WOMEN IN MATHEMATICS:
Scaling the Heights

Deborah Nolan, Editor
University of California, Berkeley

What are Numbers?

Svetlana Katok

Pennsylvania State University

The goal of this seminar was to reveal the concept of *number* in modern mathematics. The title was inspired by Kirillov's book (1993). My original idea was to use it as the main source for the seminar, but unfortunately, it is too sophisticated for the students, and I ended up using only his general philosophy of consequent extensions of the notion of number, which appears in the beginning of this article. The material is presented in a series of problems with a skeletal framework that provides a context for them. In the seminar, students solved these problems and worked on projects, individually or in groups. Solutions and hints to some of these problems are included in the Appendix.

Introduction

We start with the following chain:

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

This chain of consequent extensions of the concept of number you probably know well enough, at least up to its fourth and fifth members. Symbols of this chain became standard notation for, respectively, sets of natural, integer, rational, real, complex numbers, quaternions, and Cayley numbers (also known as octaves). We discuss transitions from one term of this chain to the next, and show how the ideas underlying these transitions may lead to different, sometimes very unexpected and beautiful theories.

The material is divided according to the following topics. Some of these topics are covered in the group projects, which are listed prior to the Appendix.

- Arithmetic: from natural numbers to integers, to rational numbers; arithmetic operations, groups, rings, fields.
- Analysis: from rational numbers to reals, a concept of completion, p-adic numbers.
- Rational numbers as an ordered field, a way of obtaining real numbers via cuts.
- More on real numbers, algebraic and transcendental numbers.
- Algebra: from real to complex numbers, algebraically closed fields; commutative, associative, and division algebras.
- The exceptional position of four algebras: real numbers, complex numbers, quaternions, and Cayley numbers—Hurwitz's Theorem.

The majority of problems included here are devoted to the theory of p-adic numbers, which are a remarkable diversion from the above mentioned chain. The material on which they are based can be found in the books by Borevich and Shafarevich (1996), Kirillov and Gvishiani (1982), and Koblitz (1977). The material on division and quaternion algebras can be found Katok (1992). The book by Kantor and Solodovnikov (1989) was the primary source for the last topic.

Arithmetic: from $\mathbb{N}$ to $\mathbb{Z}$ and from $\mathbb{Z}$ to $\mathbb{Q}$; arithmetic operations, groups, rings, fields

Natural numbers can be added but not always subtracted; integers can be multiplied but not always divided. The urge to overcome these "inconveniences" leads to the transitions from $\mathbb{N}$ to $\mathbb{Z}$, and from $\mathbb{Z}$ to $\mathbb{Q}$.

Let us recall how to make those transitions. We want to subtract m from n. If $m \geq n$, then the answer is not in $\mathbb{N}$. We denote it by $n \ominus m$. We want all axioms of addition to hold in the extended set. Hence, we have to *identify* $n \ominus m$ with $(n+k) \ominus (m+k)$ for all $k \in \mathbb{N}$, and also with $(n-k) \ominus (m-k)$ for $1 \leq k < \min(m, n)$.

We see that the symbols $n_1 \ominus m_1$ and $n_2 \ominus m_2$ are identified if $n_1 + m_2 = n_2 + m_1$. Now let us consider all expressions

$$n \ominus m, m, n \in \mathbb{N}$$

with the given identification. We can add them by components

$$(n_1 \ominus m_1) + (n_2 \ominus m_2) = (n_1 + n_2) \ominus (m_1 + m_2),$$

and subtract them by the following rule:

$$(n_1 \ominus m_1) - (n_2 \ominus m_2) = (n_1 + m_2) \ominus (n_2 + m_1).$$

For instance,

$$(0 \ominus 0) - (m \ominus n) = n \ominus m.$$

1. Show that the equivalence classes of symbols

$$\{m \ominus n \mid m, n \in \mathbb{N}, \quad n_1 \ominus m_1 \sim n_2 \ominus m_2 \text{ iff } n_1 + m_2 = n_2 + m_1\}$$

form a group by addition, and that this group is isomorphic to $\mathbb{Z}$.

The procedure is completely analogous for the construction of the multiplicative group $\mathbb{Q}^*$ of non-zero rational numbers starting from a *semigroup* $\mathbb{Z} \setminus \{0\}$.

2. Prove that the equivalence classes of symbols

$$\{m : n \mid m, n \in \mathbb{Z} \setminus \{0\}, \quad m_1 : n_1 \sim m_2 : n_2 \text{ iff } m_1 n_2 = m_2 n_1\}$$

form a group by multiplication, and that this group is isomorphic to $\mathbb{Q}^*$.

In both of these exercises we extended the domain to obtain a group using the same principle. We introduced new symbols (negative numbers, fractions), and formed the *equivalence classes* in such a way that the laws which held in the original domain continued to hold in the extended domain. We shall see *equivalence relations* very often as we go alone.

3. Which of the following relations are equivalence relations?

a) Relation of equality of two numbers;

b) relation of similarity of two triangles;

c) relation of order on the real line;

d) relation of linear dependence in a vector space L of dimension $n > 1$;

e) relation of linear dependence on the let $L* = L \setminus 0$, where L is a vector space.

Analysis: from $\mathbb{Q}$ to $\mathbb{R}$; a concept of completion, p-adic numbers

The real numbers are obtained from rationals by a procedure called *completion*. This procedure can be applied to any *metric space*, i.e., a space M with a distance function d on it. A sequence $\{r_n\} \in M$ is called a *Cauchy sequence* if for any $\epsilon > 0$ there exists $N > 0$ such that $n, m > N$ implies $d(r_n, r_m) < \epsilon$. If any Cauchy sequence in M has a limit in M, then M is called a *complete metric space*. If M is not complete, there exists a metric space $\overline{M}$ such that

1. $\overline{M}$ is complete;
2. $\overline{M}$ contains a subset $\overline{M}_0$ isometric to M;
3. $\overline{M}_0$ is dense in $\overline{M}$ (i.e., each point in $\overline{M}$ is a limit point for $\overline{M}_0$).

The elements of $\overline{M}$ are equivalence classes of Cauchy sequences in M: (two Cauchy sequences x_n and y_n are called equivalent if $d(x_n, y_n) \to 0$).

4. Prove that a metric space is complete if and only if the intersection of every descending sequence of closed balls whose radii approach zero consists of a single point.

Let us apply this construction to the rational numbers. We have the usual Euclidean distance between rational numbers:

$$d(r_1, r_2) = |r_1 - r_2|. \tag{1}$$

The geometric interpretation of rational numbers as points on the "number axis" is obviously connected with this distance. It is easy to construct a Cauchy sequence of rational numbers which has no limit in $\mathbb{Q}$:

$$.1,\ .1011,\ .10110111,\ .1011011101111, \ldots.$$

5. Prove that the rational numbers are represented by eventually periodic decimal fractions.

On the other hand, any point on the "number axis" can be represented by an infinite decimal fraction, and any Cauchy sequence of rational numbers has a limit that is an infinite decimal fraction. In other words, the construction of real numbers through infinite decimal fractions is equivalent to the completion procedure described above. We shall denote the set of real numbers by $\mathbb{R}$.

6. Prove that the following metric spaces are not complete, and construct their completions:

1. $\mathbb{R}$ with the distance $d(x, y) = |arctan\, x - arctan\, y|$;
2. $\mathbb{R}$ with the distance $d(x, y) = |e^x - e^y|$.

7. On the set of closed intervals of the real line we define a distance by the formula:

$$d([a, b], [c, d]) = |a - c| + |b - d|.$$

Prove that the obtained metric space is not complete, and find its completion.

8. On the set $\{\Delta\}$ of closed intervals of the real line we define a distance by the formula:

$$d(\Delta_1, \Delta_2) = |\Delta_1| + |\Delta_2| - 2|\Delta_1 \cap \Delta_2|.$$

Prove that the obtained metric space is not complete, and find its completion.

9. Prove that the space of polynomials with real coefficients $\mathbb{R}[x]$ is not complete with respect to the following distances:

1. $d(P,Q) = \max_{[0,1]} \mid P(x) - Q(x) \mid$;
2. $d(P,Q) = \int_0^1 \mid P(x) - Q(x) \mid dx$;
3. $d(P,Q) = \sum_i |c_i|$, where $P(x) - Q(x) = \sum_i c_i x^i$.

Notice that the Euclidean distance "came from" the Eulcidean norm on $\mathbb{Q}$, which is the absolute value. Suppose we have a norm on a field F, i.e. a map denoted by $\| \ \|$ from F to the non-negative real numbers, such that

1. $\|x\| = 0$ iff $x = 0$,
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$,
3. $\|x + y\| \leq \|x\| + \|y\|$.

Then we can define a distance $d(x,y) = \|x - y\|$. We say that this distance is *induced* by the norm $\| \ \|$. We say that the norm is *trivial* if $\|0\| = 0$ and $\|x\| = 1$ for all $x \neq 0$.

Now let us ask ourselves a question: is the Euclidean distance between rational numbers really the most "natural" one? Is there any other way to describe the "closeness" between them? It turns out that the answer to this question is YES!

Let us fix a prime number p. Then any rational number r can be uniquely written in the form

$$r = p^k \frac{m}{n},$$

where $k \in \mathbb{Z}$, and

$$(m,n) = (m,p) = (n,p) = 1.$$

This number k is denoted by $ord_p r$. If r is an integer, then $ord_p r$ is the greatest k such that $r \equiv 0 \pmod{p^k}$.

Definition.

$$\|r\|_p = \begin{cases} p^{-ord_p r}, & \text{if } r \neq 0 \\ 0 \quad , & \text{if } r = 0. \end{cases}$$

is called the *p-adic norm* of r.

10. Prove the following formulae:

1. $\|r_1 r_2\|_p = \|r_1\|_p \|r_2\|_p$;
2. $\|r_1 + r_2\|_p \leq \max(\|r_1\|_p, \|r_2\|_p)$;
3. if $\|r_1\|_p < \|r_2\|_p$ then $\|r_1 + r_2\|_p = \|r_2\|_p$.

We introduce a new (p-adic) distance on $\mathbb{Q}$ by the formula:

$$d_p(r_1, r_2) = \|r_1 - r_2\|_p. \tag{2}$$

Definitions. A norm satisfying

$$\|r_1 + r_2\|_p \leq \max(\|r_1\|_p, \|r_2\|_p)$$

instead of the triangle inequality is called *non-Archimedian*. A norm which is not non-Archimedian is called *Archimedian*. A distance induced by a (non-) Archimedian norm is called (non-) Archimedian.

We sometimes let $\| \ \|_\infty$ denote the usual absolute value norm on $\mathbb{Q}$.

11. Prove that d_p is the distance function on $\mathbb{Q}$, i.e.

1. d_p is symmetric: $d_p(r_1, r_2) = d_p(r_2, r_1)$,
2. d_p is non-negative: $d_p(r_1, r_2) \geq 0$, and $d_p(r_1, r_2) = 0$ iff $r_1 = r_2$,
3. d_p satisfies the triangle inequality:

$$d_p(r_1, r_3) \leq d_p(r_1, r_2) + d_p(r_2, r_3).$$

It follows from Problem **10** that d_p satisfies a stronger inequality:

$$d_p(r_1, r_3) \leq \max(d_p(r_1, r_2), d_p(r_2, r_3)). \tag{3}$$

Definition. A metric space with a distance satisfying (3) is called an *ultrametric* space.

Thus a field with a non-Archimedian norm is an ultrametric space.

12. Prove that all triangles in an ultrametric space are isosceles, and that the length of the base does not exceed the length of the side.

Let us define a disc of radius r (r is a non-negative real number) with center $a \in M$ (M is a metric space) :

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

13. Prove that if M is an ultrametric space, then any point in D(a,r) is its center.

14. Prove that in any complete normed field, with a non-Archimedian norm, a series $\sum_n x_n$ converges if and only if $x_n \to 0$.

15. Prove that rational integers $\mathbb{Z}$ form a bounded set of diameter 1 with respect to the p-adic distance d_p.

Definitions. We say two metrics d_1 and d_2 are *equivalent* if a sequence is Cauchy with respect to d_1 iff it is Cauchy with respect to d_2. We say two norms are equivalent if they induce equivalent metrics. The symbol $\sim$ is used to represent the equivalence of norms.

16. Let $\| \ \|_1$ and $\| \ \|_2$ be two norms on a field F. Prove that $\| \ \|_1 \sim \| \ \|_2$ iff there exists a positive real number α such that $\|x\|_1 = \|x\|_2^\alpha$ for all $x \in F$.

17. Prove that if $0 < \rho < 1$, then the function on $\mathbb{Q}$

$$\|x\| = \begin{cases} \rho^{ord_p x}, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0, \end{cases}$$

is a non-Archimedian norm. Notice that by Problem **16** it is equivalent to $\| \ \|_p$. (What is α?) What happens if $\rho = 1$, or if $\rho > 1$?

18. Prove that $\| \ \|_{p_1}$ is not equivalent to $\| \ \|_{p_2}$ if p_1 and p_2 are different primes.

19. Let $\| \ \| = | \ |^\alpha$, where α is a fixed positive number. Show that $\| \ \|$ is a norm iff $\alpha \leq 1$, and that in this case it is equivalent to $| \ |$.

20. Prove that two equivalent norms on a field are either both Archimedian or both non-Archimedian.

The field of p-adic numbers

We can apply our completion procedure to $\mathbb{Q}$ with respect to d_p to obtain a complete metric space denoted by $\mathbb{Q}_p$. Its elements are equivalence classes of Cauchy sequences with respect to the following relation: $\{a_i\} \sim \{b_i\}$ if $\|a_i - b_i\|_p \to 0$ as $i \to \infty$.

For any $x \in \mathbb{Q}$, let $\{x\}$ denote the constant Cauchy sequence. We have $\{x\} \sim \{y\}$ iff $x = y$. The equivalence class of $\{0\}$ is denoted by 0.

We define the norm $\| \ \|_p$ of an equivalence class a to be $\lim_{i\to\infty} \|a_i\|_p$, where $\{a_i\}$ is any representative of a.

21. Prove that if $\{a_i\}$ is a Cauchy sequence in $\mathbb{Q}$, then $\lim_{i\to\infty} \|a_i\|_p$ exists.

Remark. In going from $\mathbb{Q}$ to $\mathbb{R}$ the possible values of $\| \ \|_\infty = | \ |$ were enlarged to include all non-negative real numbers, but in going from $\mathbb{Q}$ to $\mathbb{Q}_p$ the possible values of $\| \ \|_p$ remain the same: $\{p^n\}_{n\in N \cup 0}$. This is the reason the p-adic norm is also called the *discrete valuation*.

Ostrowski Theorem. Every non-trivial norm $\| \ \|$ on $\mathbb{Q}$ is equivalent to $\| \ \|_p$ for some prime p or for $p = \infty$. □

Proof. We give a proof as a series of exercises.

I. Suppose there exists a positive integer n such that $\|n\| > 1$, and let n_0 be the least such n. Then we can write $\|n_0\| = n_0^\alpha$ for some positive real number α.

a) Prove that for any $n \in \mathbb{Z}$, $\|n\| = n^\alpha$.

b) Prove that for any $x \in \mathbb{Q}$, $\|x\| = x^\alpha$.

c) Use Problem **19** to conclude that $\| \ \|$ is equivalent to the absolute value $| \ |$.

II. Suppose $\|n\| \leq 1$ for all positive integers n. Let n_0 be the least n such that $\|n\| < 1$.

a) Why does such an n_0 exist?

b) Show that n_0 must be a prime: $n_0 = p$.

c) Prove that if q is a prime, $q \neq p$, then $\|q\| = 1$.

d) Prove that for any positive integer a, $\|a\| = \rho^{ord_p a}$, where $\rho = \|p\| < 1$.

e) Use Problem **17** to conclude that in this case $\| \ \|$ is equivalent to $\| \ \|_p$.

Given two equivalence classes a and b of Cauchy sequences, we define $a \cdot b$ to be the equivalence class of the sequence $\{a_i b_i\}$ where $\{a_i\} \in a$ and $\{b_i\} \in b$. The sum is defined similarly term-by-term.

22. Prove that the definition of the sum and the product of equivalence classes of Cauchy sequences does not depend on the choice of representatives.

The additive inverses are defined in an obvious way. For multiplicative inverses we need the following fact:

23. Prove that any Cauchy sequence is equivalent to one with no zero terms.

Then as a multiplicative inverse for $\{a_i\}$ we can take $\{1/a_i\}$ which is Cauchy unless $\|a_i\|_p \to 0$, i.e. unless $\{a_i\} = \{0\}$. Why?

Thus we obtain a *field* of p-adic numbers $\mathbb{Q}_p$.

Let us consider the following series

$$\frac{b_{-k}}{p^k} + \frac{b_{-k+1}}{p^{k-1}} + \ldots + b_0 + b_1 p + b_2 p^2 + \ldots. \tag{1}$$

By the construction and a general theorem about completions, each series of the form (1) represents an element of $\mathbb{Q}_p$. The converse statement is also true.

Theorem. Every equivalence class a in $\mathbb{Q}_p$ has exactly one representative Cauchy sequence which is a sequence of partial sums of a series in the form (1). □

Proof. First notice that it is sufficient to give a proof in the case $\|a\|_p \leq 1$.

24. Deduce the theorem from the statement for $a \in \mathbb{Q}_p$ with $\|a\|_p \leq 1$.

Now consider our Cauchy sequence $\{a_i\} \in a$, and let $N(j)$ be a natural number such that $\|a_i - a_{i'}\|_p \leq p^{-j}$ whenever $i, i' \geq N(j)$. We have for $i \geq N(1)$,

$$\begin{aligned} \|a_i\|_p &\leq \max(\|a_{i'}\|_p, \|a_i - a_{i'}\|_p) \\ &\leq \max(\|a_{i'}\|_p, 1/p), \end{aligned}$$

for all $i' \geq N(1)$. But $\|a_{i'}\|_p \to \|a\|_p$ as $i' \to \infty$. Hence for $i \geq N(1)$, we have $\|a_i\|_p \leq 1$.

25. If $x \in \mathbb{Q}$ and $\|x\|_p \leq 1$, then for any j there exists an integer n chosen from the set $\{0, 1, \ldots, p^j - 1\}$ such that $\|n - x\|_p \leq p^{-j}$.

Now apply Problem **25** to find a sequence c_j where $0 \leq c_j < p^j$ such that

$$\|c_j - a_{N(j)}\|_p \leq 1/p^j.$$

We want to show that $\{c_j\} \sim \{a_j\}$ and that it is a sequence of partial sums of a series of the form (1). The first assertion follows from the estimate for $i \geq N(j)$,

$$\begin{aligned} \|c_i - a_i\|_p &= \|c_i - c_j + c_j - a_{N(j)} - (a_i - a_{N(j)})\|_p \\ &\leq \max(\|c_i - c_j\|_p, \|c_j - a_{N(j)}\|_p, \\ &\quad \|a_i - a_{N(j)}\|_p) \\ &\leq \max(1/p^j, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

Hence $\|c_i - a_i\|_p \to 0$ as $i \to \infty$. The second assertion follows from the estimate

$$\begin{aligned} \|c_{j+1} - c_j\|_p &= \|c_{i+1} - a_{N(j+1)} + a_{N(j+1)} \\ &\quad - a_{N(j)} - (c_j - a_{N(j)})\|_p \\ &\leq \max(\|c_{i+1} - a_{N(j+1)}\|_p, \\ &\quad \|a_{N(j+1)} - a_{N(j)}\|_p, \|c_j - a_{N(j)}\|_p) \\ &\leq \max(1/p^{j+1}, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

This proves that $c_j \equiv c_{j+1} \pmod{p^j}$, which is exactly equivalent to the claim.

26. Prove the uniqueness result: given $a \in \mathbb{Q}_p$ there is a unique Cauchy sequence $\{c_i\}$ for which

1. $0 \leq c_i < p^i$ for $i = 1, 2, \ldots$.
2. $c_i \equiv c_{i+1} \pmod{p^i}$ for $i = 1, 2, \ldots$.

Thus any element in $\mathbb{Q}_p$ can be represented by an infinite-to-the-left fraction in base p:

$$\ldots b_n \ldots b_2 b_1 b_0 . b_{-1} \ldots b_{-k}, \quad 0 \leq b_i \leq p-1. \tag{2}$$

Arithmetic operations in $\mathbb{Q}_p$

Here are some examples in $\mathbb{Q}_7$:

$$\ldots 263 \times \ldots 154 = \ldots 455$$

$$\ldots 30.2 - \ldots 56.4 = \ldots 40.5$$

$$\ldots 421 : \ldots 153 = \ldots 615.$$

27. Prove that in $\mathbb{Q}_5$ there exists a square root of $-1 (= \ldots 44)$, and find its last three digits. How many such roots are there?

28. Solve the equation $x^2 - 6 = 0$ in $\mathbb{Q}_5$.

29. Solve the equation $x^2 - 7 = 0$ in $\mathbb{Q}_5$.

Let $\mathbb{Z}_p$ be the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, the set of *p-adic integers.*

30. Prove that $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid \|a\|_p \leq 1\}$.

31. Prove that $\mathbb{Z}_p$ is the set of elements in $\mathbb{Q}_p$ of the form (2) in the previous section with $b_i = 0$ for $i < 0$.

The p-adic integers form a subring of $\mathbb{Q}_p$. Let $\mathbb{Z}_p^\times$ be the set of invertible elements in $\mathbb{Z}_p$ (also called *p-adic units*), i.e.

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid 1/x \in \mathbb{Z}_p\}.$$

Then $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid \|x\| = 1\}$.

32. Prove that the p-adic expansion of $a \in \mathbb{Q}_p$ has repeating digits onward from some point (i.e., it is eventually periodic) if and only if $a \in \mathbb{Q}$.

33. Prove that if $x \in \mathbb{Q}$ and $\|x\|_p \leq 1$ for every prime p, then $x \in \mathbb{Z}$.

The method used in the solution of Problem **28** is quite general.

Hensel's Lemma. Let $F(x)$,

$$F(x) = c_0 + c_1 x + \ldots + c_n x^n,$$

be a polynomial whose coefficients are p-adic integers. Let $F'(x)$,

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots + n c_n x^{n-1},$$

be the derivative of F. Let a_0 be a p-adic integer such that $F(a_0) \equiv 0 \pmod{p}$ and $F'(a_0) \neq 0 \pmod{p}$. Then there exists a unique p-adic integer a such that

$$F(a) = 0 \quad \text{and} \quad a \equiv a_0 \pmod{p}.$$

(Note, in the special case of Problem **28**

$$\begin{aligned} F(x) &= x^2 - 6, \\ F'(x) &= 2x, a_0 = 1). \end{aligned}$$

□

34. Explain why $\mathbb{Q}_{10}$ is not a field.

Additional problems on p-adic numbers

35. What is the cardinality of $\mathbb{Z}_p$? Prove your answer.

36. Let us consider a map

$$\varphi : \mathbb{Q}_p \to \mathbb{R},$$

which maps a p-adic number,

$$\ldots b_2 b_1 b_0 . b_{-1} b_{-2} \ldots b_{-k} \to b_{-k} \ldots b_{-2} b_{-1} . b_0 b_1 b_2 \ldots,$$

to a real number in base p. Prove that φ is a continuous map of $\mathbb{Q}_p$ onto $\mathbb{R}_+$, the set of non-negative real numbers, and that it maps $\mathbb{Z}_p$ onto the closed interval $[0, 1]$.

Notice that due to non-uniqueness of writing the real numbers in base p, this map is not 1-to-1.

37. Construct a 1-to-1 continuous map of $\mathbb{Z}_p$ onto a Cantor set such that the inverse map is also continuous.

38. Prove that for any finite p, any sequence of integers has a subsequence which is Cauchy with respect to $\| \ \|_p$.

Is it possible to determine by a p-adic expansion of a rational number whether it is positive or negative? The answer is YES, and it is given in the following problem.

39. Let $r \in \mathbb{Q}$. Prove that its p-adic expansion can be represented in the form $\ldots aaaaaab$, where the fragments a and b have the same number of digits. Prove that $r > 0$ is equivalent to $b > a$ in the usual sense (as integers written in base p).

40. Prove that it is impossible to introduce an *order relation* in $\mathbb{Q}$ such that

1. if $x > 0$ and $y > 0$, then $x + y > 0$;
2. if $x > 0$ and $y > 0$, then $xy > 0$;
3. if $x_n > 0$ and there exists a limit, $\lim_{n\to\infty} x_n = x$, then $x \geq 0$.

More on real numbers: algebraic and transcendental numbers

41. Prove that $\mathbb{Q}(\sqrt[3]{2})$ is a field.

42. Prove that any finite extension of $\mathbb{R}$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.

43. Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ are not isomorphic as fields.

Algebra: from reals to complex numbers, algebraically closed fields; Commutative, associative, and division algebras

Definition. Let F be a field of characteristic $\neq 2$, $a, b \in F^* = F \setminus \{0\}$, and

$$A = (\frac{a, b}{F})$$

be a *quaternion algebra over* F, i.e., an algebra (a vector space and a ring) over F of dimension 4 with a basis $\{1, i, j, k\}$ where

$$i^2 = a, \quad j^2 = b, \quad k = ij = -ji.$$

Hamiltonian quaternions $\mathbb{H}$ correspond to the case $a = b = -1$.

44. Prove that multiplication of quaternions is associative.

45. Prove that if $a \in (F^*)^2$, then $A = (\frac{a,b}{F}) \approx M(2, F)$.

46. Prove that for any $\lambda \in F^*$, $(\frac{a,b}{F}) = (\frac{\lambda^2 a,b}{F})$.

Definition. A quaternion algebra A is called a *division algebra* if each non-zero element of A has an inverse.

47. Prove that A is a division algebra if and only if $N(x) = 0$ only for $x = 0$.

48. Prove that if A,

$$A = (\frac{a, b}{F}),$$

is not isomorphic to $M(2, F)$, then A is a division algebra.

49. Prove that there are only two quaternion algebras over $\mathbb{R}$ up to an isomorphism:

$$A = (\frac{a, b}{\mathbb{R}}) \approx \mathbb{H},$$

if $a < 0, b < 0$, and otherwise

$$A = (\frac{a, b}{\mathbb{R}}) \approx M(2, \mathbb{R}).$$

50. Prove that $\overline{q_1 q_2} = \overline{q_2 q_1}$ and $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$.

Group Projects

- A non-Archimedian extension of the field of real numbers: Conway numbers and non-standard analysis
- Surreal numbers
- Representation of real numbers by continued fractions
- Alternative arithmetic on the numbers $a + bi$: double and dual numbers
- Transcendental numbers
- Quaternions and vector algebra in 3-dimensional real vector space
- From complex numbers to quaternions—the doubling procedure—Cayley numbers
- Proof of Hurwitz's theorem
- Quaternion algebras over $\mathbb{Q}$
- The connection with units in algebraic number fields

APPENDIX: Hints and Solutions to Selected Problems

6. After completion, $(-\frac{\pi}{2}, \frac{\pi}{2})$ becomes $[-\frac{\pi}{2}, \frac{\pi}{2}]$, and $(0, \infty)$ becomes $[0, \infty)$.

7. Let $\Delta_n = [0, \frac{1}{n}]$. Then $\{\Delta_n\}$ is a Cauchy sequence, since given $\varepsilon > 0$, take $N > \frac{2}{\varepsilon}$, then for $m, n > N$,

$$d(\Delta_n, \Delta_m) < \varepsilon.$$

But $\{\Delta_n\}$ cannot converge to any closed interval of positive length. Hence the space is not complete, and we need to add "0-intervals," $a = [a, a]$, to complete it.

8. Any sequence of intervals with lengths converging to 0 is a Cauchy sequence; they all correspond to a single point α in the completion, such that $d(\alpha, \Delta) = |\Delta|$. To prove that this is the only point we have to add, show that for each sequence $\{\Delta_n\}$ for which $|\Delta_n|$ does not approach 0, there is a subsequence such that all intersections $\Delta_i \cap \Delta_j$ are not empty. Then use the fact that for intersecting intervals the distance coincides with the distance from Problem **7**.

9. The sequence $\{P_k\}$, where $P_k = \sum_{i=0}^{k} (\frac{x}{2})^i$, is a non-converging Cauchy sequence for all three distances.

16. Suppose $\| \ \|_1 \sim \| \ \|_2$, and $a \neq 0$ such that $\|a\|_2 \neq 1$ (we assume $\| \ \|$ is non-trivial), say $\|a\|_2 > 1$. Then $\|a\|_1 = \|a\|_2^{\alpha}$ for some α. Show that for all $x \in F$, $\|x\|_1 = \|x\|_2^{\alpha}$.

17. If $\rho = 1$ then you get a trivial norm. If $\rho > 1$, then you do not get a norm at all, since the triangle inequality will not hold.

18. The sequence $\{p_1^n\} \to 0$ in $\| \ \|_1$ but not in $\| \ \|_2$.

19. Prove the triangle inequality.

20. First prove that the norm is non-Archimedian iff $\|n\| \leq 1$ for any integer $n = 1 + \ldots + 1$, n times. Then use the sequence $\{1/n^i\}$.

21. If $a = 0$, then by definition $\lim_{i\to\infty} \|a_i\|_p = 0$. If $a \neq 0$, then there exists an $\varepsilon > 0$ such that for every $N > 0$, there exists an $i_N > N$ with $\|a_{i_N}\|_p > \varepsilon$. If we choose N large enough such that $\|a_i - a_j\|_p < \varepsilon$ for $i, j > N$, we have

$$\|a_i - a_{i_N}\| < \varepsilon \quad \text{for all } i > N.$$

Since $\|a_{i_N}\|_p > \varepsilon$, it follows from Problem **12** that the triangle with vertices $0, a_i, a_{i_N}$ is isoceles. Hence $\|a_i\|_p = \|a_{i_N}\|_p$. Thus, for all $i > N$, $\|a_i\|$ has the constant value $\|a_{i_N}\|$, which is then the $\lim_{i\to\infty} \|a_i\|$.

23. If $a_i = 0$, take $a_i' = p^i$. For a given $\varepsilon > 0$, choose $N > \max(M, \log_{1/p} \varepsilon)$, where M is chosen for a given sequence $\{a_n\}$. If $\{a_n\}$ is not equivalent to $\{0\}$, then we can always choose a subsequence which contains no zero terms.

24. Consider $a' = ap^k$, where $\|a\|_p = p^k$.

25. Let

$$x = \frac{a}{b},$$

written in lowest terms. Since $\|x\|_p \leq 1$, p does not divide b, $\{(b, p^j) = 1\}$. We can find integers s and t such that $sb + tp^j = 1$. Let $n = as$. Then

$$\begin{aligned} \|n - x\|_p &= \|as - (\frac{a}{b})\|_p \\ &= \|\frac{a}{b}\|_p \|sb - 1\|_p \\ &\leq \|sb - 1\|_p \\ &= \|tp^j\|_p \\ &= \|t\|_p / p^j \\ &\leq 1/p^j. \end{aligned}$$

We can add a multiple of p^j to n to get an integer between 0 and p^j for which $\|n - x\|_p \leq p^{-j}$ still holds.

28. Let $x = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \ldots$. Then

$$(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \ldots)^2 = 1 + 1 \cdot 5.$$

Comparing coefficients at 5^0, we get $a_0^2 \equiv 1 \pmod 5$. Hence $a_0 = 1$ or $a_0 = 4$. Let $a_0 = 1$. Comparing the coefficients at 5^1, we get

$$2a_1 \cdot 5 \equiv 1 \cdot 5 \pmod 5.$$

Hence $2a_1 \equiv 1 \pmod 5$, and $a_1 = 3$. Continuing this way, we determine all the a_i uniquely. We obtain $x = \ldots 4031$.

43. First show that any field isomorphism must act as an identity on $\mathbb{Q}$.

References

Borevich, Z. I., and Shafarevich, I. R. (1966). *Number Theory.* Academic Press, New York.

Courant, R., and Robbins, H. (1963). *What is Mathematics?.* Oxford University Press, 12th printing, Oxford.

Kantor, I. L., and Solodovnikov, A. S. (1989). *Hypercomplex Numbers.* Springer-Verlag, New York.

Katok, S. (1992) *Fuchsian groups.* The University of Chicago Press, Chicago.

Kirollov, A. (1993). *Chto Takoe Chislo?.* Sovremennaia Matematika Dlia Studentov, Nauka, Moscow.

Kirillov, A., and Gvishiani, A. (1982) *Theorems and problems in functional analysis.* Springer-Verlag, New York.

Koblitz, N. (1977). *P-adic numbers, P-adic analysis, and Zeta Functions.* Graduate texts in mathematics **58**, Springer-Verlag, New York.