

現代代数学と異分野連携 メンバー構成

Division of Modern Algebra and Cooperation with Engineering

設置期間：2016年10月1日～2021年3月31日

所属	職位	氏名	学位	主な研究分野
理工学部数学科(部門長)	教授	伊藤浩行	博士(理学)	代数幾何学・応用代数学
理学部第一部数学科	教授	眞田克典	理学博士	多元環のコホモロジー論・多元環の表現論
理学部第一部数学科	教授	木田雅成	Ph.D	整数論
理学部第一部応用数学科	教授	佐藤洋祐	Ph.D	計算機代数・計算論理
理学部第一部応用数学科	教授	関川浩	博士(数理科学)	計算機代数
理工学部数学科	准教授	青木宏樹	博士(理学)	保型形式
理工学部数学科	准教授	八森祥隆	博士(数理科学)	代数学・整数論
理工学部情報科学科	准教授	宮本暢子	博士(経営工学)	離散数学・組合せデザイン
理学部第一部数学科	准教授	功刀直子	博士(理学)	有限群の表現論
理学部第二部数学科	准教授	佐藤隆夫	博士(数理科学)	代数的位相幾何学
理工学部教養	講師	中村隆	博士(数理学)	数論・確率論
理工学部数学科	講師	小松亨	博士(理学)	代数的数論・数論幾何学
理工学部数学科	講師	加塩朋和	博士(理学)	整数論
理工学部数学科	講師	大橋久範	博士(理学)	代数幾何学
理工学部電気電子情報工学科	講師	五十嵐保隆	博士(学術)	理論的暗号解読
理学部第一部数学科	嘱託助教	板垣智洋	博士(理学)	多元環の表現論
理学部第一部数学科	嘱託助教	板場綾子	博士(理学)	多元環の表現論、非可換代数幾何学
理学部第二部数学科	嘱託助教	野村次郎	博士(理学)	代数的整数論
理工学部数学科	嘱託助教	松本雄也	博士(数理科学)	代数幾何学
理工学部情報科学科	嘱託助教	地寄頌子	博士(理学)	離散数学

設置目的

代数学内部の相互連携による代数学研究の深化と、20世紀後半からの代数学ベースの新しい応用分野との連携を発展させると共に、未来へ向けた新しい連携分野を発掘することを目的とする。

組織の現状

基礎研究3グループ

- ・整数論・数論幾何学
- ・可換環論・代数幾何学
- ・群論・表現論・保型形式論

応用研究3グループ

- ・計算機代数・計算論理
- ・暗号理論・符号理論
- ・離散数学・組合せデザイン

将来展望

新たな代数学ベースの異分野連携分野の開拓と、基礎研究から応用研究まで代数学研究の拠点形成を目指す。

研究成果その2

純粹数学

代数多様体論
可換環論

相互作用

代数的整数論
岩澤理論

相互作用

保型形式論
表現論

応用数学

超平面配置
Difference systems
of set の構成

数値解析
線形アルゴリズム

Artin-Schreier拡大塔を
利用した巨大有限体の構成

```

Algorithm
Input:  $r, (s_1, \dots, s_{2r}), (t_1, \dots, t_{2r})$ 
Output:  $(n_1, \dots, n_{2r})$ 
Procedure:
1.  $M_i^0 \leftarrow t_i (1 \leq i \leq 2^r), U^0 \leftarrow 1;$ 
2. for  $(j = 1, j \leq r, j = j + 1);$ 
   for  $(i = 1, i \leq 2^{j-1}, i = i + 1);$ 

$$M_i^j \leftarrow \begin{pmatrix} M_{2i-1}^{(j-1)} & M_{2i}^{(j-1)} \\ M_{2i-1}^{(j-1)} U^{(j-1)} & M_{2i-1}^{(j-1)} + M_{2i}^{(j-1)} \end{pmatrix}$$


$$U^j \leftarrow \begin{pmatrix} 0 & U^{(j-1)} \\ (U^{(j-1)})^2 & U^{(j-1)} \end{pmatrix}$$

3.  $(n_1, \dots, n_{2r}) \leftarrow (s_1, \dots, s_{2r}) M_1^r$ 
4. return  $(n_1, \dots, n_{2r})$ 
    
```

連携分野

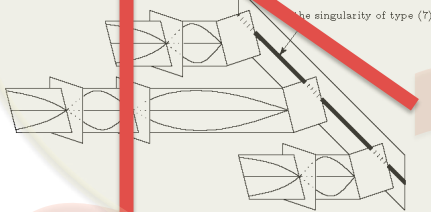
代数的符号
公開鍵暗号

新しい疑似乱数生成器ASTの構成
・長大な周期を持つ疑似乱数を生成
・MersenneTwistorを超える性能

数理シミュレーション

研究成果その1

代数多様体
代数方程式の解空間



特異点

- ・群スキーム商による新理論の構築
- ・正標数でのMcKay対応

Groebner基底

計算機代数、数式処理

K3曲面

Enriques曲面

- ・自己同型群の決定
- ・複素力学系の研究

Calabi-Yau多様体

- ・周期写像の記述
- ・病的現象の究明

(準)楕円曲面

- ・切断のなす群の構造決定
- ・曲面論的性質の解明

モジュライ空間
シンプレクティック幾何

物理学

- ・ミラー対称性
- ・超弦理論
- 数理物理学

暗号理論

- 情報セキュリティ
- 符号理論

未知の領域へ

学習理論
データサイエンス

