第 9 回情報数理セミナー プログラム

日時：2025 年 8 月 18 日 (月) ～ 8 月 19 日 (火)
会場: 日本大学理工学部駿河台キャンパス タワー・スコラ 2 階 S201

プログラム

8 月 18 日 (月)

9:00～ 会場準備・諸注意・自由討論

10:30～12:30 金井 和貴 (呉工業高等専門学校)
Rationality problem for multinorm one tori

14:30～16:30 今村 浩二 (熊本大学)
マトロイド理論における臨界問題について

～18:30 自由討論

8 月 19 日 (火)

9:00～ 会場準備・諸注意・自由討論

10:30～12:30 荒武 永史 (小山工業高等専門学校)
一般化された代数のスペクトラムおよび層表現について

14:30～16:30 中村 周平 (茨城大学)
NIST 耐量子計算機暗号標準化計画の追加署名方式プロジェクト第 2 ラウンドにおける多変数多項式署名方式 UOV とその変種の動向

～18:30 自由討論

世話人
金井 和貴 (呉工業高等専門学校 自然科学系分野)
神代 真也 (大阪工業大学工学部 一般教育科)
品川 和雅 (筑波大学 システム情報系)
長峰 孝典 (日本大学理工学部 数学科)
宮本 賢伍 (茨城大学大学院 理工学研究科)

本セミナーは, 以下の助成を受けています.
JSPS 科研費 (KAKENHI) 若手研究 JP21K13782 (研究代表者: 品川 和雅)
JSPS 科研費 (KAKENHI) 若手研究 JP24K16909 (研究代表者: 神代 真也)
JSPS 科研費 (KAKENHI) 若手研究 JP24K16885 (研究代表者: 宮本 賢伍)
JSPS 科研費 (KAKENHI) 若手研究 JP25K17239 (研究代表者: 長峰 孝典)
国立高等専門学校機構 研究ネットワーク形成事業 (重点支援) (研究代表者: 金井 和貴)

アブストラクト

金井 和貴 (呉工業高等専門学校)

Rationality problem for multinorm one tori

代数的トーラスの安定有理性は, 2 次元の場合は Voskresenskii (1967), 3 次元の場合は Kunyavskii (1990), 4, 5 次元の場合は星–山崎 (2017) によって分類されているが, より高次の場合は未解決である. 代数的トーラスの中でも, 体の n 次拡大のノルムに付随して得られるノルム 1 トーラスは $n-1$ 次元となり, 高次の例を与え, その有理性は遠藤–宮田 (1975) や Colliot-Thélène–Sansuc (1987) などにより古くから研究されてきた.

本講演では, ノルム 1 トーラスの自然な一般化として, 体 k 上の有限次拡大の有限個の直積 (有限エタール代数) のノルムに付随して得られるマルチノルム 1 トーラスの有理性問題を扱う. 特に, 直積因子の合併体のガロア閉包を L としたとき, (1) 拡大次数 $[L:k]$ が素数べき (2) L/k のガロア群がべき零群の場合に対して, 安定有理性問題を解決したことを報告する. 沖泰裕氏 (北海道大学), 長谷川寿人氏と共同研究.

今村 浩二 (熊本大学)

マトロイド理論における臨界問題について

有限体上のベクトル空間において，所与の部分集合と排反な部分空間の最大次元はいくつだろうか．この問題は 1970 年に H. Crapo と G.-C. Rota によって「臨界問題」として定式化された．臨界問題は，符号理論における被覆問題や，グラフ理論における彩色問題など，極値的組合せ論における重要な問題を特別な場合として含んでいる．本講演では，符号理論とマトロイド理論における臨界問題の定式化と，グラフの彩色問題との関係について紹介する．

荒武 永史 (小山工業高等専門学校)

一般化された代数のスペクトラムおよび層表現について

可換環 A に対し、Zariski スペクトラム $\mathrm{Spec}(A)$ の構造層 $\mathcal{O}$ によって、A が大域切断全体 $\mathcal{O}(\mathrm{Spec}(A))$ として復元されるのは周知の事実である。一般に、環付き空間を位相空間 X とその上の可換環の層 F の組 (X, F) で表すとき、先の事実から「任意の可換環は、ある局所環付き空間 (X, F) の構造層の大域切断全体 $F(X)$ として表現できる」ことがわかる。それでは、局所環付き空間ではなく、“整域付き空間”（= 構造層の任意の茎が整域であるような環付き空間）や “体付き空間” によって表現されるような可換環はどのようなものだろうか？ 古くからの “環の層表現” の研究により、これらの可換環はそれぞれ “domain representable ring”, “von Neumann 正則環” として特徴づけられることが知られている。

上述の層表現においては、「可換環の圏と○○付き空間の圏の間の随伴」という一般化された意味でのスペクトラムが用いられている。私の研究では、圏論的論理学の文脈で知られているスペクトラムの一般化の理論に基づいて、良い層表現を持つような（一般化された意味での）代数について調べている。本講演では、“整域の層” や “体の層” による層表現においてスペクトラムの変種がどのように現れるかを説明した後、局所有限表示可能圏の任意の対象へとスペクトラムの構成が一般化できることを圏論的論理学に触れつつ説明する。そして最後に、大域切断函手とスペクトラム函手の随伴が冪等性を満たすとき、「良い層表現を持つような代数のクラス」がいくつかの圏論的構成で閉じることを具体例を使って概説する。

中村 周平 (茨城大学)

NIST 耐量子計算機暗号標準化計画の追加署名方式プロジェクト第 2 ラウンドにおける多変数多項式署名方式 UOV とその変種の動向

公開鍵暗号において現在広く利用されている方式は, 大規模な量子計算機の実現により危殆化する可能性が指摘されており, そのため, 量子計算機でも解くことが困難な数学的問題に基づく新たな暗号方式の設計が重要な課題となっている. NIST（米国標準技術研究所）では, この耐量子計算機暗号の標準化プロジェクトを 2017 年に開始しており, 現在, メインプロジェクトの第 4 ラウンドの終了時点で, 格子暗号, ハッシュ暗号, 符号暗号などから計 5 件の方式が選定されている. 一方, 2023 年からは署名方式のみを対象とした追加プロジェクトも開始され, 2024 年 10 月にはその第 2 ラウンドに進む方式が発表された. 多変数多項式暗号は, 短い署名長や高速な検証を可能にする点から署名方式の有力候補の一つとされており, UOV およびその変種である MAYO, SNOVA, QR-UOV の計 4 件がこの第 2 ラウンドに選ばれている. 本講演では, まず多変数多項式暗号の基礎を概観し, NIST 標準化計画の追加プロジェクトに残るこれら 4 つの署名方式の特徴を整理する. その後, 最近の研究成果も含め, これらの方式に対する攻撃手法を可能な限り網羅的に紹介し, 現時点での安全性評価について報告する.