14

東京理科大学 TOKYO UNIVERSITY OF SCIENCE

RIST TUS Research Institute for Science & Technology

先端的代数学融合研究部門における基礎研究の一例

研究推進機構　総合研究院　先端的代数学融合研究部門

▶ 研究概要

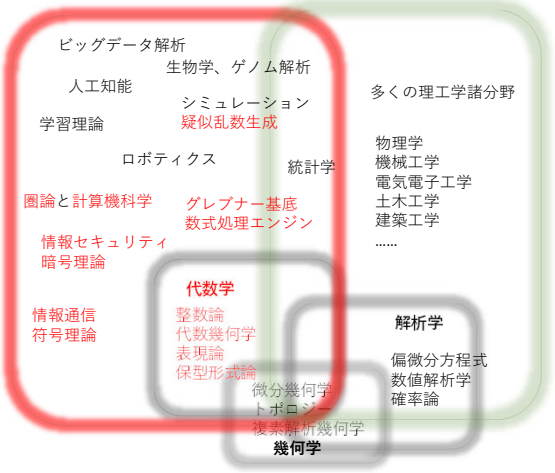
・代数学内部の相互連携による代数学研究の進化(理論構築)

「正標数代数幾何学と環論」と「総合的視点からの整数論」の研究拠点化

・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(実践応用)

計算機代数学、符号・暗号理論、応用代数学、代数統計学、DXとの連携

・数理解析連携研究部門、DX研究部門、東北大学数理科学共創社会センターと連携



▶ 研究開発成果

■ 正標数代数幾何の研究　～ 多項式の共通零点集合である代数多様体とそこに現れる特異点が中心的研究対象

・正標数有理二重特異点の理解 ---- 正多面体 (Platonic solid) の対称性を記述する2次特殊線形群SL_2(C)の作用により得られる商特異点に関して正標数における諸性質の究明

・正標数商特異点の一般理論構築 ---- 有理二重点の理解に必要な野生的群作用と導分商に関する理論構築、特異点のモジュライに関する理解

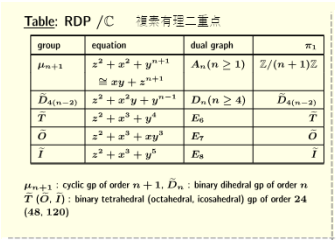
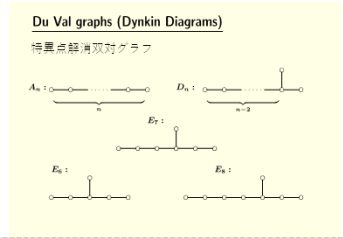
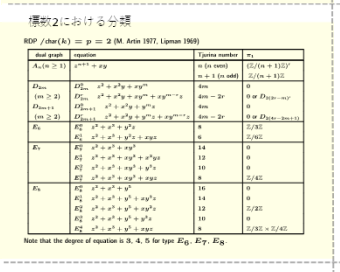


Table: RDP /ℂ　複素有理二重点

group	equation	dual graph	π_1
μ_{n+1}	$z^2+x^2+y^{n+1}$ $\cong xy+z^{n+1}$	$A_n (n \geq 1)$	$\mathbb{Z}/(n+1)\mathbb{Z}$
$\tilde{D}_{4(n-2)}$	$z^2+x^2y+y^{n-1}$	$D_n (n \geq 4)$	$\tilde{D}_{4(n-2)}$
$\tilde{T}$	$z^2+x^3+y^4$	E_6	$\tilde{T}$
$\tilde{O}$	$z^2+x^3+xy^3$	E_7	$\tilde{O}$
$\tilde{I}$	$z^2+x^3+y^5$	E_8	$\tilde{I}$

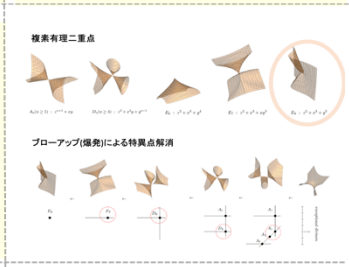
μ_{n+1} : cyclic gp of order $n+1$, $\tilde{D}_n$: binary dihedral gp of order n
$\tilde{T}$ $(\tilde{O}, \tilde{I})$: binary tetrahedral (octahedral, icosahedral) gp of order 24 (48, 120)

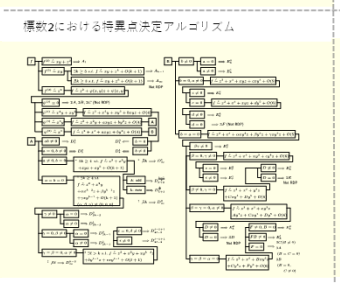


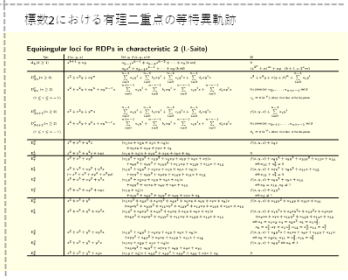

標数2における分類

dual graph	equation	Tjurina number	π_1
D_{2m} $(m \geq 2)$	$z^2+x^2y+xy^m$	$4m$	0
D_{2m+1} $(m \geq 2)$	$z^2+x^2y+y^m+xy^{m-1}z$	$4m-2r$	0 or $D_{2(2m-m)}$
E_6	$z^2+x^3+y^4z$	8	$\mathbb{Z}/3\mathbb{Z}$
E_7	$z^2+x^3+xy^3$	14	0
	$z^2+x^3+xy^3+x^2yz$	12	0
	$z^2+x^3+xy^3+y^3z$	10	0
	$z^2+x^3+xy^3+xyz$	8	$\mathbb{Z}/4\mathbb{Z}$
E_8	$z^2+x^3+x^2y^3$	16	0
	$z^2+x^3+x^2y^3+xy^3z$	14	0
	$z^2+x^3+x^2y^3+xy^2z^2$	12	$\mathbb{Z}/2\mathbb{Z}$
	$z^2+x^3+x^2y^3+y^3z$	10	0
	$z^2+x^3+x^2y^3+xyz$	8	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Note that the degree of equation is 3, 4, 5 for type E_6, E_7, E_8.




標数2における特異点決定アルゴリズム



■ 巨大有限体の構成と擬似乱数生成器の開発 ～ MTを超える

・有限体係数のArtin-Schreier型方程式 $X^p - X - \alpha = 0$ により有限体構成法を再帰的に続けることで巨大有限体
$\mathbf{F}_p \to \mathbf{F}_{p^p} \to \mathbf{F}_{p^{p^2}} \to \mathbf{F}_{p^{p^3}} \to \cdots \quad \mathbf{F}_{p^{p^r}}$ を構成

・(再帰構造を持つ)巨大有限体と効率的計算量の演算アルゴリズム

・巨大次数の原始多項式を生成、性能的にはMersenne Twistor

$$x_{j+n} = x_{j+m} + (x_j^u | x_{j+1}^l) A \quad (j = 0, 1, \ldots)$$

を凌駕！

・2元体上の2^r 次正方行列 (r=11のとき、位数～2^2048)

・Twistor MT19937と同性能 (r=14のとき)

Algorithm
Input: $r, (s_1, \ldots, s_{2^r}), (t_1, \ldots, t_{2^r})$
Output: $(u_1, \ldots, u_{2^r})$
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 $(i = 1, i \leq 2^{r-j}, i = i+1)$;

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

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

3. $(u_1, \ldots, u_{2^r}) \leftarrow (s_1, \ldots, s_{2^r}) M_1^r$
4. return $(u_1, \ldots, u_{2^r})$

▶ 今後の展開

・ポストコロナにおける新たなスタイルでの研究交流の推進により「正標数代数幾何学と環論」と「総合的視点からの整数論」に関する世界的研究拠点化

・基礎(理論構築)と(応用実践)の先にある異分野連携研究の推進

・若手育成として「代数学の萌芽」(若手中心の成果発表)と「代数学の広がり」(大学の枠を超えた大学院生の研究交流)の継続

・数理解析研究部門、DX研究部門、東北大学数理科学共創社会センターとの連携の強化

【連絡先】研究部門長（創域理工学部数理科学科）　伊藤　浩行
ito_hiroyuki@rs.tus.ac.jp