škola v přírodě

katedry algebry

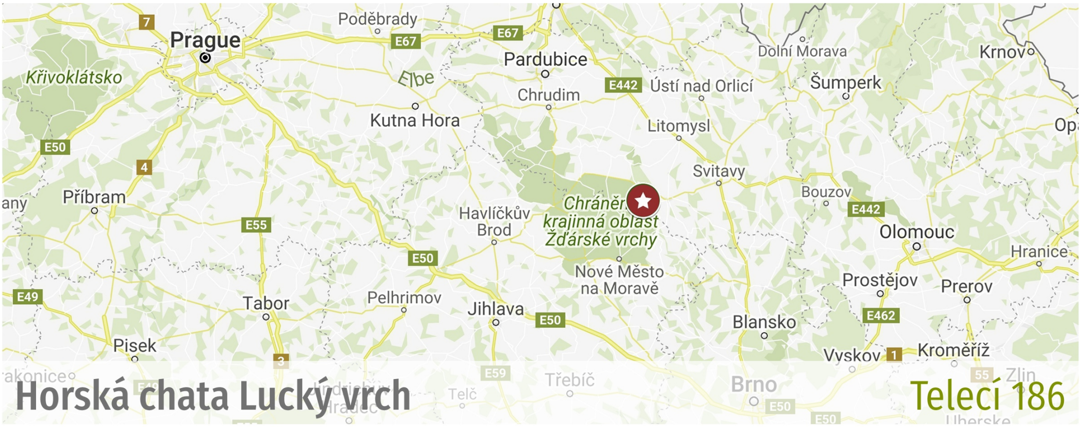
4. - 7. listopadu

2021

TEĎ UŽ VÁŽNĚ?

Zveme všechny se zájmem o témata pěstovaná na katedře algebry na další ročník algebraické školy v přírodě!

#algebra **#geometrie** **#kryptografie** **#teoriecisel** **#logika**



Horská chata Lucký vrch

Telecí 186

skolavprirode@karlin.mff.cuni.cz

karlin.mff.cuni.cz/~skolavprirode

Abstracts

Discovery of Ceres: How Gauss became an astronomer

Daniel Bedats

In 1801, European astronomers found, observed and lost an unknown faint star-like object. Many mathematicians tried to reconstruct the orbit of the object (named Ceres) and failed. Only young C.F.Gauss was able to succeed. In my talk, I hope to provide some insight into how he managed to do so.

Constructing the Petersen and Hoffman-Singleton graphs

Jan Černý

This short lecture will be about few interesting creatures from Graph theory. To be specific it will be about Hoffman-Singleton graph and Petersen graph. We will examine their properties and how to construct them (if possible). This lecture relies on basic knowledge of graph theory, combinatorics and linear algebra.

Baer's Criterion and Its Dual Version

Kateřina Fuková

In a module theory the Baer's criterion (BC) is a way how to test injectivity, which allow us to classify injective modules over particular rings. This talk will be an introduction of injectivity and (dually) projectivity of modules and some weaker versions of these properties. Also I would like to mention a still open Faith's problem about dualization of this criterion.

Intuition behind a curvature

Štěpán Hudeček

This talk is about understanding the curvature as a concept, not as a formula. It will build slowly upon curvature of a curve, of a surface up to a Riemann curvature tensor. Its main goal is to give an intuitive understanding and tell some awesome theorems along the way. In the end there will even be a well-known, but not so much mentioned application of the theory.

Coclones of Minimal Taylor Algebras

Filip Jankovec

In this talk we will introduce the definitions of clone and coclone and we will discuss Galois correspondence between them. Also we will discuss how to find generators of coclones of majority minimal Taylor algebras (and what does minimal Taylor and the majority property mean). Concept of clones and coclones belongs to universal algebra and has a strong connection with CSP (constraint satisfaction problem).

Perfect card shuffles

Michal Košek

In this talk we will present mathematical structures which arise when shuffling a deck of cards. Namely, we will consider groups generated by the so called *faro* shuffles, where a deck is split in two and interleaved. These *shuffle groups* have been fully classified using elementary group theory and by taking advantage of some symmetry preserved by these shuffles. We will show what this symmetry is and how it allows us to find the structure of the shuffle groups. We will also consider a generalization to more than two parts, which will leave us with a few interesting open problems.

Restricted minimum condition for domains

Dominik Krasula

One can learn much about a ring from the study of its lattice of ideals. We say that a ring is *Artinian* if it has no infinite descending chain of ideals. This concept turned out to be quite strong - the Hopkins-Levitzky theorem entails that Artinian rings have finite composition series. However, in some settings this condition is too strong, for example, Artinian domains are simply fields.

Recall that any factor of an Artinian ring is Artinian. Hence we can characterize Artinian rings by this property. If we demand that only factors by *nontrivial* ideals are Artinian, we get a new larger class of rings - *RM rings.*

In the lecture, we will study basic properties of RM rings and then we will use the theory to prove a new characterization of Dedekind domains.

n-dimensional rotations using geometric (Clifford) algebra

Maroš Grego

Complex numbers are often used to express rotations in the plane and quaternions are used to express rotations in 3D space. Geometric (AKA Clifford) algebra is a stucture that can give an explanation why it works and provide a trivial generalisation for spaces of arbitrary dimension. These rotations can be specified using the most intuitive data (the rotation plane and the angle of rotation), making it easy to smoothly interpolate the rotation and straightforward to compose multiple ones. In particular, the 3-dimensional quaternion rotations can be explained with geometric algebras using only 3D concepts that one can imagine and draw. The power doesn't end there, though. Any orthogonal transformation, any similarity and for a suitable model of the space, even any conformal (angle-preserving) transformation can be naturally expressed using geometric algebra.

Mathematical Description of Juggling

Cyril Matoušek

When a juggler performs a juggling trick, he periodically throws and catches balls in a specified order. It is possible to encode this order into a finite sequence of natural numbers, which satisfies certain properties. Conversely, each finite sequence satisfying these properties is called a juggling sequence, and it determines a juggling trick that can be performed in the real world. In this talk, we show theorems that tell us whether a given finite sequence of natural numbers is a valid juggling sequence or not. Moreover, we present an algorithm constructing all juggling sequences of given parameters.

Poncelet's porism

Anna Mlezivová

This talk will present the Poncelet's porism from the point of view of algebraic geometry. Poncelet's porism states that if we are given an n and two conic sections then there exists an n-gon, which is inscribed in one and is circumscribing the other, there are infinitely many such n-gons. We will show a sketch of a proof of this theorem which among others uses isomorphisms of projective varieties and a group structure on elliptic curves.

Method of animation for solving olympiad geometry

Radek Olšák

We will take a look at a method for solving high school olympiad geometry. It has basic theory, but is widely applicable. The method process consists of upperbounding degrees of some polynomials and then checking that the problem holds for enough degenerate cases. Its main advantage is that it requires little to no computation.

Incompressible encodings and their limitations

Petr Sedláček

This talk is based on my bachelor thesis *Limitations of incompressible encodings.* I introduce you to the notion of what incompressible encodings are and where it is advantageous to use them. After the motivation, I define the incompressible encodings more precisely, and I focus on the limitations of their information-theoretic security. The core of the speech is a theorem implying that it is not possible to construct secure non-trivial incompressible encodings information-theoretically. I show flaws in proof in a preceding article and present counterexamples to them. Afterwards, I present my own proof of the statement.

Paramedial quasigroups of prime and prime square order

Žaneta Semanišinová

A *quasigroup* is an algebra $(Q, \cdot)$ such that the multiplication table of $\cdot$ forms a latin square (possibly infinite). A quasigroup is called *paramedial*, if it satisfies the identity

$$(xy) \cdot (uv) = (vy) \cdot (ux),$$

for all $x, y, u, v \in Q$. We prove that for every odd prime number p, there are $2\ p\ -\ 1$ paramedial quasigroups of order p and $6p^2 - p - 1$ paramedial quasigroups of order p^2, up to isomorphism. Our approach is based on the affine representation of paramedial quasigroups (due to Němec and Kepka) over the groups $\mathbb{Z}_p, \mathbb{Z}_{p^2}$ and $\mathbb{Z}_p^2$ and an enumeration algorithm by Drápal. The central part of the calculation involves an analysis of square roots and conjugacy classes in the group $GL(2, p)$ and its subgroups.

Generalization of continued fractions

Ester Sgallová

This talk is on the topic of the generalization of continued fractions. Concretely, I will talk about the Jacobi-Perron algorithm, which is a multidimensional generalization of the usual continued fractions algorithm. This talk aims to show the connection between these two algorithms and compare their properties, especially when these algorithms are periodic.

Linear Algebra Meets Topology

Alexander Slávik

For a vector space V over a field k, we define its *dual space* V^* to be the space of all linear maps from V to (the 1-dimensional space) k. We present the relation between elements of the double dual V^{**} and ultrafilters on sets, highlighting several aspects of the analogy. If time permits, we might show the way compact (Hausdorff) topological spaces “arise” in a completely categorical way.

Investigating the holomorph of a group with GAP

Filippo Spaggiari

The holomorph of a group G is the subgroup of its permutation group generated by automorphisms and right multiplication maps. It is a huge extension of the group which contains information about both the self-maps of G and the structure of the group itself. The interest in the holomorph is very recent, if not contemporary, due to its connections with the theory of *skew braces.*

The idea of this talk (based on the research project of the Master's Thesis of the speaker) is to understand the pattern in the behaviour of a particular graph related to the holomorph, maintaining the focus on the computational aspects of such a research, and highlighting the fundamental help that the software GAP provided.

On permutations among polynomials with Niho type exponents

Adolf Středa, Jiří Pavlů

In cryptology, permutation polynomials over fields of even characteristic are of great importance, as they allow for creation of efficient cryptosystems. However the security of cryptosystems is also important. Considering the field $\mathbb{F}_{2^{2m}}$, Niho type polynomials are polynomials with exponents of the form: $s(2^m-1)+1$ for $0 \leq s \leq 2^m$. These polynomials are known to have good cryptographic properties, thus they allow for creation of secure cryptosystems, however, when they correspond to permutations is still an open question today. In the talk, we will show some methods for determining necessary conditions for some of these polynomials to be permutations. We will show our method on the polynomials of the form: $X + CX^{2-q} + DX^{2q-1} \in \mathbb{F}_{q^2}[X]$, $q = 2^m$, $m \in \mathbb{N}$.

Surreal numbers and their application in partisan games

Pavel Surý

When John Conway studied end-games of Go, he ended up discovering surreal number system - an ordered field, which contains not only real numbers, but also ordinals and infinitesimals as subfields. We shall describe Conway's construction and showcase the operations on surreals.

Then it will be shown that surreal numbers are related to partisan games - which are games, such that each player has a different set of moves, and finally, we will evaluate the positions in a Domineering game as an exercise.

Number of variables of universal quadratic forms

Bára Tížková

In this talk we will give an overview of the basic theory concerning universal quadratic forms and go through some relevant notions from algebraic number theory. After that, we will take a look at the number of variables of universal quadratic forms in number fields and briefly introduce the main ideas behind the proof of the following theorem: In each degree 2n, there are infinitely many totally real number fields that require universal quadratic forms to have arbitrarily large rank.

Brouwer fixed point theorem, Borsuk-Ulam theorem and their geometric relation

Tomáš Vítek

Lecture will speak about two fundamental topological theorems widely cited in popular mathematics. Brouwer fixed point theorem commonly known as the fact that it is impossible to stir your cup of tea perfectly, and Borsuk-Ulam theorem probably better known as the saying that at every moment there exist two points on the surface of the Earth that are directly opposite to each other but have exactly the same temperature and atmospheric preassure. We will explore a geometric relation between those theorems and how they stem from a combinatorial lemma about simplicial structures.

Dual quaternions and space kinematics

Jana Vráblíková

Any proper rigid transformation in $\mathbb{R}^3$ is a composition of a rotation around an axis and a translation in the direction of the axis. Quaternions over real numbers provide an efficient method of representing rotations in three dimensional space. Dual quaternions offer a way to represent any proper rigid body displacement in $\mathbb{R}^3$ in a similarly elegant manner.

In this talk we define the algebra of dual numbers and dual quaternions. We show the correspondence between dual quaternions and the Special Euclidean group, the group of all proper rigid transformations. We define motion polynomials that parameterize proper rigid body motions in $\mathbb{R}^3$ and we discuss an algorithm for factorization of the polynomials. We illustrate the concepts with some toy problems from robotics.

Isotropy of quadratic forms in characteristic 2

Kristýna Zemková

It is well-known that quadratic forms can be diagonalized over fields and that there is a one to one correspondence with bilinear forms; the algebraic theory of quadratic forms is based on these two properties. But there is a catch – they require division by two. Over a field of characteristic 2, neither of them is true, and the whole quadratic form theory needs to be rebuild from scratch.

In the talk, I will briefly introduce the theory of quadratic forms in characteristic 2. Then I will focus on the diagonalisable ones; they resemble the "usual“ theory less then one might expect. In particular, I will talk about the isotropy: a quadratic form is called *isotropic*, if it nontrivially represents zero, and *anisotropic* otherwise. The goal is to describe field extensions over which an anisotropic form becomes isotropic.

Definition and properties of iterative norms

M. Zindulka

We begin with a norm N defined on $\mathbb{R}^2$ which is assumed to be

- absolute: $N(x, y) = N(|x|, |y|)$ for $x, y \in \mathbb{R}$,
- normalized: $N(1, 0) = N(0, 1) = 1$.

We define its extension N_n to $\mathbb{R}^n$ for $n > 2$ iteratively by

$$N_n(x_1, \dots, x_n) = N(N_{n-1}(x_1, \dots, x_{n-1}), x_n).$$

By passing to the limit we obtain a norm on certain space of sequences which turns out to be Banach (the definition of Banach space will be included in the talk). The goal is to describe norm equivalence of N_n, dual norms and properties of the unit ball.

Schedule

Thursday 4th

9:00 *breakfast*
12:45 *lunch*
14:30 **Kateřina Fuková**: Baer's Criterion and Its Dual Version
15:00 **Filip Jankovec**: Coclones of Minimal Taylor Algebras
15:30 **Štěpán Hudeček**: Intuition behind a curvature
16:00 *coffee break*
16:30 **Pavel Surý**: Surreal numbers and their application in partisan games
17:00 **Filippo Spaggiari**: Investigating the holomorph of a group with GAP
17:45 **Kristýna Zemková**: Isotropy of quadratic forms in characteristic 2
18:30 dinner
20:00 **Ester Sgallová**: Generalization of continued fractions
20:30 **Žaneta Semanišinová**: Paramedial quasigroups of prime and prime square order

Friday 5th

8:00 *breakfast*
9:00 **Michal Košek**: Perfect card shuffles
9:30 **Bára Tížková**: Number of variables of universal quadratic forms
10:00 **Alexander Slávik**: Linear Algebra Meets Topology
10:30 *coffee break*
11:00 **Anna Mlezivová**: Poncelet's porism
11:30 **Petr Sedláček**: Incompressible encodings and their limitations
12:15 **Daniel Bedats**: Discovery of Ceres: How Gauss became an astronomer
12:45 *lunch*
17:00 **Tomáš Vítek**: Brouwer fixed point theorem, Borsuk-Ulam theorem and their geometric relation

17:30 **Radek Olšák**: Method of animation for solving olympiad geometry

18:00 **Cyril Matoušek**: Mathematical Description of Juggling

18:30 *dinner*

20:00 **Jiří Pavlů** & **Adolf Středa**: On permutations among polynomials with Niho type exponents

20:30 **Mikuláš Zindulka**: Definition and properties of iterative norms

Saturday 6th

8:00 *breakfast*

9:30 **Jan Černý**: Constructing the Petersen and Hoffman-Singleton graphs

10:00 **Grego Maroš**: n-dimensional rotations using geometric (Clifford) algebra

10:45 *coffee break*

11:15 **Jana Vráblíková**: Dual quaternions and space kinematics

12:00 **Dominik Krasula**: Restricted minimum condition for domains

12:45 *lunch*