max_i ||a_i||_p$.

9. Start from the case $p = 2$.

10. a) (0); b) (4); c) (3)4.

11. Recall the proof of the analogous property of decimal fractions.

12. If $r = (A)B$ where the fragments A and B have the same length, then $r > 0$ iff $A > B$ in the usual sense.

13. Express the indicator function of a given ball using the p-adic signum.

14. Follows from the definition of convergence in $\mathbf{Q}_p$

15. Use the multiplicativity of the norm and check the statement for prime numbers and for -1.

16. Let $\mathbf{A}_0$ denote the open[5] subgroup in $\mathbf{A}$ consisting of those a for which $a \in \mathbf{O}_p$ for all p. Show that

$$\mathbf{A} = \mathbf{A}_0 + \mathbb{Q} \quad \text{and} \quad \mathbf{A} \bigcap \mathbb{Q} = \mathbb{Z}.$$

17. Show, using the function sgn_p and $\exp_p$, that for $p = 4k - 1$ the multiplicative group $\mathbf{Q}_p^\times$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_{4k-2} \times \mathbf{O}_p$.

18. Answers: $\tau\big(SO(3, \mathbb{R})\big) = 2, \quad \tau\big(SU(2, \mathbb{C})\big) = 1.$

[5] Actually, the fact that $\mathbf{A}_0$ is open in $\mathbf{A}$ defines the topology on $\mathbf{A}$.

1.3 From $\mathbb{Q}$ to $\mathbb{R}$: the idea of order; non-standaed analysis

> Look at first puddle and there
> you'll find a sod which surpasses
> and blacks out all other sods.
>
> Saltykov-Shchedrin, "A story of a town"

There is one more way to pass from rational numbers to reals. This way does not use the notion of a distance, but instead is based on the natural order in $\mathbb{Q}$. We define a real number as a section c in the set $\mathbb{Q}$, that is a partition of $\mathbb{Q}$ into two parts A and B so that every element of A is less than any element of B. If the set A has maximal element $a_{\max}$ or the set B has a minimal element $b_{\min}$, we identify c with one of them. Actually, $a_{\max}$ and $b_{\min}$ can not exist simultaneously for a given c. Indeed, otherwise the number $\frac{a_{\max}+b_{\min}}{2}$ does not belong neither A nor B.

If A has no maximum and B has no minimum, then the section c defines a new number which does not belong to $\mathbb{Q}$. By definition, we consider c as bigger than any $a \in A$ but smaller than any $b \in B$.

For the sections one can define all arithmetic operations and check that the set of all sections forms a field. This field is, by definition, the field $\mathbb{R}$ of real numbers.

However, there is here something to think about. Can we go further and consider sections in $\mathbb{R}$ as elements of a still bigger field? For example, can we introduce an infinitesimal number ε which is positive, but smaller than any fraction $\frac{1}{n}$?

Formally, it contradicts to the well-known theorem about least upper bound which claims that for any section c in $\mathbb{R}$ there exists either $a_{\max}$ or $b_{\min}$. If we analyse the proof of this theorem[6], we find out that it is based on the axiom of Archimedes which claims that for any positive real numbers M, ε, there exist a natural number N such that $N\varepsilon > M$.

But if we agree to sacrifice the axiom of Archimedes, we can indeed construct many "non-archimedean" fields strictly containing $\mathbb{R}$. Till some time these fields were considered as funny examples and the analysis in these fields as a crazy theory without applications. But in 1966 A. Robinson and A.P. Bernstein, using non-standard analysis, have solved a difficult problem

[6]Sometimes, the existence of a least upper bound is taken as an axiom; then the Achimedean property below becomes a theorem.

of functional analysis: existence of a non-trivial invariant subspace for a polynomially compact operator in Hilbert space.

This solution soon was translated to the ordinary mathematical language by P.Halmos and a more general result was obtained by V.I.Lomonosov. But now nobody can say that the non-standard analysis has no applications. There are many popular introductions to the non-standard analysis - see [22] and the bibliography there.

Here I describe only one original approach to the construction of a non-archimedean extension of a real field. This approach was invented by John Horton Conway, a famous Princeton mathematician. It requires as little of prerequisit, that a fiction book [23] and an article [13] in a journal "Quant" for school students were written based on this approach. Conway himself calls his numbers *surreal* and we shall call them Conway numbers, or C-numbers.

First of all about notations. In arithmetics of C-numbers only two digits are used: $\uparrow$, or "up" and $\downarrow$, or "down".

By definition, C-number is any completely ordered word in the alphabet $\uparrow, \downarrow$.[7] The cardinality of a word can be arbitrary, but already countable words form a very big field containing all real numbers and many non-standard ones. We shall see soon that the empty word plays the role of zero, so we denote it by 0.

There are two order relations on the set of C-numbers. First uses terms bigger and smaller, denoted by $>$ and $<$. It is defined lexicographically: we compare two numbers a and b digit par digit. If all digits coincide, $a = b$, if the first non-equal digit in a is bigger than in b, then $a > b$. As for digits, we agree that $\uparrow > 0 > \downarrow$.

For the second relation Coway uses the terms earlier or later and symbols $\leftarrow$ and $\rightarrow$. By definition, $a \leftarrow b$ if a is an initial subword of b.

To define arithmetical operations we need the

Theorem 6 (Basic Lemma) *Let A and B be two sets of C-numbers such that $a < b$ for any $a \in A$, $b \in B$. Then*

a) There exist C-numbers c which separate A and B, i.e. $a < c < b$ for all $a \in A$, $b \in B$.

b) Among all C-numbers c, separating A and B there exists a unique earliest number, denoted by $[A : B]$.

Conway defines all the arithmetic operations, following two principles: succession and simplicity. The first principle means that an arithmetic op-

[7] Recall that a completely ordered set is an ordered set in which any non-empty subset has a minimal element.

eration, e.g. addition is defined not at once for all C-numbers at once, but , starting with earlier numbers. According to the second principle, the result must be the simplest possible, i.e. the earliest number which does not contradicts to the results already known.

Example. Let us find the sum $0+0$. Since 0 is the earliest number, there are no results already known. So, we can choose the answer among all C-numbers. The earliest possibility is 0. Thus, $0+0=0$.

Certainly, this example is curious, but for a reader got accustomed to rigorous definition of analysis it could seem a bit lightheaded. Let us give the definition of addition for a general case. For this we introduce some notations.

We call *upper slice* of a C-number x the set of all C-numbers which are bigger and earlier than x. Let us denote this set by $x\rceil$. Analogously, we define a *lower slice* of x as the set $x\rfloor$ of all C-numbers which are less and earlier than x.

E.g., if $x=\uparrow\downarrow\uparrow\uparrow$, then

$$x\rceil=\{\uparrow\}\qquad x\rfloor=\{\uparrow\downarrow\uparrow,\uparrow\downarrow,0\}.$$

And if $x=\uparrow$, then $x\rceil=\emptyset,\quad x\rfloor=\{0\}$.

Now we define the sum of two C-numbers by the formula

$$x+y=\left[\Big((x\rfloor+y)\cup(x+y\rfloor)\Big):\Big((x\rceil+y)\cup(x+y\rceil)\Big)\right]. \tag{1.41}$$

The formula (1.41) defines $x+y$ under condition that we already know the sums of all earlier summands (succession principle) and makes it in a simplest way (simplicity principle) - see the Basic Lemma.

Exercise 19 *Let $\uparrow^n$ and $\downarrow^n$ denote C-numbers written by n symbols $\uparrow$ or $\downarrow$. Prove the equalities*

$$a)\ \uparrow^m+\uparrow^n=\uparrow^{m+n};\qquad b)\ \downarrow^m+\downarrow^n=\downarrow^{m+n};$$
$$\uparrow^m+\downarrow^n=\begin{cases}\uparrow^{m-n} & if\quad m>n\\ 0 \quad if & m=n\\ \downarrow^{n-m} & if\quad m<n.\end{cases} \tag{1.42}$$

From the exercise we see, that the set of C-numbers contains a subgroup isomorphic to the group $\mathbb{Z}$.

Exercise 20 *Prove that $\uparrow\downarrow+\uparrow\downarrow=\uparrow$.*

Hint: $\uparrow\downarrow\rceil = \{\uparrow\}, \quad \uparrow\downarrow\rfloor = \{0\}, \quad \uparrow + \uparrow\downarrow = \uparrow\uparrow\downarrow$.

So, the C-number plays the role of one half of the number $\uparrow$. Further, you can check that $\uparrow\downarrow\downarrow$ plays the role of one quarter of $\uparrow$, $\uparrow\downarrow\downarrow\downarrow$ is one eight of $\uparrow$ etc.

After these simple example one can guess, that all finite C-numbers form a group isomorphic to the group $\mathbb{Z}[\frac{1}{2}]$ of all dyadic fractions. Moreover, the writing of a dyadic fraction $r = \frac{k}{2^n}$ as a C-number is nothing but "record" of searching this number in the following sense. We start from $0 \in \mathbb{R}$ (it is convenient to imaging the real line disposed vertically, so that numbers increase from below upwards.) and are moving to our number r by steps of size 1. Each step is marked in the record by the symbol $\uparrow$ or $\downarrow$ depending on the direction of a move. We continue this way until we reach r (if it is integer) or overstep it. In the last case we keep going in the direction of r, but each next step is twice shorter than the previous one. As before, every step is marked in the record by $\uparrow$ or $\downarrow$ depending on the direction of a move. E.g., for a number $r = 2\frac{3}{16}$ the record of our search is described by the writing down $r = 3 - \frac{1}{2} - \frac{1}{4} - \frac{1}{8} + \frac{1}{16}$ and leads to the C-number $\uparrow\uparrow\uparrow\downarrow\downarrow\downarrow\uparrow$.

The same method can be applied to all real numbers and produce their writing down as infinite C-numbers.

Exercise 21 *Show that rational but not dyadic rational numbers correspond to eventually periodic C-numbers (i.e. periodic, stating with some place).*

For writing down periodic C-numbers it is convenient to use the symbol $\overbrace{\ \ }$ to denote a period. For example, the expression $\uparrow \overbrace{\uparrow\downarrow}$ denotes the C-number $\uparrow\uparrow\downarrow\uparrow\downarrow\uparrow\downarrow$ ..., corresponding to a real number $\frac{5}{3}$.

All C-numbers occuring until now were just fancy written real numbers. This new way of writing down, though rather transparent, is much less convenient than the ordinary decimal or dyadic system. The advatage of it can be seen when we pass to non-standard numbers which are written down as easy as the standard (real) numbers.

Consider, for example, the C-numbers $\omega = \overbrace{\uparrow}$ and $\varepsilon = \overbrace{\downarrow}$.

Exercise 22 *Prove that $\omega > n$ and $0 < \varepsilon < \frac{1}{n}$ for any $n \in \mathbb{N}$.*

So, ω is "infinitely big" and ε is "infinitely small" number. Moreover, after we define a product of two positive C-numbers by the formula

$$x \cdot y = \Big[\Big((x\rfloor \cdot y) \cup (x \cdot y\rfloor)\Big) : \Big((x\rceil \cdot y) \cup (x \cdot y\rceil)\Big)\Big], \tag{1.43}$$

we can check that $\omega \cdot \varepsilon = \uparrow$. Unfotunately, this check is rather long and tedious, since we have to know the products of all earlier numbers. But it is very instructive to those who wants to feel free with C-numbers.

It is time now to recall that in the definition of C-numbers the notion of a complete order is used. The remakable fact is that all finite sets with given cardinality admit essentially unique complete order. Namely, any two such sets are isomorphic objects in the category COS of completely ordered sets.

Still more remarkable fact is that the countable completely ordered sets form infinite (and even uncountable) equivalence classes. You can find more details in textbooks in set theory (see also some exercises in [11, 12]).

Observe that all C-numbers occuring until now belong to the class of $\mathbb{N}$. Here is an example of other type: the number $\overbrace{\uparrow}\uparrow$. It could seem that it is the same word as $\omega = \overbrace{\uparrow}$, but these words are ordered differently: the first has a maximal element, while the first has not.

Exercise 23 *Prove the equalities:*

$$a) \overbrace{\uparrow}\uparrow^n = \omega + n, \quad b) \overbrace{\overbrace{\uparrow}} = \omega^2.$$

Here I finish my introduction to non-standard analysis. The interested readers can make experiments with C-numbers or try to read more serious articles (see, e.g. [4].

Answers and hints.

1. Straightforward check by induction.

3. Compare the deduction of the formula for the some of the infinite decreasing geometric progression.

5. a) Use induction. b) Use the formula (1.43).

1.4 From $\mathbb{R}$ to $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$: Clifford algebras, Dirac equations and the projective plane over the field $\mathbb{F}_2$

> Most of ignorant people
> understand by the occultism the
> table-turning. It is not so.
>
> Arkadij Averchenko.
> "Occult sciences".

1.4.1 Complex numbers

The role of complex numbers in mathematics is really outstanding. First, it is a simplest (and the only one, known to students) example of *algebraically closed field*. It means that any polynomial with complex coefficients has a complex root, hence, decomposes into linear factors.[8]

Second, the complex analysis, i.e. the the theory of complex-valued functions of one or several complex variables, is a natural way to study analytic functions of real variables. Many "purely real" facts about analytic functions can be understood only by studying their extensions into complex domain. For example, why the Taylor series for $\sin x$ and $\cos x$ are coverging everywhere on $\mathbb{R}$, while the Taylor series of $\frac{1}{x^2+1}$ and $\arctan x$ are coverging only for $|x| < 1$? Or, why the antiderivative of $(1-x^2)^\alpha$ can be found explicitly for $\alpha = \frac{1}{2}$, but can not for $\alpha = \frac{1}{3}$, $\frac{1}{4}$ etc?

Finally, the transition from real to complex numbers admits generalizations, one of which is the theory of *Clifford algebras*.

We assume that complex numbers are known well enough and will speak here about further generalizations.

1.4.2 Quaternions

The inventor of quaternions, the famous irish mathematician Sir William Rowan Hamilton has spent many years in attempt to find multiplication law for 3-vectors which would generalize the multiplication of complex numbers (2-vectors). We know now that it is impossible. Only when Hamilton dared to pass to 4-vectors, he found the solution. You can read about this in [22]. These new numbers have been named *quaternions*. They form a 4-dimensional vector space $\mathbb{H}$ over reals with one real unit 1 and three imaginary units $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, satisfying the relations

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1. \tag{1.44}$$

The legend is that these very relations were carved by Hamilton into the side of the Broom Bridge on the Royal Canal in Dublin on October 16 of

[8] Unfortunately, the algebraic closures of other fields are more complicated. For example, the algebraic closure of $\mathbb{Q}_p$ is not complete with respect to natural extension of p-adic norm. The corresponding completion $\mathbb{C}_p$ is described in [14]. This field is more and more used in modern number theory, but its role is still incomparable with the role of complex numbers.

The algebraic closure of a finite field $\mathbb{F}_p$ has rather simple structure: it is a union of finite fields $\mathbb{F}_q$, $q = p^n$ (see the description in chapter 2). However, this field has no natural topology except discrete one.

1843.

But the algebraic structure of $\mathbb{H}$ is better reflected by another system of equations, which is almost equivqlent to (1.44)

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \qquad \mathbf{ij} + \mathbf{ji} = \mathbf{jk} + \mathbf{kj} = \mathbf{ki} + \mathbf{ik} = 0. \tag{1.45}$$

Exercise 24 *Show that* (1.45) *implies that* $\mathbf{ijk} = \pm 1$. *So, the algebras, generated by* $\mathbf{i}, \mathbf{j}, \mathbf{k}$, *satisfying* (1.45) *and* $\mathbf{i}', \mathbf{j}', \mathbf{k}'$, *satisfying* (1.44) *are isomorphic and the isomorphism is given by*

$$\mathbf{i} \mapsto \mathbf{i}', \quad \mathbf{j} \mapsto \mathbf{j}', \quad \mathbf{k} \mapsto \pm\mathbf{k}'.$$

The system (1.44) in its turn is equivalent to

$$(a\mathbf{i} + b\mathbf{j} + c\mathbf{k})^2 = -(a^2 + b^2 + c^2) \quad \text{for all} \quad a, b, c \in \mathbb{R}. \tag{1.46}$$

Hamilton himself wrote a quaternion in the form $\mathbf{q} = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ and call $x_0 \in \mathbb{R}$ the *scalar part* of $\mathbf{q}$ and $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$ the *vector part* of $\mathbf{q}$.

The product of two quaternions is defined as follows. The scalar parts are multiplied as ordinary real numbers. The product of a scalar and a vector is also the ordinary product of a real vector by a real number. As for the product of two vectors, it has the form

$$\mathbf{x}\,\mathbf{y} = \mathbf{x} \cdot \mathbf{y} + \mathbf{x} \times \mathbf{y}. \tag{1.47}$$

Here the first summand is the so-called *scalar* or *dot* product:

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + x_3y_3$$

and the second summand is a *vector* product:

$$\mathbf{x} \times \mathbf{y} = \det \begin{Vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ i & j & k \end{Vmatrix}.$$

These two operations are now used far beyond the quaternion theory. The scalar (or dot) product is an essential part in the definition of Euclidean and Hilbert spaces (see chapter 2). The vector product is the first example of a *Lie algebra commutator* (see the definition in section 1).

It is convenient to realize the elements $\mathbf{q} \in \mathbb{H}$ by 2×2 complex matrices of a special form:

$$\mathbf{q} = x_0 + \mathbf{x} = x_0 + x_1i + x_2j + x_3k \longleftrightarrow \begin{pmatrix} x_0 + ix_1 & x_2 + ix_3 \\ -x_2 + ix_3 & x_0 - ix_1 \end{pmatrix}$$

This correspondence observed all arithmetical operations. Note also that the subfield $\mathbb{C} \subset \mathbb{H}$ is realized by matrices of the form $\begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$.

1.4.3 Clifford algebras

The identity (1.46) suggests the general definition of a *Clifford algebra* $\mathrm{Cl}(V, Q)$, related to a vector space V over a field K and a quadratic form Q on V.[9] By definition, $\mathrm{Cl}(V, Q)$ is the algebra, generated over K by the unit 1 and the space V with defining relations

$$v^2 = Q(v) \cdot 1 \quad \text{for any} \quad v \in V. \tag{1.48}$$

Exercise 25 *Show that the algebras $\mathbb{C}$ and $\mathbb{H}$ are the clifford algebras respectively for $K = V = \mathbb{R}$, $Q(x) = -x^2$ and $K = \mathbb{R}$, $V = \mathbb{R}^2$, $Q(x, y) = -x^2 - y^2$.*

Exercise 26 *Let $K = \mathbb{C}$, $V = \mathbb{C}^n$, Q is any non-degenerate quadratic form on V (all such form are equivalent). Show that*

$$\mathrm{Cl}(V, Q) \simeq \begin{cases} \mathrm{Mat}_{2^k}(\mathbb{C}) & \textit{for} \quad n = 2k, \\ \mathrm{Mat}_{2^k}(\mathbb{C}) \oplus \mathrm{Mat}_{2^k}(\mathbb{C}) & \textit{for} \quad n = 2k+1. \end{cases} \tag{1.49}$$

The Clifford algebras over $\mathbb{R}$ are more diverse. I am giving here the table of algebras $C_{p,q} = \mathrm{Cl}(\mathbb{R}^{p+q}, Q_{p,q}$ where $Q_{p,q}$ is the quadratic form of the type

$$Q_{p,q}(x_1, \dots, x_{p+q}) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2.$$

$q \diagdown p$	0	1	2	3	4	5	6	7
0	$\mathbb{R}$	$2\mathbb{R}$	$\mathbb{R}(2)$	$\mathbb{C}(2)$	$\mathbb{H}(2)$	$2\mathbb{H}(2)$	$\mathbb{H}(4)$	$\mathbb{C}(8)$
1	$\mathbb{C}$	$\mathbb{R}(2)$	$2\mathbb{R}(2)$	$\mathbb{R}(4)$	$\mathbb{C}(4)$	$\mathbb{H}(4)$	$2\mathbb{H}(4)$	$\mathbb{H}(8)$
2	$\mathbb{H}$	$\mathbb{C}(2)$	$\mathbb{R}(4)$	$2\mathbb{R}(4)$	$\mathbb{R}(8)$	$\mathbb{C}(8)$	$\mathbb{H}(8)$	$2\mathbb{H}(8)$
3	$2\mathbb{H}$	$\mathbb{H}(2)$	$\mathbb{C}(4)$	$\mathbb{R}(8)$	$2\mathbb{R}(8)$	$\mathbb{R}(16)$	$\mathbb{C}(16)$	$\mathbb{H}(16)$
4	$\mathbb{H}(2)$	$2\mathbb{H}(2)$	$\mathbb{H}(4)$	$\mathbb{C}(8)$	$\mathbb{R}(16)$	$2\mathbb{R}(16)$	$\mathbb{R}(32)$	$\mathbb{C}(32)$
5	$\mathbb{C}(4)$	$\mathbb{H}(4)$	$2\mathbb{H}(4)$	$\mathbb{H}(8)$	$\mathbb{C}(16)$	$\mathbb{R}(32)$	$2\mathbb{R}(32)$	$\mathbb{R}(64)$
6	$\mathbb{R}(8)$	$\mathbb{C}(8)$	$\mathbb{H}(8)$	$2\mathbb{H}(8)$	$\mathbb{H}(16)$	$\mathbb{C}(32)$	$\mathbb{R}(64)$	$2\mathbb{R}(64)$
7	$2\mathbb{R}(8)$	$\mathbb{R}(16)$	$\mathbb{C}(16)$	$\mathbb{H}(16)$	$2\mathbb{H}(16)$	$\mathbb{H}(32)$	$\mathbb{C}(64)$	$\mathbb{R}(128)$
8	$\mathbb{R}(16)$	$2\mathbb{R}(16)$	$\mathbb{R}(32)$	$\mathbb{C}(32)$	$\mathbb{H}(32)$	$2\mathbb{H}(32)$	$\mathbb{H}(64)$	$\mathbb{C}(128)$

In this table we use the short notation $K(n)$ for the algebra $\mathrm{Mat}_n(K)$ and $2K(n)$ for the algebra $\mathrm{Mat}_n(K) \oplus \mathrm{Mat}_n(K)$

[9] Recall that a quadratic form is a map $Q : V \to K$ given by the formula $Q(v) = B(v, v)$ where $B : V \times V \to K$ is a symmetric bilinear map. Actually, B can be restored from Q by the formula $B(v_1, v_2) = \frac{1}{2}\Big(Q(v_1 + v_2) - Q(v_1) - Q(v_2)\Big)$.

The proof of these relations and also the role of Clifford algebras in topology are given in [5] (see also [11] and exercises in chapter 1).

Until now we considered only the Clifford algebras related to non-degenerate quadratic forms. The opposite case of a zero quadratic form is also of interest. This algebra is called *exterior* or *Grassmann* algebra. We shall speak about it in chapter 2.

One of Clifford algebras was used after three quarters of a century since its discovery by the great british physicist P.A.M. Dirac in the quantum electrodynamics. The idea of Dirac was very simple but rather crazy. He wanted to replace the wave equation[10]

$$\Box f := \left(\partial_t^2 - \partial_x^2 + \partial_y^2 + \partial_z^2\right) f = 0 \tag{1.50}$$

by some equivalent equation of the first order in time. For this Dirac assumed that the operator (1.50) is a square of some operator of the first order:

$$\Box = \left(\gamma_0\partial_t + \gamma_1\partial_x + \gamma_2\partial_y + \gamma_3\partial_z\right)^2. \tag{1.51}$$

Of course, this equality is impossible if coefficients γ_i are the ordinary numbers. "Too bad for ordinary numbers" – said Dirac and defined a new sort of numbers which he needed. Namely, suppose that

$$\gamma_0^2 = -\gamma_1^2 = -\gamma_2^2 = -\gamma_3^2 = 1 \quad \text{and} \quad \gamma_i\gamma_j + \gamma_j\gamma_i = 0 \quad \text{for} \quad i \neq j. \tag{1.52}$$

Then (1.51) will be satisfied. Of course, our reader recognizes in (1.52) the definition of a real Clifford algebra $\mathbb{C}_{1,3} \simeq \mathrm{Mat}_2(\mathbb{H})$. So, the new Dirac numbers are just 2×2 quaternionic matrices, or, 4×4 complex matrices of special kind.

Note, that the algebra, generated by $i\gamma^k$, $k = 0, 1, 2, 3,$ is isomorphic to the Clifford algebra $C_{3,1} \simeq \mathrm{Mat}_4(\mathbb{R})$. Therefore, the 4×4 matrices γ_k can be chosen pure imaginary.

The famous Dirac equation which describes the elementary particles of Fermi type (electrons, muons, neutrinos) has the form

$$i\eth\theta := i\left(\gamma_0\partial_t + \gamma_1\partial_x + \gamma_2\partial_y + \gamma_3\partial_z\right)\theta = m\theta \tag{1.53}$$

where m is a real number (the mass of the particle) and θ is a real 4-vector (so-called *Majorana spinor*.

[10] The symbol := or =: tells that the equation in question is the definition of the part to which the colon is directed. In our case it is the definition of the symbol $\Box$.

1.4.4 Octonions, or Cayley numbers

Among real Clifford algebras exactly three are fields, or skew-fields: $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. The Frobenius theorem claims that there are no other associative finite-dimensional division algebras over $\mathbb{R}$. However, if we drop the associativity restriction, a curious exemple of a division algebra can be constructed.

It is an algebra $\mathbb{O}$ of so-called *Cayley numbers*, or *octonions*. As a real vector space it is spanned by the ordinary unit 1 and by seven imaginary units e_k, $1 \le k \le 7$ with defining relations:

$$e_k^2 = -1,\ 1 \le k \le 7; \qquad e_i e_j = \pm e_{k(i,j)} \tag{1.54}$$

where the choice of signs and the function k are defined by the table.

0	1	2	3	4	5	6	7
1	−0	3	−2	5	−4	7	−6
2	−3	−0	1	6	−7	−4	5
3	2	−1	−0	7	6	−5	−4
4	−5	−6	−7	−0	1	2	3
5	4	−7	6	−1	−0	3	−2
6	7	4	−5	−2	−3	−0	1
7	−6	5	4	−3	2	−1	−0

If on the intersection of i-th row and j-th column we see the number $\pm k$, it means that $e_i \cdot e_j = \pm e_k$.

This table has remarkable properties (which allow to recover it essentially uniquely):

1. In each row and in each column all digits from 0 to 7 occur.
2. In each row and in each column there are 4 signs + and 4 signs −.
3. In each fragment of the type $\begin{matrix} \pm a & \pm b \\ \pm b & \pm a \end{matrix}$ the number of + and − are odd (i.e. there are 3 + and 1 − or 1 + and 3 −).

We dicuss below the geometric interpretation of the table and now give another realization of $\mathbb{O}$. An element $X \in \mathbb{O}$ is written as a pair of quaternions $(\mathbf{q}, \mathbf{r})$; the addition is defined componentwise and multiplication is given by the formula

$$(\mathbf{q}_1, \mathbf{r}_1) \cdot (\mathbf{q}_2, \mathbf{r}_2) = (\mathbf{q}_1 \cdot \mathbf{q}_2 - \bar{\mathbf{r}}_2 \cdot \mathbf{r}_1,\ \mathbf{r}_2 \cdot \mathbf{q}_1 + \mathbf{r}_1 \cdot \bar{\mathbf{q}}_2). \tag{1.55}$$

Here the bar denotes the quaternionic conjugation: $\overline{(x_0, \mathbf{x})} = (x_0, -\mathbf{x})$.

The distribution of signs and indices in (1.54) is related with a beautiful geometric configuration: the projective plane over the field $\mathbb{F}_2$ of two

elements. We recall that the projective plane over a field K is a collection $\mathbb{P}^2(K)$ of all 1-dimensional subspaces (lines) in a 3-dimensional vector space over K. Usually, a point in $\mathbb{P}^2(K)$ is given by 3 homogeneous coordinates $(x_0 : x_1 : x_2)$. These coordinates can not vanish simultaneously and are defined up to common factor. In our case the only invertible element of K is 1; so, the homogeneous coordinates are defined uniquely. So, $\mathbb{P}^2(\mathbb{F}_2)$ is identified with $\mathbb{F}_2^3 \backslash \{origin\}$ and consists of seven points. A *projective line* on $\mathbb{P}^2(\mathbb{F}_2)$ is a subset, defined by a linear equation

$$a_0x_0 + a_1x_1 + a_2x_2 = 0.$$

The coefficients $(a_0 : a_1 : a_2)$ in this equation can be considered as homogeneous coordinates of a point a in the dual projective plane $\mathbb{P}^2(\mathbb{F}_2)^*$. So, we have 7 lines and 7 points in $\mathbb{P}^2(\mathbb{F}_2)$. It is easy to understand that every line contains 3 points and every point belongs to 3 lines. The multiplication table in $\mathbb{O}$ is related to the geometry of $\mathbb{P}^2(\mathbb{F}_2)$ in the following sense: we can enumerate the points on the projective plane in such a way, that $e_i \cdot e_j = \pm e_K$ iff the points p_i, p_j and p_k belong to the same line.

As for the sign in (1.54), it can be defined by the orientation of lines. Here by orientation we understand the cyclic order on a line, i.e. a numeration of the points up to cyclis permutation. The sign rule have the form: $e_i \cdot e_j = e_k$ if the points p_i, p_j, p_k define the orientation of the line in question.

In conclusion, I propose to readers the following subject to think about. The projective plane contains projective subspaces of smaller dimensions: lines and points. Let us consider the subalgebra of $\mathbb{O}$ generated by units, corresponding to a given projective subspace.

a) Show that this subalgebra is isomorphic to $\mathbb{C}$ for points and to $\mathbb{H}$ for lines.

b) Which algebras (if any) correspond to projective spaces of bigger dimensions?

Exercise 27 *How many points, lines, planes etc are in the n-dimensional space over the finite field $\mathbb{F}_q$ with $q = p^l$ elements?*

Hint. Introduce the notation $\left[\begin{array}{c} n \\ k \end{array} \right]_q := \frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q^k-1)\cdots(q-1)(q^{n-k}-1)\cdots(q-1)}$.

Answer: there are $\left[\begin{array}{c} n \\ k \end{array} \right]_q$ k-dimensional subspaces.

Chapter 2

The other variants of numbers

Bibliography

[1] Atiyah M. *Lectures on K-theory*

[2] Berezin F.A. *Method of second quantization*

[3] Bratelli O., Robinson D.W. *Operator algebras and quantum statistic mechanics* vol. 46 No 11 1999, 1999-1208

[4] Cartier P.

[5] Husemoller D. *Fibre bundles*, Springer-Verlag, 1994.

[6] Grothendieck A.

[7] Gelfand I.M., Graev M.I., Pyatetskij-Shapiro I.I. *Representation theory and automorphic functions* (Generalized functions, VI), "Nauka", Moscow, 1966

[8] Gelfand I.M., Kirillov A.A. *The structure of the field related to a split semisimple Lie algebra*, Funct. Analysis and App. vol. 3, No 1,(1969), 7-26.

[9] Gelfand S.I., Manin Yu.I. *Methods of homological algebra 1: Introduction to cohomology theory and derived categories*, "Nauka", Moscow, 1988.

[10] Dixmier J. *On the Weyl algebras*

[11] Kirillov A.A. *Elements of representation theory*, "Nauka", Moscow, 1972, 1978 (English transl. Springer, 1976.)

[12] Kirillov A.A., Gvishiani A.D. *Theorems and problems in Functional analysis*, "Nauka", Moscow, 1979, 1988 (English transl. Springer, 197?.)

[13] Kirillov A.A., Klumova I.N., Sossinski A.B. *Surreal numbers*, Kvant No , 1979.

[14] Koblitz N. *p-adic numbers, p-adic analysis and dzeta-function*

[15] Leites D.A. *Introduction to supermanifolds*, Soviet Math. Uspekhi, vol. 35 (1980), 3-57

[16] Lesmoir-Gordon N.,Rood W. and Edney R. *Fractal Geometry*, Icon Books, UK, Totem books, USA, 2000.

[17] Mac Lane S. *Categories for working mathematician*, Graduate Texts in Math., Vol.5, Springer, New York, 1971.

[18] Mandelbrot B. *The fractal geometry of Nature*, Freeman, San Francisco, 1982.

[19] Manin Yu.I. *Gauge fields and complex geometry*, "Nauka", Moscow, 1984. (English transl.).

[20] Reshetikhin N.Yu., Tahtadjan L.A., Faddeev L.D. *Quantization of Lie groups and Lie algebras*, Algebra and Analysis vol. ? No ? (1989), 178-206.

[21] *Encyclopaedia of Mathematical Sciences, vol I-V*, "VINITY", Moscow, 19??-2007, English translation: Springer,

[22] Wikipedia: http://en.wikipedia.org/wiki/Portal:Mathematics

[23] Knuth, D.E. Surreal Numbers, Addison-Wesley Publishing Company: Reading, Massachusetts. 1974.

[24] Vladimirov V.S., Volovich I.V. *Introduction to superanalysis*, Teor. i Math. Physics, vol. 59, No 1, vol. 60, No 2 (1984), pages 3-27, 169-198

[25] Weil A. *Basic number theory*,