

# Division of Modern Algebra and Cooperation with Engineering

Project term : October 1, 2016~March 31, 2021

Project member :

Affiliation	Job title	Name	Academic degree	Main research field
Department of Mathematics Faculty of Science and Technology	Professor	Hiroyuki Ito (Leader)	Doctor(Science)	Algebraic geometry Applied algebra
Department of Mathematics Faculty of Science Division I	Professor	Katsunori Sanada	Doctor of Science	Ring theory
Department of Mathematics Faculty of Science Division I	Professor	Masanari Kida	Ph.D	Number theory
Department of Applied Mathematics Faculty of Science Division I	Professor	Yosuke Sato	Ph.D	Computer algebra
Department of Applied Mathematics Faculty of Science Division I	Professor	Hiroshi Sekigawa	Doctor (Mathematical Science)	Computational Mathematics
Department of Mathematics Faculty of Science and Technology	Associate professor	Hiroki Aoki	Doctor(Science)	Automorphic forms
Department of Mathematics Faculty of Science and Technology	Associate professor	Yoshitaka Hachimori	Doctor (Mathematical Science)	Algebra Number theory
Department of Information Sciences Faculty of Science and Technology	Associate professor	Nobuko Miyamoto	Ph.D (Management Science and Engineering Course)	Discrete mathematics Combinatorial designs and their applications
Department of Mathematics Faculty of Science Division I	Associate professor	Naoko Kunugi	Doctor(Science)	Representation theory
Department of Mathematics Faculty of Science Division II	Associate professor	Takaoh Sato	Doctor (Mathematical Science)	Algebra, Geometry
College of General Education Faculty of Science and Technology	Junior associate professor	Takashi Nakamura	Doctor (Mathematical Science)	Analytic number theory
Department of Mathematics Faculty of Science and Technology	Junior associate professor	Toru Komatsu	Doctor(Science)	Number theory
Department of Mathematics Faculty of Science and Technology	Junior associate professor	Tomokazu Kashio	Doctor(Science)	Number theory
Department of Mathematics Faculty of Science and Technology	Junior associate professor	Hisanori Ohashi	Doctor(Science)	Algebraic geometry
Department of Electrical Engineering Faculty of Science and Technology	Junior associate professor	Yasutaka Igarashi	Doctor(Philosophy)	Information security Cryptanalysis
Department of Mathematics Faculty of Science Division I	Assistant professor	Tomohiro Itagaki	Doctor(Science)	Algebra
Department of Mathematics Faculty of Science Division I	Assistant professor	Ayako Itaba	Doctor(Science)	Representation theory of algebras Noncommutative algebraic geometry
Department of Mathematics Faculty of Science Division II	Assistant professor	Jiro Nomura	Doctor(Science)	Algebraic Number Theory
Department of Mathematics Faculty of Science and Technology	Assistant Professor	Yuya Matsumoto	Doctor (Mathematical Science)	Algebraic Geometry
Department of Information Sciences Faculty of Science and Technology	Assistant professor	Shoko Chisaki	Doctor(Science)	Combinatorial designs and their applications

## Objectives

To research and develop algebra itself and algebra based engineering, also to find new engineering fields cooperation with algebra, thereby making a contribution to mathematics and engineering.

## Research Groups

### Pure Mathematics Groups

- Number Theory and Arithmetic Geometry
- Commutative Algebra and Algebraic Geometry
- Group Theory, Representation Theory and Automorphic Forms

### Applied Mathematics Groups

- Computer Algebra and Computational Mathematics
- Cryptology and Coding Theory
- Discrete Mathematics and Combinatorial Design

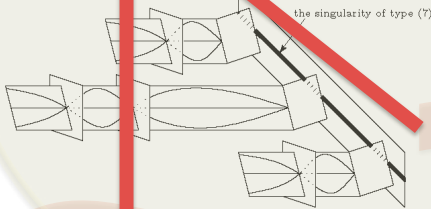
## Future Plan

Developing a new cooperative research fields on algebra. Becoming a research center for algebra and algebra based engineering.

## Research Contents 2

### Algebraic Varieties

Systems of Algebraic Equations



### Singularities

- New theory using group scheme quotients
- McKay correspondence in positive characteristic

Groebner basis

Computer algebra  
Symbolic calculation

K3 surfaces

Enriques surfaces

- Determination of automorphism groups
- Study on Complex Dynamical Systems

Calabi-Yau varieties

- Description of period maps
- Study on pathological phenomena

(Quasi-)Elliptic surfaces

- Determination of Mordell-Weil groups
- Surface theoretic characterization

Unknown cooperative fields

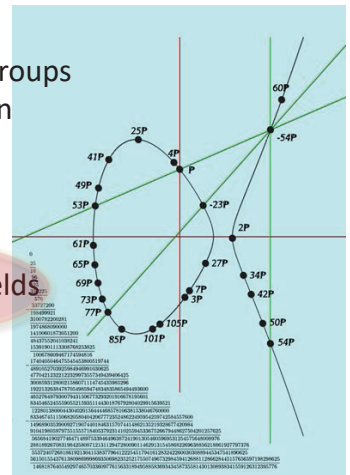
Learning theory  
Data science

Physics

- Mirror Symmetry
  - Superstring theory
- Mathematical Physics

Cryptography

- Information security
- Coding theory



## Research Contents 2

Pure Mathematics

Algebraic Varieties  
Commutative Algebras

Algebraic Number Theory  
Iwasawa Theory

Automorphic Forms  
Representation Theory

Applied Mathematics

Hyperplane arrangement  
Construction of Difference  
systems of sets

Numerical Analysis  
Linear Algorithms

Construction of huge finite fields  
using Artin-Schreier Tower

Beyond Mathematics

Algebraic Coding Theory  
Public Key Cryptography

New Pseudo-Random Number Generator AST  
▪ Long Period ▪ Beyond MersenneTwistor

Mathematical  
Simulations

Algorithm  
Input:  $r, (s_1, \dots, s_{2^r}), (t_1, \dots, t_{2^r})$   
Output:  $(u_1, \dots, u_{2^r})$   
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 ( $i = 1, i \leq 2^{r-j}, i = i + 1$ );  
    $M_{2i}^j \leftarrow \begin{pmatrix} M_i^{j-1} & M_{2i}^{j-1} \\ M_i^{j-1} U^{j-1} & M_{2i}^{j-1} + M_{2i}^{j-1} \end{pmatrix}$   
    $U^j \leftarrow \begin{pmatrix} U^{j-1} & U^{j-1} \\ U^{j-1} & U^{j-1} \end{pmatrix}$   
3.  $(u_1, \dots, u_{2^r}) \leftarrow (s_1, \dots, s_{2^r}) M_1^r$   
4. return  $(u_1, \dots, u_{2^r})$