

第4回情報数理セミナー

日時：2023年1月7日(土)～1月9日(月)

会場：小山工業高等専門学校 専攻科棟4階多目的ホール

プログラム

1月7日(土)

8:00～会場準備・諸注意

9:00～10:30 服部 京平 (新潟大学)

Rings of nilpotent elements of monomial derivations on polynomial rings

12:30～14:00 橋本 侑知 (東京電機大学)

効率的な超特異性判定アルゴリズムについて

14:30～16:00 品川 和雅 (茨城大学)

有限群の一様巡回群分解

～18:00 自由討論

1月8日(日)

9:30～会場準備・諸注意

10:00～11:30 高橋 祐太 (筑波大学)

Super Lie Groups and Harish-Chandra pairs

13:00～14:30 澤原 雅知 (埼玉大学)

On Du Val del Pezzo surfaces of Picard rank one over non-closed fields

15:00～16:30 金井 和貴 (新潟大学)

Hasse norm principle for M_{11} extensions

～18:00 自由討論

1月9日(月)

9:30～会場準備・諸注意

10:00～11:30 佐藤 宏平 (小山工業高等専門学校)

On modified tropical hyperfield

世話人:

神代 真也 (小山工業高等専門学校 一般科) 品川 和雅 (茨城大学 大学院理工学研究科)

長峰 孝典 (小山工業高等専門学校 一般科) 宮本 賢伍 (茨城大学 大学院理工学研究科)

本セミナーは JSPS 科研費 JP20K14302 および JP21K13782 の助成を受けたものです。

小山高専までのアクセスについては、下記をご覧ください。

バス時刻表 (小山高専-小山駅東口) <https://www.city.oyama.tochigi.jp/uploaded/attachment/221306.pdf>

アブストラクト

服部 京平 (新潟大学)

Rings of nilpotent elements of monomial derivations on polynomial rings

R を \mathbb{Q} を含む UFD とし, $R[\mathbf{x}] = R[x_1, \dots, x_n]$ を R 上の n 変数多項式環, D を $R[\mathbf{x}]$ 上の R 導分とする. D が $f \in R[\mathbf{x}]$ でべき零であるとは, $D^l(f) = 0$ となる $l \geq 1$ が存在するときをいい, そのような元全体を $\text{Nil } D$ で表す. 導分について, その核に関する結果はこれまでに多く知られているが, 一方で $\text{Nil } D$ に関する結果はほとんど知られていない. 本講演では, 2 変数多項式環 $R[x, y]$ 上の単項式導分の $\text{Nil } D$ の分類を与える. またその応用として, 3 変数多項式環 $R[x, y, z]$ 上の R 導分の核の極小生成系の濃度に上界がないことを示す.

橋本 侑知 (東京電機大学)

効率的な超特異性判定アルゴリズムについて

楕円曲線には通常曲線と超特異楕円曲線の二つのタイプが存在する. ある楕円曲線が与えられたとき, その楕円曲線が超特異楕円曲線であるかどうかを効率的かつ確定的に判定するアルゴリズムは, 暗号方式のパラメータ設定や楕円曲線のデータを送付し合うような暗号プロトコルを利用する際に安全性を保証する上で重要な役割を果たす. 上記のような楕円曲線の種類を判定するアルゴリズムは超特異性判定アルゴリズムと呼ばれる. 本発表では, 効率的な超特異性判定アルゴリズムについて解説する.

品川 和雅 (茨城大学)

有限群の一樣巡回群分解

G を有限群とする. $\mathcal{H} = (H_1, H_2, \dots, H_k)$ を G の部分群 (あるいは, 巡回部分群) の列とし, 各元 $g \in G$ について $g = h_1 h_2 \cdots h_k$ ($h_i \in H_i$) となる組 (h_1, h_2, \dots, h_k) の個数が g に依らず一定であるとき, \mathcal{H} を G の一樣群分解 (あるいは, 一樣巡回群分解) であると定義する. 特に, 一樣巡回群分解は有限群の一樣ランダムな元の効率的な生成に応用することができるため, さまざまな有限群に対する一樣巡回群分解を構成することは重要な研究課題である. 本講演では, まず任意の有限可解群が一樣巡回群分解を持つことを示す. また, 任意の有限群が一樣巡回群分解を持つことと, 任意の有限単純群が一樣群分解を持つことは同値であることを示す. したがって, 一樣巡回群分解を得るためには, 単純群の一樣群分解さえ構成できればよいことになる. 本研究は, 金井和貴氏, 宮本賢伍氏, 縫田光司氏との共同研究である.

高橋 祐太 (筑波大学)

Super Lie Groups and Harish-Chandra pairs

$\mathbb{Z}_2 = \{0, 1\}$ により次数付けられた対象 (リー群や代数群) は, スーパー (スーパー・リー群やスーパー代数群) と呼ばれる. スーパー・リー群は通常の (スーパーでない) リー群 G と, ある条件を満たす G -加群 V により構成されるという理論があり, この G と V のペアを Harish-Chandra pair と言う. この理論によりスーパーにおける対象を Harish-Chandra pair を通して考察することができる. 本発表では, この Harish-Chandra pair の理論について述べる.

澤原 雅知 (埼玉大学)

On Du Val del Pezzo surfaces of Picard rank one over non-closed fields

本講演では、講演者の論文 “Cylinders in canonical del Pezzo fibrations” において重要な役割を担う「非代数閉体上に定義された Du Val 特異点をもつピカル数 1 の del Pezzo 曲面」について解説する。より詳細には、関連する事柄について具体例を交えながら説明したのち、上述の論文の主結果を紹介する。時間の関係上、理論の雰囲気・イメージを伝える事にウエイトを置く予定である。(よって、厳密な証明等は説明できないかと思いますが、何卒ご容赦願います。)

金井 和貴 (新潟大学)

Hasse norm principle for M_{11} extensions

Hasse norm principle(HNP) は、代数体の拡大に対して局所的なノルムの束ね合わせと大域的なノルムの “ずれ” が存在しないことを表す原理であり、Hasse により巡回拡大に対して、成立することが示された (1931)。しかしながら、一般には不成立であり、成立する必要十分条件を与えることが重要な問題となる。今回、ガロア群が散在型有限単純群の一つである 11 点に作用するマシュー群 M_{11} となる代数体の拡大に対して、HNP が成立する必要十分条件を与えた。特にこの場合においては、HNP と 2 シロー部分群の構造が密接に関わることの解説を試みる。

佐藤 宏平 (小山工業高等専門学校)

On modified tropical hyperfield

Tropical hyperfield is a triple which consists of the set of complex numbers, tropical addition and usual multiplication, and was advocated by O. Viro. We modify this hyperfield so that the resulting set endowed with the addition and the multiplication is doubly distributive. Moreover, we show that the modified tropical hyperfield is “algebraically closed”. These results are joint work with Shinsuke Odagiri.