Mordell-Weil Lattices and Galois Representations --- Old and New

Tetsuji Shioda (Kyoto U. /Rikkyo U.)

モーデル・ヴェイユ格子とガロア表現---20年

塩田　徹治　（立教大学／京都大学）

代数学シンポジウム（明治大学）

8/4/2009

予定

- MWL誕生前後（秘話） (1989~)
- 代数方程式とMWL
- MWL概観
- 例外型 (E_6, E_7, E_8)方程式論
- 整数点とグレブナ基底 (2007~)
- ガロア群＝$W(E_8)$となる多項式の実例 (2009)

● はじめに　MWL誕生前後

代数学シンポジウムで 一般向けの話を、 とプログラム責任者の宮岡洋一さんに声をかけられたとき、すぐお引き受けしたのは、私の (一つ覚えのような）話題である**「モーデル・ヴェイユ格子」** は、まず**やさしい**し**実例も豊富**だから、一般の方に話すこともできるだろう、と漠然と思ったからである。

私が「モーデル・ヴェイユ格子」なるものを研究し始めたのは１９８９年、今からちょうど２０年前である。そして、その成果を初めて公表したのは、同年８月札幌で開催された「代数学シンポジウム」であった。そこでの標題 (和訳）は
「モーデル・ヴェイユ群、格子とガロア表現」
であって、まだ「モーデル・ヴェイユ格子」なる用語を使うことが適当か否か思案中だった。直後に書いた報告集の原稿および同年９，１０月に学士院紀要で発表した論文では「モーデル・ヴェイユ格子」を採用し、それ以降幸いにもこの用語は完全に定着した。以下、MWL　は「モーデル・ヴェイユ格子」(Mordell-Weil Lattices)　の略である。

背景

代数曲線や多様体の**整数点**や**有理点**に焦点を合わせた問題を、一般にディオファンタス問題とよぶ。もっとも有名な例はフェルマーの最終定理の名で知られる問題で、これは

$$X^n + Y^n = Z^n$$

の整数解 (X, Y, Z)、あるいは

$$x^n + y^n = 1$$

の有理数解　(x, y) について問うものである。その最終的解決は十数年前にワイルスにより与えられ、世紀の話題となったことは周知の通りである。

このような問題は、代数幾何的な舞台で整数論的な性格をもつ主役、脇役の働きを見たい訳だから、様々な角度から観察・研究することが可能である。

今から考える **MWL** の枠組みでは、

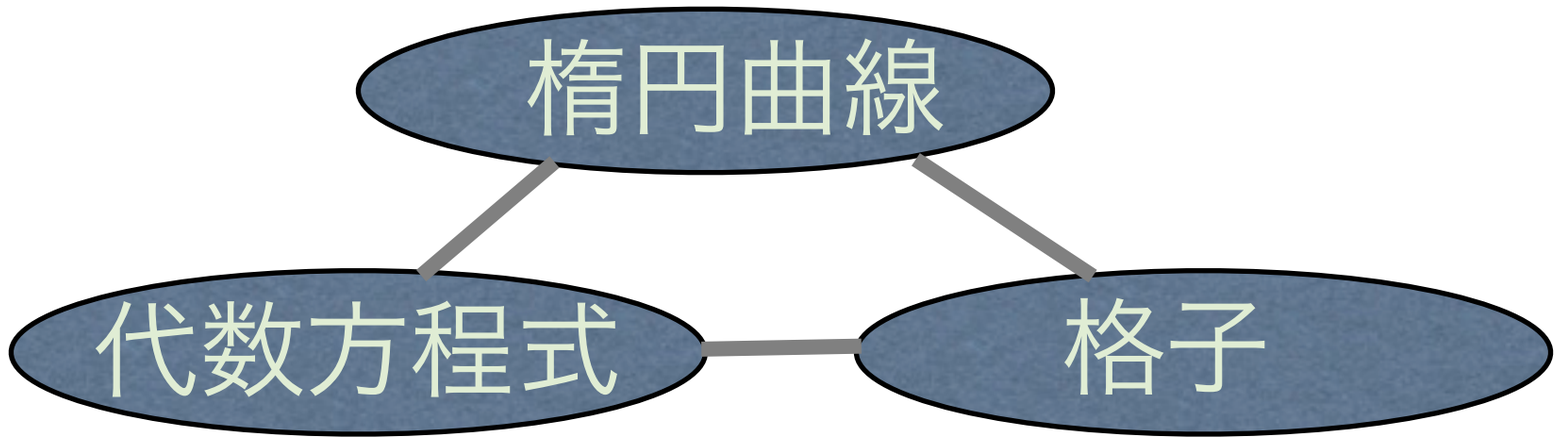
楕円曲面

という舞台で次のトリオ

代数方程式、 楕円曲線、 格子

が、活躍する。

これらはいずれも数学（とくに代数学）において基本的な対象であって、それぞれが大舞台の主役を張れるものであるが、ここでの関心はそれらの間の関係である。



MWL

予定

- MWL誕生前後（秘話）
- 代数方程式とMWL
- MWL概観
- 例外型 (E_6, E_7, E_8)方程式論
- 整数点とグレブナ基底
- ガロア群＝$W(E_8)$となる多項式の実例

代数方程式とMWL

まず、主な登場人物：

- 楕円曲線
- 格子
- 代数方程式
- MWL (モーデル・ヴェイユ格子)

について例で説明する。

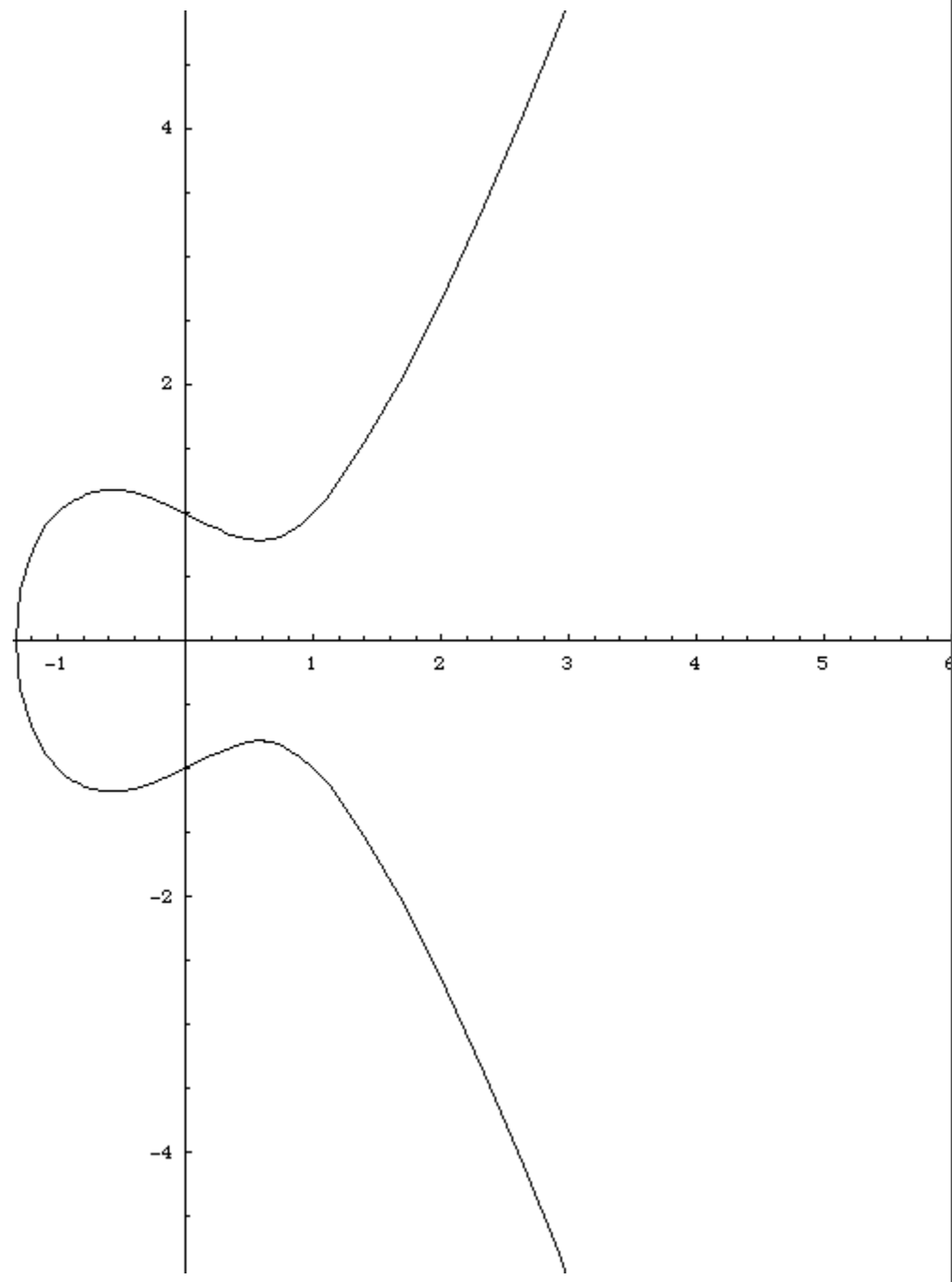
MWLについては、一番簡明な結果を紹介する。

話の流れを感じとっていただければ幸いである。

楕円曲線

$$E : y^2 = x^3 + Ax + B$$

$$\Delta = 4A^3 + 27B^2 \neq 0$$



大切な性質：

加法で群になる。
原点 O は図に現れない。

楕円曲線

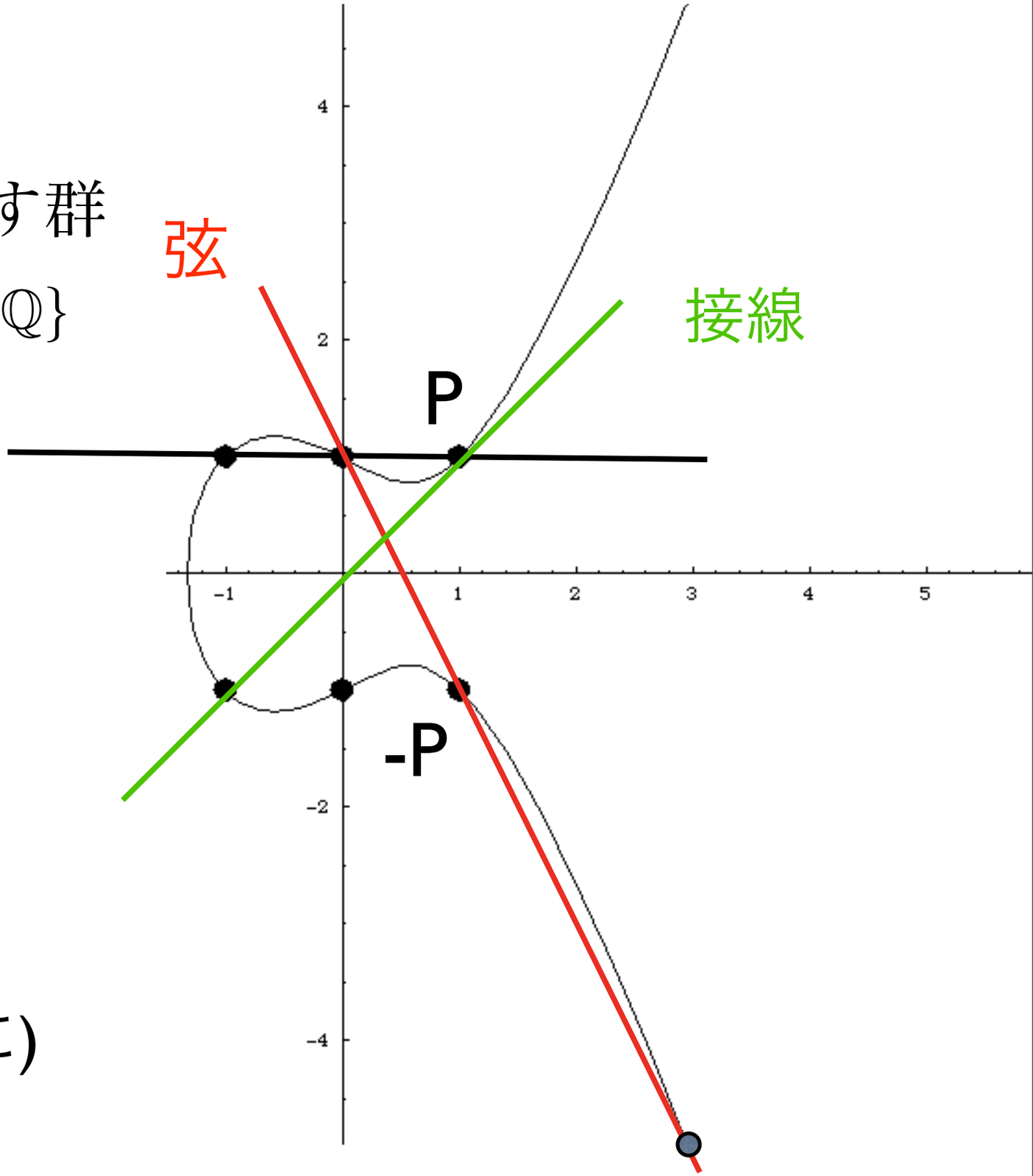
$$E : y^2 = x^3 - x + 1$$

$E/\mathbb{Q}$

$\mathbb{Q}$ は有理数体

$E(\mathbb{Q})$：E の有理点のなす群

$E(\mathbb{Q}) = \{O\} \cup \{\ (x, y) | x, y \in \mathbb{Q}\}$



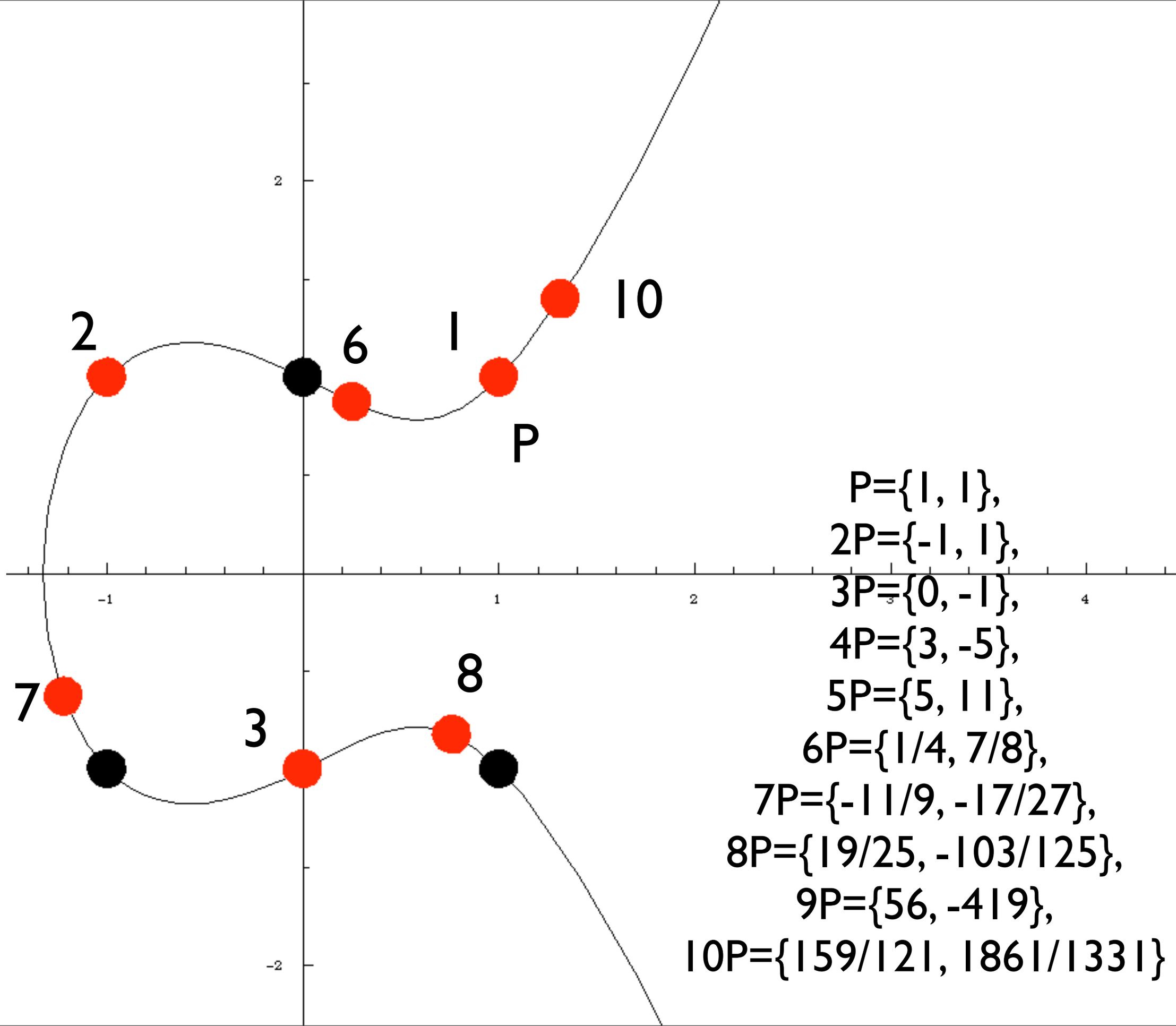
加法定理

3 点　P, Q, R について：

$P + Q + R = 0 \Leftrightarrow$

$\{P, Q, R\}$ が 1 直線上にある。

(1つの弦または接線上に)



P={1, 1},
2P={-1, 1},
3P={0, -1},
4P={3, -5},
5P={5, 11},
6P={1/4, 7/8},
7P={-11/9, -17/27},
8P={19/25, -103/125},
9P={56, -419},
10P={159/121, 1861/1331}

$$E : y^2 = x^3 + Ax + B \qquad A, B \in K$$

$$\Delta = 4A^3 + 27B^2 \neq 0$$

体

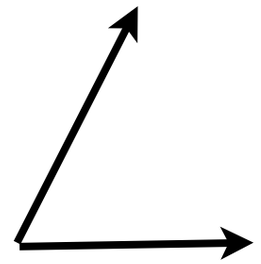
体 K が有理数体 $\mathbb{Q}$ や有理関数体 $\mathbb{C}(t)$ のとき、
K-有理点の群　$E(K)$ は
有限個の点で生成される加法群になる。
（**モーデル・ヴェイユの定理**）
$E(K)$ をモーデル・ヴェイユ群とよぶ。　略してMW群

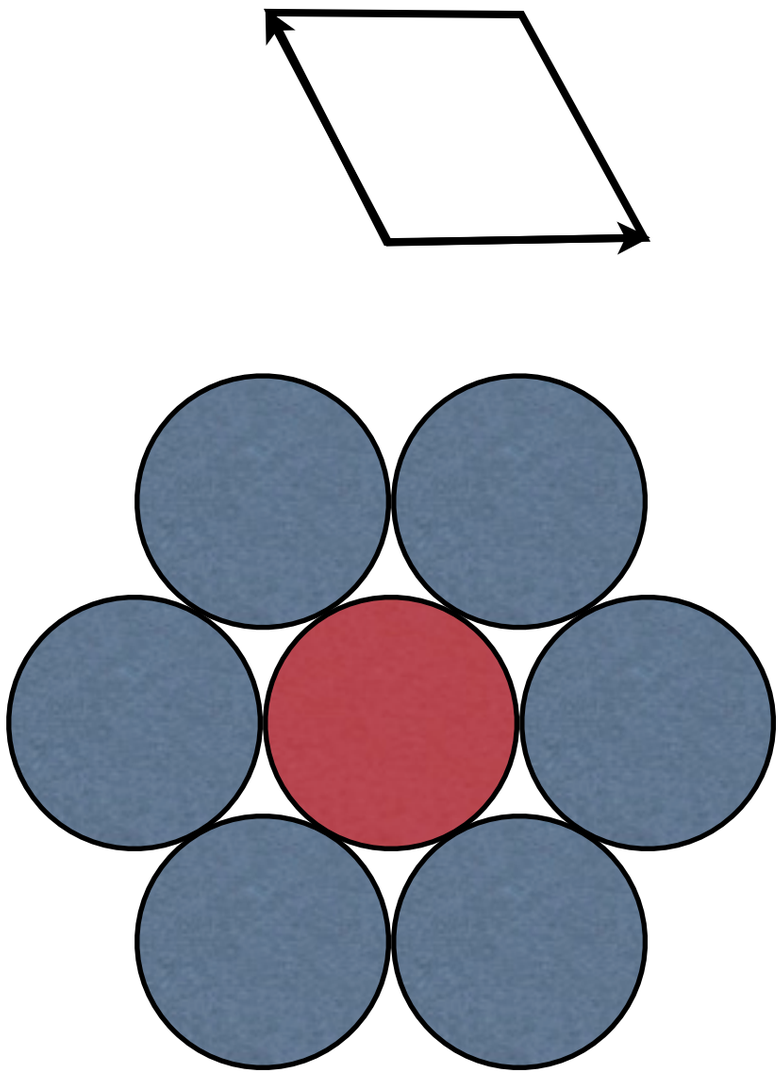
そして、A, B が整数のとき、
その整数点は有限個しかない　（ジーゲルの定理）

ことが知られている。

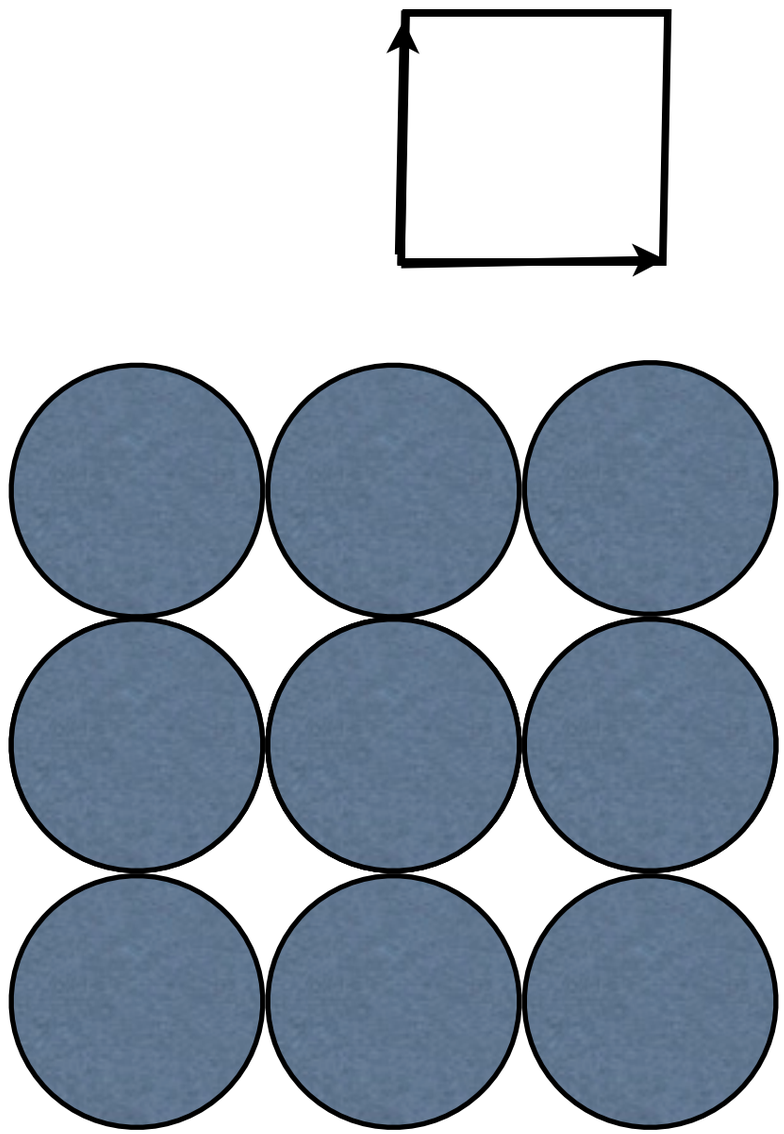
先の例では、
$E(\mathbb{Q})$ は 1 点 P で生成される
ランク 1 の群：
$E(\mathbb{Q}) \cong \mathbb{Z}$

格子(Lattice)

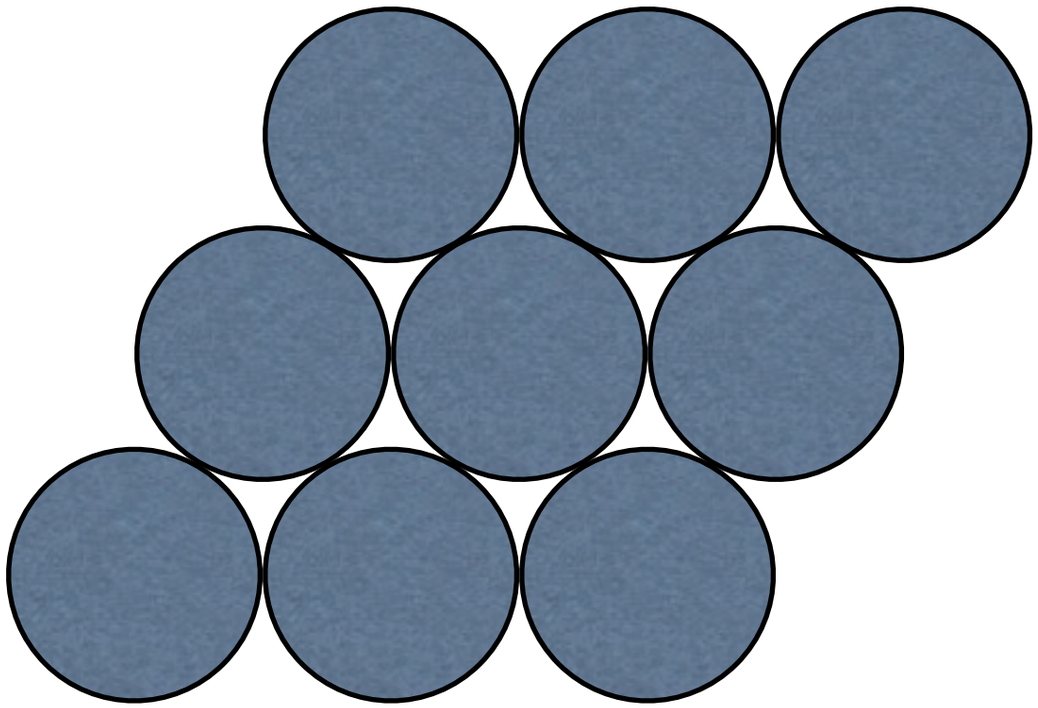
- 2 次元格子は：  で張られる。
- 正方格子、６角格子、その他、無数にある。
- 格子は「球の詰込み」（２次元のとき「円板の詰込み」）を与える。



６角格子

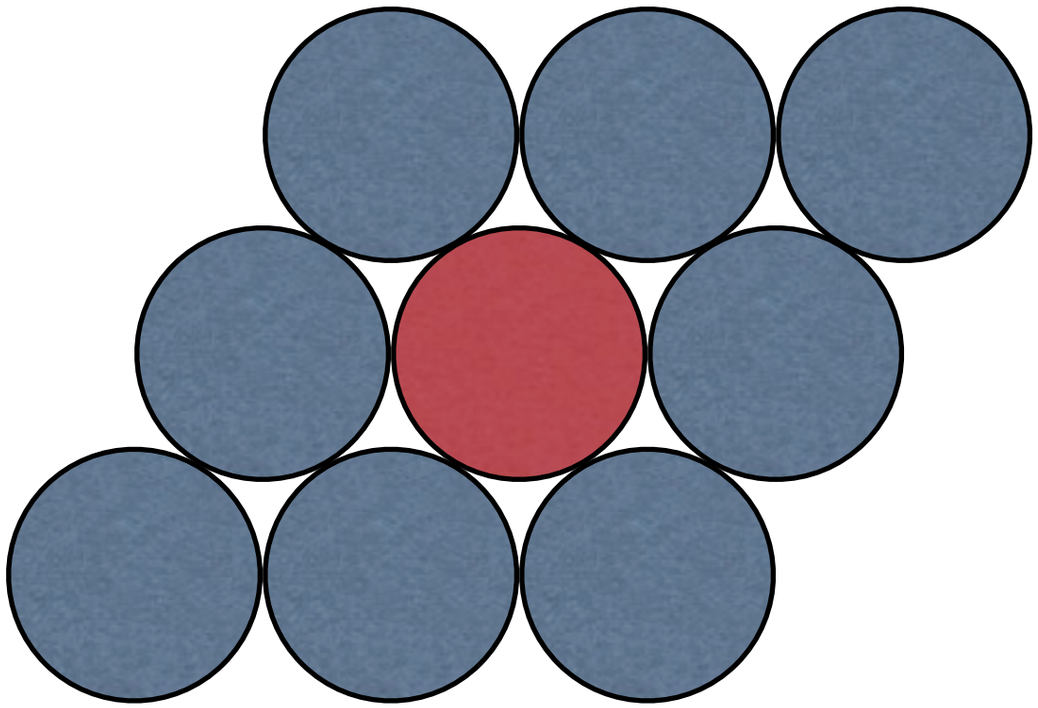


正方格子



格子点

６角格子と円板のつめこみ



６角格子と円板のつめこみ

2次元で最も密度の高いつめこみ.

接触数(kissing number) =6,

これも2次元で最大

ルート格子　A_2

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

６角格子に相似、
２次元の最密格子
最短ノルム：２
最短ベクトルの個数：６個

ルート

A_2^*：A_2 の双対格子

$$\begin{pmatrix} 2/3 & 1/3 \\ 1/3 & 2/3 \end{pmatrix}$$

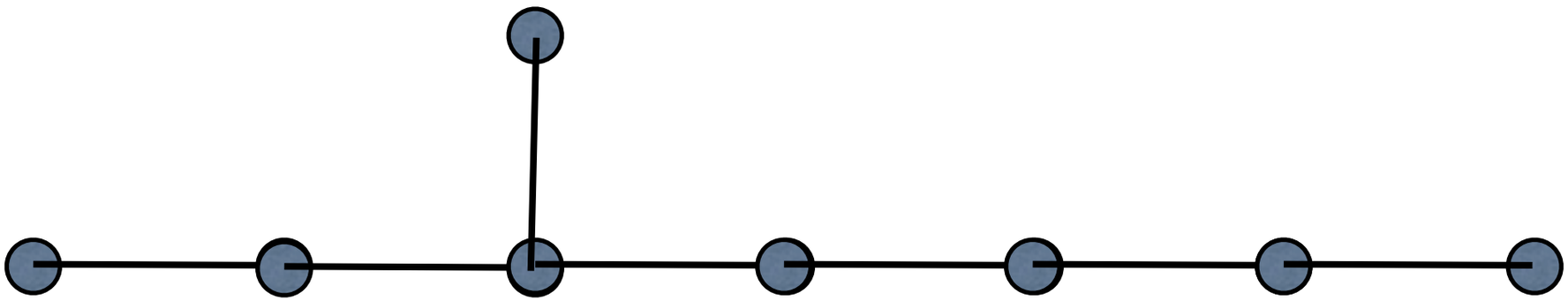
これも　６角格子に相似、
最短ノルム：$\frac{2}{3}$
最短ベクトルの個数：６個

高次元の格子：

すべてMWL
として登場

３次元以上の格子では：
ルート格子　$A_3, D_4, D_5, E_6, E_7, E_8$
が最密格子を与える。また最大接触数を与える。

８次元の例外型ルート格子　E_8 は、



上のディンキン図形に対応して、
E_8 は、２４０個の **ルート**　をもつ。
ルート　とは、ノルム２の元 (長さ $\sqrt{2}$ の元) のこと。

代数方程式

- ３次方程式

$$f(x) := x^3 + Ax + B \quad = 0$$

３根　x_1, x_2, x_3　　$(x_1 + x_2 + x_3 = 0)$

相異なる　$\Leftrightarrow \Delta_0 = 4A^3 + 27B^2 \neq 0$

たとえば、A, B が有理数のとき、
３根をふくむ最小の体
$\mathcal{K} = \mathbb{Q}(x_1, x_2)$
を $f(x)$ の（最小）　**分解体**という。

ガロア群 $G = Gal(\mathcal{K}/\mathbb{Q})$
は、3 次の対称群 $\mathcal{S}_3$ の部分群。

MW群　vs　MWL

次の楕円曲線を考える：　$(A_2\text{-model})$

$$E : y^2 = x^3 + Ax + B + t^2$$

$$f(x) := x^3 + Ax + B$$

3 根　x_1, x_2, x_3　　t は変数

直線 $y = t$ の上には、次の 3 点がある：

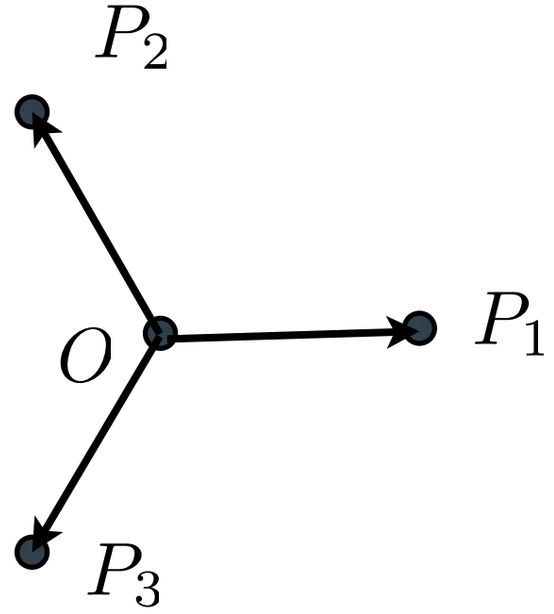
$$P_1 = (x_1, t)$$
$$P_2 = (x_2, t) \qquad P_1 + P_2 + P_3 = O$$
$$P_3 = (x_3, t)$$

Th.1 $E(\mathbb{C}(t))$ は（MW 群として）、
2 点 P_1, P_2 で生成されるランク 2 のアーベル群

$$E(\mathbb{C}(t)) \cong \mathbb{Z}^2 \text{ (群として)}$$

MWLとしての結果は、Th.Iより強い主張：

Th.2 $E(\mathbb{C}(t))$ は（MWL として）、
6 角格子と相似で、6 個の最短ベクトルは
$P_1, P_2, P_3, -P_1, -P_2, -P_3$



Th.3 $E(\mathbb{C}(t))$ は A_2^* と同型

Th.4
$$\begin{array}{ccc} E(\mathbb{C}(t)) & \cong & A_2^* \\ \cup & & \cup \\ E(\mathbb{C}(t))^0 & \cong & A_2 \end{array}$$

狭い (narrow) MWL

6 個の $P_i - P_j$ $\longleftrightarrow$ 6 個のルート

証明は後で.

具体例

例 1 . $f(x) = x^3 - x = x(x-1)(x+1)$,
3 根 {0,1,-1}
$E : y^2 = x^3 - x + t^2$
$E(\mathbb{Q}(t))$ は $P_1 = (0,t), P_2 = (1,t)$
で生成され、ランク 2 .

例 2. $f(x) = x^3 - 1 = (x-1)(x^2+x+1)$
$= (x-1)(x-\omega)(x-\omega')$,
3 根 $\{1, \omega, \omega'\}$. ω: 1 の 3 乗根
$E : y^2 = x^3 - 1 + t^2$
$E(\mathbb{Q}(t))$ は $P_1 = (1,t)$ で生成され、ランク 1.
分解体　$\mathcal{K} = \mathbb{Q}(\sqrt{-3})$,
$E(\mathbb{C}(t)) = E(\mathcal{K}(t))$: ランク 2 .

例 3.　$f(x) = x^3 - 2$ は既約、
3 根 $\{x_1 = \sqrt[3]{2}, x_2 = \sqrt[3]{2}\omega, x_3 = \sqrt[3]{2}\omega'\}$.
$E : y^2 = x^3 - 2 + t^2$
$E(\mathbb{Q}(t)) = 0$、ランク 0.
分解体　$\mathcal{K} = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$,
$E(\mathbb{C}(t)) = E(\mathcal{K}(t))$: ランク 2 .

MWL によるガロア表現

$G = Gal(\mathcal{K}/\mathbb{Q})$　　$L = E(\mathcal{K}(t))$　MWL

$\rho : G \hookrightarrow Aut(L)$

$Im(\rho) \subset W(A_2) \cong \mathcal{S}_3$　　A_2 のワイル群

例 1 .　$G = \{1\}$
例 2.　$G = \{1, (23)\}$
例 3.　$G = \mathcal{S}_3$

予定

- MWL誕生前後（秘話）
- 代数方程式とMWL
- MWL概観
- 例外型 (E_6, E_7, E_8)方程式論
- 整数点とグレブナ基底
- ガロア群＝$W(E_8)$となる多項式の実例

- MWL概観

楕円曲線

$$E : y^2 = x^3 + Ax + B$$

$$A, B \in K \qquad \Delta = 4A^3 + 27B^2 \neq 0$$

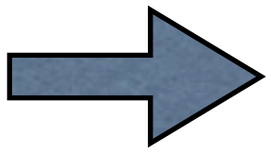
K は　有理関数体　$K = k(t)$ とする。
（k は　有理数体、複素数体　など）

以下、A, B は　多項式　$A(t), B(t)$ とする。

楕円曲面

このとき、式

$$y^2 = x^3 + A(t)x + B(t)$$

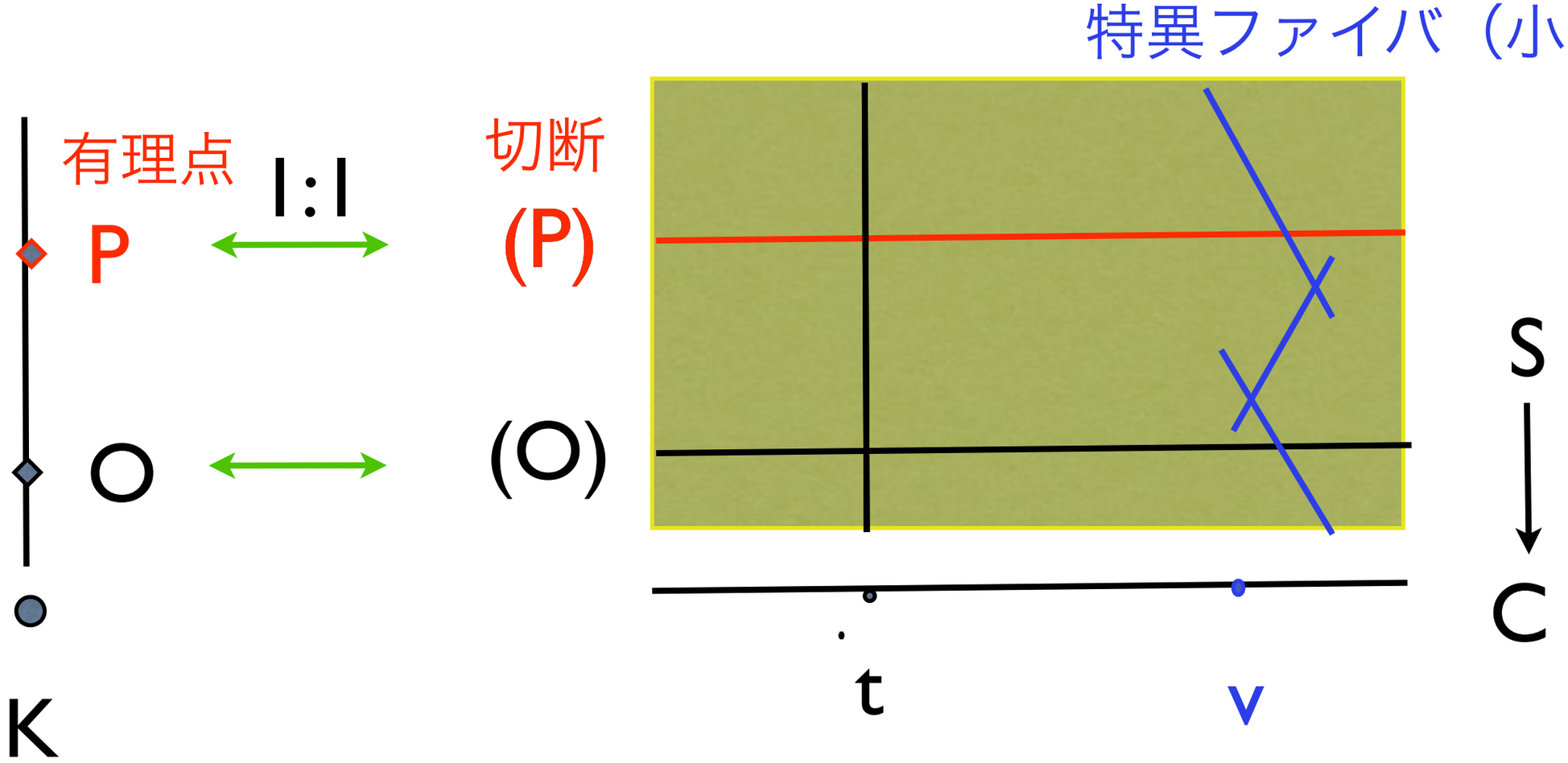


(x, y, t)-空間の中の**曲面**　S'

関数体上の

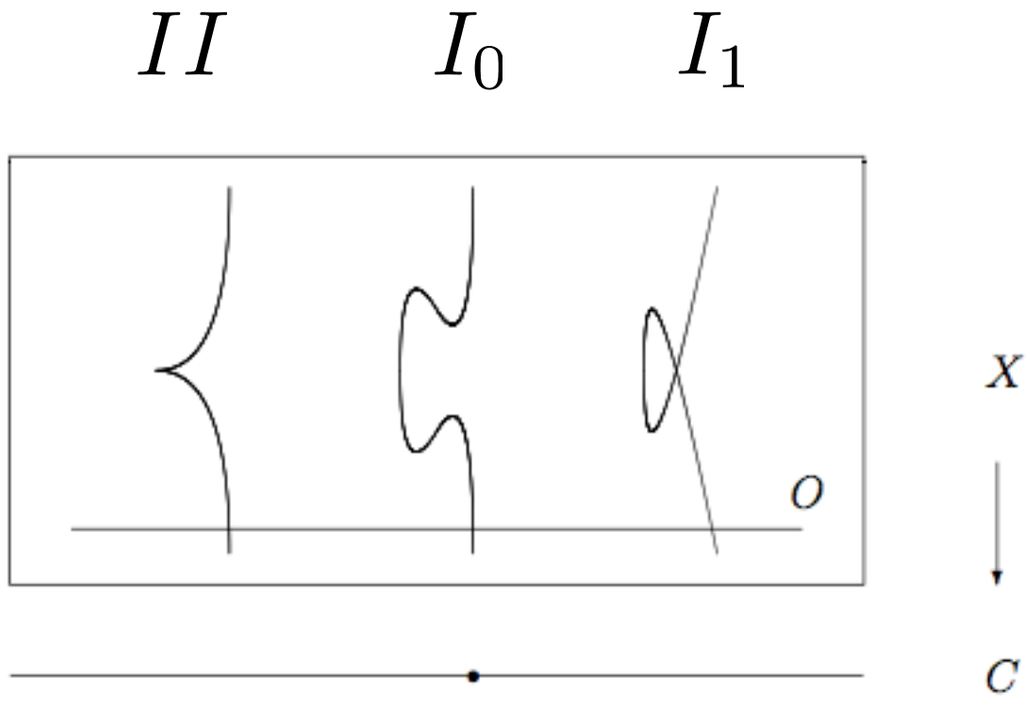
楕円曲線

E / K ⟷ S: 楕円曲面



特異ファイバの分類（小平 Kodaira）

既約なファイバ



I_0 は
非特異ファイバ
（楕円曲線）

可約なファイバ (multiplicative type)

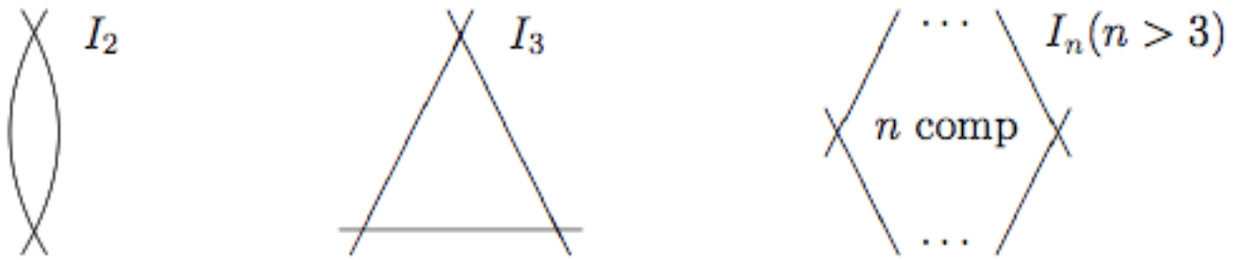
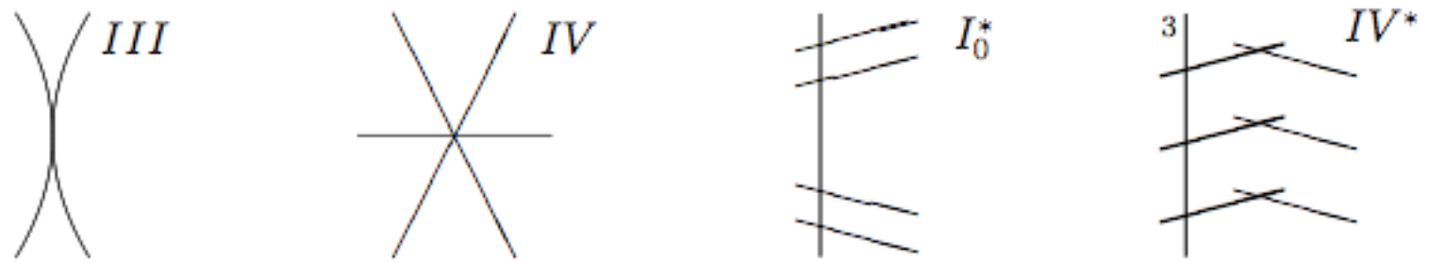


FIGURE 3. Singular fibre of type I_n $(n > 1)$

可約なファイバ　(additive type)



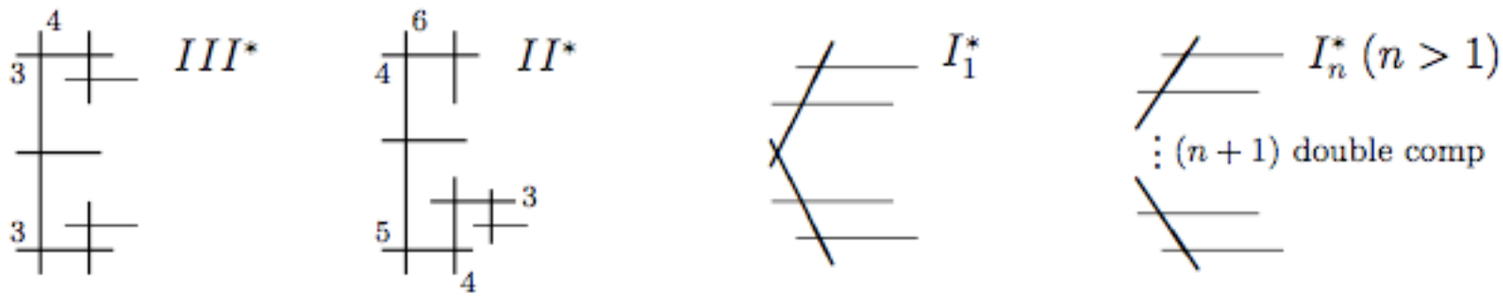


FIGURE 4. Reducible additive singular fibres

モーデル・ヴェイユ格子：基本的アイディア

モーデル・ヴェイユ群 E(K)を格子として見る。

自然な内積（ハイト）を、

曲面の交点理論を用いて定義 。

ハイト公式 :

$$< P, P >= 2\chi + 2(PO) - \sum_v contr_v(P)$$

可約ファイバ

定義：E(K) を内積付きで考えたものを、

楕円曲線 E/K (または、 楕円曲面 S) の

モーデル・ヴェイユ格子という。

有理楕円曲面

$$y^2 = x^3 + A(t)x + B(t)$$

$A(t)$ が 4 次以下、 $B(t)$ が 6 次以下のとき。

$\chi = 1$

ハイト公式：

$$< P, P >= 2 + 2(PO) - \sum_v contr_v(P)$$

(PO) は切断 (P) とゼロ切断 (O) の**交点数**

有理楕円曲面 で可約ファイバがないとき、

MWL はルート格子 E_8 に同型：

$$E(k(t)) \cong E_8$$

240個のルートに対応する $P \Leftrightarrow (P) \cap (O) = \emptyset$ なる P

(A_2-model)

$E : y^2 = x^3 + Ax + B + t^2$ についての証明：

仮定　$4A^3 + 27B^2 \neq 0$ ⟹

$t = \infty$ で　IV^*

可約ファイバは、これのみ

$P_1 = (x_1, t)$

$P_2 = (x_2, t)$

$P_3 = (x_3, t)$

にハイト公式を適用：

$$< P, P >= 2 + 2 \cdot 0 - 4/3 = 2/3$$

⟹ **Th.2, 3** の証明ができる。

Th.4 で　$P_i - P_j$ のハイト $= 2$

も同様に示される。　(終)

予定

- MWL誕生前後（秘話）
- 代数方程式とMWL
- MWL概観
- 例外型 (E_6, E_7, E_8)方程式論
- 整数点とグレブナ基底
- ガロア群＝$W(E_8)$となる多項式の実例

- 例外型 (E_6, E_7, E_8)方程式論

特異点の変形

Milnor lattice : MWL

monofromy : Galois rep.

vanishing cycle: P

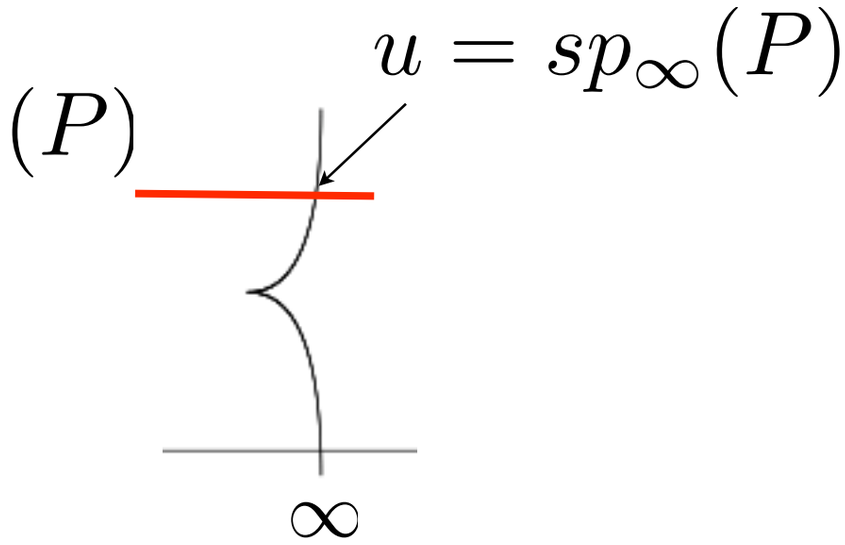
$$(E_8 - model)$$
$$E_\lambda : y^2 = x^3 + A(t)x + B(t) \qquad (1)$$

$$A(t) = p_0 + p_1 t + p_2 t^2 + p_3 t^3$$
$$B(t) = q_0 + q_1 t + q_2 t^2 + q_3 t^3 + t^5$$
$$\lambda = (p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3)$$

λ が一般のとき、 240個の

次の形の有理点＝切断がある：

$$P = (x(t), y(t))$$
$$x(t) = \frac{1}{u^2}t^2 + at + b,$$
$$y(t) = \frac{1}{u^3}t^3 + ct^2 + dt + e \qquad (2)$$



前のページの（１）式に（２）を代入すると、
t についての恒等式ができる。これから、
e, d, c, b, a を順次消去することにより、
u に関する 240 次方程式を得る：

$$\Phi(u, \lambda) = u^{240} + \cdots = 0$$

その係数は $\mathbb{Q}[\lambda] = \mathbb{Q}[p_i, q_j]$ に属する。

E_8 型代数方程式の基本定理
$\Phi(u, \lambda)$ は係数体 $k_0 = \mathbb{Q}(\lambda) = \mathbb{Q}(p_i, q_j)$ の上で
既約な２４０次多項式、
その分解体を　$\mathcal{K}_\lambda$ とすると、ガロア群
$Gal(\mathcal{K}_\lambda / k_0)$ は　ワイル群　$W(E_8)$ に同型。

ワイル群　$W(L)$

ルート格子 L の各ルート α による鏡映 w_α で生成される群
これは　格子 L の自己同型群の有限部分群。

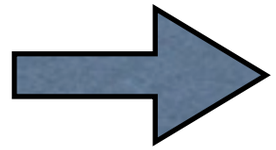
$L = A_2$ のとき、$W(A_2)$ は 3 次の対称群に同型。
$L = A_{n-1}$ のとき、$W(A_{n-1})$ は n 次の対称群に同型。

$L = E_8$ のとき、$W(E_8)$ は?
位数　$= 2^{14}3^5 5^2 7 = 696729600$
ほとんど　単純群　$O_8^+(2)$ に等しい：
$W(E_8) = 2.O_8^+(2).2$ (Atlas の記法)

基本定理の応用：

$W(A_{n-1}) \cong \mathcal{S}_n$
一般 n 次方程式と対称群
の場合と同様に：

まず、”大きなガロア群”について：

Hilbert の既約性定理 

1. $\lambda = (p_i, q_j)$ を有理数値 λ_0 に特殊化するとき、
ほとんどの場合 $\Phi(u, \lambda_0)$ の分解体
のガロア群 は $W(E_8)$ に等しい.

2. 有理数体 $\mathbb{Q}$ の 任意の $W(E_8)$-拡大は、
１．のようにして得られる。

実例の構成については、後述。

一方、”小さなガロア群”のアイディアから、

3. $\mathbb{Q}(t)$ 上の楕円曲線でランク８のものの標準的構成

他の例外型　E_6, E_7　についても
以上と同様なことが成立する。
しかもこのときは、以前実例も与えた。
（Proc. ICM Kyoto1990 に公表）

尚、E_6, E_7 型のMWLから生ずる代数方程式は、代数学の古典（19 世紀）

3 次曲面上の 27 本の直線の代数方程式
4 次曲線上の 28 本の双接線の代数方程式

を再現したので、その方面への応用もある。

予定

- MWL誕生前後（秘話）
- 代数方程式とMWL
- MWL概観
- 例外型 (E_6, E_7, E_8)方程式論
- 整数点とグレブナ基底
- ガロア群＝$W(E_8)$となる多項式の実例

他の例外型　E_6, E_7　についても
E_8　と同様なことが成立する。
しかもこのときは、以前実例も与えた。
（Proc. ICM Kyoto1990 に公表）

しかし　E_8　のときは、ワイル群　$W(E_8)$
の情報が十分でなく、実例が出来なかった.

今回(2009)　このトピックについて
進展があったので、報告する：

Jouve, F., Kowalski, E., Zywina, D.: An explicit integral polynomial whose splitting field has Galois group W(E8), Preprint: http://arxiv.org//0801.1733 (2008).

彼らは、代数群 E_8 の随伴表現の
固有多項式を用いて、求める性質をもつ
整数係数多項式　$F(X) = H(T), (T = X^2)$
の実例を作った。　次の 2 ページの表は
$T^i (i = 0, 1, 2, \ldots, 120)$ の係数である：

$T = X + \frac{1}{X}$

Degree i	Coefficient of T_i
0	365587894983967922854560421106658794835269162025801581455381270108994772086354097689969
1	−1118876467131374305210485226046235386760375678024159816738831177514460567841062867332448
2	16925369623839902955919213579836968159686902059211857903966654821912633936827870813036589 6
3	−16871599202625244945718248910288337200396954706370569562234622933721635292901264313045851 00
4	12466538870569350428117512482674638738192598391028225510113876433671029848121166234252784168
5	−72826947156697363455035723423426971890324922381314772703337692580409097282009564861222315768
6	35033152967267360160971156153301972138609051542077535113616131855324463034424756631828284550 4
7	−14272385656156168368749660272808498929314673919470833506310980085795474519493655121654453245 48
8	50263544385873500423930191888593226193092230679124555907653162220747690066547153954921675340 64
9	−15543242692747890030945651958468728793028138424448388052344884541152421476286890160281606087912
10	427277228565865779631258585803103025992527144045229019252972643856542811647037266340733636381 12
11	−10545667387009517371170316314366972722469781437827359945942344277859636001285464053826079492 1080
12	23560781709575519936885819014989987885616397851556143145545140313155791480736195001685660311 9900
13	−47977014926490760959163686706653014844472931786280060863293713860842703218461074385521942862 6708
14	89563562317306180360022685131221177231250493241893330608638361615654826194968801452453133315 3508
15	−15404725557900897543920616526892789322575057588531943665078395233296664539635151880714782759956 40
16	24517887105868717455896642288615398909449144212833280643521607626458786354064607653718484644803 40
17	−36246405059016381880096973378579544834733851095899308729495581845519879111807813600427905830836 04
18	49940240721269515051263990988246209046524538955672942957626738345548546942487278689065770165375 40
19	−64317216376729737642535595540281297526088594700806822406404046275413317311739576880362006590350 92
20	77632414686239795450081245011055537715400390377563503642617005193102571007602802991510555427324 92
21	−88029428803814993882456510702592738725713388701989068247162987665852769148305558249198323737774 96
22	93974289055945167434272994648723480627388482229079787142952893896718214943986324214893309848340 96
23	−94629218618382315042326481806835662090606875428502227568305728738964153218348237888053524700369 44
24	90040429101453184522804621878449505469794295622120101531594525119763165112378933891821445640718 16
25	−81084667774479733506251438660208891459050017814840332333031727506629066035022576350407636971208 00
26	69208779936916441995033254908680766392263224682288948634523567597583536965385123846036846792122 36
27	−56063932866503550506324453123925456480774854129350863994270150132224551154233425506682292285263 80
28	43155529715439187122926898027499196128660963197830160021626261098263780827922790948130159086295 60
29	−31601472929455739616255844240977179203702257576502824833906824088158215654435321174194343608278 40
30	22036605811212608086680346245152659003533243734440584493723376141060440248462261456784117521039 44
31	−14647443433030195462739000661717887394730254225374667277401926157764819457746613618746765535428 88
32	92883774735190013984751091153921929166688083649260096030176161248221227968678534897117163382767 8
33	−56238098745202346065784106733870297253537434102818213916537861978278949661942923133141646546713 6
34	32535623582490630491426244697617679657176485645668627980755743631734927752480441520620794382966 8
35	−17998058139799631880483340068425264282268518374816863788048021823271341767333008007141832612656
36	95259358673342811962577374968024344116759528191118197330901994055953518185301961938058278687152
37	−48268244673830087725415910980532812904398769665363772047167723957702501678922709545345961314952
38	23427392442378901750354958702292727966207504749183723357421289869802194332649685331485983388676
39	−10897163294836081802023740205919221704582045121673085440709523835797116373484015837949721485760
40	48599454814266523936579329821234046480518193517694005958063820441971877885767010759555226651 48

Degree i	Coefficient of T_i
41	−207904128957238188098185113751724325074533022345668006765764345172812939612009330482688553934 4
42	85345156934034839540951711326197573924788985446092029514149493756443513671973966376325917064 8
43	−33630610161443996495786052524700000585795684115954533243583700531832203419403965344775712858 0
44	12725454470346719980621978458560756895786836501871594988003771917946907639722151183549006452 0
45	−46251344543607872597100973940088670916183046876614132396624422211322670222925432802603348764
46	16151229449214495754070501316928248080301470592125995573153793317058666430416170267465079692
47	−54202962300536877409611808661321832293192128042675696098572451721906995630103030459113689 44
48	17485239960158192071225036720539738017598071163290566196637164541987698920667859026525548 78
49	−54229494765515737613852604381445673235158951911804719415165933016830430821515359048620884 4
50	16172935862088003197127926697747570755437801676229023800089356728255453102074455907437632 4
51	−46386918898623721747469881003020417214566850265053511450799223706659896381395790959743804
52	12797051499162896398440721779023796724984325295916014796039628931842465948343894845111380
53	−33960731291127282183393375367146977243292517457421945063649500087943698009424109051521 36
54	86702720947306457174543831661717661462515996518595659847893780613272170139794886945890 0
55	−21296287590476615680805395803290733357695004616562577467766725190478765564375750517632 4
56	50327885532415893880483155785349071253807731172747773207451521031252671732632230388978
57	−11443438667187908543351570986876579176110747490338119245195350888150296055016975582004
58	25035047631266650050175891266591656291838012912819252435787121714620997718496192547 44
59	−52695894494490726849363910367787731695418436441898266807943892019318841189964356850 8
60	10671505159243832893068923900465425354557372171945136004016865774045318994091519231 4
61	−20790779910335793865471457635357833163154112951516080880730395764735512013025652796
62	38965419903200871455947164504224604099782875990822836934859523093659253180056445 00
63	−70244167205371564805355486815123562065021474123895843220794770649160821108131240 0
64	12179062939336260454435758912359743625260655874343481526200304392389746412116719 7
65	−20306355805901050837901846972656773418756565045468863673412540172210337271902340
66	32553505074422165889378358146006809082043237692839569615250232384514395449417 60
67	−50169005990568305372052474188215767011782213273324558007016119024958364468470 28
68	74312275258414477271317122327593160444507387370961124773453087824921327894416
69	−10577404455255469741143362965021672227782124046356528509651977109935992639428
70	14463983282847119606985456600479732190445223334382075635560957615398466072 56
71	−18996519559050912030516397229000562937779126459948317675246839823376324948 4
72	23956016062333717865546677021452562824319209365764369018142153751707952028
73	−28998555162644294897063621488671355604768904635664960247763168224676836 64
74	33683359931378850055967918177671604721038854040218043765411928833939374 0
75	−37529836525283747105371855723169247756700129909528157240024250001998788
76	40095301522358096876408276723413584658915952975974783012918981896548 76
77	−41056981271536043901585339737059454717054548742763593641450004503065 2
78	40277795973917435115762646297317343617205272567786230485171910510652
79	−37837685520390896825866186396558769421033223562235974202642793967 24
80	34020798795632750387882725045726332826531783030015971989498320638 2
81	−29261155514270620208017844865051944340304021710386304703117145200

Degree i	Coefficient of T_i
82	24061104052487871662441632140265623428786778657344129161332003 36
83	−18903837344375768094233491946935556825071199873064095229984149 2
84	14181101939087673375192221173276978973988251595771099469911248
85	−10150596917111792111225081318426758188924091689670001315565 04
86	69273982784497519473037155287005412956159996851830481504940
87	−45040051635760220507955565445689180731282287056046834148 56
88	27874492276556351212259285317610512393696693933756780006
89	−16405810574710923918958669050194823065267996065080494420
90	91737344809504331513970198331912663036906041722630824 0
91	−48685180731396433963474339952113579549797184903456932
92	24494037368619527645021943139544816304646219133773 62
93	−11668388909698006040174735122352180969678329971809 6
94	52563186818231356463761947573837433869055424019 84
95	−22359451725994110851393494125627233660348658308 0
96	89678375699630074810636566180843573845235132 89
97	−33856661178129922433623406133551967355572996 8
98	12010206026853145744238047620715510383030860
99	−39953633627309178324877248552967982461937 2
100	12437443190985072692004053616601920326304
101	−36145402733875238808036434361703296270 4
102	97812705323525026011519194550541504 68
103	−24575889610167342154448004414957471 6
104	57148469132478949027730823596428 58
105	−12255294627563559299465981545866 0
106	24138496344939026324457385784 04
107	−43467840407415668458306853984
108	71188450481406597511706575 4
109	−10538669572997700747046736
110	140021126816597308605612
111	−1655565532193307303324
112	17242140511966984109
113	−156184748605164508
114	1211012431626440
115	−7871527038772
116	41688975082
117	−172657460
118	524076
119	−1036
120	1

これに対し、最近
われわれが　MWL　の方法で構成した例を
次ページに示そう。

とても大きな係数の多項式で
あることは見ての通りだが、
前出の　JKZ　と比較するならば、
はるかに小さな整数係数をもつことが
見てとれるであろう。

T. Shioda:
Some explicit integral polynomials
with Galois group $W(E_8)$
~~Preprint (June 2009).~~
PJA85A (2009), 118–121.

ficients $\Psi(v) = 0$, which is explicitly given as $\Psi(v) = F(v^2)$ with a polynomial $F(X) \in \mathbf{Z}[X]$ of degree 120 below:

$$
\begin{aligned}
& F(X) \qquad (3)\\
= \;& 1 + 60\,X + 1764\,X^2 + 33880\,X^3 + 478890\,X^4 + 5327856\,X^5\\
+ \;& 48793140\,X^6 + 380483064\,X^7 + 2598324795\,X^8 + 15932785020\,X^9\\
+ \;& 89749362936\,X^{10} + 473980028160\,X^{11} + 2387129524492\,X^{12}\\
+ \;& 11610734817520\,X^{13} + 54946822132728\,X^{14} + 253570184893640\,X^{15}\\
+ \;& 1139170471812505\,X^{16} + 4966863067888332\,X^{17} + 20975997259257420\,X^{18}\\
+ \;& 85751930578096488\,X^{19} + 338777493097323270\,X^{20}\\
+ \;& 1286110326634556720\,X^{21} + 4645243511039448812\,X^{22}\\
+ \;& 15781295779679038440\,X^{23} + 49982542358210104135\,X^{24}\\
+ \;& 147131229010289262732\,X^{25} + 404490375319591401040\,X^{26}\\
+ \;& 1051866512316875968008\,X^{27} + 2627876995725411369560\,X^{28}\\
+ \;& 6344305570523224297840\,X^{29} + 14520529565511555036172\,X^{30}\\
+ \;& 29688209277164999351080\,X^{31} + 46109411843449203201495\,X^{32}\\
+ \;& 118746043083251917053 00\,X^{33} - 304520712140489244332444\,X^{34}\\
- \;& 171050760749422630542 7600\,X^{35} - 65643732862172620229726 26\,X^{36}\\
- \;& 20640733068869514203178928\,X^{37} - 55485376072870265785653512\,X^{38}\\
- \;& 12879371307148972920602 3952\,X^{39} - 25774374278394981377949 3007\,X^{40}\\
- \;& 44246997536649454324553 1996\,X^{41} - 65505277692161352414071 7120\,X^{42}\\
- \;& 88447210722247535652156 8192\,X^{43} - 12805755957774303584653 07604\,X^{44}\\
- \;& 22327470939684184754687 36712\,X^{45} - 37096634512516500885282 16368\,X^{46}\\
- \;& 27876421711104355549244 45112\,X^{47} + 10836668436242566282618 846201\,X^{48}\\
+ \;& 58617803145640098757603141084\,X^{49} + 16990117464551970161031508 4748\,X^{50}
\end{aligned}
$$

$$
\begin{aligned}
&+ \quad 364619363395851165251556074640\,X^{51} + 621760817442592188743112149958\,X^{52}\\
&+ \quad 853996995954752839123279092256\,X^{53} + 936403079514859290353492992584\,X^{54}\\
&+ \quad 813242989399427654276532027720\,X^{55} + 561901601257250767568960750119\,X^{56}\\
&+ \quad 135336745534853793043766886324\,X^{57} - 135905665402287183073637739224 8\,X^{58}\\
&- \quad 646319636909292075743622650428 8\,X^{59} - 192746661506033390827809883033 22\,X^{60}\\
&- \quad 430002669623449167760744920713 04\,X^{61} - 738785226609173089001556112534 88\,X^{62}\\
&- \quad 930753262880552741003725365944 00\,X^{63} - 645369846990479645268135815145 42\,X^{64}\\
&+ \quad 493009292938009964620692280764 64\,X^{65} + 252860159656242452092675829367640\,X^{66}\\
&+ \quad 489725119826300703593418835619104\,X^{67} + 660488031167958421155995175713950\,X^{68}\\
&+ \quad 685712147170409615430086676252264\,X^{69} + 551683526957510476762145457969296\,X^{70}\\
&+ \quad 288512672181776185291212516963736\,X^{71} - 742675723987192237475810530869 90\,X^{72}\\
&- \quad 500903915968439620592031943919824\,X^{73} - 910549984484808540102258882764384\,X^{74}\\
&- \quad 120696887361721324519504968215996 0\,X^{75} - 138862930818144679670872232989456 6\,X^{76}\\
&- \quad 156935484471692428275364068856788 8\,X^{77} - 182370747566017074175262718685296 0\,X^{78}\\
&- \quad 204886451142882870578477259955399 2\,X^{79} - 203516627856723318551526862286024 8\,X^{80}\\
&- \quad 168743362738473739530266691638690 4\,X^{81} - 111548275908674001451283908513718 4\,X^{82}\\
&- \quad 526761122020931966446367902077448\,X^{83} - 585778648799393756054504186793 90\,X^{84}\\
&+ \quad 250069449965626638272171839412808\,X^{85} + 387136100056401973048117693037508\,X^{86}\\
&+ \quad 357325360560127756205870421947760\,X^{87} + 211364951183975868623079248436736\,X^{88}\\
&+ \quad 514186277248226946372341123452 96\,X^{89} - 467738653934118744872422114111 32\,X^{90}\\
&- \quad 717745534745000930784056206180 56\,X^{91} - 538294658054476625645705334803 00\,X^{92}\\
&- \quad 230621395973051025402027211479 28\,X^{93} + 181610088533428638393897939104 8\,X^{94}\\
&+ \quad 113809696458089621452140867045 20\,X^{95} + 885536836200186293522568634820 1\,X^{96}\\
&+ \quad 350882311948395822379655302609 2\,X^{97} + 698584814104495914238234637808\,X^{98}\\
&- \quad 706078710984494230280625007 28\,X^{99} - 981800556683347475495524341 82\,X^{100}\\
&+ \quad 139069087931147919858901980 96\,X^{101} + 612926366776909800536055203 92\,X^{102}\\
&+ \quad 401961206524742790546396411 44\,X^{103} + 178551819170392256499519280 83\,X^{104}\\
&+ \quad 633449306664507019256741478 0\,X^{105} + 227878741256845877459023889 6\,X^{106}\\
&+ \quad 737551796202189011654576888\,X^{107} + 432931186611007826071544506\,X^{108}\\
&+ \quad 429301341790049890169381 68\,X^{109} + 538259733452669451411924\,X^{110}\\
&- \quad 849592431713619927676092 0\,X^{111} - 101833461610703030850412 7\,X^{112}\\
&+ \quad 300905188142683299657 00\,X^{113} + 679863686062085630984 64\,X^{114}\\
&+ \quad 589594315627301560499 2\,X^{115} - 448019811798352498176\,X^{116}\\
&- \quad 280668086084640358400\,X^{117} - 3365783326104268800\,X^{118}\\
&+ \quad 1750559212171657216\,X^{119} + 313989595009449984\,X^{120}.
\end{aligned}
$$

証明

$E/\mathbb{Q}(t)$ を楕円曲線

$$y^2 = x^3 + \left(1 + t + t^2 + t^3\right) x + 1 + t + t^2 + t^3 + t^5. \tag{1}$$

$\bar{\mathbb{Q}}$ を $\mathbb{Q}$　の代数的閉包、ガロア群　$Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ は自然に
$E(\bar{\mathbb{Q}}(t)) \cong E_8$ に作用するから、次のガロア表現ができる：

$$\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(E(\bar{\mathbb{Q}}(t))) \cong Aut(E_8) = W(E_8) \tag{2}$$

その像を G は多項式 $\Psi(v) = F(v^2)$ の
ガロア群と等しい。
$G \subset W(E_8) \subset \mathcal{S}_{240}$

証明すべきこと：$G = W(E_8)$

素数 p について、$\Psi_p(X) = \Psi(X)(mod\ p)$
の多項式環 $\mathbb{Z}/p\mathbb{Z}[X]$ での因数分解を考える。

$p = 5, 7, 11, 13, 17$ のとき、
$\Psi_p(X)$ のサイクル型は、それぞれ
$(15)^{16},\ (3)^8(12)^{18},\ (15)^{16},\ (20)^{12},\ (4)^2(8)^{29}.$
になる。よって、次の　lemma から証明終。

Lemma (Jouve-Kowalski-Zywina)
$W(E_8)$ の部分群 H が
サイクル型 $(15)^{16}$，および $(4)^2(8)^{29}$ の元を含めば、
$H = W(E_8)$ である。

予定

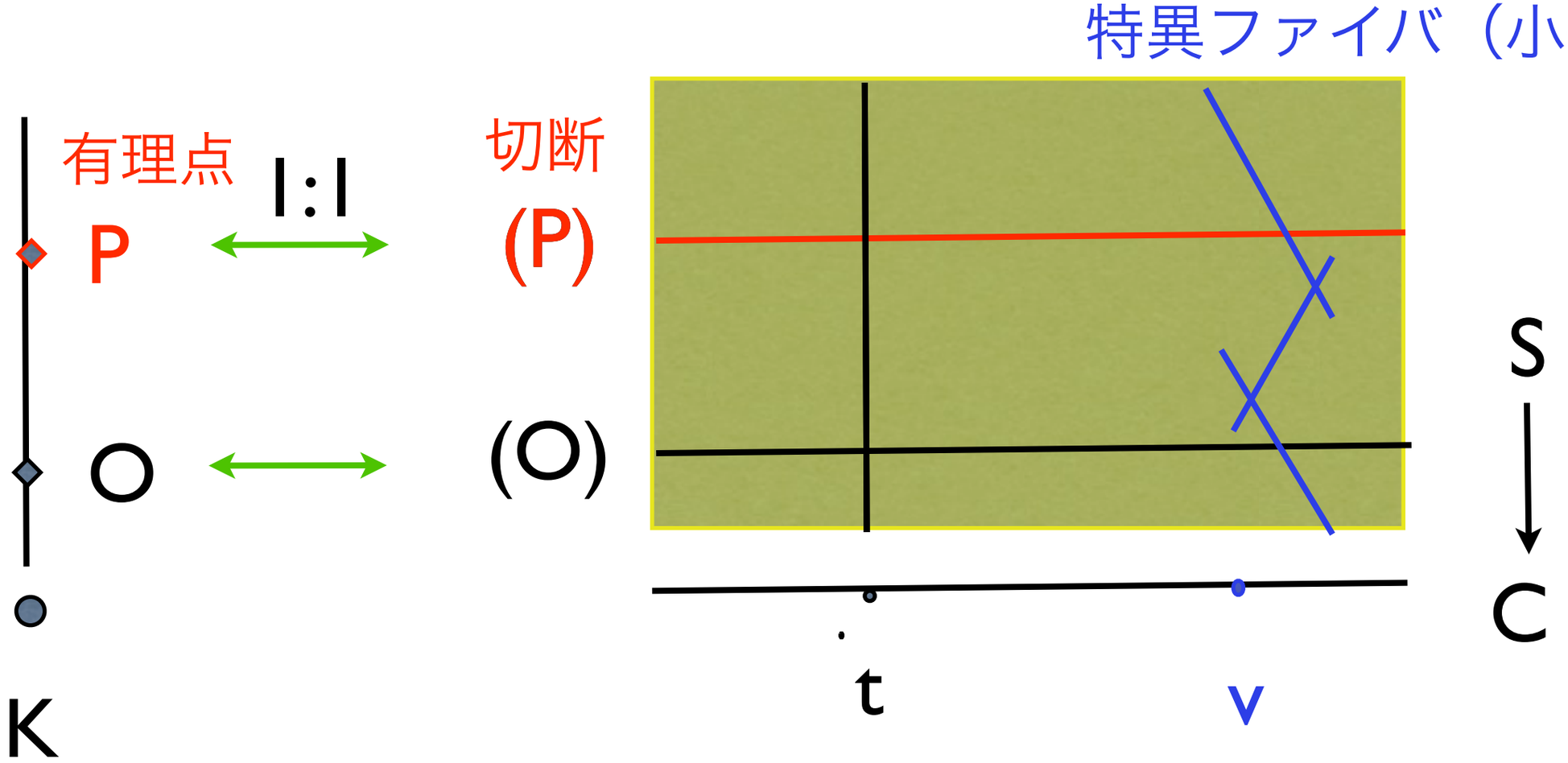
- MWL誕生前後（秘話）
- 代数方程式とMWL
- MWL概観
- 例外型 (E_6, E_7, E_8)方程式論
- 整数点とグレブナ基底
- ガロア群＝$W(E_8)$となる多項式の実例

整数点とグレブナ基底

関数体上の

楕円曲線

E / K ⟷ S: 楕円曲面



P：　　切断 ⟷ 有理点

定義　ゼロ切断と交わらない切断を
整切断, または**整点**とよぶ。

整切断 ⟷ 整数点

$\mathcal{P} := \{P | (P) \cap (O) = \emptyset\}$　　整点の集合
は有限集合である　（ジーゲルの定理の類似）

S：有理楕円曲面 ⟶

P:整点 $\Leftrightarrow$ $P = (x(t), y(t)), \deg x(t) \leq 2, \deg y(t) \leq 3$

$$x(t) = gt^2 + at + b,$$
$$y(t) = ht^3 + ct^2 + dt + e$$

有理楕円曲面 S　の方程式

$$y^2 = x^3 + A(t)x + B(t)$$

に代入、t　について整理

→ t　について６次の恒等式：

$$\phi_0 + \phi_1 t + \cdots + \phi_6 t^6 = 0$$

→ $I = (\phi_0, \phi_1, \cdots, \phi_6)$

多項式環　$R = k[g, h, a, b, c, d, e]$　のイデアル

イデアル　I　　の共通零点　　$V(I)$

→　整点の集合　$\mathcal{P}$

←

（重複度を無視すれば）

問題　　１．整点の個数は？

２．イデアル　I　の線形次元　？

３．重複度は？

I　の準素イデアル分解は？

MWL＋ ルート格子 E_8 ⟹

有理楕円曲面の場合には完全な答：

定理　１．整点の個数 $n \leq 240$

$n = 240 \Leftrightarrow T = 0$ (可約ファイバなし)

２．$\dim_k R/I = 240 - \nu(T)$　　*T: trivial lattice*

３．$I = \mathbf{q}_1 \cap \cdots \cap \mathbf{q}_n$

各重複度　$\dim_k R/\mathbf{q}_i$ = m(P_i)　　*comb. mult.*

他方、上の問題は
グレブナ基底の方法で直接計算できる

（原理的に）

例（ルジャンドル曲面）

$$E : y^2 = x(x-1)(x-t)$$

$$\mathcal{P} = \{P_1 = (0,0), P_2 = (1,0), P_3 = (t,0)\}$$

$$n = 3 \qquad E(K) = \mathcal{P} \cup \{O\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

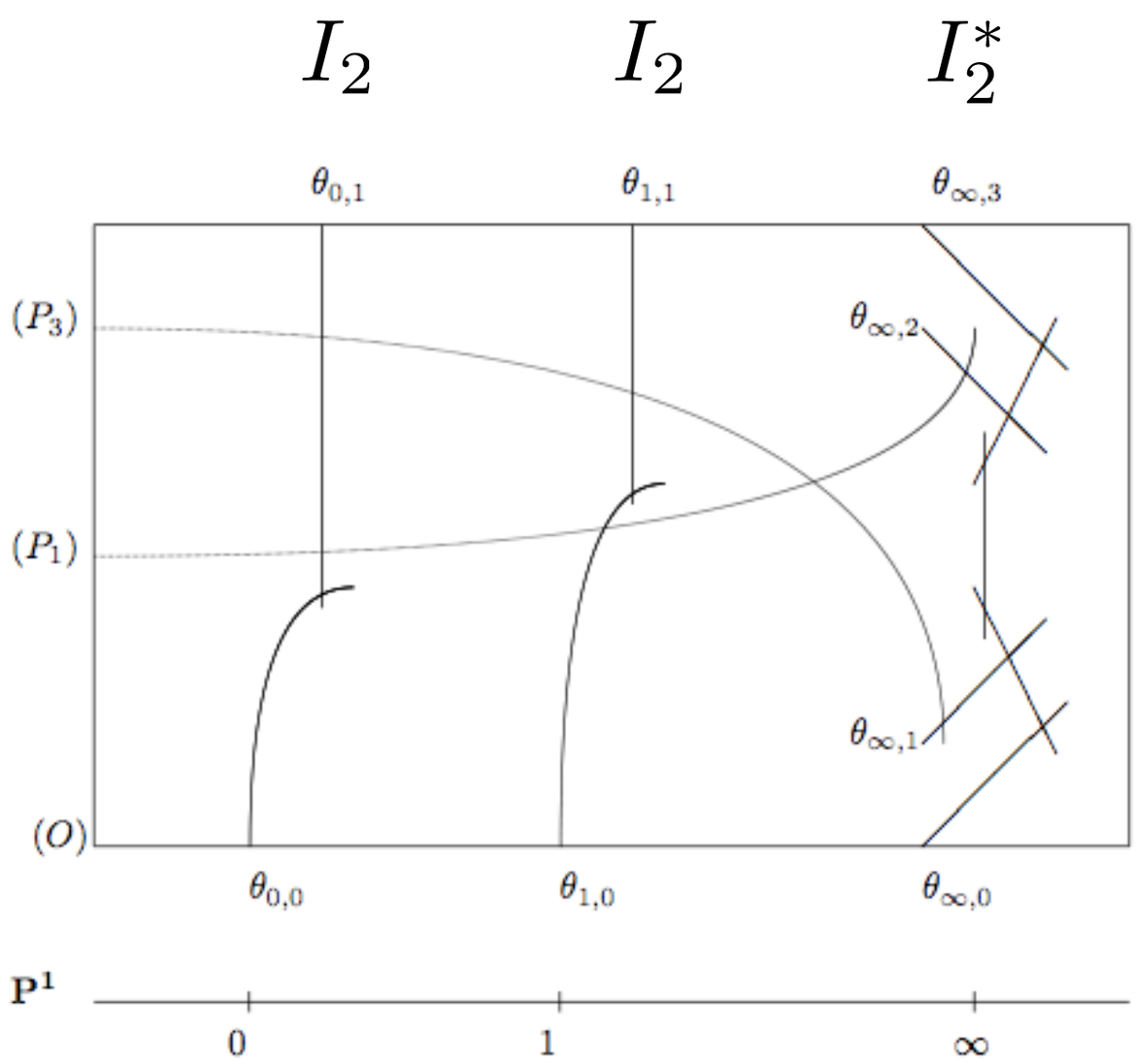
$$I = \mathbf{q}_1 \cap \mathbf{q}_2 \cap \mathbf{q}_3$$

$$\dim_k R/\mathbf{q}_i \quad \textbf{= m(P\_i)} \quad = 64, 64, 48$$

グレブナ基底の直接計算でもチェック

ルジャンドル

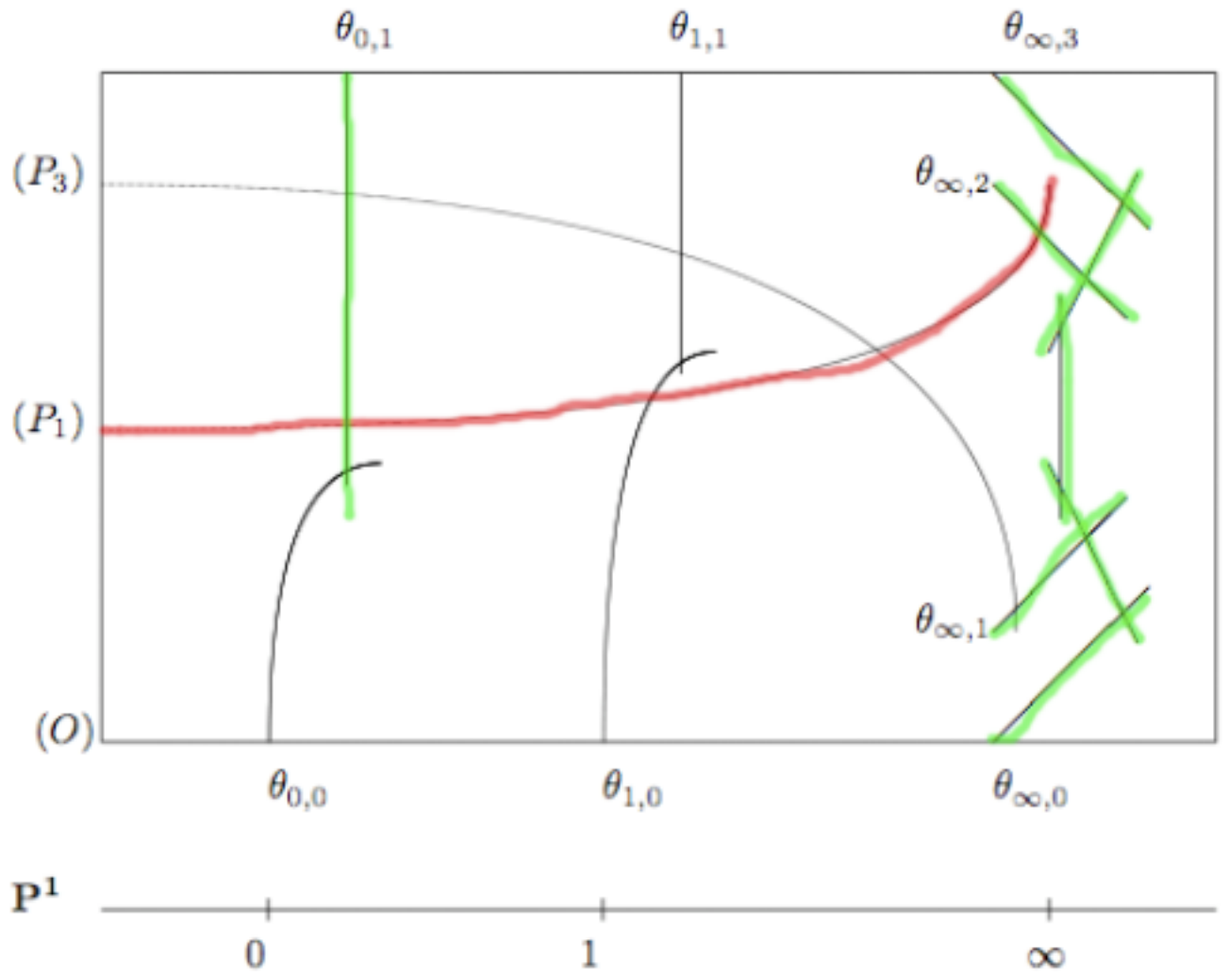
楕円曲面



Trivial lattice: $T = A_1^{\oplus 2} \oplus D_6 \subset E_8$

$$\nu(T) = 2 + 2 + 60 = 64$$

$$\dim_k R/I = 240 - \nu(T) = 176$$



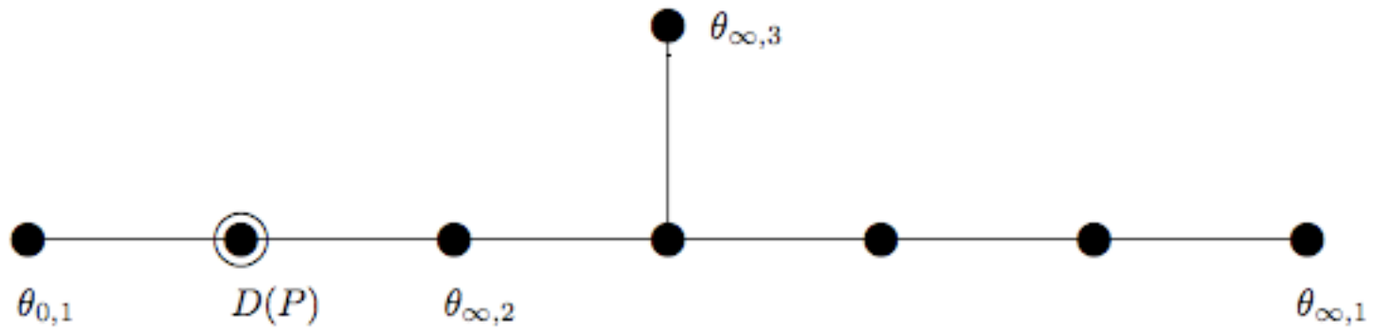
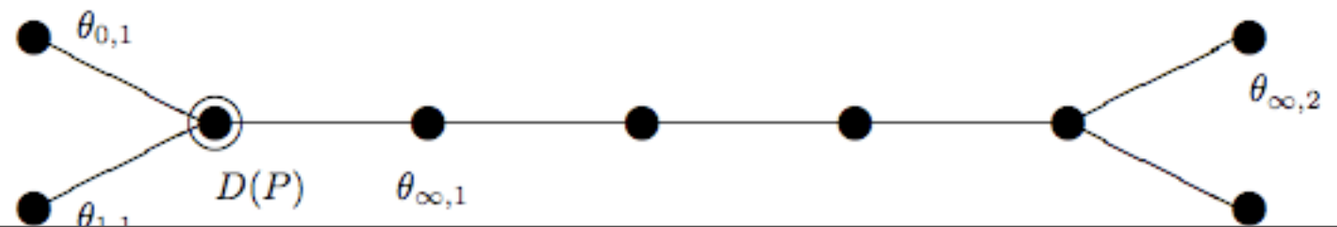


Figure 3: Root graph $\Delta(P)$ for $P = P_1$



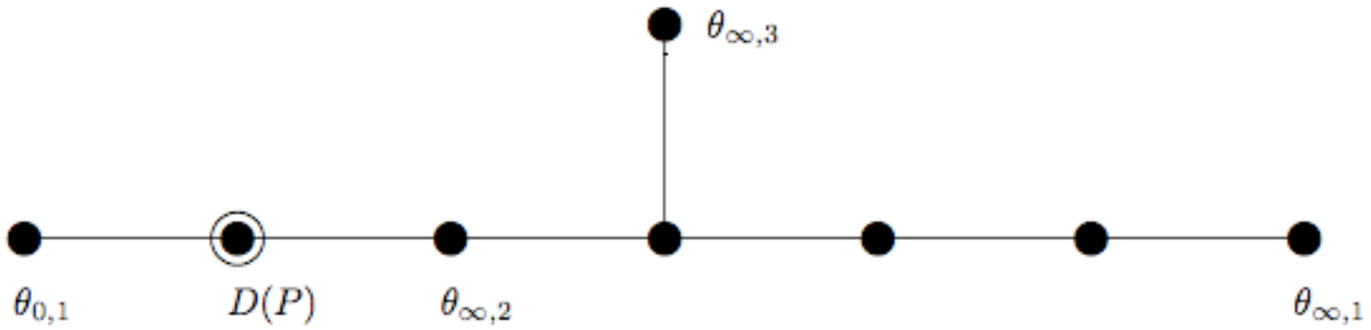


Figure 3: Root graph $\Delta(P)$ for $P = P_1$

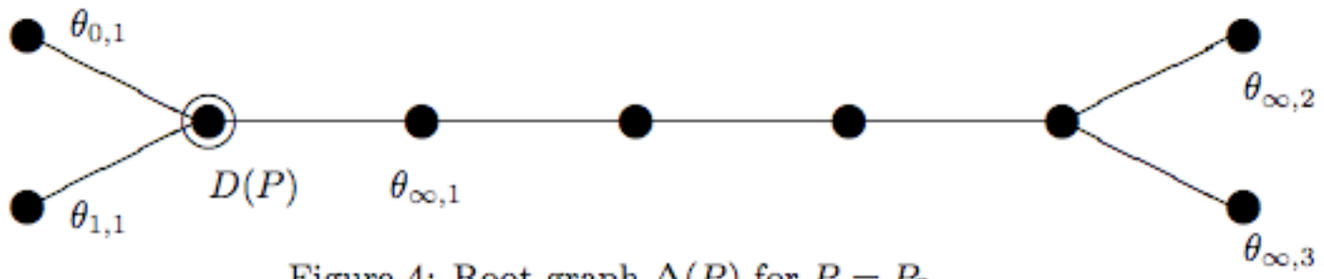


Figure 4: Root graph $\Delta(P)$ for $P = P_3$

combinatorial multiplicity:

m(P)=number of "distinguished roots"
in the root graph for P.

D(P)+lin.combination of other roots .

有理楕円曲面の分類（小木曽・塩田）：

MWL と T により、74種類のタイプに分かれる

(T = trivial lattice)

各タイプについて、

整点の重複度などが決定される。

有理楕円曲面を超えたＫ３曲面等では、

上記の問題はまだよく解明されていない。

以上

Thank you!