数理解析研究所講究録
第721巻 1990年 142-159

Mordell-Weil lattice と
意味のある代数方程式の新しい型

立教大理学部 塩田徹治

1. 序

代数方程式を幾何学的に当って、まず次の3つの概念の関係を思いおこしたい。 k_0 を1つの体とする。

(1) 代数方程式

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n = 0$$

$$(a_1, \cdots, a_n \in k_0)$$

(2) 有限次 Galois 拡大

$$K / k_0$$

(3) $k = \overline{k_0}$ (代数的閉包)として). 有限 Galois set

M と、Galois equivariant map $s : M \to k$」

これらの関係は、周知のように次の如くである:

まず(1)から出発するとき、(f を分離的として)

K = $f(X)$ の分解体

$M = \{$根 $\alpha_1, \cdots, \alpha_n\}$ $\quad s : M \hookrightarrow k$

として、(2), (3) の data が自然に一意的に定まる。

次に (2) から出発すると、k の生成元 α をとうぶと $k = k_0(\alpha)$ とできる。そこで、

$f(X) = \alpha$ の k_0 上の最小多項式

$M = \{f(X)$ の根$\} = \{\alpha$ の k_0-共役$\}$.

とすれば、(1), (3) の data がきまる。注意すべきは、ここでは、これらの data は 生成元のとり方によっていることである。また、(1) ⇒ (2) ⇒ (1) と、考えるとき、一般に、もとの f に戻らず、しかも、次数 n も、大きくなってしまう (たとえば、$n=3$ で切うかなようん)。

最後に、有限 $Gal(k/k_0)$-set M からうこうれると、

$k = k_0(P \mid P \in M)/k_0$ Galois 拡大

かつ、そうん、Galois equiv. map. $s : M \longrightarrow k$ があれば、Galois 理論より、

$$f(X) = \prod_{P \in M} (X - s(P)) \in k_0[X]$$

である。k_0 を、$f(X)$ の分解体とすると、$k_0 \subset k$. s が $M \xrightarrow{1:1} k$ ならば、$k_0 = k$.

さて、"意義のある" 代数方程式 とは、もちろん定義のできない主観的な響きの言葉だが、とりあえず、数学を豊かにする内容のある方程式、としておこう。

まず、注目知られているものを幾つか例示すると、

1) 低次の方程式 (1, 2, 3, 4次まで). これらが数学の発展にうえた影響は測り知れない.

2) 一般 n 次方程式

$a_1, \cdots, a_n$ を基礎の体, たとえば $\mathbb{Q}$ 上代数的に独立とし, $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in k_0[X]$, $k_0 = \mathbb{Q}(a_1, \cdots, a_n)$, 解を $\alpha_1, \cdots, \alpha_n$ とすると

$$K = k_0(\alpha_1, \cdots, \alpha_n) = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$$

$a_i = \alpha_1 \cdots \alpha_n$ の i 次基本対称式

(根と係数の関係)

$$\mathrm{Gal}(K/k_0) = \mathfrak{S}_n \quad n \text{ 次対称群}.$$

となる. $K^{\mathfrak{S}_n} = k_0$ であるから, より強く

$$\mathbb{Q}[\alpha_1, \cdots, \alpha_n]^{\mathfrak{S}_n} = \mathbb{Q}[a_1, \cdots, a_n]$$

(対称式の基本定理: $\mathbb{Q} \to \mathbb{Z}$ としてよい.)

これは, 多少の変更を加えて, 次のように述べることもできる:

$a_1 = 0$ とし, $a_2, \cdots, a_n$ は代数的独立として おくと, $\alpha_1 + \cdots + \alpha_n = 0$. このとき

$$K = k_0(\alpha_1, \cdots \alpha_n) = \mathbb{Q}(\alpha_2, \cdots, \alpha_n)$$

$$\mathrm{Gal}(K/\mathbb{Q}(a_2, \cdots, a_n)) = \mathfrak{S}_n = W(A_{n-1})$$

$$\mathbb{Q}[\alpha_2, \cdots, \alpha_n]^{W(A_{n-1})} = \mathbb{Q}[a_2, \cdots, a_n]$$

ここで, $W(A_{n-1})$ は, A_{n-1} 型の Weyl 群 (cf. Bourbaki, Alg. de Lie Ch 4-6). 最後の式は, reflection group に関する Chevalley

の定理の、特別な場合と みなすことができる。

上の 1), 2) とは、趣を異にするが、素数のある代数方程式の例として、

3) 円分方程式　$x^n = 1$.

　2項方程式　$x^n = a$.

前者は、円分体の理論へ、後者は、巡回拡大ないし Kummer 拡大の理論へと、人を導く。一つの見方には、これは、乗法群 G_m の n等分点の方程式、あるいは、n乗写像の核ないし、一般に a の逆像を記述する方程式 以外ならない。この見えから 次の 4), 5) は 自然な拡張である

4) 楕円曲線(楕円関数)の等分方程式、および isogeny (変換の理論)。

これは、現在にも重要な研究対象である modular 関数, modular curves, およびそれに関連する様々の数論的研究の発祥の地である。(志村・谷山: "近代的整数論"、はじめの歴史、を参照されたい。)

この場合、楕円曲線 E/k_0 の n等分点のなす set $E[n] = \{P \in E(\bar{k}_0) \mid nP = 0\}$ は、群 ($\simeq (\mathbb{Z}/n)^2$ if $\mathrm{Char} \nmid n$) となるので、単なる Galois set ではなく、Galois module であり、Galois 表現

$$\rho : Gal(k/k_0) \longrightarrow Aut(E[n]) = GL_2(\mathbb{Z}/n)$$

から より自然かつ重要な研究対象 となることは、周知の通りである。

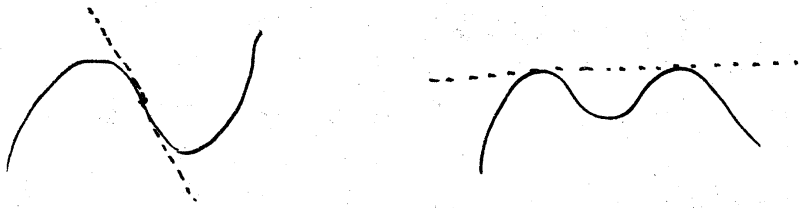
5). 4) の高次元アーベル多様体への拡張。

これらについては、これ以上ふれないが、ただ、等分点、すなわち、有限位数の点が主役で、無限位数のものは、考えられていないことを注意しておきたい。

以上の 3), 4), 5) とは、少し流れを異にして、より幾何学的な観点から よく研究された古典的な例として、

イ) 平面3次曲線の 9コの変曲点。

ロ) 平面4次曲線の 28本の double tangents



ハ) 3次曲面 ($\subset \mathbb{P}^3$) 上の 27本の lines, がある。

これらの有限集合は、曲線ないし曲面の定義体 k を k_0 とすると、$Gal(k/k_0)$-set である。解論の初期から、(たとえば、Jordan の"置換群論" 以来) 群論と Combinatorics の代表的な例として、(単なる例以上のものとして) 扱われている。(cf Weber: Lehrbuch der Algebra; v.d. Waerden: Alg. Geometrie)

さて、イ)は、楕円曲線の3分点に他ならず、前記4)の特別な例ともみなされる。また ロ)は、4次曲線(種数3)のヤコビ多様体Jの2等分点と関係し、従って、問題の群は $SL_2(\mathbb{Z}/3)$ 又は $Sp(6, \mathbb{Z}/2)$ (もしくはその部分群)となる。ハ)は、直接アーベル多様体の等分点とは関係なく、これは、より一般に、del Pezzo surface と呼ばれる有理曲面上の第1種例外曲線の理論に拡張される。(cf. Manin: Cubic Forms.)。ハの群は、$W(E_6)$ で、特数2の非可換単純群(位数 $2^6 \cdot 3^4 \cdot 5$)を含む。(k_0 が"generic"なとき。)

後にふれるように、ロ)、ハ)は、ある楕円曲線の無限位数の点と関係づけることができ、その観点から、この古典的理論に新しい光をあてることができる。(本文末尾、補)

より一般に、我々は、閉数体上の楕円曲線の Mordell-Weil lattice から、自然な finite Galois sets および代数的な方程式を定義することができ、その応用として、たとえば ① $\mathbb{Q}(t)$ 上(比較的)高い rank をもつ楕円曲線の構成(+ explicit basis)や ② "大きな"有限ガロア表現の構成、③(特別な場合として)円分体の無限次拡大、などを得ることができる。

2. Mordell-Weil Lattices.

この理論の詳細は、準備中であるが、概略は、Proc. Japan Acad. 65A. (1989) の "Mordell-Weil lattices and Galois representation, I, II, III", あるいは、同題の代数学シンポジウム報告集 (1989夏、北海) 内収の note を参照されたい。ここでは、その一部を述べる。まず記号

k : 任意標数の代数的閉体.

$K = k(C)$: k 上の曲線 C の関数体, i.e. 1変数関数体,

E/K : K 上定義された楕円曲線. たとえば,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$(a_1, \cdots, a_6 \in K)$$

のような Weierstrass form に表されたものと考えてよい.

$E(K)$: E の K-有理点のなす群.

$= \{(x, y) \mid$ 上式をみたす $x \in K, y \in K$ の組$\} \cup \{0\}$.

$f : S \longrightarrow C$, E/K の Kodaira-Néron model.

(即ち. S は, (k 上の) 楕円曲面, f は, その elliptic fibration を与える morphism & f の generic fibre $= E/K$)

(仮定) f は少くとも1つ singular fibre をもつ. 即ち f は non-smooth. (たとえば, E の j-invariant が $\notin k$ ならば, この仮定がみたされるが, これは, 必要条件ではない)

この仮定のもとに、$E(K)$ は、有限生成のアーベル群となる（Mordell-Weil の定理）ので、$E(K)$ は M.W. 群とよばれる。$E(K) \simeq \mathbb{Z}^{\oplus r} +$（有限アーベル群）となる $r \geq 0$ を、E/K の（Mordell-Weil）rank という。

$E(K)$ の元、即ち E の K-有理点は、$f : S \to C$ の section $s : C \to S$, $f \circ s = id_C$, と 1:1 に対応する。$E(K) \ni P$ に対応する section を同じ記号 P で表わし、なお section の像として、S の曲線（因子）と考えるときは、(P) とかく。

代数曲面 S の上の交点理論を用いて、$E(K)$ 上の自然な pairing $E(K) \times E(K) \longrightarrow \mathbb{Q}$ を、次のように定義することができる。$P, Q \in E(K)$ に対し

$$\langle P, Q \rangle = \chi + (PO) + (QO) - (PQ) - \sum_{v \in R} \mathrm{Contr}_v(P, Q)$$

$$\langle P, P \rangle = 2\chi + 2(PO) - \sum_{v \in R} \mathrm{Contr}_v(P).$$

ここで、χ は、S の arithmetic genus（仮定のもとに $\chi > 0$）。(PO) は、S 上の因子 (P) と (O) の交点数。（O は、0-section）。(QO), (PQ) は、同様の意味。$\mathrm{Contr}_v(P, Q)$ は、各 $v \in R$（ただし、R は、f の reducible fibres の集合）に対し、$(P), (Q)$ が $f^{-1}(v)$ のどの既約成分と通るかで定まる局所的な Contribution（$\in \mathbb{Q}$, ≥ 0）, $\mathrm{Contr}_v(P) = \mathrm{Contr}_v(P, P)$.

Th1 (i) 上の pairing は、$E(K)/(\text{tor})$ 上に、正定値な pairing を与える。

(ii). $E(K)^\circ \subset E(K)$ を、$\{P \in E(K) \mid (P)$ は、$\forall v \in R$ について、$f^{-1}(v)$ の (O) と交わる既約成分 $\Theta_{v,0}$ を通る$\}$ により定義すると、$(E(K)^\circ, \langle , \rangle)$ は、正定値、even、integral lattice になる。$([E(K):E(K)^\circ] < +\infty)$.

Def. $E(K)/(\text{tor})$ を、E/K の Mordell-Weil lattice、$E(K)^\circ$ を、narrow Mordell-Weil lattice とよぶ。

一般に、M.W. lattice は、narrow M.W. lattice の dual lattice に含まれるが、一致するとは限らない。

以下、S が有理曲面（すなわち、その関数体 $k(S)$ が、k 上の2次元純超越拡大）のときを主に扱う。このとき、$f: S \to C$ に関する（弧立）は、自動的にみたされる。また $K = k(t)$.

Th2 E/K について、S が有理曲面とする。このとき、

(i) $r = 8 - \sum_{v \in R} (m_v - 1)$, $\left(m_v = \#\{\text{irred. comp. of } f^{-1}(v),\ v \in R\} \right)$
≤ 8

(ii) $L = E(K)^\circ$ とおくと、

$$\begin{array}{ccc} E(K)/(\text{tor}) & \cong & L^* = L \text{ の dual lattice} \\ \cup & & \cup \quad] \text{ index } \nu \\ E(K)^\circ & \cong & L \end{array}$$

$\nu = \det L = \det T / n^2$, ($T$ は "trivial lattice".)

(iii) $n^2 = |E(K)_{tor}|^2 \mid \det T = \prod_{v \in R} m_v^{(1)}$, $\left(m_v^{(1)} = \#\text{simple irred. comp. of } f^{-1}(v)\right)$.

(Tの定義は、省略するが、可約な singular fibres $f^{-1}(v)$ $(v \in R)$ のタイプで定まるものである。)

Th 3. (構造定理). 上の仮定の下に、

(i) $r = 8 \iff R = \phi$, このとき

$$E(K) = E(K)^0 \simeq E_8.$$

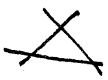
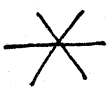
右辺は、E_8 型の root lattice, すなわち、rk 8 の正定値 even integral かつ $\det = 1$ の (unique) lattice である。

(ii) $r = 7 \iff R = \{v\}$ (1つ), $m_v = 2$. (type I_2 は III, 即ち、2本の $\mathbb{P}^1$ が、2点で交わっているか、1点で接する)

このとき、

$$\begin{array}{ccc} E(K) & \simeq & E_7^* \\ \cup & & \cup \quad \text{index } 2 \\ E(K)^0 & \simeq & E_7 \end{array}$$

(iii) $r = 6 \iff$ a) $R = \{v\}$ (1つ). $m_v = 3$.
2は
b) $R = \{v, v'\}$ (2つ), $m_v = m_{v'} = 2$.

$R = \{v\}$ のときは、type I_3  又は、IV  のように3本の $\mathbb{P}^1$ が、交わっている singular fibre $f^{-1}(v)$ があらわれる。

このとき

$$\begin{array}{ccccc} & & \text{a)} & & \text{b)} \\ E(K) & \simeq & E_6^* & & D_6^* \\ \cup & & \cup & \text{index } 3, & \cup \quad \text{index } 4. \\ E(K)^0 & \simeq & E_6 & & D_6 \end{array}$$

etc. ⌟

ここに現われる root lattices $E_8, E_7, E_6, \cdots$ などは非常によく研究の分った lattice で、とくに次表のような data が知られている。(cf. Bourbaki(前出), 又は Conway - Sloane: "Sphere packings, lattices & Groups".)

	E_8	E_7	E_7^*	E_6	E_6^*
det	1	2	1/2	3	1/3
min. norm	2	2	3/2	2	4/3
# min. vectrs	240	126	56	72	54
Aut	$W(E_8)$	$W(E_7)$		$W(E_6)\{\pm 1\}$	

さらに、これらの lattice の各々は、minimal vectrs の中から、生成元をとることができる。この事実を、上の Th. 3 により、Mordell-Weil lattices に適用すると、$E(K)$ の生成元についての重要な情報を与える。

E/K が Weierstrass form で与えられるときは、さらに、具体的な結果が得られる。簡単のため、$\mathrm{char}(k) \neq 2, 3$ とし、

$$E : y^2 = x^3 + p(t)x + q(t),$$

$p(t) \in k[t]$, $q(t) \in k[t]$, $\deg p \leqq 4$, $\deg q \leqq 6$ とする。Th. 2 (ii), (iii) のうえで $t = \infty$ をえらぶことにする (即ち $f^{-1}(\infty)$ を reducible fibre とする)。このとき、

Th, 4. (Min. vectrs & generators)

(i). $r=8$ のとき. $\langle P,P\rangle=2$ なる $P\in E(K)$ は 240 コ存在して. それらは. 次の形で与えられる. $P=(x,y)$

$$x=gt^2+at+b,\quad y=ht^3+ct^2+dt+e$$

$(g,h,a,b,c,d,e\in k)$

(ii) $r=7$ のとき. $\langle P,P\rangle=\frac{3}{2}$ なる P が 56 コ存在して. 次の形 : $P=(x,y)$,

$$x=at+b,\quad y=ct^2+dt+e$$

(iii) $r=6$, E_6^* のとき $\langle P,P\rangle=\frac{4}{3}$ なる P が 54 コ存在して. (ii) と同じ形で与えられる.

いずれの場合も. Mordell-Weil 群 $E(K)$ は. 上の形の r コの点により生成される」

3. Mordell-Weil lattice から生ずる代数方程式

今度は k_0 を任意の体とし. $k=\overline{k_0}$ を代数的閉包とする. C を k_0 上定義された曲線, $k_0(C)$ をその関数体. $K=k(C)$, E を $k_0(C)$ 上定義された楕円曲線とし. Mordell-Weil lattice $E(K)/(\text{tor})$ とは $E(K)^0$ を考える.

ガロア群 $Gal(k/k_0)$ は. 自然に $E(K)$ に作用し, しかも pairing $\langle\ ,\ \rangle$ が $Gal(k/k_0)$-不変であることから. 表現

$$\rho: Gal(k/k_0)\longrightarrow Aut_{\langle\ ,\ \rangle}(E(K)^0)\ (=\text{有限群})$$

を得る. 拡大 $\mathfrak{K}/k_0$ を, $Ker(\rho)$ に対応するものとする. いいかえれば: $\mathfrak{K}$ は, $E(k(C)) = E(\mathfrak{K}(C))$ となる最小の拡大である. $Gal(\mathfrak{K}/k_0) \subset Aut_{\langle,\rangle}(E(K)^\circ)$ となる.

ガロア表現 ρ の像 $I_m(\rho)$ については, ① $I_m(\rho)$ が大, 即ち全体のとき, ② $I_m(\rho)$ が小, 即ち $I_m(\rho)=\{1\}$ のとき, および ③ それ以外のとき, 夫々の面白さがある.

それはともかく, 代数方程式を定義するために, §1 の記号で, 有限 Galois set $M \subset E(K)$ を定義したいが, 今の場合, それは, 多様なえらび方が出来る. たとえば

$$M_n = \{ P \in E(K) \mid \langle P, P \rangle = n \}. \quad (n>0)$$

とれ. $n_0 = \min.\text{norm}$ に対する M_{n_0} は重要である. $\mathfrak{K}_n = k_0(P \mid P \in M_n)$ とおくと. $\mathfrak{K}_n \subset \mathfrak{K}$, $\mathfrak{K}_n/k_0$ がガロア拡大であり, M_n が, 1つの分岐点 P を止めれば: $\mathfrak{K}_n = \mathfrak{K}$.

次に. Galois equivariant map $s : M \longrightarrow k$ として. Specialization homomorphism sp'_v の M への制限をとることができる. ここで

$$sp'_v : E(K) \longrightarrow \mathbb{G}_a(k) \text{ または } \mathbb{G}_m(k)$$

は, 各 v ($f^{-1}(v)$ は sing. fibre) に対し定義される homo.

$$sp_v : E(K) \longrightarrow f^{-1}(v)^\# = \text{smooth part of } f^{-1}(v)$$
$$P \longmapsto (P) \cap f^{-1}(v)$$

と, $f^{-1}(v)^\#$ の単位元成分 $\mathbb{G}_a$ または $\mathbb{G}_m$ への"射影"との合成である.

上のように、$E/k_0(C)$, $M \subset E(K)$, v を定めると、

$$\boxed{\Phi(X) = \prod_{P \in M} (X - sp'_v(P)) \in k_0[X]}$$

なる次数 $=\#M$ の k_0 係数多項式が得られる。これが、我々の提唱する代数方程式である。

具体的な例をとって、その"意義"をみてみよう。今、

$$(E_8) \quad y^2 = x^3 + x(p_0 + p_1 t + p_2 t^2 + p_3 t^3) + (q_0 + q_1 t + q_2 t^2 + q_3 t^3 + t^5)$$

$$(E_7) \quad y^2 = x^3 + x(p_0 + p_1 t + t^3) + (q_0 + q_1 t + \cdots + q_4 t^4)$$

$$(E_6) \quad y^2 = x^3 + x(p_0 + p_1 t + p_2 t^2) + (q_0 + q_1 t + q_2 t^2 + t^4).$$

を $k_0 = \mathbb{Q}(p_i, q_j)$ 上の楕円曲線と考える。これらは rational double points とよばれる特異点の universal deformation として知られる family である。p_i, q_j は $\mathbb{Q}$ 上代数的独立とする。$k = \overline{k_0}$ とすると、Mordell-Weil lattice $E(K)$ は、夫々 E_8, E_7^*, E_6^* と同型になる。(Th.3 参照)。その理由は、対応する楕円曲面 $f : S \longrightarrow \mathbb{P}^1$ が、(E_8) の場合、可約 fiber をもたず $(R = \phi)$, (E_7), (E_6) のときは、夫々、唯一つの可約 fibre $f^{-1}(\infty)$ をもち、そのタイプは、III なし IV である(ことが容易に分る)からである。$M \subset E(K)$ として、min. norm をもつ P の集合をとる。Th 4 の記号を用いて、$sp_\infty(P)$ は、次のように

ようこうれる.

Lemma. $sp'_\infty(P) = \begin{cases} \frac{g}{h} & r=8 \text{ のとき} \\ -c & r=7 \\ \pm a & r=6 \end{cases}$

このようにして、我々は (E_r) 型の"基本方程式"

$$\Xi_{E_r}(X) = \prod_{P \in M} (X - sp'_\infty(P)) \in k_0[X]$$

$\deg \Xi_{E_8} = 240$, $\deg \Xi_{E_7} = 56$, $\deg \Xi_{E_6} = 54$

を得る. ここで、Ξ_{E_8}, Ξ_{E_7} は、定理は、X^2 の多項式となり、Ξ_{E_6} は $\Xi(X)\cdot\Xi(-X)$, $\deg \Xi = 27$, と分解する.

Th. 「Ξ_{E_8}, Ξ_{E_7}, Ξ_{E_6} は、$\mathbb{Q}[p_i, g_j][X]$ (あるいはより強く、$\mathbb{Z}[p_i, g_j][X]$) に属する既約多項式で、そのガロア群は、$W(E_8)$, $W(E_7)$, $W(E_6)$ 全体になる。」 (§1. の例 2) と比較されたい.)

上うに上の Lemma と、sp'_∞ が group homo. である (実は、今の場合 sp'_∞ が group isom. になっている!) ことより これら"基本方程式"を explicit に求めることができる. これは、(E_8), etc の定義式にあらわれる係数 p_i, g_j を、Weyl 群 $W(E_8)$, etc. の基本不変式として、具体的に書き表わせることを意味している.

(+) $\quad p_i, g_j = I_W(u_1, \cdots, u_r) \quad (u_i = sp'_\infty(P_i), 1 \le i \le r)$.

4. 応用として、$\mathbb{Q}(t)$ 上比較的高い rank をもつ楕円曲線 $E/\mathbb{Q}(t)$ を、Mordell-Weil 群 $E(\mathbb{Q}(t))$ の生成元とともに、構成する方法を述べる。(実は、$\mathbb{Q}$ の代りに、とくな体をとってもよい。(標数 $\neq 2,3$, 比有限コの p を除く))

仮に、$u_1, \cdots, u_8$ が E_8-lattice の基本 roots とするとき、240コの全ての roots u_i を、$u_1, \cdots, u_8$ の $\mathbb{Z}$-1次結合と表す。次に、$\delta(u) = \prod_{i<j}(u_i - u_j)$ を $u_1, \cdots, u_8$ の多項式とみなす。このとき

Th. (E_8) 任意の $(u_1, \cdots, u_8) \in \mathbb{Q}^8$ で $\delta(u) \neq 0$ なるものをとり、$p_i, q_j \in \mathbb{Q}$ を、基本対称式 $\Phi_{E_8}(X)$ の係数と係数の関係から定める。このとき、式 (E_8) で定義される楕円曲線 $E/\mathbb{Q}(t)$ は、rank $r = 8$ で、そのMordell-Weil 群の生成元として、P_i $(1 \leq i \leq 8)$

$$P_i : \begin{cases} x = u_i^{-2} t^2 + a_i t + b_i \\ y = u_i^{-3} t^3 + c_i t^2 + d_i t + e_i \end{cases}$$

がとれる。ここで u_i $(1 \leq i \leq 8)$ は、はじめに任意にとった値であり、他の $a_i, \cdots, e_i$ は、$u_1, \cdots, u_8$ から有理的に定まるものである。」

同様な Th. が (E_7), (E_6) および、他のいくつかの他のルート系の型についても成立する。しかも、これは、実例を構成するにも十分な algorithm をもっている。

以上の詳細は目下準備中*である。

また"大きな"Galois表現(あるいは拡大)の構成、その他の応用については、他日に譲りたい。

(以上)

*) "Construction of elliptic curves with high rank via the invariants of the Weyl groups."

#) §1. (例ロ), ハ)との関連について。 $E/K = k(t)$ が、Th.3のように、$E(K) \cong E_8, E_7^*$ または E_6^* となる場合には、対応する楕円曲面 S から、$d = 9 - r$ (= 1, 2 または 3) 個の(第1種)例外曲線を、つぎつぎに blow down することにより、degree d の del Pezzo 曲面 V ができる。$r=6, d=3$ のときは、V は、$\mathbb{P}^3$ の3次曲面になる。$r=7, d=2$ のときは、canonical map $|K_V| : V \to \mathbb{P}^2$ は、2次の写像で、分岐は、$\mathbb{P}^2$ の4次曲線に沿っておこる。いづれの場合にも、$\langle K_V \rangle^\perp (\subset NS(V))$ は、narrow M.W. lattice $E(K)^0$ と同型になり(pairingの符号を反対にして)、V 上の第1種例外曲線は、$E(K)$ 内の minimal vectors として($r=6$ のときは、その半分として)全部に特徴付けられる。よって、(例ロ), ハ)は、Modell-Weil lattices の理論の枠でより(1)よく理解され、とくに、$sp : M \to k$ なる写像は、古典的理論では、必ずしも明らかでない。

と いいかえるのは 少々 言い過ぎであって、昔の数学者の知恵は素晴らしく、del Pezzo surface の理論でも、cuspidal cubic と、その上の座標（つまり $\mathbb{G}_a$ の相当物）を用いている。（cf. Demazure, SLN.777. に現代的解説がある。）しかし、elliptic surface における specialization map Sp_v は、はるかに分り易くなっている、といってよいであろう。

以上の方法で、上のような del Pezzo surfaces と、その上の有理的例外曲線（$d=1,2,3$ に応じて、たぐ. 240, 58, 27 個存在）を具体的に構成することが出来、とくに、その上への ガロア群の作用をみることが出来る。さらに、（全ての有理的例外曲面が $\mathbb{Q}$ 上定義されるような、del Pezzo surfaces の実例を手にすることもできる。

（以上）