Contents

Transcendence of e and π – Part I

Vojta Luhan

In the first part of our trilogy we will prove that e is transcendental.

1. Introduction

There are many ways to define the number e. We will use the one showing e as a sum of the infinite series:

Definition 1. We define number e as follows:

$$e := \sum_{n=0}^{\infty} \frac{1}{n!}.$$

For a later use, we also define special functions p, q and f and its integrals:

Definition 2. Let parameters $i, k, n \in \mathbb{N}$ are chosen arbitrarily. Then we define functions p, q, f, v_i and w_i as follows:

- $p(x) := x(x-1)(x-2)\cdots(x-n)$,
- $q(x) := (x-1)(x-2)\cdots(x-n)e^{-x}$,
- $f(x) := p(x)^k \cdot q(x) = \sum_{j=k}^{k+nk+n} b_j x^j e^{-x}$ for some $b_j \in \mathbb{Z}$,
- $v_i := \int_0^i f(x)\ \mathrm{dx}$,
- $w_i := \int_i^\infty f(x)\ \mathrm{dx}$.

2. Few Lemmas

In this section we state and prove few Lemmas, which we will always need later, either for proving succeeding Lemmas or The Main Theorem.

Lemma 3 (Lemma J)**.**

$$\int_0^\infty x^j e^{-x}\ dx = j!.$$

Lemma 4 (Lemma Š)**.**

$$w_0 = (-1)^n (n!)^{k+1} k! + c_0 (k+1)! \text{ for some } c_0 \in \mathbb{Z}.$$

Lemma 5 (Lemma K)**.**

$$w_i = e^{-i} c_i (k+1)! \text{ for } 1 \leq i \leq n \text{ and for some } c_i \in \mathbb{Z}.$$

Lemma 6 (Lemma A)**.**

$$|v_i| \leq iP^kQ \text{ for some constants } P, Q \text{ depending only on } n.$$

3. Main Theorem

Now we have stated 4 lemmas which will be used in the talk for proving the statement of The Main Theorem. Though the proof is neither difficult, neither tricky, it is too long to be included in the abstract. Hence only the statement will be noted:

Suppose now that the number e is algebraic. Then there exists a polynomial with integer coefficients such that e is its root. Let

$$p(x) := a_n x^n + \cdots + a_1 x + a_0, \qquad a_0, \ldots, a_n \in \mathbb{Z}, \quad a_n \neq 0$$

be such a polynomial.

Theorem 7 (The Main One)**.** *Consider polynomial $p(x)$ as mentioned above. Then there exist numbers $R \in \mathbb{R}$, $B \in \mathbb{R}, |B| \lhd 1$ and $0 \neq A \in \mathbb{Z}$ such that*

$$R \cdot p(e) = A + B.$$

While the left side of the equation is exactly 0 (e is a root of $p(x)$), the right side cannot be (because $A \neq -B$). Hence there cannot be any such polynomial $p(x)$ which means that e can't be algebraic.

Therefore e is transcendental.

Transcendence of e and π – Part II

Michaela Kučerová

In this part we will introduce basic definitions and theorems for the proof of transcendence of π and e.

1. Introduction

We will start with stating important definitions from commutative algebra together with easy lemmas.

Definition 1. A finite extension K of the field of rational numbers is called a *number field.*

Definition 2. Let K be a number field. An element $\alpha \in K$ is called an *algebraic integer* if there exist a polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

with $n \geq 1$ and coefficients $a_i \in \mathbb{Z}$ such that $f(\alpha) = 0$.

Lemma 3. *Let K be a number field. An element $\alpha \in K$ is algebraic integer iff there exists a finitely generated $\mathbb{Z}$-module $M \neq 0$ (contained in some algebraic extension of K) such that $\alpha M \subset M$.*

This gives us the next important lemma.

Lemma 4. *The set of algebraic integers in number field K is a ring.*

Definition 5. We denote the ring of algebraic integers in K by I_K.

Definition 6. Let K be a number field. $\alpha \in K$. A positive integer d will be called a *denominator* for α if $d\alpha \in I_K$.

Definition 7. Each embedding $\sigma\colon K \to \mathbb{C}$ will be called a *conjugate* of K. If $\alpha \in K$ then we call $\sigma(\alpha)$ a *conjugate* of α.

Definition 8. We define the *size* of a set of elements of K to be the maximum of the absolute values (in $\mathbb{C}$) of all conjugates of these elements. By the *size* of a vector $X = (x_1, ..., x_n)$ we shall mean the size of its coordinates. By the *size* of a polynomial we shall mean the size (of a set) of its coefficients. We denote size with $\| \cdot \|$.

The next lemma will enable us to estimate the size of solution of linear equations over integers.

Lemma 9 (Siegel)**.** *Let*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0 \end{aligned}$$

be a system of linear equations with integer coefficients a_{ij}, and $n > r$. Let a be a number $A \geq 1$ such that $|a_{ij}| \leq A$ for all i, j. Then there exists an integral, non-trivial solution with

$$|x_j| \leq 2(3nA)^{r/(n-r)}.$$

Now we will generalize the previous lemma for system of linear equations over an algebraic integers.

Lemma 10 (Siegel)**.** *Let K be a number field. Let*

$$\begin{aligned} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n &= 0 \\ &\vdots \\ \alpha_{r1}x_1 + \cdots + \alpha_{rn}x_n &= 0 \end{aligned}$$

be a system of linear equations with coefficients in I_K, and $n \geq r$. Let A be a number such that $\|\alpha_{ij}\| \leq A$ for all i, j. Then there exists a non-trivial solution X in I_K such that

$$\|X\| \leq 2(CnA)^{r/(n-r)}.$$

Where C is a constant depending only on K.

It is straightforward to generalize the previous lemma for system of linear equations with coefficients in K.

2. Few definitions from the complex analysis theory

The rest of the lecture we will spend on stating various definitions and facts from the complex analysis theory.

Definition 11. A complex function that is complex differentiable at every point in a region is called *analytic function*.

Definition 12. If a complex function is analytic at all points of the complex plane $\mathbb{C}$, then it is said to be *entire*.

Definition 13. *Meromorphic function* is a function $f(z)$ of the form $f(z) = \frac{g(z)}{h(z)}$ where $g(z)$ and $h(z)$ are entire functions with $h(z) \neq 0$.

Definition 14. An entire function f is said to be of *order* $\leq \rho$ if there is a constant $C > 1$ such that for all large R we have

$$|f(z)| \leq C^{R^\rho},$$

whenever $|z| < R$.

A meromorphic function f is said to be of order $\leq \rho$ if it can be expressed as a quotient of entire functions of order $\leq \rho$.

Transcendence of e and π – Part III

Milan Boháček

In this part we will finally prove the transcendence of π (and countably many other transcendental numbers).

1. Definitions and lemmas

But, first we will continue with definitions.

Definition 1. Point $a \in \mathbb{C}$ is called a *pole* of analytic function f iff $\lim_{z\to a} f(z) = \infty$ and there exists $p \in \mathbb{N}$ such that $\lim_{z\to a}(z-a)^p f(z) \in \mathbb{C}$.

Fact 1 (Maximum Modulus principle)**.** Let f be a non-constant analytic function on a connected open set $U \subseteq \mathbb{C}$. Then $|f|$ cannot attains maximum in U, i. e. there exists no $a \in U$ such that

$$|f(a)| \geq |f(z)|$$

for all $z \in U$.

Definition 2. A *derivation* on the polynomial ring $K[T_1, \ldots, T_N]$ is an additive homomorphism

$$\mathbf{D}\colon K[T_1, \ldots, T_N] \to K[T_1, \ldots, T_N],$$
$$\mathbf{D}(P+Q) = \mathbf{D}(P) + \mathbf{D}(Q),$$

also satisfying *Leibniz condition*

$$\mathbf{D}(PQ) = \mathbf{D}(P)Q + P\mathbf{D}(Q).$$

Lemma 3. *Let K be a number field. Let $f_1, \ldots, f_N$ be functions analytic on a neighborhood of a point $w \in \mathbb{C}$, and assume that $\mathbf{D} = \frac{\partial}{\partial z}$ maps the ring $K[f_1, \ldots, f_N]$ into itself. Assume that $f_i(w) \in K$ for all i. Then there exists a number C having the following property.*

Let $P(T_1, \ldots, T_N)$ be any polynomial with coefficients in K, of degree $\leq r$. If we set $f := P(f_1, \ldots, f_N)$, then we have for all positive integers k,

$$\|\mathbf{D}^k f(w)\| \leq \|P\| r^k k! C^{k+r}.$$

Furthermore, there is a denominator for $\mathbf{D}^k f(w)$ bounded by $\operatorname{den}(P)C^{k+r}$.

2. Main theorem

This theorem states that algebraically independent meromorphic functions are somewhat limited in number of values lying in K.

Theorem 4. *Let K be a finite extension of the rational numbers. Let $f_1, \ldots, f_N$ be meromorphic functions of order $\leq \rho$. Assume that the field $K(f_1, \ldots, f_N)$ has transcendence degree ≥ 2 over K, and that the derivative $\mathbf{D} = \frac{\partial}{\partial z}$ maps the ring $K[f_1, \ldots, f_N]$ into itself. Let $w_1, \ldots, w_m$ be distinct complex numbers not lying among poles of the f_i, such that*

$$f_i(w_\nu) \in K$$

for all $i = 1, \ldots, N$ and $\nu = 1, \ldots, m$. Then $m \leq 32\rho[K : Q]$.

The proof uses estimates obtained from previous lemmas and some global arguments involving Maximum Modulus principle which will be shown at the lecture.

3. Corollaries

And finally we will reap what we have sown.

Corollary (Hermite-Lindemann)**.** *If α is algebraic (over $\mathbb{Q}$) and $\alpha \neq 0$, then e^α is transcendental. Hence π is transcendental.*

Proof. Let $K = \mathbb{Q}(\alpha, e^\alpha)$ be a number field. It is easy to see that functions $f_1 = e^z, f_2 = z$ (which complies with assumptions of the Main theorem) takes on algebraic values at all

$$w_1 := \alpha, w_2 := 2\alpha, \ldots, w_m := m\alpha,$$

for any $m \in \mathbb{N}$. But according to the Main theorem $m \leq 32[K : \mathbb{Q}]$. So $\mathbb{Q}(\alpha, e^\alpha)$ is not finite extension of $\mathbb{Q}$. So at least one of α, e^α is transcendental.

Finally $\alpha = i\pi$ is transcendental because $e^{i\pi} = -1$ and so π is transcendental. □

Corollary (Gelfond-Schneider)**.** *If α is algebraic, $\alpha \neq 0, 1$ and if β is algebraic and irrational then $\alpha^\beta = e^{\beta \log \alpha}$ is transcendental.*

This gives us countably many transcendental numbers such as $p^{\sqrt{p}}$ for p prime.

p-adic numbers – Part I

Petr Nižnanský

In the first talk about p-adic numbers, we remind a few definitions and show all non-equivalent norms in $\mathbb{Q}$.

Definition 1. Let X be a set. The function $d\colon X \times X \to [0, \infty)$ is a *metric* on X if the following holds:

- $d(x, y) = 0 \iff x = y$.
- $d(x, y) = d(y, x)$.
- $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.

A set X together with metric d is called a *metric space*.

Definition 2. Let F be a field. The function $\| \|\colon F \to [0, \infty)$ is a *norm* on F if the following holds:

- $\|x\| = 0 \iff x = 0$.
- $\|x \cdot y\| = \|x\| \cdot \|y\|$.
- $\|x + y\| \leq \|x\| + \|y\|$.

Definition 3. Let $p \in \mathbb{P}$ be any prime number ($\mathbb{P}$ is set of all prime numbers). The *p-adic valuation* (or *p-adic order*) is defined as $\nu_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$

$$\nu_p(x) = \begin{cases} \max\{v \in \mathbb{N}_0 \mid p^v \text{ divides } x\} & \text{if } x \neq 0 \\ \infty & \text{if } x = 0. \end{cases}$$

We can naturally extend p-adic valuation on rational numbers $\mathbb{Q}$ as follows: let $x = a/b$ then $\nu_p(x) = \nu_p(a) - \nu_p(b)$.

Examples 4. $\nu_5(35) = 1, \nu_2(97) = 0, \nu_3(27) = 3, \nu_2(3/8) = -3$.

The p-adic valuation gives us tool to define norm on $\mathbb{Q}$ as follows:

$$|x|_p = \begin{cases} \frac{1}{p^{\nu_p(x)}} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

To defined equivalent norms we need to remind that sequence $\{a_1, a_2, \ldots\}$ is Cauchy if $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall m, n > N\colon d(a_m, a_n) < \varepsilon$.

Definition 5. Two metrics d_1 and d_2 on a set X are *equivalent* if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2 and two norms are *equivalent* if they induce equivalent metrics.

Theorem 6 (Ostrowski)**.** *Every nontrivial norm $\| \|$ on $\mathbb{Q}$ is equivalent to $| |_p$ for some prime p or is equivalent to the absolute value $| |$.*

p-adic numbers – Part II

Hana Holmes

In the second talk of the cycle we will use the defined metric $|\ |_p$ to construct the field of p-adic numbers. We will define p-adic integers and show that there is a unique representation for each of them. In the end we will prove Hensel's lemma for p-adic numbers, which tells us how to find roots of polynomials with p-adic integer coefficients.

Definition 1. Let us have a set of sequences in $\mathbb{Q}$ that are Cauchy with respect to $|\ |_p$.

- sequences $\{a_i\}$ and $\{b_i\}$ are equivalent if $|a_i - b_i|_p \overset{i\to\infty}{\to} 0$
- for the equivalence class a we define $|a|_p = \lim_{i\to\infty} |a_i|_p$

Definition 2. The operations on the equivalence classes are defined naturally. Let $(a_i) \in a$ and $(b_i) \in b$ be any representatives of their classes:

- $a * b = [\{a_i * b_i\}]$ where * is multiplication or addition,
- $-a = [\{-a_i\}]$,
- $\frac{1}{a} = \left[\left\{\frac{1}{\bar{a}_i}\right\}\right]$ where $\bar{a_i} = p^i$ if $a_i = 0$, otherwise $\bar{a_i} = a_i$.

Lemma 3. *The set of equivalence classes of Cauchy sequences is a field with multiplication, addition and inverses defined as above. We call this the field $\mathbb{Q}_p$ of p-adic numbers.*

Lemma 4. *Every equivalence class $a \in \mathbb{Q}_p$ for which $|a|_p \leq 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which*

(1) $0 \leq a_i \leq p^i$ *for* $i \in \mathbb{N}$,

(2) $a_i \equiv a_{i+1} \pmod{p^i}$ *for* $i \in \mathbb{N}$.

Corollary. *For each equivalence class a where $|a|_p \leq 1$ we can write the elements of the sequence in the form $a_i = b_0 + b_1 p + \cdots + b_{i-1}p^{i-1}$ where each digit $b_i \in \{0, 1, \ldots, p-1\}$ is the same for every a_j. $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a| \leq 1\}$ form a "subring" of p-adic integers. $\mathbb{Z}_p^* = \{a \in \mathbb{Q}_p : |a| = 1\}$ is a set of p-adic units.*

Lemma 5. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any i there exists an integer $\alpha \in \mathbb{Z}$ such that $|\alpha - x|_p \leq p^{-1}$. The integer α can be chosen from the set $\{1, 2, \ldots, p^i - 1\}$.*

Theorem 6 (Hensel's lemma)**.** *Let $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ be a polynomial whose coefficients are p-adic integers. Let $F'(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1}$ be the formal derivative of $F(x)$. Let a_0 be a p-adic integer such that $F(a_0) \equiv 0 \pmod{p}$ and $F(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p-adic a integer such that*

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

p-adic numbers – Part III

Adam Ráž

1. Triangulation of a square

We can use the p-adic valuation for an interesting proof of the following Triangulation of a square theorem. For that it'll be helpful to prove a coloring lemma and a coloring theorem, which use our specifically defined coloring of $\mathbb{Q}^2$.

It is defined the following way:

Definition 1. A point (x, y) is colored $\begin{cases} \text{red} & \text{if } |x|_p < 1 \ \& \ |y|_p < 1 \ , \\ \text{green} & \text{if } |x|_p \geq 1 \ \& \ |y|_p \leq |x|_p \ , \\ \text{blue} & \text{if } |y|_p \geq 1 \ \& \ |x|_p < |y|_p \ . \end{cases}$

Lemma 2 (Coloring lemma)**.** *For any red poing (x_r, y_r), green point (x_g, y_g) and blue point (x_b, y_b) in $\mathbb{Q}^2$ it holds:*

$$\left| \begin{pmatrix} x_r & y_r & 1 \\ x_g & y_g & 1 \\ x_b & y_b & 1 \end{pmatrix} \right|_p \geq 1$$

Theorem 3 (Coloring theorem)**.** *The set $\mathbb{Q}^2$ can be colored (and is by our coloring) with exactly three colors such that any line contains exactly two colors.*

Theorem 4 (Triangulation of a square)**.** *It is impossible to divide a square into an odd number of triangles of equal area.*

2. Norm extension on $\mathbb{Q}_p$

We'll study some basic properties of finite algebraic extensions of $\mathbb{Q}_p$. In order to extend the p-adic norm, we will use the following definition, which is used in a proof of the next theorem.

Definition 5. Let $K = \mathbb{Q}_p[\alpha]$ be a finite extension of a field $\mathbb{Q}_p$ generated by an element α which satisfies a monic irreducible equation

$$0 = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \quad a_i \in \mathbb{Q}_p.$$

Then we define a p-adic norm on α by

$$|\alpha|_p := |\Pi_{i=1}^n \alpha_i|_p^{1/n}, \quad \text{where the } \alpha_i \text{ are the conjugates of } \alpha \text{ over } \mathbb{Q}_p.$$

Theorem 6. *Let K be a finite extension of $\mathbb{Q}_p$. Then there exists a unique field norm on K which extends the norm $|\ |_p$ on $\mathbb{Q}_p$.*

Numeration Systems – Complex Basis

Ondřej Väter

We usually use the positional notation to record numbers because it makes arithmetic easy. Typically, the base used is a positive integer $n > 1$ and digits are $\{0, \dots, n-1\}$.

In the first talk of the series, we show what opportunity brings the positional notation, if we use a complex number as the base. We show what a number system with a complex base looks like. We also mention theorems which tell us how to choose base and digits in this case.

Theorem 1. *Let $\beta = -1 + i \in \mathbb{C}$. Every $z \in \mathbb{Z}[i] := \{a + ib; a, b \in \mathbb{Z}\}$ can be uniquely written in the form:*

$$z = \sum\nolimits_{k=0}^{n} z_k \cdot \beta^k \text{ where } z_k \in \{0, 1\}$$

Definition 2. Let β be a base and $\mathcal{A} \subseteq \mathbb{C}$ be a set of digits. If

$$z = \sum\nolimits_{k=0}^{n} z_k \cdot \beta^k + \sum\nolimits_{k=-m}^{-1} z_k \cdot \beta^k \text{ where } z_k \in \mathcal{A}$$

instead of the sum we use the notation:

$$(z)_\beta = z_n z_{n-1} \dots z_0 \bullet z_{-1} z_{-2} \dots z_{-m}$$

where $\bullet$ is called the fraction dot.

Definition 3. We denote the set of numbers which have finite a number of digits as $Fin(\beta)$.

Theorem 4. *Let $\beta = -1 + i$ and $\mathcal{A} = \{0, 1\}$, then $Fin(\beta)$ is a dense set in $\mathbb{C}$.*

Theorem 5. *We define the Euclidean norm on $\mathbb{Z}[i]$: $N(z) = z\overline{z}$. Let any $z, \beta \in \mathbb{Z}[i]$ and $\beta = a + bi$, $\gcd(a, b) = 1$. Then there are $y \in \mathbb{Z}[i]$ and $r \in \{0, \dots, N(\beta) - 1\}$ such that $z = \beta \cdot y + r$.*

Theorem 6. *Let $\beta = a + bi \in \mathbb{Z}[i]$, $\gcd(a, b) = 1$ and let $\mathcal{A} = \{0, \dots, N(\beta) - 1\}$. Then every $z \in \mathbb{Z}[i]$ can be written in the form:*

$$z = \sum\nolimits_{k=0}^{n} z_k \cdot \beta^k \text{ where } z_k \in \mathcal{A}$$

if and only if $\beta = -n \pm i$ where $n \in \mathbb{N}$.

Algorithm 7 (Greedy)**.** Let $\mathcal{R}$ be a Euclidean domain with linear ordering.

Input: $\beta, a \in \mathcal{R}$
Output: $(a)_\beta = a_n \dots a_0$

while $a \neq 0$ **do**
  $k \leftarrow \max\{n \in \mathbb{N}; \beta^n \leq a\}$
  $a_k \leftarrow a \div \beta^k$
  $a \leftarrow a \bmod \beta^k$
end while
return $(a)_\beta = a_n a_{n-1} \dots a_0$

Theorem 8. *Let $\beta \in \mathbb{C}$, $|\beta| > 1$ be a base and $\mathcal{A} \subset \mathbb{C}$ be a finite set of digits. Let $V \subset \mathbb{C}$ be a bounded set such that 0 lies in the interior of V. If:*

$$\beta \cdot V \subset V + \mathcal{A} := \{v + a; v \in V, a \in \mathcal{A}\}$$

then every $z \in \mathbb{C}$ can be written in the form:

$$z = z_k \cdot \beta^k + z_{k-1} \cdot \beta^{k-1} + z_{k-2} \cdot \beta^{k-2} + \dots$$

where $\forall j \leq k$, $z_j \in \mathcal{A}$.

Note. A *redundant number system* is a number system with more digits than is necessary to represent every number. Numbers in such a system usually have multiple representations. Redundant systems allow for faster arithmetics (with parallel computing).

Numeration systems – Irrational basis

Adéla Skoková

This talk is about numeration systems using the irrational basis β. The greedy search from the previous part is not restricted to β coefficients in $\mathbb{Z}$. In the case of the irrational basis β the digits for any number will be $0, 1, \ldots, \lfloor\beta\rfloor$.

Definition 1. Let $\beta > 1$. The *set of β-integers* with a finite representation is

$$\mathbb{Z}_\beta = \left\{\pm x \,|\, in\mathbb{R}, x \geq 0, (x)_\beta = x_k x_{k-1} \ldots x_0 \bullet\right\}.$$

The set of all finite numbers with basis β will be defined as

$$\mathrm{Fin}(\beta) = \bigcup_{n\in\mathbb{N}} \frac{1}{\beta^n}\mathbb{Z}_\beta.$$

Example. Let us choose as the basis of our system the golden ratio $\beta = \frac{1+\sqrt{5}}{2}$. It is a root of the quadratic equation $x^2 = x + 1$, so $\beta^l = \beta^{l-1} + \beta^{l-2}$. The digits of our system will be 0 and 1 because $\lfloor\beta\rfloor = \lfloor\frac{1+\sqrt{5}}{2}\rfloor = 1$.

Observe that:

- $(1)_\beta = 1\bullet$
- $(2)_\beta = 10 \bullet 01$
- $(3)_\beta = 11 \bullet 01$
- $(4)_\beta = 101 \bullet 01$
- $(5)_\beta = 110 \bullet 1001$

Lemma 2. *If the basis $\beta \notin \mathbb{Z}$ then $\mathbb{Z}_\beta + \mathbb{Z}_\beta \not\subset \mathbb{Z}_\beta$.*

In number theory, an *algebraic integer* is a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$. The degree of an algebraic integer is the degree of its minimal polynomial. An algebraic integer α of degree n is a root of an irreducible monic polynomial $P(x)$ of degree n with integer coefficients, which is a minimal polynomial of α. The other roots of $P(x)$ are called the *conjugates* of α.

Theorem 3 (C. Frougny and B. Solomyak)**.** *Let $\beta > 1$ be such that* $\mathrm{Fin}(\beta) + \mathrm{Fin}(\beta) \subset \mathrm{Fin}(\beta)$*. Then β is an algebraic integer all his conjugates have absolute value less than* 1*.*

The proof can be found in an article *Finite beta-expansions* by C. Frougny and B. Solomyak.

Definition 4. If $\beta > 1$ is a root of a rational polynomial $P(x)$ and all other roots are real or complex numbers of absolute value less than 1, then β is called a *Pisot number*.

Lemma 5. *For every Pisot number β exists a $\lambda \neq 0$ such as*

$$\lim_{n\to\infty} ||\lambda\beta^n|| = 0,$$

where $||x||$ means the distance to the closest integer.

If a basis β is a Pisot number, than the set of β-integers is finite and there exists only a finite number of various spaces between the following numbers. Furthermore, it is possible to find a rule for length of these spaces.

Definition 6. *Tiling* of a space $\mathbb{R}^n$ is given by finite set D of tiles, which can fill the space without gaps and covering each other.

We will focus on Pisot numbers $1 \leq \beta \leq 2$ for the rest of the talk.

Let R be the set of all finite binary sequences produced by the greedy algorithm on $\mathbb{Z}$.

Definition 7. If $w \in R$ is a finite sequence of digits, we denote by $T_{\bullet w}$ the set

$$T_{\bullet w} = \left\{ x \geq 0 \,|\, (x)_\beta = x_k x_{k-1} \dots x_0 \bullet w \right\}.$$

In particular, if w is an empty sequence, then $T_\bullet = \mathbb{Z}_\beta \cap [0, \infty)$.

Let γ be a root of $P(x)$ conjugate to β. Then the fields $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\gamma)$ are isomorphic. Denote the isomorphism by σ. This isomorphism changes basis from $\beta > 1$ to γ, the norm of γ is less than 1. Observe that σ is the identity mapping on $\mathbb{Q}$.

Having chosen γ, we have the bounded set $(T_\bullet)' = \left\{ x' = \sigma(x) \,|\, x \geq 0, x \in \mathbb{Z}_\beta \right\} \subset \mathbb{C}$. The closure of $(T_\bullet)'$ is called the *central tile* $D_\bullet$ belonging to the Pisot number β. Tiling of the whole Gauss plane is defined by tiles given by $w \in R$:

$$D_{\bullet w} = \overline{\{x' = \sigma(x) \,|\, x \in T_{\bullet w}\}}.$$

The bar means a closure in classical metrics in $\mathbb{C}$. This tiling has following properties:

- Any tile $D_{\bullet w}$ is a copy of one of tiles $D_\bullet$, $D_{\bullet 1}$ or $D_{\bullet 11}$.
- Any tile multiplied by $\frac{1}{\gamma}$ could be composed of tiles $D_\bullet$, $D_{\bullet 1}$ and $D_{\bullet 11}$.

Pisot unit is a Pisot number which is a root of some polynomial with integer coefficients and the absolute coefficient equal to ± 1.

Theorem 8 (Tiling)**.** *Let $\beta > 1$ be a Pisot unit of degree $d \geq 2$. Then the sets $D_{\bullet w}$ form tiling of a space $\mathbb{R}^{d-1}$ if and only if* $\mathrm{Fin}(\beta) + \mathrm{Fin}(\beta) \subset \mathrm{Fin}(\beta)$.

In the case of $D_{\bullet w}$ can tile a space, the number of various tiles is at least equal to the degree of β. This number depends on the set R.

The difference between our tiling and the tiling from the previous talk, where $\beta = i - 1$, is that our tiling is aperiodic: Our tiling is not invariant under translations.

Numeration systems – Quasicrystals

Josef Dvořák

A "crystal" is intuitively understood as an organization of matter which shows a certain rigid structure, namely strong symmetry; all possible symmetries of crystals were characterized at the end of 19th century. However, in 1982 structures showing "prohibited" symmetries were discovered and therefore named *quasicrystals*.

We will be interested in a certain class of subsets of $\mathbb{R}^d$ which have quasicrystalline properties, so called "cut & project"-sets (C&P-sets). Properties of these sets can be described using methods of combinatorics on words. Finally, we connect the topic of the previous talks with physics, namely β-expansions of numbers with C&P-words and sets.

Theorem 1 (The Crystalographic Restriction Theorem)**.** *The only symmetries of a crystal are of orders* 1, 2, 3, 4, *and* 6.

Definition 2. A *lattice* in $\mathbb{R}^d$ is the set $\{a_1\mathbf{x}_1 + \ldots + a_d\mathbf{x}_d \, a_i \in \mathbb{Z}\}$, where the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_d$ are linearly independent.

Definition 3. Write $\mathbb{R}^d$ as a direct sum of two subspaces $V_1 \oplus V_2$ with the natural projections π_1, π_2. Let Ω be a bounded subset of V_2 and let L be a lattice in $\mathbb{R}^d$ such that π_1 is monic on L and $\pi_2(L)$ is dense in V_2. A *cut & project* set is the set

$$\Sigma(\Omega) := \{\pi_1(x) \,|\, x \in L \text{ and } \pi_2(x) \in \Omega\}.$$

The most important case for our purposes will be $d = 2$, so we can simplify the definition of *C&P-set* as follows:

Definition 4. Let ϵ and η be irrational numbers and let $\Omega \subset \mathbb{R}$ be a bounded interval. Then a *one-dimensional C&P-set* is the set

$$\Sigma_{\epsilon,\eta}(\Omega) = \{a + b\eta \,|\, a, b \in \mathbb{Z},\ a + b\epsilon \in \Omega\}.$$

One dimensional *C&P*-sets are unexpectedly nice:

Theorem 5. *For each* $\Sigma_{\epsilon,\eta}(\Omega)$ *there exist positive numbers* Δ_1, $\Delta_2 \in \mathbb{Z}[\eta]$ *depending only on* $\eta, \epsilon, |\Omega|$ *such that the distances between adjacent points of* $\Sigma_{\epsilon,\eta}(\Omega)$ *take values in* $\{\Delta_1, \Delta_2, \Delta_1 + \Delta_2\}$.

Furthermore, we can (up to scaling) restrict our attention to only certain ranges of parameters $\eta, \epsilon, |\Omega|$

Theorem 6. *For each* $\eta \neq \epsilon, \Omega$ *there exist* $\overline{\eta}, \overline{\epsilon}, \overline{\Omega}$ *satisfying*

$$\overline{\epsilon} \in (-1, 0), \overline{\eta} > 0, max(1 + \overline{\epsilon}, -\overline{\epsilon}) < |\overline{\Omega}| \leq 1$$

such that $\Sigma_{\epsilon,\eta}(\Omega) = s\Sigma_{\overline{\epsilon},\overline{\eta}}(\overline{\Omega})$ *for some* $s \in \mathbb{R}$.

For the purpose of describing $\Sigma_{\epsilon,\eta}(\Omega)$ in a different way, we need the following property of quadratic Pisot numbers:

Lemma 7. *Each quadratic Pisot unit can be expressed as the positive root of a quadratic equation* $\beta^2 = m\beta + 1$ *for* $m \geq 1$ *or* $\beta^2 = m\beta - 1$ *for* $m \geq 3$.

Finally we can formulate the theorem which connects the theory of *C&P*-sets and the theory of number systems:

Theorem 8. *The positive part of the set* $\mathbb{Z}_\beta$ *coincides with the positive part of C&P-set* $\Sigma_{\epsilon,\eta}(\Omega)$ *if and only if* β *is a quadratic Pisot unit.*

The set of arithmetical sets is not arithmetical

Tomáš Jakl

Cohen introduced forcing in 1963 to prove independence of the Axiom of choice and the Continuum hypothesis from Zermelo–Fraenkel set theory. From a topological point of view the construction of generic filter in the method of forcing is nothing more than Baire category theorem.

In this talk I will show how arithmetical forcing (one of the most transparent kinds of forcing) can be used for recursion theoretic proof of theorem that the set of all arithmetical sets is not arithmetical.

1. Preliminaries

Definition 1. Let $\mathfrak{L}$ be the first-order language with a constant $\bar{n}$ for each $n \in \mathbb{N}$, an unary relation '$\cdot \in X$' and function and relation symbols $+, \times, <, =$.

Given a formula φ of $\mathfrak{L}$, φ *is true for* $A \subseteq \mathbb{N}$ ($A \models \varphi$) is inductively defined as follows:

$$
\begin{array}{lcl}
A \models \varphi \text{ is atomic without '} \cdot \in X\text{'} & \iff & \varphi \text{ is true in } \mathbb{N} \\
A \models \bar{n} \in X & \iff & n \in A \\
A \models \neg\psi & \iff & \text{not } A \models \psi \\
A \models \psi_0 \vee \psi_1 & \iff & A \models \psi_0 \text{ or } A \models \psi_1 \\
A \models (\exists x)\psi(x) & \iff & \text{for some } n \in \mathbb{N}\ A \models \psi(\bar{n}).
\end{array}
$$

Cohen's idea was based on intuition that the truth can be approximated by a finite information. For example if some finite string σ of 0s and 1s tells us that φ is true, then $A \models \varphi$ for all $A \supseteq \sigma$ (we identify a set and its characteristic function).

Definition 2. Given a formula φ of $\mathfrak{L}$, σ *forces* φ ($\sigma \Vdash \varphi$) is inductively defined as follows:

$$
\begin{array}{lcl}
\sigma \Vdash \varphi \text{ is atomic without '} \cdot \in X\text{'} & \iff & \varphi \text{ is true in } \mathbb{N} \\
\sigma \Vdash \bar{n} \in X & \iff & \sigma(n) = 1 \\
\sigma \Vdash \neg\psi & \iff & (\forall \tau \supseteq \sigma)(\tau \nVdash \psi) \\
\sigma \Vdash \psi_0 \vee \psi_1 & \iff & \sigma \Vdash \psi_0 \text{ or } \sigma \Vdash \psi_1 \\
\sigma \Vdash (\exists x)\psi(x) & \iff & \text{for some } n \in \mathbb{N}\ \sigma \Vdash \psi(\bar{n}).
\end{array}
$$

Definition 3. For given $A \subseteq \mathbb{N}$ we say A *forces* φ ($A \Vdash \varphi$) if for some finite $\sigma \subseteq A$, $\sigma \Vdash \varphi$.

Definition 4. A is *n-generic* if for all sentences $\varphi \in \Sigma_n$ either $A \Vdash \varphi$ or $A \Vdash \neg\varphi$. A is *ω-generic* if the same happens for all sentences of $\mathfrak{L}$.

Lemma 5 (Forcing = Truth for generic sets)**.** *A is n-generic iff for any sentence $\varphi \in \Sigma_n \cup \Pi_n$, $A \models \varphi$ iff $A \Vdash \varphi$.*

Definition 6. A set $A \subseteq \mathbb{N}$ *is defined by* a formula φ if $n \in A \iff \emptyset \models \varphi(\bar{n})$. A set A is said to be *arithmetical* if it is defined by some formula of $\mathfrak{L}$.

2. Demonstration of the method

Theorem 7. *There is a n-generic set defined by Σ_{n+1} formula.*

Proof idea. (1) We have Σ_0 enumeration of $\mathfrak{L}$ sentences: $\psi_0, \psi_1, \ldots$.

(2) For each ψ_i we Σ_{n+1}-find a string σ_i extending σ_{i-1} such that $\sigma_i \Vdash \psi_i$ or $\sigma_i \Vdash \neg\psi_i$.

(3) $\bigcup_i \sigma_i$ is a characteristic function of a n-generic.

□

The proof goes the same way as the proof of Baire category theorem (theorem says: in a complete metric/locally compact Hausdorff space a countable intersection of open dense sets is dense).

The sets $[\sigma] = \{A \subseteq \mathbb{N} : A \supseteq \sigma\}$ form a basis of product topology of 2^ω. Since 2^ω is locally compact Hausdorff space and the fact that the set $\mathcal{O}_\varphi = \{A : A \Vdash \varphi \text{ or } A \Vdash \neg\varphi\}$ is open and dense in 2^ω there is a n-generic set in $\bigcap_{\varphi\in\Sigma_n} \mathcal{O}_\varphi$.

Theorem 8. *The set of arithmetical sets is not arithmetical.*

3. Conclusion

In Recursion theory, in order to force desired properties it often suffices to find some generic set, on the other hand in Set theory one has to construct a model "along" constructed generic filter which will then have desired properties. Model construction then makes the method much more difficult.

Primary and cyclic decomposition theorems – Part I

Vojta Tůma

This part of the series introduces/reviews basic notions and concludes with a proof of the *Primary Decomposition Theorem*, which serves as a tool for proving the central result for this series – the *Cyclic Decomposition Theorem*.

In this series T denotes a linear operator on a finite dimensional vector space V over a field $\mathbf{F}$. In order to understand some general mysterious operator T, we would like to decompose it into parts that are easier to comprehend. First of all, we investigate when does T vanish:

(1) the *characteristic polynomial* of T is the polynomial $\det(xI - A)$ (where A is a matrix that represents T)
(2) a polynomial p *annihilates* T if $p(T) = 0$,
(3) the *minimal polynomial* of T is the monic polynomial that annihilates T and has minimum degree over all such polynomials,

Decomposition of the minimal polynomial of T allows us to decompose the underlying space V into parts such that T does not jump between them:

(1) *projection* is an operator E such that $E^2 = E$,
(2) subspace W is T*-invariant* if $T(W) = W$,
(3) let $V = V_1 + V_2 + \cdots V_k$ such that $V_1, V_2, \ldots, V_k$ are independent, then V is a *direct sum* of $V_1, V_2, \ldots, V_k$, denoted by $V = \bigoplus_{i=1}^{k} V_i$.

The result of this talk gives a transparent decomposition of T:

Theorem 1 (Primary Decomposition Theorem)**.** *Let the minimal polynomial $M_T(X)$ of a linear operator T equal $p_1(X)^{m_1} \cdot p_2(X)^{m_2} \cdots p_s(X)^{m_k}$, where $p_1(X), p_2(X), \ldots, p_s(X)$ are distinct irreducible polynomials. Put $V_i = \ker p_i(T)^{m_i}$. Then*

(1) each V_i is T-invariant,
(2) for $T_i = T|_{V_i}$ the minimal polynomial $M_{T_i}(X)$ equals $p_i(X)^{m_i}$,
(3) $V = \bigoplus_{i=1}^{s} V_i$.

As a teaser, we state the central result of this series.

Theorem 2 (Cyclic Decomposition Theorem)**.** *There are vectors $v_1, v_2, \ldots, v_r$ of V with T-annihiators $f_j(X) = f_{v_j}(X)$ so that*

(1) $V = Z(v_1) \oplus Z(v_2) \oplus \cdots \oplus Z(v_r)$,
(2) $f_{j+1}(X) \mid f_j(X)$, $j = 1, 2, \ldots, r-1$,
(3) $v_r \neq 0$.

Furthermore, the listed properties uniquely determine r and the T-annihilators.

Primary and cyclic decomposition theorems – Part II

Alexander Slávik

The aim of this part is simply to give an elementary proof the main result, the Cyclic Decomposition Theorem. Our setting throughout the whole text and the lecture is following: V is a finite-dimensional vector space over a field $\mathbb{F}$, $T\colon V \to V$ a linear operator and m_T its minimal polynomial. Further, for any $v \in V$ let $Z(v) = \{f(T)v \mid f \in \mathbb{F}[x]\}$ (the *cyclic subspace* generated by v) and denote f_v the monic polynomial of minimal degree satisfying $f(T)v = 0$ (the *T-annihilator* of v).

In the proof we employ the following observations.

Lemma 1. *$Z(v) = \{f(T)v \mid f \in \mathbb{F}[x], \deg f < \deg f_v\}$, and $\{v, Tv, \dots, T^{(\deg f_v)-1}v\}$ is a basis of $Z(v)$.*

Lemma 2. *Let p be an irreducible factor of f_v of degree d. Then $\{v, Tv, \dots, T^{d-1}v\}$ is a linearly independent set, and if $Y(v) = \langle v, Tv, \dots, T^{d-1}v\rangle$, then $Z(v) = Y(v) \oplus Z(p(T)v)$.*

Lemma 3. *If $u, v \in V$ have relatively prime T-annihilators f_u, f_v, then $Z(u+v) = Z(u) \oplus Z(v)$ and $f_{u+v} = f_u f_v$.*

Theorem 4 (Cyclic Decomposition Theorem)**.** *Under the conditions above, there are vectors $v_1,\ v_2, \dots, v_r \in V$ with T-annihilators $f_j = f_{v_j}$ so that*

(1) $V = Z(v_1) \oplus Z(v_2) \oplus \cdots \oplus Z(v_r)$,
(2) $f_{j+1} \mid f_j$, $j = 1, 2, \dots, r-1$,
(3) $v_r \neq 0$.

Furthermore, the listed properties uniquely determine r and the T-annihilators.

Proof strategy. The first step is to prove the statement in the case $m_T = p^k$ for some $k \in \mathbb{N}$, $p \in \mathbb{F}[x]$ being irrediculble of degree d. The proof proceeds by induction on $\dim V$.

We construct a suitable T-invariant subspace $V_1 \subsetneq V$ containing $\operatorname{Im} p(T)$ with d-dimensional complement of the form $Y(v) = \langle v, Tv, \dots, T^{d-1}v\rangle$. By induction hypothesis, V_1 can be decomposed in the fashion described in the statement. Now it suffices to "repair" the cyclic subspace decomposition in such a way that $Y(v)$ fits into it.

The general case, when m_T is a product of powers of irreducible polynomials, is handled by the Primary Decomposition Theorem. This allows us to use the already prooved fact on T-invariant subspaces corresponding to the irreducible polynomials, and the proof is finished by applying Lemma 3.

Primary and Cyclic Decomposition Theorems – Part III

Marcel Šebek

In the following, V will be a finite-dimensional vector space over F with a linear operator T. Furthermore, m and c will be the minimal and characteristic polynomial of T, respectively.

Proposition 1. *Let W be a T-invariant subspace of V. Then W is T-admissible, if and only if W has a T-invariant complementary subspace.*

Proposition 2. *Then minimal and characteristic polynomial of T coincide, if and only if T has a cyclic vector, i. e., $V = Z(\alpha, T)$ for some $\alpha \in V$.*

Theorem 3 (Generalized Cayley-Hamilton Theorem)**.** *The following holds:*

(1) m divides c.

(2) m and c have the same prime factors, except for multiplicities.

(3) Let $m = f_1^{r_1} \dots f_k^{r_k}$ be a prime factorization. Then $c = f_1^{d_1} \dots f_k^{d_k}$ where d_i is the nullity of $f_i(T)^{r_i}$ divided by $\deg f_i$.

Definition 4. A matrix is in the *rational form* if it is block diagonal, matrices on the diagonal are companion matrices of some polynomials $p_1, \dots, p_k$, and p_{i+1} divides p_i for $i = 1, \dots, k-1$. The polynomials $p_1, \dots, p_k$ are called *invariant factors*.

Theorem 5. *Each matrix is similar to a unique matrix in the rational form.*

Definition 6. A $k \times k$ matrix of the form

$$J^{(\lambda)} = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{pmatrix}$$

is called an *elementary Jordan matrix with characteristic value* λ.

Definition 7. A matrix is said to be in the *Jordan form* if it is block diagonal with blocks $A_1, \dots, A_k$, each block is associated with a distinct characteristic value c_i, each A_i is again block diagonal consisting of elementary Jordan matrices with characteristic value c_i, and for each A_i the orders of its blocks are non-increasing.

Theorem 8. *Let c factor completely over F, i. e., $c = (x - c_1)^{d_1} \dots (x - c_k)^{d_k}$. Then there exists a basis of V in which T has a block diagonal matrix A in the Jordan form. The matrix A is determined uniquely, up to ordering of the blocks A_i.*

Introduction to quaternion algebras

Lenka Macálková

1. Basic definitions

Definition 1. Let F is field, char $F \neq 2$. A *quaternion algebra* $\mathcal{A}$ over F is a four-dimensional F-space with basis $1, i, j, k$. Multiplication on $\mathcal{A}$ is defined by following rules:

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

where $a, b \in F^*$. We will be denoted this quaternion algebra by $(\frac{a,b}{F})$.

Definition 2. Let $\mathcal{A}_0$ be subspace of quaternion algebra $\mathcal{A}$ spanned by i, j, k. Then elements of $\mathcal{A}_0$ are the *pure quaternions* in $\mathcal{A}$.

Each element x of quaternion algebra $\mathcal{A}$ has a unique decomposition as $x = a + \alpha$, where $a \in F$ and $\alpha \in \mathcal{A}_0$. We can define *conjugate* $\overline{x}$ of x by $\overline{x} = a - \alpha$.

Definition 3. For $x \in \mathcal{A}$ the *reduced norm* and *reduced trace* are defined by $n(x) = x\overline{x}$ and $\mathrm{tr}(x) = x + \overline{x}$.

Example. We introduce some kind of quaternion algebras, demonstrate additive and multiplicative operation and show computing norm and trace in this quaternion algebras.

- Hamilton quaternions is division algebra.
- $(\frac{-a,a}{F})$ in not division algebra.

2. Classification of Quaternion Algebras

Theorem 4. *Every four-dimensional simple central algebra over F of characteristic $\neq 2$ is a quaternion algebra.*

Theorem 5. *For $\mathcal{A} = (\frac{a,b}{F})$, the following are equivalent:*

(1) $\mathcal{A} \cong (\frac{1,1}{F})$.
(2) $\mathcal{A}$ *is not a division algebra.*
(3) $\mathcal{A}$ *is isotropic as a quadratic space with the norm form.*
(4) $\mathcal{A}_0$ *is isotropic as a quadratic space with the norm form.*
(5) The quadratic form $ax^2 + by^2 = 1$ *has solution in* F.
(6) If $E = F(\sqrt{b})$, *then* $a \in N_{E|F}(E)$.

Example. A quaterion algebra over $\mathbb{R}$ is isomophic to Hamilton quaternions or $(\frac{1,-1}{\mathbb{R}})$.

Lambda-modules

Jana Medková

The goal of this presentation is to formulate and proove the structure theorem for Λ-modules, where Λ is the ring of formal power series over the ring of p-adic integers. In effort to keep the lecture short and get to the point in given time here are listed some properties of the ring Λ. If interested, proofs can be found in the book Introduction to cyclotomic fields by Lawrence C. Washington.

Theorem 1. *Let $f, g \in \Lambda$ and $f = \sum_{i=0}^{\infty} a_i T^i$, where $a_0, \ldots, a_{n-1} \in (p)$, $a_n \in \mathbb{Z}_p^\times$. Then theere exist unique $q \in \Lambda$, $r \in \mathbb{Z}_p[T]$ such that $g = qf + r$ and $\deg(r) < n$.*

Definition 2. Polynomial $P \in \mathbb{Z}_p[T]$ is called distinguished if $P = T^n + a_{n-1}T^{n-1} + \cdots + a_0$, where $a_0, \ldots, a_{n-1} \in (p)$.

Theorem 3. *Let $f \in \Lambda$ be non-zero. Then f can be uniquely written as $f = p^s PU$, where s is a non-negative integer, P is a distinguished polynomial and $U \in \Lambda^\times$.*

Lemma 4. *Let $P \in \mathbb{Z}_p[T]$ be a distinguished polynomial and let $g \in \mathbb{Z}_p[T]$ be arbitrary. If $\frac{g}{P} \in \Lambda$, then $\frac{g}{P} \in \mathbb{Z}_p[T]$.*

Lemma 5. *Let $f \in \Lambda$, $f \notin \Lambda^\times$. Then the quotient ring $\Lambda/(f)$ is infinite.*

Lemma 6. *Let $I \neq 0$ be an ideal of the ring Λ. Then I contains a nonzero polynomial. Moreover, there is a distinguished polynomial $H \in \mathbb{Z}_p[T]$ such that there is a non-negative integer s such that $p^s H(T) \in I$ and every element in I is divisible by polynomial $H(T)$.*

Lemma 7. *Assume that $f, g \in \Lambda$ are relatively prime. Then the quotient ring $\Lambda/(f, g)$ is finite.*

Lemma 8. *The ring Λ is a noetherian ring, unique factorizaton domain, its prime ideals are only of following form: $\{0\}$, (p), (p, T) a ideals (P), where P is an irreducible distinguished polynomial and (p, T) is the only maximal ideal.*

Here follows lots of preparation lemmas. The main reason for these lemmas to be stated are to make the proof of structure theorem as simple as possible.

Lemma 9. *Let M be a finitely generated Λ-module and $f, g \in \Lambda$ are relatively prime. If the ideal (f, g) annihilates M, then M is finite.*

Definition 10. We call two Λ-modules M, M' pseudoisomorphic, denote $M \sim M'$, if there is a homomorphism $\varphi : M \to M'$ with a finite kernel and cokernel.

Lemma 11. *Assume that $f, g \in \Lambda$ are relatively prime. Then*

(1) the natural homomorphism $\Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g)$ is an injection with finite kernel,

(2) there exists an injective homomorphism $\Lambda/(f) \oplus \Lambda/(g) \to \Lambda/(fg)$ with a finite cokernel.

Lemma 12. *Let M, M', M'' be modules such that $M \sim M'$, $M' \sim M''$. Then $M \sim M''$.*

Lemma 13. *Let M, M', N, N' be Λ-modules such that $M \sim M'$, $N \sim N'$. Then $M \oplus N \sim M' \oplus N'$.*

Lemma 14. *Let R be a noetherian commutative ring, M finitely generated R-module. Then every submodule $N \subseteq M$ is finitely generated.*

Every finitely generated Λ-module $M \cong \Lambda^n/N$. The submodule $N \subseteq \Lambda^n$ is also finitely generated by $(\lambda_{11}, \ldots, \lambda_{1n}), \ldots, (\lambda_{m1}, \ldots, \lambda_{mn}) \in \Lambda^n$. We will denote $\mathrm{r}(M) = (\lambda_{ij})_{m\times n}$.

On the other hand we will denote $\mathrm{m}(R) = \Lambda^n/((\lambda_{11}, \ldots, \lambda_{1n}), \ldots, (\lambda_{m1}, \ldots, \lambda_{mn}))$ for each $m \times n$ matrix $R = (\lambda_{ij})_{m\times n}$.

Lemma 15. *Let A, B be matrices over the ring Λ. Then*

$$\mathrm{m}\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) \cong \mathrm{m}(A) \oplus \mathrm{m}(B).$$

Finally the structure theorem for Λ-modules.

Theorem 16. *Let M be a finitely generated Λ-module. Then $M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(P_j^{m_j})\right)$, where $r, s, t, n_i, m_j \in \mathbb{Z}$ are non-negative integers and P_j are irreducible distinguished polynomials.*

Operation 1: We may interchange two rows (columns).

Operation 2: We may add a multiple of a row (column) to another row (column).

Operation 3: We may multiply a row (column) by $\lambda \in \Lambda^\times$.

Operation 4: If R contains a row $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$, $p \nmid \lambda_1$, then we may change R to R' which contains a row $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and all elements of the first column except for λ_1 are multiplied by p.

Operation 5: If all elements in the first column of R are divisible by p^k and if there is a row $(p^k\lambda_1, p^k\lambda_2, \ldots, p^k\lambda_n)$, $p \nmid \lambda_1$, then we may change R to R' which contains a row $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and otherwise is the same as R.

Operation 6: If R contains a row $(p^k\lambda_1, p^k\lambda_2, \ldots, p^k\lambda_n)$ and $(\lambda\lambda_1, \lambda\lambda_2, \ldots, \lambda\lambda_n)$ is also a relation for some $\lambda \in \Lambda$, $p \nmid \lambda$ then we may change R to R' which contains a row $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and otherwise is the same as R.

Lemma 17. *Using the six operations, every matrix R over Λ can be transformed to a matrix in diagonal form, which has only zeros or distinguished polynomials on the diagonal.*

Bounding Helly numbers from Betti numbers

Zuzana Safernová[1]

Introduction

Helly's theorem asserts that if in a finite collection of convex subsets of $\mathbb{R}^d$ any $d+1$ have a point in common then the whole collection must have a point in common. In the contrapositive, this theorem states that any family of convex subsets of $\mathbb{R}^d$ with empty intersection must contain a sub-family of size at most $d+1$ that already has empty intersection. This invited the definition of the *Helly number* of a family $\mathcal{F}$ with empty intersection as the size of the largest sub-family $G \subseteq \mathcal{F}$ with the following properties: G has empty intersection and any proper sub-family of G has non-empty intersection. (If a family has non-empty intersection then its Helly number is, by convention, 0.) With this terminology, Helly's theorem simply states that any finite family of convex sets in $\mathbb{R}^d$ has Helly number at most $d+1$. Such *uniform* bounds, that is bounds independent of the cardinality of the family, are of particular interest.

We will prove that if the Helly number of a finite family of sets in $\mathbb{R}^d$ has huge Helly number then some intersections of the sets must be topologically really complicated.

The study of topological conditions ensuring bounded Helly number has been studied for a long time.

Main result

Before we precisely state our main result, we need the following definition.

Definition 1. The *k-th Betti number* b_k of a space X is a dimension of the k-th $\mathbb{Z}_2$-homology group of X.

Informally, the kth Betti number refers to the number of unconnected k-dimensional surfaces. The first few Betti numbers have the following intuitive definitions: b_0 is the number of connected components, b_1 is the number of two-dimensional or "circular" holes, b_2 is the number of three-dimensional holes or "voids", etc.

Theorem 2. *For any non-negative integers b and d there exists an integer $h(b,d)$ such that the following holds. If $\mathcal{F}$ is a finite family of subsets of $\mathbb{R}^d$ such that $\beta_i\left(\bigcap_{X\in G} X\right) \leq b$ for any $G \subsetneq \mathcal{F}$ and every $0 \leq i \leq \lceil \frac{d}{2} \rceil - 1$ then $\mathcal{F}$ has Helly number at most $h(b,d)$.*

Idea of the proof. Suppose for contradiction that for every n we have set system with bounded Betti numbers of intersections and which Helly number is at least n. We may take without loss of generality minimal such system, i. e. system with $n+1$ sets only. We proceed by induction and show if n is sufficiently large, we can construct a homological drawing of the $\lceil d/2 \rceil$-skeleton of the $(d+2)$-simplex, which is a contradiction, since it is not possible in $\mathbb{R}^d$ (Van Kampen type obstruction).

Let $\mathcal{F} = \{U_1, U_2, \ldots, U_n\}$ denote a family of subsets of $\mathbb{R}^d$. For any (possibly empty) proper subset I of $[n] = \{1, 2, \ldots, n\}$ we write V_I for $\bigcap_{i\in[n]\setminus I} U_i$.

Step 1. For every i pick a point $v_i \in V_i$, this gives a 0-dimensional skeleton of $(n-1)$-simplex (i. e. set of n points).

[1] *joint work with Xavier Goaoc, Pavel Paták, Martin Tancer and Uli Wagner*

Step 2. Suppose we have already constructed k-dimensional skeleton of a sufficiently large simplex Q. Suppose that the vertices are linearly ordered. We will construct a $(k+1)$-dimensional skeleton S of a m-dimensional simplex. In any sufficiently large (say with ℓ elements) subset T of its vertices, there exist $2^{k+1}-1$ elements, such that all k-cycles formed by them are in the same homological class in V_T (Ramsey's theorem). Colour each ℓ-element subset of Q by the relative position of these elements. Let q be the number of vertices in barycentric subdivision of S. We apply Ramsey's theorem again, to obtain a $\left(q+\binom{m+1}{k+1}(\ell-2^{k+1}+1)\right)$-element monochromatic set P. One can choose a q-element subset C of P, and for every its $(2^{k+1}-1)$-element subset D $\psi(D) \subseteq C \setminus D$ such that $\psi(D)$ and $\psi(D')$ are disjoint for $D \neq D'$, and every cycle in D has the same homological class in $V_{D\cup\psi(D)}$. But since D is a barycentric subdivision of a $(k+1)$-face of S, it contains an even number of cycles, which sum up to zero (in $\mathbb{Z}_2$), hence we have a boundary and can fill its interior inside $V_{D\cup\psi(D)}$.

Cantor's diagonal argument – Part I: Usage in set theory

Jakub Töpfer

The aim of this topic is to show, how Cantor's diagonal argument can be very useful in many fields of mathematics. This inductory part presents the method and covers some classical theorems and paradoxes from the set theory.

1. Overview of the argument

The most famous usage of the argument is for proving the following theorem:

Theorem 1 (Cantor)**.** $\mathbb{N} \prec \mathbb{R}$

Proof. Let's suppose that there is a bijection between $\mathbb{N}$ and $(0,1)$. Then all real numbers from $(0,1)$ can be ordered in a sequence $a_1, a_2, \ldots$ Let's denote d a number from $(0,1)$ which has on i-th position of his decinal expansion 1 if in decimal expansion of a_i isn't on i-th position 1 and 2 otherwise. Then d is a real number, which isn't at list of all real numbers, which is a contradiction, so $\mathbb{N} \prec (0,1)$. □

Another theorem claims:

Theorem 2 (Cantor)**.** $x \prec \mathcal{P}(x)$

Proof. A map which every $t \in x$ matches with $\{t\}$ is clearly an ijection, so $x \preceq \mathcal{P}(x)$. We will show that $x \not\approx \mathcal{P}(x)$. Let f be a bijection from x to $\mathcal{P}(x)$ and let $y \subseteq x$ be a set such as

$$y = \{t : t \in x \ \&\ t \notin f(t)\}.$$

Then y hasn't any preimage under a map f. If $f(v) = y$ for some $v \in x$, then $v \in y$ or $v \notin y$. Both leads to a contradiction. □

2. Paradoxes

Cantor's diaginal argument is used also in many paradoxes, which at the beginning of the twentieth century led to formulation of axiomatic set theories.

Paradox 3 (Russell)**.** *Let*

$$x = \{y : y \notin y\}.$$

Then $x \in x$ if and only if $x \notin x$.

Paradox 4 (Richard)**.** *Let's consider all real numbers $x \in (0,1)$ such as they can be described by a finite sequence of words, e.g. "one half", "3rd square root of seven". This set is finite, so it can be ordered in a sequence $a_1, a_2, \ldots,$ where every a_i has infinite decimal expansion. Now we can define a number d by a finite sequence of words: "d is a real number between 0 and 1 which has i-th digit in its decimal expansion equal to 1 if i-th digit of decimal expansion of a_i is differnt from 1 and 2 otherwise". Is d in the original set?*

Cantor's diagonal argument – Part II

Jiří Sýkora

In this part we show applications of the diagonal method in mathematical logic. We present the diagonal lemma and its consequences, e.g. Gödel's first incompleteness theorem.

We also show the undecidability of Peano arithmetic. Furthermore, we focus on ultrafilters and ultrapowers.

Lemma 1 (Diagonal lemma)**.** *Let T be an extension of the theory Q and let $\varphi(v_0)$ be a formula of T. Then there exists a sentence φ^* such that $T \vdash \varphi^* \leftrightarrow \varphi(\underline{\varphi^*})$.*

Theorem 2 (Gödel's first theorem)**.** *Let T be a consistent and effectively generated extension of the theory Q. Then there exists a Π_1-sentence in the language of arithmetic which is true in $\mathcal{N}$ and unprovable in T.*

Definition 3. Formula $\tau(x)$ of a numerical theory T is a *definition of truth in T* if for each sentence φ of T the following statement holds: $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

Theorem 4.

(1) There is no definition of truth in a consistent extension of the theory Q.

(2) $\mathrm{Th}(\mathcal{N})$ *is not an arithmetical set.*

Theorem 5. *Let T be a consistent extension of the theory Q. Then T is undecidable. Moreover, if T is effectively generated, then T is not complete.*

Definition 6. An *ultrafilter* over a set X is a set $\mathscr{U} \subseteq \mathcal{P}(X)$ such that

(1) if $A \in \mathscr{U}$ and $A \subseteq B$ then $B \in \mathscr{U}$,

(2) if $A, B \in \mathscr{U}$ then $A \cap B \in \mathscr{U}$,

(3) $\emptyset \notin \mathscr{U}$, and

(4) for each subset $A \subseteq X$, exactly one of $A, X \setminus A$ is in $\mathscr{U}$.

Theorem 7 (Łoś's theorem)**.** *Let L be a first-order language, $(A_i : i \in I)$ a non-empty family of non-empty L-structures and $\mathscr{U}$ an ultrafilter over I. Then for any formula $\phi(\bar{x})$ of L and tuple $\bar{a}$ of elements of $\prod_I A_i$,*

$$\prod_I A_i/\mathscr{U} \models \phi(\bar{a}/\mathscr{U}) \quad \text{if and only if} \quad \|\phi(\bar{a})\| \in \mathscr{U}.$$

Corollary. *If $A^I/\mathscr{U}$ is an ultrapower of A, then the diagonal map $e\colon A \to A^I/\mathscr{U}$ is an elementary embedding.*

Corollary (Existence of nonstandard models of arithmetic)**.** *There is a model A of the theory of natural numbers and $a \in A$ such that $A \models a > n$ for every natural number n.*

Cantor's diagonal argument – Part III

Tomáš Kobrle

In the third lecture we introduce the Cantor's diagonal argument in computation theory, the Halting problem, and in recursion theory, the Kleene's theorem.

We also mention quines, programs generating its own source code, and fast growing functions.

Definition 1. The set of partial recursive functions (PRF) is the smallest set of partial functions $\mathbb{N}^d \to \mathbb{N}$ for $d = 0, 1, 2, \ldots$ such that

- the function $0\colon \mathbb{N}^0 \to \mathbb{N}$ with value 0 is PRF, and the successor function $S\colon \mathbb{N} \to \mathbb{N}$ is PRF;
- the projective function $P_d^i\colon \mathbb{N}^d \to \mathbb{N}$ for $1 \leq i \leq d$ is PRF;
- whenever $g\colon \mathbb{N}^m \to \mathbb{N}, h_1, \ldots, h_m\colon \mathbb{N}^d \to \mathbb{N}$ are PRF, so is $g(h_1, \ldots, h_m)$;
- whenever $g\colon \mathbb{N}^{d-1} \to \mathbb{N}, h\colon \mathbb{N}^{d+1} \to \mathbb{N}$ are PRF, then a function $f\colon \mathbb{N}^m \to \mathbb{N}$ such that for all $x_1, \ldots, x_d$

$$f(x_1, \ldots, x_{d-1}, 0) = g(x_1, \ldots, x_{d-1})$$
$$f(x_1, \ldots, x_{d-1}, x_d + 1) = h(x_1, \ldots, x_{d-1}, x_d, f(x_1, \ldots, x_{d-1}, x_d))$$

  is PRF too. The function f is said to be obtained by primitive recursion from g and h and it is unique determined;
- whenever $g\colon \mathbb{N}^{d+1} \to \mathbb{N}$ is PRF, then so is $f\colon \mathbb{N}^d \to \mathbb{N}$, where $f(x_1, \ldots, x_d)$ gives a minimal y such that $g(x_1, \ldots, x_n, y) = 0$.

Definition 2. We call a set $A \subset \mathbb{N}^d$ recursive if characteristic function $\chi_A\colon \mathbb{N}^d \to \mathbb{N}$ is recursive. Instead of saying that the set A is recursive we also say that A is decidable.

Theorem 3. *For each d we have PRF $\phi^{(d)}\colon \mathbb{N} \times \mathbb{N}^d \to \mathbb{N}$, such that each $\phi^{(d)}(e, \bullet) = \phi_e^{(d)}\colon \mathbb{N}^d \to \mathbb{N}$, for $e \in \mathbb{N}$, is partial recursive and for each PRF $f\colon \mathbb{N}^d \to \mathbb{N}$ there is an e such that $f = \phi_e^{(d)}$.*

Theorem 4 (Halting Problem)**.** *The halting problem*

$$\{(e, n) \mid \phi(e, n)\downarrow\}$$

is undecidable. (The symbol $\phi(e, n)\downarrow$ means that (e, n) is in domain of ϕ.)

Theorem 5 (Kleene's Theorem)**.** *Let $g\colon \mathbb{N} \to \mathbb{N}$ be recursive. Then there exists an e_0 such that $\Phi_{e_0} = \Phi_{g(e_0)}$.*

Programme

Friday, April 12

10:55 *Opening*
11:00 Vojta Luhan – *Transcendence of e and π – Part I*
11:45 Michaela Kučerová – *Transcendence of e and π – Part II*
12:30 *Lunch*

13:30 Milan Boháček – *Transcendence of e and π – Part III*
14:15 Petr Nižňanský – *p-adic numbers – Part I*
15:00 *Coffee break*
15:15 Hana Holmes – *p-adic numbers – Part II*
16:00 Adam Ráž – *p-adic numbers – Part III*

18:30 *Supper*
19:30 Marian Kechlibar – *TBA*

Saturday, April 13

08:00 *Breakfast*
09:00 Ondřej Väter – *Numeration systems – Complex Basis*
09:45 Adéla Skoková – *Numeration systems – Irrational basis*
10:30 *Coffee break*
10:45 Josef Dvořák – *Numeration systems – Quasicrystals*
11:30 Tomáš Jakl – *The set of arithmetical sets is not arithmetical*

12:30 *Lunch*

18:30 *Supper*
19:30 Graduate talks

Sunday, April 14

08:00 *Breakfast*
09:00 Vojta Tůma – *Primary and cyclic decomposition theorems – Part I*
09:45 Alexander Slávik – *Primary and cyclic decomposition theorems – Part II*
10:30 *Coffee break*
10:45 Marcel Šebek – *Primary and cyclic decomposition theorems – Part III*
11:30 Lenka Macálková – *Introduction to quaternion algebras*

12:30 *Lunch*

13:30 Jana Medková – *Lambda-modules*
14:15 Jaroslav Šeděnka – *TBA*

19:30 *Final dinner*

Monday, April 15

08:00 *Breakfast*

09:00 Zuzana Safernová – *Bounding Helly numbers from Betti numbers*

09:45 Jakub Töpfer – *Cantor's diagonal argument – Part I: Usage in set theory*

10:30 *Coffee break*

10:45 Jiří Sýkora – *Cantor's diagonal argument – Part II*

11:30 Tomáš Kobrle – *Cantor's diagonal argument – Part III*

12:30 *Lunch*