

第1回情報数理セミナー

日時：2021年10月23日(土)～10月24日(日)

対面開催の場合：小山工業高等専門学校 テクノ棟3階1L教室

オンライン開催の場合：Zoom

プログラム

10月23日(土)

9:00～ 会場準備・諸注意

10:00～12:00 長峰 孝典 (小山工業高等専門学校)

A family of strongly invariant algebras

13:30～15:30 神代 真也 (小山工業高等専門学校)

Graded filtrations and ideals of reduction number two

16:00～18:00 金井 和貴 (新潟大学)

First obstruction to the Hasse norm principle and norm one tori

18:00～18:30 自由討論

10月24日(日)

9:30～ 会場準備・諸注意

10:00～12:00 佐藤 宏平 (小山工業高等専門学校)

足利連分数展開について

13:30～15:30 宮本 賢伍 (茨城大学)

Finite Heller components for symmetric order over a complete discrete valuation ring

16:00～18:00 品川 和雅 (茨城大学)

平方剰余に基づく秘密計算

18:00～18:30 自由討論

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 工学部)

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 工学部)

本セミナーは JSPS 科研費 JP20K22317 の助成を受けたものです。

アブストラクト

長峰 孝典 (小山工業高等専門学校)

A family of strongly invariant algebras

本講演の目的は、アフィン代数多様体における消去問題に対して、次数構造を用いた新たな研究手法を与えることである。消去問題とは、アフィン代数多様体 X, Y が $X \times \mathbb{A}^1 \cong Y \times \mathbb{A}^1$ をみたすとき $X \cong Y$ となるかを問う問題である。座標環上に定まる次数構造に着目することで、消去問題が肯定的となるための条件を与えることができる。本講演では、その証明を丁寧に与え、応用として消去問題が肯定的となるアフィン代数多様体の無限族を構成する。

神代 真也 (小山工業高等専門学校)

Graded filtrations and ideals of reduction number two

本講演では可換環におけるヒルベルト関数の解析を目指す。そのために新たなフィルトレーションを考察する。有名なフィルトレーションの構成方法に（次数付）ブルバキ完全列があり、重複度公式の導出などに用いられる。しかしながら、ブルバキ完全列では最高次でないヒルベルト係数を調べることは難しい。そこで本講演では、新たなフィルトレーションの構成方法を考察する。応用として節減数が2であるイデアルについて、ヒルベルト係数に関する不等式を与える。

金井 和貴 (新潟大学)

First obstruction to the Hasse norm principle and norm one tori

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、不成立となる必要十分条件を与えることが重要な問題となる。Drakokhrust–Platonov (1986) は HNP に対して、First obstruction と呼ばれる不変量を導入し、HNP の研究に大きな進展をもたらした。今回、この First obstruction の理論と Voskresenskii (1969)、遠藤静男氏と宮田武彦氏 (1975)、Colliot-Thelene–Sansuc (1977) らによる代数的トーラスの理論と、計算機によるコホモロジー論的不変量の計算を併せて用いることで、15 次以下の代数体に対して、HNP が不成立となる必要十分条件を分解群による条件で与えることに成功した。この結果について、具体例を中心とした解説を試みる。星明考氏 (新潟大学)、山崎愛一氏 (京都大学) との共同研究。

佐藤 宏平 (小山工業高等専門学校)

足利連分数展開について

複素 2 次元 Gorenstein 商特異点に対しては極小特異点解消が存在し、特に巡回商特異点の場合にはそれと Hirzebruch–Jung 連分数との間に対応があることが知られている。これらに対する拡張となる、クレパント特異点解消や足利連分数について説明し、足利連分数から得られる藤木・岡の特異点解消についての諸性質について述べる。

宮本 賢伍 (茨城大学)

Finite Heller components for symmetric order over a complete discrete valuation ring

Let \mathcal{O} be a complete discrete valuation ring, κ the residue field of \mathcal{O} , A a symmetric \mathcal{O} -order.

In this talk, we report that if A has only finitely many Heller lattices, which are special CM modules obtained by taking projective covers, then the configurations of components of the stable Auslander–Reiten quiver of A without loops is determined by infinite Dynkin diagrams and its admissible groups. This result is an analogue of Riedtmann–Todorov configurations for finite-dimensional self-injective representation-finite algebras.

品川 和雅 (茨城大学)

平方剰余に基づく秘密計算

秘密計算とは、多人数で計算を行う多者間計算であり、各自の入力情報を他のプレイヤーに対して秘匿するものである。本講演では秘匿同時メッセージ (Private Simultaneous Messages) という種類の秘密計算を紹介する。特に、平方剰余の性質を用いた秘匿同時メッセージに関する我々の研究成果を紹介する。なお、本成果は江利口礼央氏 (東京大学) と縫田光司氏 (九州大学) との共同研究であり、2021 年暗号と情報セキュリティシンポジウム (SCIS2021) において発表したものである。