

代数学ミニシンポジウム 2016 in 倉敷

—代数幾何学及び学生の自由研究に関する会議—

報告集

高専代数学幾何学研究会編

(世話役：松田修)

2017 年 1 月

はじめに

本論文集は、2016 年 8 月に倉敷市民会館で開催した代数学ミニシンポジウム 2016 in 倉敷 ―代数学幾何学及び学生の自由研究に関する会議―の講演の記録と関連論文をまとめたものです。有志のご協力をいただきこのような報告集を出すことができました。記して感謝を申し上げます。

また、本シンポジウムの開催にあたり、平成 26- 28 年度日本学術振興会科学研究補助金・基盤研究 (C) 課題番号 26381244 (研究代表者：松田修) の支援を受けました。

2017 年 1 月 松田修

代数学ミニシンポジウム 2016

日時 平成 28 年 8 月 27 日 (土), 28 日 (日)

場所 倉敷市民会館 第 5 会議室

世話人 松田 修 (津山高専)

プログラム

8 月 27 日 (土)

9:30–10:40

(1) M_p 完全数と M_p 調和数の研究 桐山翔伍, 松田修 (津山高専)

(2) ルーロー三角形の研究 加田紘大, 圓山夏生, 松田修 (津山高専)

11:00–12:00 北川真也 (岐阜高専)

切断をもたない種数 2 曲線束と仮想モデル・ヴェイユ群

午後の部 代数学及び代数幾何の研究に関する講演

14:00–15:00 前原和寿 (元東京工芸大学)

Sheaves of Monoids and Spectral schemes

15:20–16:20 月岡透 (東海大学)

小収縮を持つ弱ファノ多様体の具体例

16:40–17:40 長峰孝典 (新潟大学)

Derivations having divergence zero

8 月 28 日 (日) 代数学及び代数幾何の研究に関する講演

9:00–10:00 酒井文雄 (埼玉大学)

Invariants of cyclic coverings of the projective line

10:20–11:20 飯高茂 (元学習院大学)

オイラーの完全数

オイラー完全数の新しい展開 (飯高 茂)	・ ・ ・ ・ ・ 1
Invariants of cyclic coverings of the projective line (酒井文雄)	・ ・ ・ ・ ・ 34
Sheaves of Monoids and Spectral schemes (前原和寿)	・ ・ ・ ・ ・ 65
切断をもたない種数2曲線束と仮想モデル・ヴェイユ群 (北川真也)	・ ・ ・ ・ ・ 79
Derivations having divergence zero (長峰孝典)	・ ・ ・ ・ ・ 119
メルセンヌ素数とその派生数の一般化に関する研究 (桐山翔伍)	・ ・ ・ ・ ・ 129
三元整数環のピタゴラス数の分類 (矢部佳史)	・ ・ ・ ・ ・ 140

オイラー完全数の新しい展開

飯高 茂 (学習院大学名誉教授)

平成 28 年 8 月 29 日

1 究極の完全数とその平行移動

本編の目的はオイラー 完全数を新しく導入しその基本定理を確立することである。その前に準備として究極の完全数の定義を復習する。

自然数 a の約数の和を $\sigma(a)$ と書きこれを a の関数と見て ユークリッド関数という。

たとえば, $a = 6$ ならその約数は, 1, 2, 3, 6 なので $\sigma(a) = 12$ となり $\sigma(a) = 2a$ を満たす。

$\sigma(a) = 2a$ を満たす数を完全数というだから 6 は完全数。

数学の好きな小学生, 高校生, 大学生それから熟年世代にいたるまで完全数は人気のあるテーマである。

「496 が完全数であることを示せ。」と言われてできる大学生は少ないと思う。

一方, プロの数学者は完全数を歓迎しない。たとえば A.Weil は『数論 歴史からのアプローチ』足立恒雄・三宅克哉訳、日本評論社、1987 年。p6, 第 1 章 § III, で次のように完全数を軽んじる発言をしている。

ギリシャのみならずそれ以前においても, 完全性という観念が, そのすべての約数の和が自分自身と一致するような整数に結び付けられていた。

ユークリッドの数論に関する巻の最後の定理において $2^n(2^{n+1} - 1)$ はその第二因子が素数であるときには完全数であることが主張されている;

著者自身も, これがその数論的な諸結果の中の白眉であると考えているように思える。この題目とそれに伴って現れるいくつかのものは, 後世の著作にも散発的に顔を出す; 恐らくこれらの概念に付された呼称が特別な興味を惹くのだろう。

フェルマの同時代の人達、メルセンヌやフェルニクル、それにフェルマ自身も結構面白がっており、彼の初期の研究においてはそれなりの位置を占めていたことも事実である。(中略) しかし理論的にはほとんど意味のないものであり、このような歴史的事実がなければ、ここに取り上げる必要もなかったろう。

私は大学を退職後、一般の市民を対象に「数学の研究をはじめよう」をスローガンにして公開の数学研究講座を開いている。そこでも完全数に関連した話しは歓迎される。

P を素数とし固定して考える。与えられた整数 m に関して $\sigma(P^e) + m$ が素数 q のとき $a = P^e q$ を m だけ平行移動した底が P の (狭義の) 究極の完全数と呼ぶ。これは次式を満たす。

$$\overline{P}\sigma(a) - Pa = (P - 2)\text{Maxp}(a) - m(P - 1). \quad (1)$$

$\text{Maxp}(a)$ は a の最大素因子を指している。

これを m だけ平行移動した底が P の狭義の究極の完全数の方程式という。

またこの式を満たす a を m だけ平行移動した底が P の (広義の) 究極の完全数と呼ぶ.

$P = 2$ のとき $\text{Maxp}(a)$ が消えて方程式は

$$\sigma(a) - 2a = -m$$

となる.

$m = 0$ のときにあてはめると $\sigma(a) - 2a = 0$ の解 (すなわち広義の完全数) は狭義の完全数になるか, という古来からある数学界の難問になる.

2 完全数の数表

ここで古典的な 完全数の数表を紹介する.

表 1: 完全数の場合

$e \bmod 4$	e	$e + 1$	$2^e * q$	a	$a \bmod 10$
1	1	2	$2 * 3$	6	6
2	2	3	$2^2 * 7$	28	8
0	4	5	$2^4 * 31$	496	6
2	6	7	$2^6 * 127$	8128	8
0	12	13	$2^{12} * 8191$	33550336 (1456)	6
0	16	17	$2^{16} * 131071$	8589869056 (Cataldi,1588)	6
2	18	19	$2^{18} * 524287$	137438691328 (Cataldi,1588)	8
2	30	31	$2^{30} * 2147483647$	A (Euler, 1772)	8

$$A = 2305843008139952128$$

完全数の定義がなされ 4 つの完全数 (6,28,496,8128) が発見されたのは紀元前のことであった. それから 1500 年以上かかって, 1456 年に第 5 の完全数が発見された. さらに 100 年以上の歳月を経て第 6,7 の完全数が発見され, さらに 100 年以上かかって第 8 の完全数がオイラー (1772 年) によって発見された.

完全数の末尾の数は 6 または 8 であることは古来から注目されていた.

3 オイラー関数と ユークリッド関数

$m = 2$ のときは $\sigma(a) - 2a = -2$ の解は $a = 2^e q$, ($q = 2^{e+1} + 1$: フェルマ素数) と書けるか, という問題になりこれも難問で未だに解けない.

$m = 4$ のときは 広義の完全数で狭義の完全数にならないものはたくさんある. このとき 広義の完全数は $a = 2^e q$ または $a = 2^e q r$ (ここで q, r : 素数) と表せるかという問題がありこれも全く解けない.

そこでいささかセコイのだが, 解けそうな問題を別に考える.

自然数 a と互いに素で a 未満の自然数の個数を $\varphi(a)$ で示しこれをオイラー関数という.

オイラー関数とユークリッド関数とはその本質において親和性がある. たとえば, 両者は乗法をもつ.

乗法性

a, b が互いに素な整数なら,

$$\varphi(ab) = \varphi(a)\varphi(b), \sigma(ab) = \sigma(a)\sigma(b).$$

素数判定法

$a > 1$ のとき, $a - \varphi(a) = 1$ は a が素数になる必要十分条件. そこでオイラー余関数 $\text{co}\varphi(a) = a - \varphi(a)$ を導入する.

$a > 1$ のとき, $a - \sigma(a) = -1$ は a が素数になる必要十分条件.

そこでユークリッド余関数 $\text{co}\sigma(a) = \sigma(a) - a$ を導入する.

3.1 ドグマ

完全数

$2a = \sigma(a)$ のとき a を 完全数 という.

$a = 2\varphi(a)$ のとき a は 2 の累乗. 逆も正しい.

a は 2 の累乗のとき $2a = \sigma(a) + 1$. しかしこの逆が正しいかどうかは不明.

次の大いなるなるドグマは信じるに値すると思う.

ドグマ

$\sigma(a)$ を用いた式や予想は $\varphi(a)$ を用いて適当に修正するとより解きやすい問題ができる. 1 つだけ例をあげる.

3.2 $a = 2p$ 問題

p : 奇素数とすると $a = 2p$ は $2\sigma(a) = 3a + 6$ を満たす. 逆に方程式 $2\sigma(a) = 3a + 6$ を満たす a は $2p$ または 8 .

このオイラー関数版は次の通り.

p : 奇素数とすると $a = 2p$ は $2\varphi(a) = a - 2$ を満たす. 逆に方程式 $2\varphi(a) = a - 2$ を満たす a は $a = 2p$.

$\sigma(a)$ のときに出てきた例外の 8 が $\varphi(a)$ のときは消えてしまう.

これは簡単な問題だが $a = 6p$ 問題を同じように考える $\sigma(a)$ で定式化するとこの問題はきわめて難しい. 古典的な奇数完全数問題よりも難しくさらに興味深い問題と思われる. ここで完全数 6 が出たことに数学における深淵を感じる.

しかし $a = 6p$ 問題を $\varphi(a)$ で定式化するときわめて簡単に解ける.

4 オイラー φ 完全数

ドグマにしたがって, ユークリッド関数の代わりにオイラー関数を使って完全数と類似した概念を定義しよう.

オイラー関数のとき $\varphi(P^e)$, ($e > 1$) は合成数になるので完全数の定義をそのままは使えない. そこで, 1 を加えて $\varphi(P^e) + 1$ が素数 q になるとき $a = P^e q$ をもって P を底とする (狭義) のオイラー φ 完全数と定義する. さて最も簡単な $P = 2$ の場合を定義に沿ってパソコンで計算してみる.

表 2: 2 を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	12	$2^2 * 3$	4
3	40	$2^3 * 5$	16
5	544	$2^5 * 17$	256
9	131584	$2^9 * 257$	65536
17	8590065664	$2^{17} * 65537$	4294967296

この結果をみると, a の素数部分には 3, 5, 17, 257, 65537 のようにフェルマ素数が並んでいるではないか. これには最初びっくりした. そして心が躍った. 冷静になって, 定義に戻り考える:

$q = \varphi(P^e) + 1 = 2^{e-1} + 1$ が素数という条件なので $e - 1 = 2^m$ と書けて結果として q がフェルマ素数になるのは当然である.

完全数の場合のようにこれら q と a の末尾の数をみてみよう. 10 を法としてみればよい.

$e > 4$ なら $e \equiv 1 \pmod{4}; q \equiv 7; a \equiv 4; \varphi(a) \equiv 6 \pmod{10}$ が成り立つ.

5 つのフェルマー素数に応じて 5 つの φ 完全数ができた. これらはフェルマ素数にちなんでフェルマ φ 完全数 と呼ぶ方がよいかもしれない. 後で一般化されたオイラー φ 完全数が導入されるであろう.

5 φ 弱完全数

$k > 0$ に関して, $e = 1 + 4k$, $q_k = 2^{4k} + 1$, $a_k = 2^e q_k$ とおき,
 a_k を 2 を底とする φ 弱完全数 という.

表 3: 2 を底とする φ 弱完全数

$e = 1 + 4k$	q_k	factor	a
5	17	17	544
9	257	257	131584
13	4097	$17 * 241$	33562624
17	65537	65537	8590065664
21	1048577	$17 * 61681$	2199025352704
25	16777217	$97 * 257 * 673$	562949986975744
29	268435457	$17 * 15790321$	144115188612726784
33	4294967297	$641 * 6700417$	36893488156009037824
37	68719476737	$17 * 241 * 433 * 38737$	9444732965876729380864

表 4: 2 を底とする φ 弱完全数, 法を 100

k	e	q_k	a_k
1	5	17	44
2	9	57	84
3	13	97	24
4	17	37	64
5	21	77	4
6	25	17	44
7	29	57	84
8	33	97	24
9	37	37	64

これから次がわかる.

φ 弱完全数 の末尾の数は 4

φ 弱完全数 の末尾 2 桁の数は 44, 84, 24, 64, 04 が繰り返される

$q = 2^{4k} + 1$ の末尾の数は 7

$q = 2^{4k} + 1$ の末尾 2 桁の数は 17, 57, 97, 37, 77 が繰り返される

5.1 3 を底とするとき

$P = 3$ の場合も計算してみる.

$$q = 2 * 3^{e-1} + 1, a = 3^e q.$$

表 5: $P = 3$ を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	63	$3^2 * 7$	36
3	513	$3^3 * 19$	324
5	39609	$3^5 * 163$	26244
6	355023	$3^6 * 487$	236196
7	3190833	$3^7 * 1459$	2125764
10	2324581983	$3^{10} * 39367$	1549681956
17	11118121262251209	$3^{17} * 86093443$	7412080755407364
18	100063090585419903	$3^{18} * 258280327$	66708726798666276

定義には自然に出てくる $q = 2 * 3^{e-1} + 1$: 素数, という条件は今まで扱ったことがない.

ここで登場する素数 7, 19, 163, 487, 1459, $\dots$ は比較的数が多く興味深いものである.

花束を持って彼らまたは 彼女ら (素数を擬人化して呼んでいる) を歓迎しよう.

¹

- $e \equiv 2 \pmod{4}$ のとき $q \equiv 7, a \equiv 3 \pmod{10}$.
- $e \equiv 1 \pmod{4}$ のとき $q \equiv 3, a \equiv 9 \pmod{10}$.
- $e \equiv 3 \pmod{4}$ のとき $q \equiv 9, a \equiv 3 \pmod{10}$.

紙数の関係で証明は略する.

¹アメリカの大学では he,she のように性別の出る単語を嫌って代わりに ze を使うのだそうだ. 新しく登場した素数を英語で書くときは ze を使うといいだろう. ze の複数形は they だそうだ (笑)

6 オイラー φ 完全数の平行移動

m だけ平行移動した オイラー φ 完全数の定義は次の通り.

$\varphi(P^e) + 1 + m, (e > 1)$ が素数 q になるとき $a = P^e q, (e \geq 2)$ を (P を底とする) m だけ平行移動した (狭義の) オイラー φ 完全数の定義とする.

特にこれを満たす a を (φ, m) 完全数とも言う.

6.1 $e = 1$ の場合

この定義では, $e = 1$ の場合を除外している.

実際 $e = 1$ の場合 $\varphi(P^e) = \varphi(P) = P - 1$ なので, $q = \varphi(P^e) + 1 + m = P + m$ は素数になることが条件である.

$a = P^e q = Pq = P(P + m)$ が狭義のオイラー φ 完全数 となって簡単になり過ぎて面白みに欠ける.

$P = 2, e = 1$ の場合は $q = 2 + m$ が素数なら $a = 2(2 + m)$ を m だけ平行移動した狭義のオイラー φ 完全数 になる.

いろいろやってみると $e = 1$ の場合を除外するのは不自然なことでこの場合も取り入れておくのがよいようだ.

6.2 $P = 2, m = -2$

もっとも簡単な $P = 2, m = -2$ の場合を計算してみる.

表 6: $P = 2, m = -2$

a	素因数分解
24	$2^3 * 3$
112	$2^4 * 7$
1984	$2^6 * 31$
32512	$2^8 * 127$
134201344	$2^{14} * 8191$
34359476224	$2^{18} * 131071$
549754765312	$2^{20} * 524287$
9223372032559808512	$2^{32} * 2147483647$

$q = \varphi(P^e) + 1 = 2^{e-1} + 1 - 2 = 2^{e-1} - 1$ が素数という条件なので, q はメルセンヌ素数になり, ここでの $a = 2^e q$ はおしなべて, ユークリッド完全数の 4 倍である.

オイラー φ 完全数を定義してみたらまたユークリッド完全数が出てきた.

6.3 $P = 2, m = 0$

次に $m = 0$ の場合を計算する.

表 7: $P = 2, m = 0$

a	素因数分解
12	$2^2 * 3$
40	$2^3 * 5$
544	$2^5 * 17$
131584	$2^9 * 257$
8590065664	$2^{17} * 65537$

素数部分は フェルマ素数である.

12, 40 はともに $m = 0$ のときのオイラー完全数である. 40 歳になったら第 2 オイラー完全数の祝いをするといい.

7 φ 完全数の方程式

$q = \varphi(P^e) + 1 + m, e > 1$ が素数になるとき $a = P^e q$ とする. (m が負の場合もいれているので, $q > P$ を仮定する.)

$$\varphi(a) = \varphi(P^e q) = P^{e-1} \overline{P} \overline{q}$$

に P を掛けて

$$P\varphi(a) = P^e \overline{P} \overline{q} = P^e \overline{P} (q - 1)$$

により

$$P\varphi(a) = P^e \overline{P} (q - 1) = P^e \overline{P} q - P^e \overline{P}.$$

一方

$$q = \varphi(P^e) + 1 + m = P^{e-1} \overline{P} + 1 + m \text{ なので } P^{e-1} \overline{P} = q - 1 - m.$$

ゆえに

$$P^e \overline{P} = P(q - 1 - m).$$

かくして

$$P\varphi(a) = \overline{P} a - P \overline{\text{Maxp}(a)} + Pm. \quad (2)$$

が得られた.

これが m だけ平行移動した オイラー φ 完全数の方程式である.

オイラー φ 完全数の方程式を満たす解が m だけ平行移動した広義のオイラー φ 完全数と呼ばれる.

$P = 2$ の場合は簡単になる.

$$2\varphi(a) = a - 2\overline{\text{Maxp}(a)} + 2m. \quad (3)$$

φ 完全数の方程式 (*) で定義された数は必ずしも φ 完全数になるわけではない.

φ 完全数においては $q = \varphi(P^e) + 1 + m$ が素数になると仮定されているので $1 + m$ は P で割れない.

φ 完全数の方程式 自身を扱うとき $1 + m$ は P で割れない, などのことにこだわらない. 実際に $m = P - 1$ の場合が重要な結果を与えるのである.

8 計算例

広義のオイラー φ 完全数は狭義のオイラー φ 完全数に比べてどの程度異質なものであるか調べよう. 定義にしたがって誠をつくして計算するほかない.

9 m : 偶数

m : 偶数という条件は健全なものである.

オイラー φ 完全数の方程式の解を全数調査の方法で探す. $a < 1000000$ について

$$2\varphi(a) = a - \overline{2\text{Maxp}(a)} + 2m$$

を満たす a とその素因数分解を求める.

計算時間の関係で a は 1000 万未満で探している.

与えられた $m, e < 100$ について指数分を動かし, $q = 2^{e-1} + 1 + m$ が素数となる場合を調べる $a = 2^e q$ とおくことに比較するとはなはだ能率が悪い.

9.1 $P = 2, m = -2$

表 8: $P = 2, m = -2$

a	素因数分解
24	$2^3 * 3$
112	$2^4 * 7$
1984	$2^6 * 31$
32512	$2^8 * 127$

3, 7, 31, 127 とメルセンヌ素数が並ぶ.

9.2 $P = 2, m = 0$

表 9: $P = 2, m = 0$

a	素因数分解
12	$2^2 * 3$
40	$2^3 * 5$
544	$2^5 * 17$
131584	$2^9 * 257$

3, 5, 17, 257 とフェルマ素数が並ぶ.

9.3 $P = 2, m = 2$

表 10: $P = 2, m = 2$

a	素因数分解
20	$2^2 * 5$
56	$2^3 * 7$
176	$2^4 * 11$
608	$2^5 * 19$
8576	$2^7 * 67$
33536	$2^8 * 131$

9.4 $P = 2, m = 4$

表 11: $P = 2, m = 4$

a	素因数分解
28	$2^2 * 7$
208	$2^4 * 13$
2368	$2^6 * 37$

$m = -2, 0, 2, 4$ とした場合, 解 a は $a = 2^e q$, ($q = 2^{e-1} + 1 + m$: 素数) の形なので想定された形の解が出てくるのみである.

せっかく広義のオイラ完全数を定義しても新しいものがでてこない. これは不思議なのでそのことの証明を試みる.

10 オイラー φ 完全数の方程式の解

φ 完全数の方程式

$$P\varphi(a) = \overline{P}a - P\overline{\text{Maxp}(a)} + Pm$$

について P を法としてみると, $\overline{P}a \equiv 0 \pmod{P}$ が直ちに出るので a は P の倍数になり $a = P^e L$, (L は P で割れない) と書ける. この e は重要な数である.

11 微小解

$m = 0, e = 1$ のとき $a = Pq_0$ ($P > q_0$: 素数), は

$$P\varphi(a) = \overline{P}a - P\overline{\text{Maxp}(a)}$$

の解になることは一般的に証明できる.

実際, $\text{Maxp}(a) = P$ によって

$$P\varphi(a) - \overline{P}a = P\overline{Pq_0} - \overline{P}Pq_0 = -\overline{P}P.$$

$m = 0$ のときの解 $a = Pq_0$ ($P > q_0$: 素数) を微小解という. 微小解は φ 完全数の方程式 (*) に特有の解である.

逆に, $m = 0, e = 1$ のときの解は微小解になることを示すことができる.

$a = PL$, (L は P で割れない) と書けるので $P\varphi(a) = P\overline{P}\varphi(L)$,

$$\overline{P}a - P\overline{\text{Maxp}(a)} = \overline{P}PL - P\overline{q}.$$

よって,

$$P\overline{P}\varphi(L) = \overline{P}PL - P\overline{q}.$$

オイラーの余関数 $\text{co}\varphi(L) = L - \varphi(L)$ を使うと

$$\overline{P}\text{co}\varphi(L) = q - 1.$$

そこで $\pi = \text{Maxp}(L)$ とおく.

1) L が素数なら $\text{co}\varphi(L) = 1$ なので $\overline{P} = q - 1$. ゆえに $P = q$. L は素数なので q_0 と書くと, $P = q = \text{Maxp}(a)$ により $P > q_0$. $a = Pq_0$ が解になる.

2) L が非素数なら $\text{co}\varphi(L) \geq \pi$.

$\overline{P}\text{co}\varphi(L) = q - 1$ によって

$$q - 1 = \overline{P} \operatorname{co} \varphi(L) \geq \overline{P} \pi.$$

a) $P > \pi$ のとき. $q = P$ になり

$$P - 1 = q - 1 = \overline{P} \operatorname{co} \varphi(L) \geq \overline{P} \pi \geq 2\overline{P}.$$

矛盾.

b) $P < \pi$ のとき. $q = \pi$ になり

$$q - 1 \geq \overline{P} \pi = \overline{P} q \geq q.$$

矛盾.

12 定理と証明

次の結果が基本定理である.

定理 1 $m \geq 0$ のとき

$$P\varphi(a) = \overline{P}a + Pm - P\overline{\text{Maxp}(a)}$$

を満たす解は

1. $m = 0, e = 1$ のとき微小解 $a = Pq_0(P > q_0)$ となる.
2. $m = P - 1$ のときの微小解 $a = P^e$ となる.
3. $e > 1$ のとき a は (φ, m) -完全数.
4. $e = 1$ のとき $a = Pq, q = P + m$ は素数.

証明.

$a = P^e L$ (P, L は互いに素) と書けるとき次式を満たす:

$$P\varphi(a) = P^e \overline{P}\varphi(L), \overline{P}a = P^e \overline{P}L.$$

$q = \text{Maxp}(a)$ とおくとこれより

$$P^e \overline{P}\varphi(L) = P^e \overline{P}L + Pm - P\overline{q}$$

余関数 $\text{co}\varphi(L) = L - \varphi(L)$ を用いて,

$$P^e \overline{P}\text{co}\varphi(L) = P\overline{q} - Pm.$$

P で割って

$$P^{e-1} \overline{P}\text{co}\varphi(L) = \overline{q} - m.$$

$L = 1$ のとき $a = P^e, q = P$. さらに $\text{co}\varphi(L) = 0$. よって, $q - 1 = m$ により, $P = q$ なので $m = P - 1$.

$m = P - 1$ のとき, $a = P^e$ も微小解という.

$L \geq 2$ のとき $a = P^e L \geq 2P^e$.

$$P^{e-1} \overline{P}\text{co}\varphi(L) = \overline{q} - m.$$

において

(1) L : 素数なら $\text{co}\varphi(L) = 1$ によって, $P^{e-1} \overline{P} = \overline{q} - m = q - 1 - m$.

$q = P^{e-1}\bar{P} + 1 + m$ が素数になり $a = P^e q$ は狭義のオイラー完全数.
すなわち a は (φ, m) -完全数.

(2) L が素数でないとき. $\pi = \text{Maxp}(L)$ とおく.
 $\text{co}\varphi(L) \geq \pi$ を用いて

$$P^{e-1}\bar{P}\text{co}\varphi(L) = \bar{q} - m \geq P^{e-1}\bar{P}\pi.$$

これより,

$$\bar{q} - m \geq P^{e-1}\bar{P}\pi.$$

(a) $P > \pi$ の場合, $q = \text{Maxp}(a) = P, \pi \geq 2$. これより

$$\bar{q} - m = P - 1 - m \geq P^{e-1}\bar{P} \times 2.$$

$m \geq 0$ によって

$$\bar{P} = P - 1 \geq P - 1 - m \geq P^{e-1}\bar{P} \times 2.$$

これは矛盾.

(b) $P < \pi$ の場合, $q = \text{Maxp}(a) = \pi \geq 2$.
これより

$$\bar{q} - m = \pi - 1 - m \geq P^{e-1}\bar{P}\pi \geq 2\pi.$$

$m \geq 0$ によって

$$\pi - 1 - m \geq 2\pi.$$

これは矛盾.

かくて $e = 1$ のとき $q = P + m$ が素数なら $a = Pq$ は解. これも微小解という. 微小解は形が単純で条件も確かめやすいが, 普通の解に比べて芸のない解なのである.

このようにして, $m \geq 0$ の場合にはオイラーの φ 完全数の基本問題は解決した.

しかし解決しても困ることがある. 問題がなくなって失業状態になるから.

そこで $m < 0$ の場合について詳しく調べることにした.

$P = 2$ の場合に限っても興味ある結果がいろいろ出てきて, 思いのほか豊穡の大地が広がっていたのである.

ここでは $P = 2$ の場合, 広義のオイラー φ 完全数を調べる. この場合, φ 完全数 についての方程式は次のように簡単になる.

$$2\varphi(a) = a + 2m - \overline{2\text{Maxp}(a)}$$

狭義の オイラーの φ 完全数の定義によれば $P = 2$ のとき $q = \varphi(P^e) + 1 + m = 2^{e-1} + 1 + m$ は素数なので m は偶数になる.

しかし方程式 $2\varphi(a) = a + 2m - \overline{2\text{Maxp}(a)}$ ができた以上, m : 奇数の場合も 平等に扱ってやりたい.

このように狭義の完全数ではありえない場合についても探求することが大切 である.

かくして広義の完全数が導入されたが, 実際に出てくるものは何だろうか. 私 はこれらを調べるにあたり心は踊り, ツチノコ²を探するような興奮を覚えたので あった.

$P = 2$ のとき m だけ平行移動した広義のオイラー φ 完全数を次のように分 類した調べる.

I 型. $m \geq 0, m$: 偶数

II 型. $m < 0, m$: 偶数

III 型. $m < 0, m$: 奇数

IV 型. $m \geq 0, m$: 奇数

²日本に生息すると言われる未確認生物. 蛇のようだがもっと太いと言われている.

13 I 型 , $m \geq 0, m : \text{偶数}$

13.1 $P = 2, m = 0; m = 2$

広義のオイラー φ 完全数をもっとも簡単な場合からパソコンで調べよう.

表 12: $P = 2, m = 0; m = 2$

$m = 0$		$m = 2$	
a	素因数分解	a	素因数分解
12	$2^2 * 3$	20	$2^2 * 5$
40	$2^3 * 5$	56	$2^3 * 7$
544	$2^5 * 17$	176	$2^4 * 11$
131584	$2^9 * 257$	608	$2^5 * 19$
		8576	$2^7 * 67$
		33536	$2^8 * 131$

これらの解はすべて $a = 2^e q, q = 2^{e-1} + 1 + m$: 素数の形になっている. これを通常解という. $m \geq 0$ の場合は, オイラー完全数の基本定理により広義のオイラー φ 完全数は狭義のオイラー φ 完全数になる. パソコンによる結果は基本定理を裏付ける.

基本定理がある以上, $m \geq 0$ についてパソコンで調べることはない. 次に $m < 0$ の場合についてパソコンで調べる.

14 II 型, $m < 0, m$: 偶数

14.1 $P = 2, m = -2$

表 13: $P = 2, m = -2$

a	素因数分解	$\varphi(a)$
24	$2^3 * 3$	8
112	$2^4 * 7$	48
1984	$2^6 * 31$	960
32512	$2^8 * 127$	16128

以上の場合は, パソコンによる全数調査の結果. $m = -2; q = 2^{e+1} - 1$: 素数の場合については wxmaxima を用いて, 指数 $e < 21$ について調べると結果はすぐ出る.

表 14: $P = 2, m = -2; q = 2^{e-1} - 1, a = 2^e q$: 素数の場合

e	a	素因数分解	$\varphi(a)$
3	24	$2^3 * 3$	8
4	112	$2^4 * 7$	48
6	1984	$2^6 * 31$	960
8	32512	$2^8 * 127$	16128
14	134201344	$2^{14} * 8191$	67092480
18	34359476224	$2^{18} * 131071$	17179607040
20	549754765312	$2^{20} * 524287$	274876858368

以上からこれらはユークリッドの完全数の 4 倍であることがわかる.

ここでは $a = 2^2 * 3^2$ が $a = 2^e q$ とかけない解でこれを非通常解という.

$a = 36 = 2^2 * 3^2$ のみが非通常解.

14.2 $P = 2, m = -6; m = -8$

$a = 100 = 2^2 * 5^2$ のみが非通常解.

この場合は異常に解が少ない.

しかし指数 $e = 40$ で解が発見された. 何という僥倖!.

$X = 302231454899259247165440$

表 15: $P = 2, m = -4$

a	素因数分解	$\varphi(a)$
36	$2^2 * 3^2$	12
80	$2^4 * 5$	32
416	$2^5 * 13$	192
1856	$2^6 * 29$	896
7808	$2^7 * 61$	3840

表 16: $P = 2, m = -4; q = 2^{e-1} - 3$: 素数の場合

e	a	素因数分解	$\varphi(a)$
3	8	2^3	4
4	80	$2^4 * 5$	32
5	416	$2^5 * 13$	192
6	1856	$2^6 * 29$	896
7	7808	$2^7 * 61$	3840
10	521216	$2^{10} * 509$	260096
11	2091008	$2^{11} * 1021$	1044480
13	33529856	$2^{13} * 4093$	16760832
15	536772608	$2^{15} * 16381$	268369920
21	2199016964096	$2^{21} * 1048573$	1099507433472

表 17: $P = 2, m = -6$

a	素因数分解	$\varphi(a)$
48	$2^4 * 3$	16
100	$2^2 * 5^2$	40
352	$2^5 * 11$	160
7552	$2^7 * 59$	3712
128512	$2^9 * 251$	64000

14.3 $P = 2, m = -10; m = -12$ の場合

$m = -10$ のときの非通常解は $a = 60 = 2^2 * 3 * 5$, $a = 72 = 2^3 * 3^2$.

表 18: $P = 2, m = -6; q = 2^{e-1} - 5$: 素数の場合

e	a	素因数分解	$\varphi(a)$
4	48	$2^4 * 3$	16
5	352	$2^5 * 11$	160
7	7552	$2^7 * 59$	3712
9	128512	$2^9 * 251$	64000
11	2086912	$2^{11} * 1019$	1042432
13	33513472	$2^{13} * 4091$	16752640
19	137436332032	$2^{19} * 262139$	68717903872

表 19: $P = 2, m = -8$

a	素因数分解	$\varphi(a)$
196	$2^2 * 7^2$	84

表 20: $P = 2, m = -8; q = 2^{e+1} - 7$: 素数の場合

e	a	素因数分解	$\varphi(a)$
40	604462909799618005958656	$2^{40} * 549755813881$	X

表 21: $P = 2, m = -10; m = -12$

$m = -10$			$m = -12$			R
a	素因数分解	$\varphi(a)$	a	素因数分解	$\varphi(a)$	
60	$2^2 * 3 * 5$	16	84	$2^2 * 3 * 7$	24	
72	$2^3 * 3^2$	24	160	$2^5 * 5$	64	
224	$2^5 * 7$	96	484	$2^2 * 11^2$	220	
1472	$2^6 * 23$	704	6784	$2^7 * 53$	3328	

$m = -12$ のときの非通常解は $a = 84 = 2^2 * 3 * 7$, $a = 484 = 2^2 * 11^2$.

15 II 型のときの証明

$P = 2$ のとき方程式は $2\varphi(a) = a + 2m - 2(q - 1), (q = \text{Maxp}(a))$ により $a = 2^e L$ (L : 奇数), $S = -m > 0$ とおくとき

$$2^{e-1}\text{co}\varphi(L) = q - 1 + S.$$

$e > 1$ を示すために $e = 1$ と仮定して矛盾を導く.

S と $q - 1$ は偶数なので $\text{co}\varphi(L)$ も偶数.

しかし L は奇数, $\varphi(L)$ は偶数なので $\text{co}\varphi(L) = L - \varphi(L)$ も奇数. これ矛盾した.

かくて $e \geq 2$ が示された.

15.1 $S = 2$ のときの証明

まず簡単な場合を扱う.

$S = 2$ のとき

$$2^{e-1}\text{co}\varphi(L) = q - 1 + S = q + 1.$$

i). L : 素数なら, $\text{co}\varphi(L) = 1$ により, $2^{e-1} = 1 + q$. $q = 2^{e-1} - 1$. これらはメルセンヌ素数. $a = 2^e q = 4 * 2^{e-2} q$; 完全数の 4 倍.

2. L : 非素数なら, $\text{co}\varphi(L) \geq q$ により,

$$2^e \text{co}\varphi(L) = 2(1 + q) \geq 2^e q.$$

$(1 + q) \geq 2^{e-1} q$ になり矛盾. したがって $m = -2$ の場合はユークリッドの完全数の 4 で出来ていること示された.

15.2 $S = 4$ のときの証明

$m = -4$ なので

$$2\varphi(a) = a - 6 - 2q.$$

$a = 2^e L$, L : 奇数, とおくとき

$$2^e \text{co}\varphi(L) = 2(3 + q).$$

1. L : 素数なら, $\text{co}\varphi(L) = 1$ により, $2^{e-1} = 3 + q$. $q = 2^{e-1} - 3$. これらが素数の場合を調べる.

2. L : 非素数なら, $\text{co}\varphi(L) \geq q$ により,

$$2^e \text{co}\varphi(L) = 2(3+q) \geq 2^e q.$$

$3+q \geq 2^{e-1}q$ になる. ゆえに $3 \geq (2^{e-1} - 1)q$. $e \geq 2$ のとき $q = 3, e = 2$ になり

$$2^{e-1} \text{co}\varphi(L) = (3+q)$$

から

$$\text{co}\varphi(L) = 3.$$

よって, $L = q^2, a = 2^2 * 3^2$ が非通常解.

15.3 $S = 10$ のときの証明

$S = 10$ によって

$$2^{e-1} \text{co}\varphi(L) = q + 9.$$

$L = q$: 素数のとき $2^{e-1} - 9 = q$. これは狭義の完全数の場合.

$L = q^2$ のとき

$$2^{e-1}q = q + 9.$$

$(2^{e-1} - 1)q = 9$ により $e = 2, 3$.

$e = 2$ なら $q = 9$ で矛盾.

$e = 3$ なら $q = 3$ となり,

$$2^2 \text{co}\varphi(L) = q + 9 = 12.$$

よって $\text{co}\varphi(L) = 3, L = 3^3; a = 2^3 * 3^2$.

$L = q\mu (q > \text{Maxp}(\mu))$ のとき

$\text{co}\varphi(L) = (q-1)\mu_0 + \mu$. ($\mu_0 = \text{co}\varphi(\mu)$ とおいた.)

i) $\mu_0 = 1$ なら μ : 素数. $L = q\mu$ により

$$2^{e-1}(q + \mu - 1) = q + 9.$$

$e = 2$ のとき

$$2(q + \mu - 1) = q + 9.$$

$$q = 9 + 2 - 2\mu.$$

L : 奇数なので $\mu \geq 3$ により

$\mu = 3$ なら $q = 5$. よって, $a = 2^2 * 3 * 5$.

$\mu \geq 4$ のとき解はない.

$e > 2$ のときは矛盾.

ii) $\mu_0 \geq 3$ なら $L = q\mu$ により

$$\text{co}\varphi(L) = (q - 1)\varphi(L) = (q - 1)\mu_0 + \mu \geq 3(q - 1) + \mu \geq 3q + 6.$$

$$2^{e-1}\text{co}\varphi(L) = q + 9 \geq 2\text{co}\varphi(L) \geq 2(3q + 6).$$

これは矛盾.

16 III 型, $m < 0, m$: 奇数

狭義の オイラーの φ 完全数では起こりえない場合, すなわち m : 奇数でかつ負の数るとき調べる. 個々の場合にパソコンによる計算で調べてみよう.

$S = -m > 0$ とおく. $q = \text{Maxp}(a)$ として a の最大素因子 q を導入すると φ 完全数 についての方程式は

$$2\varphi(a) = a - 2S - 2(q - 1).$$

a は偶数になるので $a = 2^e L$ (L : 奇数) とおくと

$$2^{e-1}\text{co}\varphi(L) = S - 1 + q.$$

S : 奇数なので $S - 1 + q$ も奇数. よって $e = 1; a = 2L$.

狭義の オイラーの φ 完全数では $e \geq 2$ が満たされている. S : 奇数という尋常でない場合なので $e = 1$ になったと理解しておく.

したがってこの場合 φ 完全数 についての方程式は次のようにごく簡単になる:

$$\text{co}\varphi(L) = S - 1 + q.$$

16.1 $S = 1$

$S = 1$ のとき φ 完全数 についての方程式 $\text{co}\varphi(L) = q$ を解く.

以前オイラーの余関数を詳しく調べていたので結果は推測できて $L = q^2$ が解. したがって $a = 2q^2$.

したがって $2\varphi(a) = a - 2q$ なら $a = 2q^2$.

この結果は美しい. この証明は後で与える.

16.2 $S = 3$ の場合の計算結果

$S = 3$ のとき φ 完全数 についての方程式を解く.

$a < 1000,000$ の範囲でパソコンによる解の全数調査をする.

結果として解が無数にでるがみな $a = 6p, (p > 3)$ の形をしている. これを通解という.

表 22: $P = 2, S = 3$

a	素因数分解
$6p, (p > 3)$	$2 * 3 * p$

17 通常解

$S = p$: 奇素数のとき, $p < q$: 奇素数 について $L = pq$ は
 $\text{co}\varphi(L) = p + q - 1$, $S - 1 + q = p - 1 + q$ により $\text{co}\varphi(L) = S - 1 + q$ を満たす.
 $a = 2pq$ は次式の解でこれが通常解である.

$$2\varphi(a) = a - 2p - 2(q - 1).$$

このように, $S = p$: 奇素数のとき通常解 $a = 2pq$ がある.

$S = p$: 合成数のとき通常解はないが散発的な解はありうる. これらの非通常解を見出すことが興味ある課題である.

17.1 $S = 5, 7$ の場合の計算結果

$S = 5$ のとき $a = 10p, (p > 5) = 2 * 5 * p$.
 $a = 10p, (p > 5)$ の形の通常解だけ.

$S = 7$ のとき通常解 $14p = 2 * 7 * p$ 以外に $54 = 2 * 3^3$ が最初にでてきた解で, これが非通常解.

非通常解の決定は興味ある問題である.

現実に行うと手間がかかるので次にパソコンによる結果を与える. すこしずるいが, 時間がないので仕方ない.

17.2 $S \geq 11$ の場合の計算結果

S : 奇数 であるが解の無い場合は記さない. たとえば $S = 9, S = 15$ のとき解はない.

パソコンによる計算の結果, $S = 17$ のとき $a = 2 * 17 * p$ という通常解と非通常解 $a = 90 = 2 * 3^2 * 5$ が出てきた.

これらの結果から非通常解は最小の通常解より小さいことが推定できる.

S : 非素数なら通常解の大きさはどのように評価できるかという問題も自然な問いかけであるが証明できそうもない.

表 23: $P = 2, m < 0, S = -m \geq 11$

S	a	素因数分解
11	$22p, (p > 11)$	$2 * 11 * p$
13	$26p, (p > 13)$	$2 * 13 * p$
17	90	$2 * 3^2 * 5$
17	$34p, (p > 19)$	$2 * 17 * p$
21=3*7	126	$2 * 3^2 * 7$
21	250	$2 * 5^3$
23	$46p, (p > 23)$	$2 * 23 * p$
29	198	$2 * 3^2 * 11$
29	$58p, (p > 29)$	$2 * 29 * p$
31	64	2^6
31	150	$2 * 3 * 5^2$
31	$62p, (p > 31)$	$2 * 31 * p$
33=3*11	234	$2 * 3^2 * 13$
37	$74p, (p > 37)$	$2 * 37 * p$
41	306	$2 * 3^2 * 17$
41	$82p, (p > 41)$	$2 * 41 * p$
43	686	$2 * 7^3$
43	$86p, (p > 43)$	$2 * 43 * p$
45 = 3 ² * 5	342	$2 * 3^2 * 19$
47	$94p, (p > 47)$	$2 * 47p$
49 = 7 ²	350	$2 * 5^2 * 7$
51	210	$2 * 3 * 5 * 7$
53	414	$2 * 3^2 * 23$
53	$106p, (p > 53)$	$2 * 53 * p$
57 = 3 * 19	294	$2 * 3 * 7^2$
59	270	$2 * 3^3 * 5$
59	$2 * 118p, (p > 59)$	$2 * 59 * p$

18 III 型の場合の証明

以上の結果はパソコンでの計算結果なので次に証明を行う。
 $S = 1$ のとき.

$$\text{co}\varphi(L) = q$$

が方程式でこれを解けばよい. q は L の最大素因子で, L は奇数.

18.1 $S = 1$ のときの証明

i) $s(L) = 1$ の場合 $L = q^j$ とおくと、 $\text{co}\varphi(L) = q^{j-1} = q$ により $j = 2$.

ii) $s(L) \geq 2$ の場合. $L = q^j \mu, (q > \text{Maxp}(\mu))$ と書き, $\mu_0 = \text{co}\varphi(\mu)$ とおくと $\text{co}\varphi(L) = q^{j-1}(\mu + \bar{q}\mu_0) = q$.

これにより $j = 1$. $\mu + \bar{q}\mu_0 > q$ が成り立つのでこれはおきない.

よって, 奇素数 q に関して $L = q^2$. よって $a = 2q^2$.

$S = 3, 5$ のときは同様に証明できるので略し, ここでは非通常解の出る最初の例 $S = 7$ を扱う.

18.2 $S = 7$ のときの証明

$$\text{co}\varphi(L) = S - 1 + q = 6 + q$$

が方程式でこれを解けばよい. q は L の最大素因子で, L は奇数.

$L = q^j, (j \geq 2)$ とおくと、 $\text{co}\varphi(L) = q^{j-1} = q + 6$ によって, $j = 3, q^2 - q = 6$.

これより $q = 3$. 非通常解 $a = 2 * 3^3$ がでる.

$L = q\mu, (q > \text{Maxp}(\varphi(\mu)))$ の場合. $\mu_0 = \text{co}(\mu)$ とおくと $\text{co}\varphi(L) = (q - 1)\mu_0 + \mu$ となる.

i) $\mu_0 = 1$.

$\text{co}\varphi(L) = q + \mu - 1$ なので $q + \mu - 1 = q + 6$. よって, $\mu = 7$. $q > 7$ が条件で $a = 2 * 7q = 14q$. これは通常解.

μ が非素数なら, μ は奇数なので 1) $\mu_0 = 3, \mu = 9, 2) \mu_0 = 5, \mu = 25, 3) \mu_0 = 7, \mu = 49, 35$ 等.

1) $\mu_0 \geq 3, \mu$: 非素数のとき, $\mu \geq 9$.

$$\text{co}\varphi(L) \geq 3q + 6, \text{co}\varphi(L) = q + 6 \geq 3q + 6.$$

これは不成立.

18.3 $S = 17$ のときの証明

$$\text{co}\varphi(L) = S - 1 + q = 16 + q$$

が方程式でこれの解を求める.

$L = q^j, j \geq 2$ とおくとき, $\text{co}\varphi(L) = q^{j-1} = q + 16$, によって, $q^{j-1} - q = 16$.
これより $j = 3, q(q-1) = 16$. 不成立

i) $\mu_0 = 1$. μ が素数になるので

$q + \mu - 1 = q + 16$. よって, $\mu = 17$. $q > \mu = 17$ が条件で $a = 2 * 17q = 34q$.

これは通常解.

ii) $\mu_0 > 2$. μ が非素数なので

1) $\mu_0 = 3, \mu = 9$ のとき,

$$\text{co}\varphi(L) = 3q + 6, \text{co}\varphi(L) = q + 16.$$

$3q + 6 = q + 16$ により $2q = 10$. したがって $q = 5, a = 2 * 3^2 * 5$.

18.4 $S = 21$ のときの証明

$$\text{co}\varphi(L) = S - 1 + q = 20 + q$$

が方程式でこれの解を求める.

$L = q^j, (j \geq 2)$ とおくとき, $\text{co}\varphi(L) = q^{j-1} = q + 20$, によって, $q^{j-1} - q = 20$.

これより $j = 3, q(q-1) = 20$. これは解けて $q = 5, a = 2 * 5^3$.

i) $\mu_0 = 1$. μ が素数になるので $q + \mu - 1 = q + 20$. よって, $\mu = 21$. これは素数でない.

μ が非素数なら

1) $\mu_0 = 3, \mu = 9$ のとき,

$$\text{co}\varphi(L) = 3q + 6, \text{co}\varphi(L) = q + 20.$$

$3q + 6 = q + 20$ により $2q = 14$. したがって $q = 7, a = 2 * 3^2 * 7$.

19 IV 型 m : 正の奇数

m : 奇数, 負の数 の場合が済んだので m : 奇数, 正の数 の場合を扱う. この場合は意外なことにきわめて簡単になる. 小さなツチノコを数多く発見した思いがした.

$$P = 2, m = 1, 3, 5, \dots$$

表 24: $P = 2, m = 1, 3, 5, \dots$

m	$a =$ 素因数分解
1	$6=2*3$
3	$10=2*5$
5	$14=2*7$
9	$22=2*11$
11	$26=2*13$
13	none($13+2=15$, 非素数)
15	$34=2*17$
17	$38=2*19$
19	none($19+2=21$, 非素数)
21	$46=2*23$
23	none($(23+2=25$, 非素数)

$m + 2 = q$ のとき解は $a = 2q$ のみ

この場合は解が完全に決まるが面白いものはでてこない.

以下証明.

$\text{co}\varphi(L) = q - 1 - m$ を解く.

L が素数なら $\text{co}\varphi(L) = 1 = q - 1 - m$ なので $q = m + 2$.

L が非素数なら $\text{co}\varphi(L) \geq q$ なので $q \leq \text{co}\varphi(L) = q - 1 - m$. 矛盾.

Invariants of Cyclic Coverings of the Projective Line

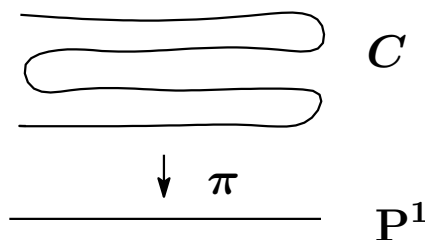
Fumio Sakai

(Kurashiki, August 28, 2016)

1

1 Introduction

A non-singular projective curve C (over $\mathbf{C}$) is a **d -fold cyclic covering of $\mathbf{P}^1$** if there is an automorphism σ of C of order d such that $C/\langle\sigma\rangle \cong \mathbf{P}^1$. Let $\pi : C \rightarrow \mathbf{P}^1$ be the d -fold covering map. We denote by **n** the number of **branch points** on $\mathbf{P}^1$. In this talk, we always consider the case in which $g = \text{genus}(C) \geq 2$.



2

1.1 Equations

Such a curve has the equations ($0 < a_k < d$ for all k):

$$(1) \quad C : y^d = \prod_{k=1}^n (x - \lambda_k)^{a_k} \quad (\text{standard form}),$$

where

$$\text{GCD}(d, a_1, \dots, a_n) = 1 \text{ and } \sum_{k=1}^n a_k \equiv 0 \pmod{d},$$

$$(2) \quad C : y^d = \prod_{k=1}^{n-1} (x - \mu_k)^{a_k} \quad (\text{short form}),$$

where

$$\text{GCD}(d, a_1, \dots, a_{n-1}) = 1 \text{ and } \sum_{k=1}^{n-1} a_k \not\equiv 0 \pmod{d}.$$

3

In (1), the branch points are $\{\lambda_1, \dots, \lambda_n\} \subset \mathbf{P}^1$. In (2), the branch points are $\{\mu_1, \dots, \mu_{n-1}, \infty\} \subset \mathbf{P}^1$.

The automorphism σ of order d is given by

$$\sigma : (x, y) \rightarrow (x, \epsilon y) \quad (\epsilon = e^{2\pi i/d})$$

Example 1. The curve $C : y^7 = x^2(x - 1)$ (short form) can be given by the following equation (standard form).

$$Y^7 = X^2(X - 1)(X + 1)^4.$$

Apply $\phi \in \text{Aut}(\mathbf{P}^1)$ so that $0 \rightarrow 0, 1 \rightarrow 1, \infty \rightarrow -1$:

$$(x, y) \rightarrow \left(\frac{x}{2 - x}, 2^{5/7} \frac{y}{2 - x} \right) = (X, Y).$$

4

1.2 Genus formula

In what follows, we mainly use the **standard form** :

$$C : y^d = \prod_{k=1}^n (x - \lambda_k)^{a_k}.$$

We call $(d; a_1, \dots, a_n)$ the **Type** of C . We may ignore the order of a_k 's. The covering map $\pi : C \rightarrow \mathbf{P}^1$ is given by $(x, y) \rightarrow x$. Over the branch point $\lambda_k \in \mathbf{P}^1$, there are $c_k = \text{GCD}(d, a_k)$ **ramification points** with ramification index d/c_k . Via Hurwitz genus formula, we obtain:

$$g = \frac{(d-1)(n-2)}{2} + \frac{n - \sum_{k=1}^n c_k}{2}.$$

5

If $c_k = 1$, then there is a unique ramification point P_k over λ_k . We say that π is **totally ramified** at P_k .

Condition (T): $\text{GCD}(d, a_k) = 1$ for all k .

We have the implication:

$$d = p \text{ (a prime number)} \Rightarrow \text{Condition (T)}.$$

Lemma 1. *Under Condition (T), we have*

$$g = \frac{(d-1)(n-2)}{2}.$$

6

1.3 Names

Cyclic coverings of $\mathbf{P}^1$ have a lot of different names.

- hyperelliptic curves for $d = 2$,
- **cyclic d -gonal curves**,
- $\mathbf{Z}_d$ -curves,
- **superelliptic curves** for the curve $y^p = f(x)$ (short form), where $f(x)$ is square free ([2]),
- **generalized superelliptic curves** if Condition (T) is satisfied ([4]).

7

1.4 Famous curves

(1) Bring's curve, 1786

$$y^5 = (x^2 - 1)(x^2 + 1)^4 \quad (g = 4)$$

This is the curve of the lowest genus on which S_5 acts.

(2) Klein quartic, 1879

$$C : x^3y + y^3z + z^3x = 0$$

Clearly $\sigma : (x, y, z) \rightarrow (\epsilon^4x, \epsilon^2y, \epsilon z)$ ($\epsilon = e^{2\pi i/7}$) induces an automorphisms of order 7 on C . We can show that C has the equation:

$$y^7 = x^2(x - 1) \quad (\text{short form}).$$

We have $C = \mathbf{H}/\Gamma(7) = X(7)$ (a modular curve).

8

(3) Picard curves, 1883

$$C : y^3 = x(x-1)(x-a)(x-b) \quad (\text{short form})$$

One can show that $\tau(P_\infty) = P_\infty$ for $\tau \in \text{Aut}(C)$.
Picard encountered "Picard modular functions" as the inverse of the period map from the parameter space.

(4) Lefschetz curve, 1920

$$C_a : y^p = x^a(x-1) \quad (\text{short form})$$

Here p is a prime number and $n = 3$. Lefschetz classified $\text{Aut}(C_a)$. Weil determined the Riemann matrices.

9

2 Equivalences and Automorphisms

2.1 Equivalences

$$\text{Let } C : y^d = \prod_{k=1}^n (x - \lambda_k)^{a_k}.$$

Lemma 2. (1) For $\phi \in \text{Aut}(\mathbb{P}^1)$, set $\mu_k = \phi(\lambda_k)$. Then C is isomorphic to the curve: $y^d = \prod_{k=1}^n (x - \mu_k)^{a_k}$.

(2) Take a positive integer m such that $\text{GCD}(d, m) = 1$. Write $ma_k \equiv b_k \pmod{d}$ ($0 < b_k < d$). Then C is isomorphic to the curve: $y^d = \prod_{k=1}^n (x - \lambda_k)^{b_k}$.

10

Proof. (2) Let $\mathbf{C}(C) = \mathbf{C}(x, y)$ be the function field. We have $\mathbf{C}(x, y) = \mathbf{C}(x, y^m)$, since $\mathbf{GCD}(d, m) = 1$. Write $ma_k = b_k + l_k d$. We have $Y^d = \prod_{k=1}^n (x - \lambda_k)^{b_k}$, where $Y = y^m / (\prod_{k=1}^n (x - \lambda_k)^{l_k})$. $\square$

We define the equivalence relation:

$$(d; a_1, \dots, a_n) \sim (d; b_1, \dots, b_n),$$

if there is m with $\mathbf{GCD}(d, m) = 1$ such that $ma_k \equiv b_k \pmod{d}$ for all k .

Example 2. Since $(7; 2, 1, 4) \sim (7; 6, 3, 5)$, we have

$$\{y^7 = x^2(x-1)(x+1)^4\} \cong \{y^7 = x^6(x-1)^3(x+1)^5\}.$$

Theorem 1 ([Nakajo \[15\], 1999](#)). *Let p be a prime number. The two cyclic coverings*

$$C : y^p := \prod_{k=1}^n (x - \lambda_k)^{a_k} \quad \text{and} \quad C' : y^p := \prod_{k=1}^n (x - \mu_k)^{b_k}$$

are isomorphic if and only if there is $\phi \in \mathbf{Aut}(\mathbf{P}^1)$ and $\rho \in S_n$ such that $\phi(\lambda_k) = \mu_{\rho(k)}$ and

$$(p; a_1, \dots, a_n) \sim (p; b_{\rho(1)}, \dots, b_{\rho(n)}).$$

The **if part** follows from Lemma 2. The key in the proof of the **only if part** is the following fact.

Theorem 2 ([Gonzalez-Diez \[9\], 1995](#)). *Let σ_i ($i = 1, 2$) be two automorphisms of order p such that $C/\langle\sigma_i\rangle \cong \mathbf{P}^1$, then the cyclic groups $\langle\sigma_1\rangle$ and $\langle\sigma_2\rangle$ are conjugate in $\text{Aut}(C)$.*

Remark 1. Theorem 1 was conjectured by **M.Namba** in 1981. By the way, **Naoyuki Nakajo** was my former student at **Saitama University**.

Remark 2. In case d is not prime, the situation is different ([Gonzalez-Diez and Hidalgo, 1997](#), for $d = 4, 8$).

13

2.2 Automorphism groups

Let C be a cyclic covering of $\mathbf{P}^1$ with $C/\langle\sigma\rangle = \mathbf{P}^1$. We denote by **Aut(C)** the **automorphism group** of C . We have the following two cases:

Case 1. $\langle\sigma\rangle \triangleleft \text{Aut}(C)$. Thus, $\overline{\text{Aut}(C)} = \text{Aut}(C)/\langle\sigma\rangle$ is a finite subgroup of $\text{Aut}(\mathbf{P}^1)$.

Case 2. $N(\sigma) \subsetneq \text{Aut}(C)$, where $N(\sigma)$ is the normalizer of the cyclic group $\langle\sigma\rangle$ in $\text{Aut}(C)$. An automorphism $\tau \notin N(\sigma)$ is called **exceptional** (Broughton, Wootton).

14

Example 3. For **hyperelliptic curves** ($d = 2$), we have $\langle \sigma \rangle \triangleleft \text{Aut}(C)$, since the double covering $\pi : C \rightarrow \mathbb{P}^1$ is unique.

Theorem 3 (**Kontogeorgis [13], 1999**). *Let $\pi : C \rightarrow \mathbb{P}^1$ be a d -fold cyclic covering with n branch points. Assume*

- (i) Condition (T) is satisfied (i.e, π is fully ramified).
- (ii) $n > 2d$

Then we have $\langle \sigma \rangle \triangleleft \text{Aut}(C)$.

Example 4. Let C be the **Klein curve** $y^7 = x^2(x - 1)$ (short form). It is known that $|\text{Aut}(C)| = 168$ and $|N(\sigma)| = 21$.

15

Example 5. $C : y^2 = \prod_{k=1}^n (x - \lambda_k)$ (hyperelliptic case).

- (1) For general λ_k , we have $\text{Aut}(C) = \mathbb{Z}_2 = \langle \sigma \rangle$.
- (2) For $y^2 = x^{2m} - 1$, we have $\overline{\text{Aut}(C)} = \langle \bar{\tau}, \bar{\rho} \rangle \cong D_{2m}$, where $\bar{\tau}(x) = \zeta x$, $\bar{\rho}(x) = 1/x$ ($\zeta^m = 1$).

In 2005, Kallel and Sjerve [12] gave a complete classification of $\text{Aut}(C)$ for the case in which $n = 3$. In particular, they observed the following phenomenon:

Theorem 4. $\text{Aut}(C)$ is determined only by **Type** $(d; a_1, a_2, a_3)$ for those curves:

$$C : y^d = (x - \lambda_1)^{a_1} (x - \lambda_2)^{a_2} (x - \lambda_3)^{a_3}.$$

16

3 Gonality

Let $\mathbf{C}(C)$ be the **function field** of a curve C . To $\varphi \in \mathbf{C}(C) \setminus \mathbf{C}$, we can associate a holomorphic map

$$\varphi : C \rightarrow \mathbf{P}^1.$$

The **gonality** of C , denoted by $\mathbf{Gon}(C)$ or by G for short, is defined to be the **minimum** of the degrees of such maps:

Let C be a d -fold cyclic covering of $\mathbf{P}^1$. We have $\mathbf{Gon}(C) \leq d$. If $d = p$ (prime) and $n > 2(p - 1)$, then we have $\mathbf{Gon}(C) = p$ (Namba [16], 1979).

17

We list the cases $G = 2$ (**hyperelliptic**) and $G = 3$ (**trigonal**). The list is given by **Types up to equivalence**.

3.1 Classification for $G = 2$

$G = 2$ (Wangyu-Kawasaki-Sakai [22, 23], 2014)

Name	n	Type	d
R	3	$(d; 1_2, d - 2)$	≥ 5
	4	$(d; 1_2, (d - 1)_2)$	≥ 3
S	≥ 6		2
A	≥ 3	except two of a_i 's are divisible by $d/2$,	$\geq 4, 2 \mid d$

18

Example 6. Let us consider Type $(d; 1_2, (d-1)_2)$ curve.

$$C : y^d = (x^2 + 1)(x^2 - 1)^{d-1}.$$

It has an involution $\tau : (x, y) \rightarrow (-x, y)$. We compute the invariant subfield:

$$\mathbf{C}(C)^{\langle \tau \rangle} = \mathbf{C}(x^2, y) = \mathbf{C}(t),$$

where we set $t = y/(x^2 - 1)$. Indeed, we obtain

$$x^2 = \frac{t^d + 1}{t^d - 1}, \quad y = \frac{2t}{t^d - 1}.$$

Thus, $\mathbf{C}(C) \cong \mathbf{C}(x, t)$. We infer from this that C is isomorphic to the hyperelliptic curve:

$$C' : x^2 = (t^d - 1)(t^d + 1).$$

3.2 Classification for $G = 3$

$G = 3$ (Wangyu [24], 2015)

Name	n	Type	d
R	3	$(d; 1, 2, d-3)$	≥ 7
	4	$(d; 1_3, d-3)$	≥ 4
		$(d; 1, 2, d-2, d-1)$	≥ 5
	5	$(d; 1_3, d-2, d-1)$	≥ 4
	6	$(d; 1_3, (d-1)_3)$	≥ 4
S	≥ 5		3
A	≥ 3	except two of a_i 's are divisible by $d/3$,	$\geq 6, 3 \mid d$

Remark 3. As for cyclic coverings on $\mathbf{P}^1$, if $g \leq 8$, then we are able to determine the gonality. For the case in which $g = 9$, it remains to determine the gonality of the following two curves:

$$(6; 1, 2_3, 3_2, 5), \quad (6; 1_2, 2, 3_2, 4_2).$$

It seems they have $G = 6$.

Conjecture. Let C be a cyclic covering of $\mathbf{P}^1$. Then, the gonality $\mathbf{Gon}(C)$ is determined only by its Type.

21

4 White numbers

Let $(d; a_1, \dots, a_n)$ be **Type** of the equation (**standard form**) of a d -fold cyclic covering of $\mathbf{P}^1$ with n branch points. So we assume

$$(C1) \quad \mathbf{GCD}(d, a_1, \dots, a_n) = 1, \quad (C2) \quad \sum_{k=1}^n a_k \equiv 0 \pmod{d}.$$

Definition. For each i with $0 < i < d$, we define

$$\rho_i(d; a_1, \dots, a_n) = \sum_{k=1}^n \left\langle \frac{ia_k}{d} \right\rangle,$$

where $\langle x \rangle$ is the fractional part. I call $\{\rho_1, \dots, \rho_{d-1}\}$ the **White numbers** of Type $(d; a_1, \dots, a_n)$.

22

We have the following properties:

Lemma 3. *Letting $\rho_i = \rho_i(d; a_1, \dots, a_n)$, we have*

- (1) $0 < \rho_i < n$ for all i ,
- (2) We have $\rho_i \in \mathbb{N}$ for all i .

Proof. (1) is a consequence of Condition (C1). We see (2). By definition, we have $\langle ia_k/d \rangle = \text{rem}(ia_k, d)/d$. By Condition (C2), $\sum_{k=1}^n \text{rem}(ia_k, d) \equiv 0 \pmod{d}$, hence we obtain $\rho_i \in \mathbb{N}$. □

Example 7.

i	1	2	3	4	5
$\rho_i(6; 1, 2, 4, 5)$	2	2	1	2	2
$\rho_i(6; 1, 1, 5, 5)$	2	2	2	2	2

For instance, we have

$$\rho_2(6; 1, 2, 4, 5) = \frac{1}{3} + \frac{2}{3} + \frac{1}{3} + \frac{2}{3} = 2.$$

Remark 4. If $(d; a_1, \dots, a_n) \sim (d; b_1, \dots, b_n)$, then by letting $\rho'_i = \rho_i(d; b_1, \dots, b_n)$, we see that $\{\rho'_1, \dots, \rho'_{d-1}\}$ is a **permutation** of $\{\rho_1, \dots, \rho_{d-1}\}$.

4.1 Duality

Lemma 4 (Duality). *We have*

$$(1) \quad \rho_i(d; a_1, \dots, a_n) + \rho_i(d - a_1, \dots, d - a_n) = n - t(i),$$

$$(2) \quad \rho_i(d; a_1, \dots, a_n) + \rho_{d-i}(d; a_1, \dots, a_n) = n - t(i),$$

where $t(i) = \#\{k \mid ia_k \equiv 0 \pmod{d}\}$.

Proof. This is a consequence of the property:

$$\left\langle \frac{ab}{d} \right\rangle + \left\langle \frac{(d-a)b}{d} \right\rangle = \begin{cases} 0 & \text{if } ab \equiv 0 \pmod{d} \\ 1 & \text{otherwise} \end{cases}$$

□

Proposition 1 (Summation formula). *We have*

$$\sum_{i=1}^{d-1} \rho_i(d; a_1, \dots, a_n) = \frac{1}{2} \left\{ nd - \sum_{k=1}^n c_k \right\},$$

where $c_k = \text{GCD}(d, a_k)$ as before.

Proof. Indeed, by Lemma 4, we have

$$\begin{aligned} \sum_{i=1}^{d-1} \rho_i(d; a_1, \dots, a_n) &= \frac{n(d-1)}{2} - \frac{1}{2} \sum_{i=1}^{d-1} t(i) \\ &= \frac{n(d-1)}{2} - \frac{1}{2} \sum_{k=1}^n (c_k - 1). \end{aligned}$$

Note that $\#\{i \mid ia_k \equiv 0 \pmod{d}\} = c_k - 1$.

□

4.2 Base of differentials

We now come back to a d -fold cyclic covering of $\mathbf{P}^1$:

$$C : y^d = \prod_{k=1}^n (x - \lambda_k)^{a_k} \quad (\text{standard form}).$$

There exists a natural automorphism of order d :

$$\sigma : C \ni (x, y) \rightarrow (x, \epsilon y) \in C \quad (\epsilon = e^{2\pi i/d}).$$

The automorphism σ acts on the space of holomorphic differentials $H^0(C, K)$ as $\omega \rightarrow \omega \circ \sigma^{-1}$. We define

$$H^0(C, K)(i) = \text{the eigenspace of } \epsilon^i.$$

27

Theorem 5. *Let C be a d -th cover of $\mathbf{P}^1$ with Type $(d; a_1, \dots, a_n)$. Then we have the equality:*

$$\dim H^0(C, K)(i) = l_i \text{ for } i = 1, \dots, d-1,$$

where $l_i = \rho_i(d; a_1, \dots, a_n) - 1$.

Proof. Note that $l_i \geq 0$. Fix k . Letting $f_k = (x - \lambda_k)$, we define

$$\omega_i = \frac{\prod_{k=1}^n f_k^{q_{k,i}} dx}{y^i},$$

where $q_{k,i} = \text{quo}(ia_k, d)$. We see that $\omega_i \in H^0(C, K)(i)$ if $l_i \geq 1$. For k , set $\Omega_k(i) = \{f_k^m \omega_i \mid m = 0, \dots, l_i - 1\}$. We infer from Proposition 1 that $\sum_{i=1}^{d-1} l_i = g$. We infer that the set $\Omega_k(i)$ is a basis of $H(C, K)(i)$. $\square$

28

Definition. I write

$$N(C) = l_1 l_2 \cdots l_{d-1}$$

and call it the **number plate** of C . In view of Lemma 4, we have the relations:

$$l_i + l_{d-i} = n - 2 - t(i).$$

Thus, we have $0 \leq l_i \leq n - 2$. If d is even, then we have

$$l_{d/2} = \frac{n}{2} - 1 - \frac{1}{2} \#\{k \mid a_k \text{ is even}\}.$$

4.3 Theorem of White

Theorem 6 (White [26], 1964). *For $(d; a_1, a_2, a_3, a_4)$ satisfying Condition (T), the following are equivalent:*

- (i) $\rho_i(d; a_1, a_2, a_3, a_4) = 2$ for all i .
- (ii) After reordering, we have $a_1 + a_2 = d$ and $a_3 + a_4 = d$.

Example 8. We checked: $\rho_i(6; 1, 1, 5, 5) = 2$ for all i .

Remark 5. The purpose of G.K.White was to classify "empty" lattice tetrahedra (a tetrahedra whose vertices are on the lattice $\mathbf{Z}^3$ and contains no lattice points inside other than the vertices).

4.4 Theorem of Chowla

Theorem 7 (Chowla [6], 1970, ...). *Let d be an integer. The numbers*

$$\cot \frac{\pi m}{d} \quad (1 \leq m \leq d/2, \text{ GCD}(d, m) = 1)$$

are linearly independent over $\mathbb{Q}$.

Remark 6. In 1987, Reid [18] obtained a generalization of White's theorem (Terminal Lemma) and observed that it is equivalent to Chowla's theorem.

5 Weierstrass points

Definition. For a point P on a curve C of genus g , let

$$\text{Gap}(P) = \{k_1 < \dots < k_g\}$$

be the gap sequence. As is well known, k is a **gap** if we cannot find a rational function having a pole of order k at P , without poles elsewhere. The **Weierstrass weight** $w(P)$ is defined as

$$w(P) = \sum_{j=1}^g (k_j - j).$$

We say that P is a **Weierstrass point** if

$$w(P) > 0.$$

So P is not a Weierstrass point if

$$\text{Gap}(P) = \{1, 2, \dots, g\}.$$

By duality, k is a gap of P if and only if there is a holomorphic differential ω such that

$$\text{ord}_P(\omega) = k - 1.$$

5.1 Algorithm

Let C be a cyclic covering of Type $(d; a_1, \dots, a_n)$. Suppose $\text{GCD}(d, a_k) = 1$. There is a unique ramification point P_k over λ_k . Recall that

$$l_i = \rho_i(d; a_1, \dots, a_n) - 1.$$

Theorem 8 (Wangyu-Sakai). *We obtain the following formula for the Weierstrass weight of P_k .*

$$w(P_k) = \frac{g(d - g - 1)}{2} + \frac{d}{2} \sum_{i=1}^{d-1} l_i^2 - d \sum_{i=1}^{d-1} l_i \left\langle \frac{ia_k}{d} \right\rangle.$$

To prove Theorem 8, we first show the following facts.

- (i) $1 + \text{ord}_{P_k}(f_k^m \omega_i) = (m + 1)d - \text{rem}(ia_k, d)$,
- (ii) $\text{Gap}(P_k) = \{1 + \text{ord}_{P_k}(\omega) \mid \omega \in \Omega_k\}$,

where $\Omega_k = \cup_{i=1}^{d-1} \Omega_k(i)$ is the basis of $H^0(C, K)$ given in Theorem 5.

With the aid of the formula in Theorem 8, we made a **program** (with **Maple**) to compute Weierstrass weights.

Example 9. Type $(7; 1_2, 2, 3)$. In this case, we have $g = 6$ and $N = 011112$. We obtain

$$\omega_2 = \frac{dx}{y^2}, \quad \omega_3 = \frac{f_4 dx}{y^3}, \quad \omega_4 = \frac{f_3 f_4 dx}{y^4}$$

$$\omega_5 = \frac{f_3 f_4^2 dx}{y^5}, \quad \omega_6 = \frac{f_3 f_4^2 dx}{y^6}$$

k	$\text{Gap}(P_k)$	$w(P_k)$
1	$\{1, 2, 3, 4, 5, 8\}$	2
2	$\{1, 2, 3, 4, 5, 8\}$	2
3	$\{1, 2, 3, 4, 6, 9\}$	4
4	$\{1, 2, 3, 5, 6, 10\}$	6

5.2 Computation

We examined cyclic coverings of $\mathbf{P}^1$ of low genera (up to **11**).

n	Type	N	$w(P_k)$
3	(12; 1, 3, 8)	00000010011	2
	(9; 1, 2, 6)	00010011	2, 1
	(8; 1, 2, 5)	0010011	2₂
	(7; 1, 2, 4)	001011	1₃
4	(4; 1 ₄)	012	2₄
	(6; 1, 3, 4 ₂)	10011	2
5	(3; 1 ₄ , 2)	12	1₄, 2

$g = 3$, non-hyperelliptic case

37

n	Type	N	$w(P_k)$
3	(15; 1, 5, 9)	00000001001011	4₂
	(12; 1, 4, 7)	00001001011	4₂
	(12; 1, 2, 9)	00001000111	3
	(10; 1, 2, 7)	000100111	2, 4
4	(6; 1 ₂ , 2 ₂)	01012	4₂
	(6; 1 ₃ , 3)	00112	3₂
	(6; 1, 2, 4, 5)	11011	2₂
	(5; 1 ₃ , 2)	0112	2₃, 4
	(5; 1, 2, 3, 4)	1111	0₄
5	(6; 2 ₃ , 3 ₂)	11002	{}
	(4; 1 ₃ , 2, 3)	112	1₃, 3
6	(3; 1 ₆)	13	4₆
	(3; 1 ₃ , 2 ₃)	22	2₆

$g = 4$, non-hyperelliptic case

38

5.3 Maximal weight

Theorem 9 (T.Kato [10], 1979). *Let P be a point on a non-hyperelliptic curve C of genus g . We have the bound:*

$$w(P) \leq K(g) = \begin{cases} \frac{g(g-1)}{3} & \text{for } g = 3, 4, 6, 7, 9, 10 \\ \frac{g^2 - 5g + 10}{2} & \text{otherwise.} \end{cases}$$

(i) The cyclic coverings $(3; 1_{g+1}, 2)$ (if $g \equiv 0 \pmod{3}$), $(3; 1_{g+2})$ (if $g \equiv 1 \pmod{3}$) have a point P attaining the weight $g(g-1)/3$.

(ii) For $g = 8$ and $g \geq 11$, the cyclic coverings $(4; 1_3, 2_{g-3}, 3)$ (if g is even), $(4; 1_4, 2_{g-3})$ (if g is odd) have a point P attaining the weight $(g^2 - 5g + 10)/2$.

Example 10. We found further curves C and $P \in C$ attaining the maximal weight $w(P) = K(g)$.

g	G	Type
5	4	$(8; 1_2, 2, 4), (4; 1_4, 2_2)$
	3	$(15; 1, 4, 10), (11; 1, 2, 8), (3; 1_5, 2_2)$
6, 7		omitted
8	4	$(4; 1_3, 2_5, 3)$
9	3	$(30; 1, 9, 20), (27; 1, 8, 18), (20; 1, 2, 17)$ $(15; 1, 9, 10_2), (10; 1_3, 7), (9; 1, 3_3, 8)$ $(6; 1, 3, 4_5), (3; 1_{10}, 2)$
	4	$(12; 1, 2, 6_2, 9), (6; 1_3, 3_5), (4; 1_3, 2_7, 3)$ $(33; 1, 11, 21), (30; 1, 10, 19), (22; 1, 2, 19)$ $(15; 1, 4, 5_2), (11; 1_3, 8), (6; 1_2, 2_5), (3; 1_{12})$
10	3	$(15; 1, 4, 5_2), (11; 1_3, 8), (6; 1_2, 2_5), (3; 1_{12})$
11	4	$(8; 1, 2, 4_4, 5), (4; 1_4, 2_8)$

5.4 Fixed points

Theorem 10 ([Lewittes \[14\], 1964](#)). *Let σ be a non-trivial automorphism acting on a curve C of genus $g \geq 2$. Set $b = \#(\text{Fix}(\sigma))$. If $b \geq 5$, then all fixed points of σ are Weierstrass points.*

After the result of Lewittes, we have the following developments.

Theorem 11 ([K.Yoshida \[27\], 1993](#)). *For $b = 2, 3, 4$, he classified the structure of the cases for which there exist non-Weierstrass fixed points.*

In his proof, Yoshida used the [Eichler trace formula](#).

41

Example 11. For cyclic coverings of $\mathbf{P}^1$, according to Yoshida's results, we have the following classification up to the equivalence of Types .

b	g	Type	$w(P_k)$	d
2	$(d-2)/2$	$(d; 1_2, d-2)$	0_2	$\geq 6, \text{ even}$
3	$(d-1)/2$	$(d; 1_2, d-2)$	$0_2, *$	$\geq 5, \text{ odd}$
4	$d-1$	$(d; 1, a, d-a, d-1)$	0_4	$d \geq 3,$ $\text{GCD}(d, a) = 1$

non-Weierstrass fixed points

42

Theorem 12 (**Perez del Pozo [17], 2006**). For $b \geq 5$, he found the lower bounds of the Weierstrass weights of fixed points of an automorphism σ of order d on a curve of genus ≥ 2 . Let P be a fixed point of σ . Then

$$w(P) \geq \bar{w},$$

where

$$\bar{w} = \begin{cases} \frac{(d-1)(b-2)(b-4)}{8} & \text{if } b \text{ is even ,} \\ \frac{(d-1)(b-3)^2}{8} & \text{if } b \text{ is odd .} \end{cases}$$

Theorem 13 (Wangyu-Kawasaki-Sakai [25]). Let C be a d -fold cyclic covering of $\mathbf{P}^1$ of genus ≥ 2 with $b \geq 5$. Let $(d; a_1, \dots, a_n)$ be its Type. Assume that C has a fixed point P_k of σ with $w(P_k) = \bar{w}$. Then we have $b = n$ and we have one of the following cases:

(i) n and d are odd.

(i-1) $d = 3$. Letting $n = 2r + 3$, Type is equivalent to $(3; 1_{r+3}, 2_r)$,

(i-2) $d \geq 5$. Letting $n = 2r + 1$ and after reordering a_k 's, we have $a_{2j-1} + a_{2j} = d$ for $j = 1, \dots, r - 1$. and $a_{2r-1} = a_{2r}$ and $a_{2r-1} + a_{2r} + a_{2r+1} = d$.

(ii) n is even. Letting $n = 2r + 2$ and after reordering a_k 's, we have $a_{2j-1} + a_{2j} = d$ for $j = 1, \dots, r + 1$.

Remark 7. We used Theorem 7. We also showed that

$$(1) \text{ Case (i)} \iff l_i = \begin{cases} (n-3)/2 & \text{for } i \leq (d-1)/2 \\ (n-1)/2 & \text{for } (d+1)/2 \leq i \end{cases}$$

(Up to equivalence of Types)

$$(2) \text{ Case (ii)} \iff l_i = n/2 - 1 \text{ for all } i.$$

g	Type	N	$w(P_k)$	Case
3	(3; 1 ₄ , 2)	12	1 ₄ , 2	(i - 1)
6	(5; 1 ₂ , 2, 3 ₂)	1122	2 ₂ , 5, 3 ₂	(i - 2)
9	(7; 1 ₃ , 5, 6)	111222	3 ₃ , 6, 12	
5	(3; 1 ₅ , 2 ₂)	23	4 ₅ , 5 ₂	(i - 1)
4	(3; 1 ₃ , 2 ₃)	22	2 ₆	(ii)
6	(4; 1 ₃ , 3 ₃)	222	3 ₆	
8	(5; 1 ₂ , 2, 3, 4 ₂)	2222	4 ₆	

5.5 Total Weierstrass weight

Let C be a d -fold cyclic covering of $\mathbf{P}^1$ with n branch points. Under Condition (T), we consider the sum of Weierstrass weights of all ramification points $P_1, \dots, P_n$.

$$TW(C) = \sum_{k=1}^n w(P_k).$$

Theorem 14. *We have the following formula:*

$$TW(C) = \frac{d(n-2)}{2} \sum_{i=1}^{d-1} l_i^2 - \frac{g\{(d-1)(n-2)^2 + 4\}}{4}.$$

Corollary. *We have the following lower bound:*

$$TW(C) \geq \begin{cases} \frac{g(n-4)n}{4} & \text{if } n \text{ is even ,} \\ \frac{g\{(n-4)n+d\}}{4} & \text{if } n \text{ is odd .} \end{cases}$$

The lower bound is attained in the following cases:

- (i) n is even. $l_i = n/2 - 1$ for all i . As a consequence, we have $w(P_k) = \bar{w}$ for all k . See Theorem 13, Case (ii).
- (ii) n is odd. $\{l_i, l_{d-i}\} = \{(n-3)/2, (n-1)/2\}$ for all i . Note that under Condition (T), d is also odd.

47

Example 12. *For $(d, n) = (11, 5)$, the lower bound 60 for $TW(C)$ is attained by the following Types.*

Type	N	$w(P_k)$
(11; 1 ₃ , 9, 10)	1111122222	5 ₃ , 15, 30
(11; 1 ₂ , 2, 9 ₂)	1111122222	5 ₂ , 20, 15 ₂
(11; 1 ₂ , 3, 8, 9)	1111122222	5 ₂ , 13, 22, 15
(11; 1 ₂ , 4, 7, 9)	1111122222	5 ₂ , 17, 18, 15
(11; 1 ₂ , 5, 6, 9)	1111122222	5 ₂ , 21, 14, 15
(11; 1 ₂ , 2, 8, 10)	1112211222	9 ₂ , 6, 10, 26
(11; 1 ₂ , 3, 7, 10)	1121122122	10 ₂ , 6, 9, 25
(11; 1 ₂ , 4, 6, 10)	1111212222	6 ₂ , 10, 9, 29
(11; 1, 2, 3, 6, 10)	1121212122	11, 10, 9, 6, 24
(11; 1, 2, 3, 7, 9)	1121122122	10, 19, 6, 9, 16
(11; 1 ₂ , 5, 7, 8)	1112121222	8 ₂ , 14, 17, 13
(11; 1, 3, 4, 5, 9)	1211122212	12 ₅

48

6 Higher Weierstrass Points

We discuss the space of m -differentials $H^0(C, mK)$. We know that $g_m = \dim H^0(C, mK) = (2m - 1)(g - 1)$ for $m \geq 2$. Let us again consider the curve:

$$C : y^d = \prod_{k=1}^n (x - \lambda_k)^{a_k}$$

with the action $\sigma : (x, y) \rightarrow (x, \epsilon y)$ of order d . As before, we denote by

$$H^0(C, mK)(i)$$

the eigen space for the eigenvalue ϵ^i . But for $m \geq 2$, we have to include the case: $i = 0$.

49

Definition. The notion of **m -Weierstrass points** is defined by the zero order of m -differentials. Namely, k is an m -gap if there is a holomorphic m -differential ω such that

$$1 + \text{ord}_P(\omega) = k.$$

We denote by $\text{Gap}^{(m)}(P) = \{k_1 < \dots < k_{g_m}\}$ be the set of m -gaps. We define the m -Weierstrass weight:

$$w^{(m)}(P) = \sum_{j=1}^{g_m} (k_j - j).$$

We say P is an m -Weierstrass point if $w^{(m)}(P) > 0$.

50

Theorem 15. Let C be a d -fold cyclic covering of $\mathbf{P}^1$ with Type $(d; a_1, \dots, a_n)$. Write $\rho_i = \rho_i(d; a_1, \dots, a_n)$. Then

(i) $\dim H^0(C, 2K)(i) = l_i^{(2)}$, where $l_0^{(2)} = n - 3$ and

$$l_i^{(2)} = l_0^{(2)} + \rho_i - \#\{k \mid \text{rem}(ia_k, d) = d - c_k\},$$

for $i \geq 1$ except for $(d, n) = (2, 4), (3, 3)$.

(ii) $\dim H^0(C, 3K)(i) = l_i^{(3)}$, where

$$l_0^{(3)} = 2n - 5 - \#\{k \mid e_k = 2\} \text{ and}$$

$$l_i^{(3)} = l_0^{(3)} + \rho_i - \#\{k \mid e_k \geq 3, \text{rem}(ia_k, d) \geq d - 2c_k\}$$

for $i \geq 1$ except for $(d, n) = (3, 3)$. Here $e_k = d/c_k$.

Theorem 16. Suppose $\text{GCD}(d, a_k) = 1$. We have

$$\begin{aligned} w^{(2)}(P_k) = & \frac{g_2(d - g_2 - 1)}{2} + \frac{d}{2} \sum_{i=0}^{d-1} (l_i^{(2)})^2 \\ & - \sum_{i=0, \neq i^*}^{d-1} l_i^{(2)} \left(d \left\langle \frac{ia_k}{d} \right\rangle + 1 \right), \end{aligned}$$

$$\begin{aligned} w^{(3)}(P_k) = & \frac{g_3(d - g_3 - 1)}{2} + \frac{d}{2} \sum_{i=0}^{d-1} (l_i^{(3)})^2 - l_{i^*}^{(3)} \\ & - \sum_{i=0, \neq i^*, i^{**}}^{d-1} l_i^{(3)} \left(d \left\langle \frac{ia_k}{d} \right\rangle + 2 \right), \end{aligned}$$

where $\text{rem}(i^* a_k, d) = d - 1$ and $\text{rem}(i^{**} a_k, d) = d - 2$.

Duma [7] (1978) obtained the upper bounds for $m \geq 2$:

(1) For a non-Weierstrass point P , one has

$$w^{(m)}(P) \leq \left(\frac{g+1}{2} \right)^2$$

(2) For a Weierstrass point P on a hyperelliptic curve, one has

$$w^{(m)}(P) = \frac{g(g+1)}{2}.$$

(3) For a Weierstrass point P on a non-hyperelliptic curve, one has

$$w^{(m)}(P) \leq w(P) + \left(\frac{g+1}{2} \right)^2.$$

Example 13. Cyclic coverings of Type $(d; 1_2, d-2)$ in Example 11 are hyperelliptic curves. The ramification point P_1 is not a Weierstrass point. We obtain

$$\begin{aligned} w^{(2)}(P_1) &= \left[\left(\frac{g+1}{2} \right)^2 \right] \text{ for } d = 10, 12, 14, \\ w^{(3)}(P_1) &= \left[\left(\frac{g+1}{2} \right)^2 \right] \text{ for } d = 6, 13, 15, 17, 18, 20, 22. \end{aligned}$$

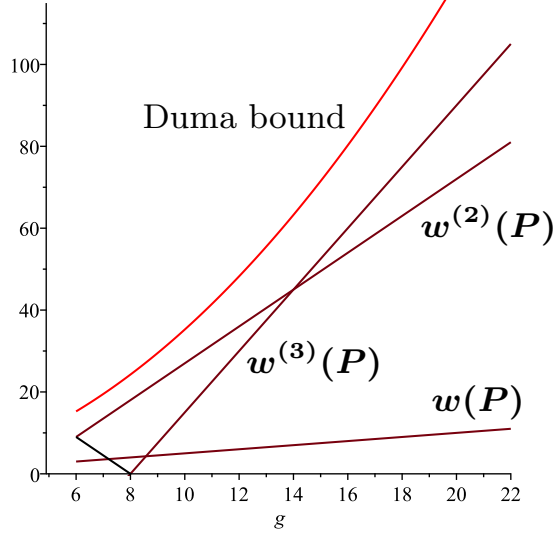
Also Cyclic coverings of Type $(d; 1_2, (d-1)_2)$ given in Example 11 are hyperelliptic curves. The ramification point P_1 is not a Weierstrass point. We obtain

$$\begin{aligned} w^{(2)}(P_1) &= \left[\left(\frac{g+1}{2} \right)^2 \right] \text{ for } d = 5, 6, 7, \\ w^{(3)}(P_1) &= \left[\left(\frac{g+1}{2} \right)^2 \right] \text{ for } d = 3, 9, 10, 11. \end{aligned}$$

Example 14. Cyclic coverings of Type $(d; 1_3, (d-1)_3)$ ($d \geq 4$) in Theorem 13, are trigonal curves ($g = 2(d-1)$). At any ramification point P , we have

$$w(P) = \frac{g}{2}, \quad w^{(2)}(P) = \frac{9}{2}(g-4), \quad w^{(3)}(P) = \frac{15}{2}(g-8).$$

But $w^{(3)}(P) = 9$,
if $g = 6$.



Example 15. We computed the **2** and **3**-Weierstrass weights of cyclic coverings. We give the table for trigonal curves of genus 8.

Type	$w(P_k)$	$w^{(2)}(P_k)$	$w^{(3)}(P_k)$
$(12; 1, 7, 8_2), (6; 1_2, 4_4)$	16_2	16_2	24_2
$(3; 1_8, 2_2)$	$14_8, 16_2$	$8_8, 16_2$	$22_8, 24_2$
$(17; 1, 2, 14)$	$9, 3, 16$	$10, 17, 16$	$13, 12, 17$
$(6; 1_2, 2_3, 4)$	14_2	8_2	22_2
$(12; 1, 4, 8, 11), (6; 1, 2_2, 4_2, 5)$	12_2	0_2	20_2
$(3; 1_5, 2_5)$	12_{10}	0_{10}	20_{10}
$(5; 1_3, 4_3)$	4_6	18_6	0_6
$(10; 1, 2, 8, 9)$	4_2	18_2	0_2
$(9; 1, 2, 7, 8)$	0_4	9_4	11_4

We found the following facts.

Theorem 17. *Let C be a d -fold cyclic covering of $\mathbf{P}^1$. Assume d is prime.*

(i) *If $l_i^{(2)} = l$ for all i , then Type is $(3; 1_r, 2_r)$ ($r \geq 3$) and $l = 2r - 3$. In this case, we have*

$$w^{(2)}(P_k) = 0 \quad \text{for all } k.$$

(i) *If $l_i^{(3)} = l$ for all i , then Type is $(5; 1_r, 2_s, 3_s, 4_r)$ and $l = 4(r + s) - 5$. In this case, we have*

$$w^{(3)}(P_k) = 0 \quad \text{for all } k.$$

Remark 8 (Added after the talk). If $2g - 1$ is a gap, then one has the equalities for all $m \geq 2$ (Accola [1], p.50):

$$w^{(m)}(P) = w(P) + g$$

Homma-Ohmori [11] observed that except for $g = 5$, the above equalities hold for (C, P) with $w(P) = K(g)$. The following curves in Example 10 are exceptional.

g	Type	$w(P_k)$	$w^{(2)}(P_k)$	$w^{(3)}(P_k)$
5	(15; 1, 4, 10)	5 ₂	5 ₂	10 ₂
	(11; 1, 2, 8)	4, 1, 5	3, 8, 6	2, 1, 6
	(3; 1 ₅ , 2 ₂)	4 ₅ , 5 ₂	1 ₅ , 5 ₂	9 ₅ , 10 ₂

For non-hyperelliptic curves, in [11], they also obtained the following upper bound for $m \geq 2$:

$$w^{(m)}(P) \leq K(g) + g.$$

References

- [1] Accola, R. D. M.:Topics in the theory of Riemann surfaces, Springer-Verlag, New York, 1994.
- [2] Bashaj, L., Shaska, T. and Zhupa, E.:The case for superelliptic curves, Advances on Superelliptic Curves, IOS Pr Inc, 1–14, 2015.
- [3] Breuer,T.:Characters and Automorphism Groups of Compact Riemann Surfaces, Cambridge Univ. Press, 2001.
- [4] Broughton, S.A. and Wootton,A.:Exceptional automorphisms of (generalized) superelliptic surfaces, Contemp. Math. **629**, 29–42, 2014.
- [5] Bujalance, E. and Conder,M.:On cyclic groups of automorphisms of Riemann surfaces. J.London Math. Soc. **59**, 573–584, 1999.
- [6] Chowla,S.:The nonexistence of nontrivial linear relations between the roots of a certain irreducible equations, J. Number Theory **2**, 120–123, 1970.

- [7] Duma, A.:Holomorphe Differentiale höherer Ordnung auf kompakten Riemannschen Flächen, Schriftenreihe der Univ. Münster, 2. Serie, Heft 14, 1978.
- [8] Farkas,H.M. and Kra,I.:Riemann Surfaces, Springer-Verlag, New York, 1992.
- [9] Gonzalez-Diez,G.:On prime Galois covering of the Riemann sphere, Ann. Math. Pure Appl. **168**, 1–15, 1995.
- [10] Kato,T.:Non-hyperelliptic Weierstrass points of maximal weight, Math. Ann. **239**, 141–147, 1979.
- [11] Homma,M. and Ohmori,S.:On the weight of higher Weierstrass points, Tsukuba J. Math. **8**, 189–198, 1984.
- [12] Kallel,S. and Sjerne,D.:On the group of automorphisms of cyclic covers of the Riemann sphere, Proc. Camb. Phil. Soc. **138**, 267–287, 2005.
- [13] Kontogeorgis,A.:The group of automorphisms of cyclic extensions of rational function fields, J. Algebra, **216**, 665–706, 1999.

- [14] Lewittes, J.: Automorphisms of compact Riemann surfaces, *Amer. J. Math.* **85**, 734–752, 1963.
- [15] Nakajo, N.: On the equivalence problem of cyclic branched coverings of the Riemann sphere, *Kyushu J. Math.*, **53**, 127–131, 1999.
- [16] Namba, M.: Equivalence problem and automorphism groups of certain compact Riemann surfaces. *Tsukuba J. Math.* **5**, 319–338, 1981.
- [17] Perez Del Pozo, A.L.: On the weights of the fixed points of an automorphism of a compact Riemann surface, *Arch. Math.* **86**, 50–55, 2006.
- [18] Reid, M.: Young person’s guide to canonical singularities, *Algebraic Geometry, Bowdoin 1985*, *Proc. of Symposia in Pure Math.*, A.M.S. **46**, 345–414, 1987.
- [19] Sakai, F.: The gonality of singular plane curves II, *Affine Algebraic Geometry, Proceedings of the Conference*, 243–266, World Scientific Publishing, Singapore, 2013.

- [20] Shaska, T.: Determining the automorphism group of a hyperelliptic curve, *Proc. Int. Symp. on Symbolic Algebraic Computation*, 2003.
- [21] Towse, C.: Weierstrass points on cyclic covers of the projective line, *Trans. Amer. Math. Soc.* **348**, 3355–3378, 1996.
- [22] Wangyu, N., Kawasaki, M. and Sakai, F.: Hyperelliptic curves among cyclic coverings of the projective line I, *Arch. Math.* **101**, 479–484, 2013.
- [23] Wangyu, N. and Sakai, F.: Hyperelliptic curves among cyclic coverings of the projective line II, *Arch. Math.* **102**, 113–116, 2014.
- [24] Wangyu, N.: Cyclic coverings of the projective line with prime gonality, *J. Pure Appl. Algebra*, **219**, 1704–1710, 2015.
- [25] Wangyu, N., Kawasaki, M. and Sakai, F.: On Perez Del Pozo’s lower bound of Weierstrass weight, Preprint.
- [26] White, G.K.: Lattice tetrahedra, *Canad. J. Math.* **16**, 389–396, 1964.
- [27] Yoshida, K.: Automorphisms with fixed points and Weierstrass points of compact Riemann surfaces, *Tsukuba J. Math.* **17**, 221–249, 1993.

Schemes of Monoids and Spectral schemes

Kazuhisa Maehara at Kurashiki

September 5, 2016

Abstract

In this article we shall research Grothendieck-Mochizuki type Galois theory ([Mch], [Gir], [GG], [SGA],[BJ],[AM]). It is a compensation of Fujita-Kawamata theory ([Fuj],[Kaw],[Vieh],[Zuo]) of positivity of direct image of multi power of relative dualizing sheaf on the one side. Furthermore it is a generalization of Kobayashi-Nomizu theory for smooth maps between compact differentiable manifolds on the other. Next to construct schemes from view point of profinite groups we explain Jacob Rulie's theory ([JR1],[JR2],[JR3],[JR4]) and get to schemes with ∞ -category of monoids as geometry. It will be expected to bridge between commutative and non commutative geometries. And we will apply it to Spectral schemes.

1 Introduction

In the first section we build Galois correspondence of the category of objects of fields and morphisms of field extensions which contain transcendental extensions to the opposite of the category of objects of absolute groups and morphisms of closed maps of absolute Galois groups. It can be applied to show Iitaka-Viehweg conjecture([I],[Vieh]) $\text{Max}_{m \geq 1} \kappa(\hat{\det} f_* \omega_{X/S}^{\otimes m}) \geq \text{var}(X/S)$ if a general generic fibre of X/S is of Kodaira dimension ≥ 0 . In the second section and later, we use Jacob Rulie's ∞ -category theory ([JR1],[JR2],[JR3],[JR4]) and ∞ -topos to generalize an ordinary algebraic geometry. By this theory we reconstruct our algebraic geometry from point of view of profinite groups which are pro-objects of finite Galois extension groups. We can dream many geometry by this theory and look forward to laws of universe.beyond them. In the third section we treat the ∞ -category of Rulie's Spectral schemes and make it to correspond the geometric homotopy theory just like in the first section.

2 Application of Mochizuki type Theory

Let k be a function field for a sake of simplicity. Let X and Y be two varieties over k . Consider a dominant rational map:

$$X \rightarrow Y$$

with a general generic fibre an irreducible variety. In case of X and Y of the same dimension, let $k(Y)^{sep}$ be a separable closure in an algebraically closed field containing the function field $k(Y)$ of Y and fix it once for all. Consider the union of all the embedded fields $\{k(X|Y)^\alpha : k(Y)^{sep} \supset k(X|Y)^\alpha \supset k(Y)\}$, where $k(X|Y)^\alpha$ is isomorphic to the abstract maximal separable extension of $k(Y)$ in $k(X)$ over k . Let $\text{Gal}(k(Y)^{sep}/k(X))$ and $\text{Gal}(k(Y)^{sep}/k(Y))$ be the absolute Galois groups of $k(X)$ and $k(Y)$ with Krull topology, respectively. Given $k(X|Y)^\alpha \supset k(Y)$, one has an injective homomorphism $\text{Gal}(k(Y)^{sep}/k(X|Y)^\alpha) \rightarrow \text{Gal}(k(Y)^{sep}/k(Y))$ closed of finite index,i.e.,open. Conversely, given an open inclusion $\text{Gal}(k(Y)^{sep}/k(X|Y)^\alpha) \rightarrow \text{Gal}(k(Y)^{sep}/k(Y))$, one obtains an

extension $k(X|Y)^\alpha/k(Y)$. If the fixed embedding $k(Y)$ into the separable closure $k(Y)^{sep}$, then each embedding is a tosor of $\ker(\text{Gal}(k(Y)^{sep}/k(Y)) \rightarrow \text{Gal}(k^{sep}/k))$. When $X = Y$, one has an isomorphism of the composition:

$$\text{Aut}_k(k(Y)) \rightarrow \text{Aut}_k^{open}(\text{Gal}(k(Y)^{sep}/k(Y))) \rightarrow \text{Aut}_k^{open}(\text{Gal}(k(Y)^{sep}/k(Y)))/\ker(\text{Gal}(k(Y)^{sep}/k(Y)) \rightarrow \text{Gal}(k^{sep}/k))$$

in the situation above.

In case of $\dim X > \dim Y$ and $k(Y)$ is algebraically closed in $k(X)$, consider all the separably closed fields $k(X|Y)_\beta^{sep}$ in the algebraically closed fields of the embedded fields $k(X|Y)_\beta$ containing $k(Y) \subset k(Y)^{sep}$, where $k(X|Y)_\beta$ is isomorphic to the abstract subfield of $k(X)$ which is maximally separable over $k(Y)$. Note that $k(X|Y)_\beta^{sep} \supset k(Y)^{sep}$. Given an extension $k(X)/k(Y)$ which is algebaricall closed in $k(X)$, since

$$k(X|Y)_\beta \cap k(Y)^{sep} = k(Y)$$

one has an open surjective homomorphism

$$\text{Gal}(k(X|Y)_\beta^{sep}/k(X|Y)_\beta) \rightarrow \text{Gal}(k(X|Y)_\beta^{sep}/k(X|Y)_\beta)|_{k(Y)^{sep}} = \text{Gal}(k(Y)^{sep}/k(Y))$$

Conversely, an open surjective homomorphism

$$\text{Gal}(k(X|Y)_\beta^{sep}/k(X|Y)_\beta) \rightarrow \text{Gal}(k(Y)^{sep}/k(Y))$$

gives a subfield extension of $k(X)/k(Y)$ which is separably closed in $k(X)$, since

$$\text{Gal}(k(X|Y)_\beta^{sep}/k(X|Y)_\beta) \rightarrow \text{Gal}(k(Y)^{sep}/(k(X|Y)_\beta \cap k(Y)^{sep})) \simeq \text{Gal}(k(Y)^{sep}/k(Y))$$

and

$$k(X|Y)_\beta \cap k(Y)^{sep} = k(Y)$$

In general case, we derive the consequence composed above. Let Γ_k denote the absolute Galois group of k and G denote the Grothendieck π_1 of the general generic fibre of $\text{Spec}k(X) \rightarrow \text{Spec}k(Y)$, where the general generic fibre is the pullback of $\text{Spec}k(X) \rightarrow \text{Spec}k(Y)$ along $\text{Spec}k(Y)^{sep} \rightarrow \text{Spec}k(Y)$,i.e.,

$$G = \ker \left(\pi_1(\text{Spec}k(X|Y)_\beta, \text{Spec}k(X|Y)_\beta^{sep}) \rightarrow \pi_1(\text{Spec}k(Y), \text{Spec}k(Y)^{sep}) \right)$$

We have the following commutative diagram by Breen([Breen1],[Breen2],[AM]):

$$\begin{array}{ccc} H^1(\Gamma_k, \text{Aut}(G)) & \longrightarrow & H^1(\Gamma_k, (G \rightarrow \text{Aut}(G))) \\ & \searrow & \downarrow \\ & & H^1(\Gamma_k, \text{Out}(G)) \end{array}$$

where $(G \rightarrow \text{Aut}(G))$ denotes the crossed module and $H^1(\Gamma_k, (G \rightarrow \text{Aut}(G)))$ represents the extensions classes of Γ_k by G , i.e., the deformation $\text{Spec}k(X)/\text{Spec}k(Y)$ of the general generic fibre of $\text{Spec}k(X) \rightarrow \text{Spec}k(Y)$.

Note that

$$\text{Aut}_k \text{Spec}k(X_{\bar{\eta}}) \simeq \text{Aut}_{\Gamma_k}^{open} G \subset \text{Aut}(G) \rightarrow \text{Out}(G)$$

where $\text{Spec}k(X_{\bar{\eta}})$ denotes a general generic fibre of $\text{Spec}k(X) \rightarrow \text{Spec}k(Y)$ and the composite map splits.

Lemma 2.1. *Let k be a field which is not separably closed, i.e., the absolute Galois group $\Gamma_k \neq 1$. Let X and Y be varieties over k . Assume that X is birationally trivial over k . Suppose given a separable dominant rational map $f : X \rightarrow Y$ over k , the general generic fibre of f should be of Kodaira dimension ≥ 0 . Then Y is birationally isotrivial over k , i.e., $\text{var}(Y/k) = 0$.*

Proof. From assumption we have a homomorphic section $\text{Speck} \rightarrow \text{Speck}(Y)$ since $\text{Speck}(X)$ is trivial and it has a homomorphic section of $\text{Speck}(X)/\text{Speck}$. Hence $\pi_1(\text{Speck}(Y))/\Gamma_k$ is semi-direct product of G with Γ_k . Thus Γ_k acts on G in the way that for any $g \in G$ we have an action $g \mapsto g^s = \varphi(s)^{-1}g\varphi(s) \in G$, which is continuous. In the commutative diagram

$$\begin{array}{ccc} H^1(\Gamma_k, \text{Aut}(G)) & \longrightarrow & H^1(\Gamma_k, (G \rightarrow \text{Aut}(G))) \\ & \searrow & \downarrow \\ & & H^1(\Gamma_k, \text{Out}(G)) \end{array}$$

we have the element of $H^1(\Gamma_k, \text{Aut}(G))$ determined by the homomorphic section, which maps to an element which defines the extension of Γ_k by G . To the element associates an homomorphism

$$\Gamma_k \rightarrow \text{Aut}(G)$$

which factors

$$\Gamma_k \rightarrow \text{Aut}_{\Gamma_k}^{\text{open}}(G) \simeq \text{Aut}_k \text{Speck}(Y_{\bar{\eta}})$$

Note that $\text{Aut}_k \text{Speck}(Y_{\bar{\eta}})$ is a locally algebraic group since $Y_{\bar{\eta}}$ is of Kodaira dimension ≥ 0 . Since Γ_k is a profinite group, we conclude the element of $H^1(\Gamma_k, \text{Aut}(G))$ is the unit after base change for a finite extension of field k . $\square$

We can show Iitaka-Viehweg type theorem:

1. Let X and S be projective smooth varieties over a field k . Assume $f : X \rightarrow S$ is a proper separable connected surjective morphism with a general generic fibre $X_{\bar{\eta}}$ of Kodaira dimension ≥ 0 . Then

$$\text{Max}_{m \geq 1} \{ \kappa(\hat{\det} f_* \omega_{X/S}^{\otimes m}) \} \geq \text{var}(X/S)$$

2. Let X and S_α be projective smooth varieties over a field k . Assume $f_\alpha : X \rightarrow S_\alpha$ are proper separable dominant rational maps parametrized by a variety over k and $\kappa(S_\alpha) \geq 0$. Then the collection of f_α is finite up to birational equivalence,
3. Let X and S_α be projective smooth varieties over a field k . Assume $f_\alpha : X \rightarrow S_\alpha$ are proper separable dominant rational maps and the canonical invertible sheaves of S_α are ample. Then the collection of f_α is finite up to birational equivalence.

In the second section we briefly explain Jacob Rulie's Theory to enlarge scheme theory([JR1],[JR2],[JR3],[JR4]).

Let X be a topological space, CRing the category of commutative rings, $\text{Shv}_{\text{Set}}(X)$ the category of sheaves of sets on X and $\mathcal{O}_X$ a sheaf of commutative rings on X . There exists an equivalent view of $\mathcal{O}_X$:

1. Let $\mathcal{U}(X)$ be the partially ordered set of open subsets on X . $\mathcal{O}_X$ is a functor $\mathcal{O}_X : \mathcal{U}(X)^{\text{op}} \rightarrow \text{CRing}$ which satisfies the sheaf axiom.
2. Given a commutative ring object $\mathcal{O}_X \in \text{Shv}_{\text{Set}}(X)$, we can define $F : \text{CRing}^{\text{op}} \rightarrow \text{Shv}_{\text{Set}}(X)$. For every commutative ring R and every open subset $U \in \mathcal{U}(X)$, we define $F(R)(U) = \text{Hom}_{\text{CRing}}(R, \mathcal{O}_X(U))$ by the set of ring homomorphisms from R to $\mathcal{O}_X(U)$. Note that $F(R)(U)$ depends functorially on R and U and it defines a functor $F : \text{CRing}^{\text{op}} \rightarrow \text{Shv}_{\text{Set}}(X)$. F carries colimits of commutative rings to limits in the $\text{Shv}_{\text{Set}}(X)$. In other words, we can define a sheaf of commutative rings on X to be a limit preserving functor $\text{CRing}^{\text{op}} \rightarrow \text{Shv}_{\text{set}}(X)$.

Let $\mathbf{CRing}^{fin}$ denote the category of finitely generated commutative rings over the ring of integers $\mathbb{Z}$.

We have the equivalence of ∞ -category

$$\mathbf{CRing} \simeq \mathbf{Ind}(\mathbf{CRing}^{fin})$$

Definition 2.1. An ∞ -category or quasi-category or weak Kan complex is a simplicial set $\mathcal{C}$ which satisfies the following extension condition:

Every map of simplicial sets $f_0 : \Lambda_i \rightarrow \mathcal{C}$ can be extended to an n -simplex $f : \Delta^n \rightarrow \mathcal{C}$, provided that $0 < i < n$, where $\Lambda_i^n \subseteq \Delta^n$ denotes the i th horn, obtained from the simplex Δ^n by deleting the interior and the face opposite to the i th vertex.

If $\mathcal{E}$ is a category, the nerve $N\mathcal{E}$ of $\mathcal{E}$ is an ∞ -category. Consequently, we can think of the theory of ∞ -categories as a generalization of category theory. Most of the important concepts from classical category theory can be generalized to the setting of ∞ -categories.

If $\mathcal{C}$ and $\mathcal{D}$ are ∞ -category, $\mathbf{Fun}^L(\mathcal{C}, \mathcal{D})$ (resp. $\mathbf{Fun}^R(\mathcal{C}, \mathcal{D})$) denotes the full subcategory of $\mathbf{Fun}(\mathcal{C}, \mathcal{D})$ spanned by the functors which admit right adjoints (resp. left adjoints). If $\mathcal{C}$ and $\mathcal{D}$ are ∞ -category which admit finite limits, $\mathbf{Fun}^{lex}(\mathcal{C}, \mathcal{D})$ denotes the full subcategory of $\mathbf{Fun}(\mathcal{C}, \mathcal{D})$ spanned by the functors that are left exact; that is the functors which preserve finite limits.

If $\mathcal{C}$ is a small ∞ -category, $\mathbf{Pro}(\mathcal{C})$ is the ∞ -category of pro-objects of $\mathcal{C}$. If $\mathcal{C}$ admits finite limits, $\mathbf{Pro}(\mathcal{C}) = \mathbf{Fun}^{lex}(\mathcal{C}, \mathcal{S})^{op}$ and $\mathbf{Ind}(\mathcal{C}) = \mathbf{Pro}(\mathcal{C}^{op})^{op}$, where $\mathcal{S}$ denotes the ∞ -category of spaces.

Definition 2.2. Let $\mathcal{X}$ be an ∞ -category. We will say that $\mathcal{X}$ is an ∞ -topos if there exists a small ∞ -category $\mathcal{C}$ and an accessible left exact localization functor $\mathcal{P}(\mathcal{C}) \rightarrow \mathcal{X}$.

This definition amounts to selecting an extrinsic approach to higher topos theory. the class of ∞ -topoi is defined to be the smallest collection of ∞ -categories which contains $\mathcal{S}$ and is stable under certain construction (left exact localizations and the formation of functor categories). Every Grothendieck topology on $\mathcal{C}$ determines a left exact localization on $\mathcal{P}(\mathcal{C})$. However, it turns out not every ∞ -topos arises via this construction. Recall that a topos is a category of sheaves of sets on a topological space or a site. Roughly speaking, an ∞ -topos is an ∞ -category which "looks like" the ∞ -category of spaces, just as an ordinary topos is a category which "looks like" the category of sets. ∞ -topos is characterized by the following ∞ -categorical analogues of Giraud's axioms:

1. The ∞ -category $\mathcal{X}$ is presentable.
2. Colimits in $\mathcal{X}$ is universal.
3. Coproducts in $\mathcal{X}$ are disjoint.
4. Every groupoid object of $\mathcal{X}$ is effective.

Let $\mathcal{G}$ be an ∞ -category and $\mathcal{X}$ ∞ -topos. A $\mathcal{C}$ -valued sheaf on $\mathcal{X}$ is a functor $\mathcal{X}^{op} \rightarrow \mathcal{C}$ which preserves small limits. $\mathbf{Shv}_{\mathcal{C}}(\mathcal{X})$ denotes the full subcategory of $\mathbf{Fun}(\mathcal{X}^{op}, \mathcal{C})$ spanned by the $\mathcal{C}$ -valued sheaves on $\mathcal{X}$. If $\mathcal{C}$ and $\mathcal{D}$ are presentable ∞ -categories. A functor $\mathcal{D}^{op} \rightarrow \mathcal{C}$ admits a left adjoint if and only if it preserves small limits. Hence for every ∞ -topos $\mathcal{X}$, we have

$$\mathbf{Shv}_{\mathcal{C}}(\mathcal{X}) = \mathbf{Fun}^R(\mathcal{X}^{op}, \mathcal{C})$$

Let $\mathcal{G}$ be a small ∞ -category which admits finite limits and $\mathcal{X}$ ∞ -topos. Let $j : \mathcal{G} \rightarrow \mathbf{Pro}(\mathcal{G})$ the Yoneda embedding. We have an equivalence of ∞ -categories

$$\mathbf{Fun}^R(\mathbf{Pro}(\mathcal{G}), \mathcal{X}) \simeq \mathbf{Fun}^{lex}(\mathcal{G}, \mathcal{X})$$

and we obtain a canonical equivalence

$$\mathrm{Fun}^{lex}(\mathcal{G}, \mathcal{X}) \simeq \mathrm{Fun}^R(\mathrm{Pro}(\mathcal{G}), \mathcal{X}) \simeq$$

$$\mathrm{Fun}^R(\mathcal{X}^{op}, \mathrm{Ind}(\mathcal{G}^{op})) \simeq \mathrm{Shv}_{\mathrm{Ind}(\mathcal{G}^{op})}(\mathcal{X})$$

The ∞ -categories $\mathrm{Shv}_{\mathrm{Ind}(\mathcal{G}^{op})}$ and $\mathrm{Fun}^{lex}(\mathcal{G}, \mathcal{X})$ are canonically equivalent.

Definition 2.3. *A geometry $\mathcal{G}$ consists of the following:*

1. $\mathcal{G}$ is an essentially small ∞ -category which admits finite limits.
2. $\mathcal{G}$ is idempotent complete (splits).
3. $\mathcal{G}$ has an admissible structure on $\mathcal{G}$.

Definition 2.4. *A transformation between geometries $\mathcal{G}$ and $\mathcal{G}'$ satisfies the following conditions:*

1. $f : \mathcal{G} \rightarrow \mathcal{G}'$ is a functor which preserves finite limits.
2. The functor f carries the admissible morphisms on $\mathcal{G}$ to the morphisms on $\mathcal{G}'$.
3. $\mathcal{G}$ has an admissible structure on $\mathcal{G}$.
4. For every admissible cover $\{U_\alpha \rightarrow X\}$ of an object $X \in \mathcal{G}$, the collection of morphisms $\{f(U_\alpha) \rightarrow f(X)\}$ is an admissible cover of $f(X) \in \mathcal{G}'$.

We say a geometry is discrete if the following conditions are satisfied:

1. the admissible morphisms in $\mathcal{G}$ are precisely the equivalence.
2. the Grothendieck topology on $\mathcal{G}$ is trivial: that is, a sieve $\mathcal{G}^0/X \subseteq \mathcal{G}/X$ on an object $X \in \mathcal{G}$ is a covering sieve if and only if $\mathcal{G}^0/X = \mathcal{G}/X$.

Definition 2.5. *Let $\mathcal{G}$ be a geometry and $\mathcal{X}$ an ∞ -topos. A $\mathcal{G}$ -structure is a left exact functor $\mathcal{O} : \mathcal{G} \rightarrow \mathcal{X}$ with the following property: for every collection of admissible morphisms $\{U_\alpha \rightarrow X\}$ in $\mathcal{G}$ which generates a covering sieve on X , the induced map $\coprod_\alpha \mathcal{O}(U_\alpha) \rightarrow \mathcal{O}(X)$ is an effective epimorphism in $\mathcal{X}$. $\mathrm{Str}_{\mathcal{G}}(\mathcal{X})$ denotes the full subcategory of $\mathrm{Fun}(\mathcal{G}, \mathcal{X})$ spanned by the $\mathcal{G}$ -structures on $\mathcal{X}$.*

If $\mathcal{G}$ is a discrete geometry and $\mathcal{X}$ is an ∞ -topos, we have the following equivalence:

$$\mathrm{Str}_{\mathcal{G}}^{loc} = \mathrm{Str}_{\mathcal{G}} = \mathrm{Fun}^{lex}(\mathcal{G}, \mathcal{X}) = \mathrm{Shv}_{\mathrm{Ind}(\mathcal{G}^{op})}(\mathcal{X})$$

$\hat{\mathrm{Cat}}_\infty$ denotes the ∞ -category of ∞ -categories. ${}^L\mathrm{Top} \subseteq \hat{\mathrm{Cat}}_\infty$ denotes the subcategory defined as follows:

1. An ∞ -category $\mathcal{X}$ belongs to ${}^L\mathrm{Top}$ if and only if $\mathcal{X}$ is an ∞ -topos.
2. $f^* : \mathcal{X} \rightarrow \mathcal{Y}$ is a morphism of ${}^L\mathrm{Top}$ if and only if f^* preserves small colimits and finite limits.

${}^L\mathrm{Top}(\mathcal{G})^{op}$ denotes the ∞ -category of $\mathcal{G}$ -structured ∞ -topi. Note that let $f : \mathcal{G} \rightarrow \mathcal{G}'$ be a transformation of geometries. The induced functor

$${}^L\mathrm{Top}(\mathcal{G}') \rightarrow {}^L\mathrm{Top}(\mathcal{G})$$

admits a left adjoint, which denotes

$$\mathbf{Spec}_{\mathcal{G}}^{\mathcal{G}'} : {}^L\mathrm{Top}(\mathcal{G}) \rightarrow {}^L\mathrm{Top}(\mathcal{G}')$$

We call it the relative spectrum functor associated to f . Let $\mathcal{G}$ be a geometry and $\mathcal{G}_{dis}$ its discrete geometry. We have the following composite called as the absolute spectrum functor associated to the geometry $\mathcal{G}$:

$$\mathbf{Spec}^{\mathcal{G}} : \mathrm{Ind}(\mathcal{G}^{op}) \rightarrow {}^L\mathrm{Top}(\mathcal{G}_{dis}) \xrightarrow{\mathrm{Spec}_{\mathcal{G}_{dis}}^{\mathcal{G}}} {}^L\mathrm{Top}(\mathcal{G})$$

where we have the fully faithful embedding

$$\mathrm{Ind}(\mathcal{G}^{op}) \simeq \mathrm{Str}_{\mathcal{G}}(\mathcal{S}) \simeq {}^L\mathrm{Top}(\mathcal{G}_{dis}) \times_{{}^L\mathrm{Top}} \{\mathcal{S}\} \subseteq {}^L\mathrm{Top}(\mathcal{G}_{dis})$$

$\Gamma_{\mathcal{G}}$ denotes a right adjoint to the absolute spectrum functor

$$\Gamma_{\mathcal{G}} : {}^L\mathrm{Top}(\mathcal{G}) \rightarrow \mathrm{Ind}(\mathcal{G}^{op})$$

Note $\mathrm{Fun}^{lex}(\mathcal{G}, \mathcal{S}) \simeq \mathrm{Ind}(\mathcal{G}^{op}) \simeq \mathrm{Pro}(\mathcal{G})^{op}$.

Definition 2.6. Let $\mathcal{G}$ be a geometry. An object $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is an affine $\mathcal{G}$ -scheme if there exists an object $A \in \mathrm{Pro}(\mathcal{G})$ and an equivalence $(\mathcal{X}, \mathcal{O}_{\mathcal{X}}) \simeq \mathbf{Spec}^{\mathcal{G}}(A)$. $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is said to be a $\mathcal{G}$ -scheme if there exist a collection of objects $\{U_{\alpha}\}$ of $\mathcal{X}$ with the following property:

1. the canonical map $\coprod_{\alpha} U_{\alpha} \rightarrow 1_{\mathcal{X}}$ is an effective epimorphism, where $1_{\mathcal{X}}$ is the final object of $\mathcal{X}$.
2. For every U_{α} , there exists an equivalence $(\mathcal{X}/U_{\alpha}, \mathcal{O}_{\mathcal{X}}|_{U_{\alpha}}) \simeq \mathbf{Spec}^{\mathcal{G}} A_{\alpha}$ for some $A_{\alpha} \in \mathrm{Pro}(\mathcal{G})$.

It may be said that a $\mathcal{G}$ -scheme $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is locally of finite presentation if it is possible to choose the covering $\{U_{\alpha}\}$ such that each A_{α} belongs to the essential image of the Yoneda embedding $\mathcal{G} \rightarrow \mathrm{Pro}(\mathcal{G})$. Let $\mathrm{Sch}(\mathcal{G})$ denote the full subcategory of ${}^L\mathrm{Top}(\mathcal{G}^{op})$ spanned by all the $\mathcal{G}$ -schemes and $\mathrm{Sch}^{fin}(\mathcal{G})$ the full subcategory spanned by the $\mathcal{G}$ -schemes which are locally of finite presentation.

Here we apply the theory to get ordinary schemes where we take a geometry as the opposite of the category of finitely generated commutative rings CRing^{fin} . We restrict ourselves to the following case. Let k be a field. Let CAlg_k^{fin} denote the category of finitely generated commutative algebras over k and RCAlg_k^{fin} the full subcategory of CAlg_k^{fin} spanned by the reduced algebras over k . Consider the subcategory of RCAlg_k^{fin} such that the morphisms are separable and denote it by SRCAlg_k^{fin} .

Let $\mathcal{G}$ be a discrete geometry the opposite of SRCAlg_k^{fin} endowed with Zariski topology. Then Grothendieck etale fundamental groups of noetherian schemes give us a functor from $\mathrm{Sch}(\mathcal{G})$ to the category of the absolute Galois groups which is the full subcategory of the category of profinite groups, which is the category of the pro-objects of the category of finite groups. Let $\mathcal{G}'$ be the discrete geometry which is the category of profinite groups. There exists a transformation of geometries $\mathcal{G} \rightarrow \mathcal{G}'$. We have the commutative diagram:

$$\begin{array}{ccc} \mathrm{Fun}^{lex}(\mathcal{G}', \mathcal{X}) & & \\ \downarrow & \searrow & \\ \mathrm{Fun}^{lex}(\mathcal{G}, \mathcal{X}) & \longrightarrow & \mathrm{Shv}_{\mathrm{Ind}(\mathcal{G}^{op})}(\mathcal{X}) \end{array}$$

Let $(X, \mathcal{O}_X)$ be a $\mathcal{G}$ -scheme and a functor from a morphism T/X

$$\Pi_X : \mathrm{Sch}/X \rightarrow (\text{profinite group}) \quad T/X \mapsto \pi_1(T, *)$$

Consider a triple $(X, \mathcal{O}_X, \Pi_X)$ for a $\mathcal{G}$ -scheme $(X, \mathcal{O}_X)$.

Proposition 2.1. *Let k be a function field and $\mathcal{G}$ a geometry which is the opposite of SRCAlg_k^{fin} . Let $f : (X, \mathcal{O}_X, \underline{\Pi}_X) \rightarrow (Y, \mathcal{O}_Y, \underline{\Pi}_Y)$ be an epimorphism of objects in $\mathcal{G}$ -schemes. Assume X is trivial over k and the automorphism group of Y over k is locally algebraic. Then $(Y, \mathcal{O}_Y, \underline{\Pi}_Y)$ is also trivial if necessary after base change over an finite extension of k .*

$(X, \underline{\Pi}_X)$ profinite scheme For a topological space X the ∞ -category of sheaves on X $\mathrm{Shv}(X)$ is a ∞ -topos. If the topological space X has the property such that for every irreducible closed subset of X has a unique generic point, then we can recover X from $\mathrm{Shv}(X)$: the points $x \in X$ can be identified with isomorphism classes of geometric points $x^* : \mathrm{Shv}(X) \rightarrow \mathcal{S}$ where $\mathcal{S}$ is the ∞ -category of spaces. open subsets of X can be identified with subobjects of the unit object $1 \in \mathrm{Shv}(X)$. Every ∞ -topos $\mathcal{X}$ represents a functor from topological spaces to ∞ -categories by the formula

$$X \mapsto \mathrm{Fun}^*(\mathcal{X}, \mathrm{Shv}_{\mathcal{S}}(X))$$

where Fun^* denotes the ∞ -category of the functors.

Consider the category of the monoids Mon and let Mon^{fin} denote the full subcategory of Mon . Take Mon^{op} as a geometry. Let $\mathcal{G}$ denote Mon^{fin} and $\mathrm{Sch}(\mathcal{G})$ the category of $\mathcal{G}$ -schemes. Kurokawa-Conne's $\mathbb{F}_1$ -schemes are included in this type schemes. Let R be a commutative ring and denote Mod_R the category of R -modules. Then a commutative monoid object in Mod_R is an R -algebra. We have a forgetfull functor:

$$\mathrm{Alg}_R \rightarrow \mathrm{Mon} \quad A \mapsto A^\times$$

which admits a left adjoint $G \mapsto R[G]$. Let Grp denote the category of groups and Grp^{fin} the category of finite groups. $\mathrm{Pro}(\mathrm{Grp}^{fin})$ is the category of profinite groups.

Let $\mathcal{G}$ be Grp^{fin} . Consider $\mathrm{Sch}(\mathcal{G})$. Given a ∞ -topos $\mathcal{X}$, a functor

$$\mathcal{O}_{\mathcal{X}} : \mathrm{Pro}(\mathcal{G}) \rightarrow \mathcal{X}$$

gives us a $\mathcal{G}$ -scheme. Given a finite group G (resp. a profinite group Γ) we have a $\mathcal{G}$ -affine scheme

$$\mathbf{Spec}^{\mathcal{G}}(G) \text{ (resp. } \mathbf{Spec}^{\mathcal{G}}(\Gamma))$$

$(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is said to be a $\mathcal{G}$ -scheme if there exist a collection of objects $\{U_{\alpha}\}$ of $\mathcal{X}$ with the following property:

1. the canonical map $\coprod_{\alpha} U_{\alpha} \rightarrow 1_{\mathcal{X}}$ is an effective epimorphism, where $1_{\mathcal{X}}$ is the final object of $\mathcal{X}$.
2. For every U_{α} , there exists an equivalence $(\mathcal{X}/U_{\alpha}, \mathcal{O}_{\mathcal{X}}|_{U_{\alpha}}) \simeq \mathbf{Spec}^{\mathcal{G}} \Gamma_{\alpha}$ for some $\Gamma_{\alpha} \in \mathrm{Pro}(\mathcal{G})$.

Let $\mathcal{G}$ be the category of full subcategories of the category of finite groups. A non-commutative scheme can be represented by this type $\mathcal{G}$ -scheme.

2.1 E_{∞} -rings

An E_{∞} -ring can be thought of as space which is equipped with continuous addition and multiplication for which the axioms for the usual commutative ring hold not only up to homotopy, but up to coherent homotopy ([JR1],[JR2],[JR3],[JR4]). The E_{∞} -rings play a role in stable homotopy theory analogous to the role played by commutative rings in ordinary algebra. Recall that ordinary commutative ring can be viewed as a commutative monoid object in the category of abelian groups, which we view as endowed with a symmetric monoidal structure given by tensor product of abelian groups. To obtain the theory of E_{∞} -rings we will use the same definitions replacing abelian groups

by spectra, i.e., certain algebro-topological objects which represent cohomology theory. The collection of spectra is realized as a symmetric monoidal category and one can define an E_∞ -ring to be a commutative monoid object of this category. The collection of all spectra can be organized into an ∞ -category. An ∞ -category $\mathcal{C}$ equipped with a tensor product functor

$$\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$$

which is commutative and associative up to coherent homotopy. For any symmetric monoidal ∞ -category $\mathcal{C}$, there is an associated theory of commutative monoid objects, which are themselves organized into an ∞ -category $\mathrm{CAlg}(\mathcal{C})$. We can then define an E_∞ -ring to be a commutative monoid object of the ∞ -category of spectra, endowed with the symmetric monoidal structure given by smash product. We let Sp denote the ∞ -category of spectra, i.e., the homotopy limit of the tower

$$\cdots \rightarrow \mathcal{S}_* \xrightarrow{\Omega} \mathcal{S}_* \xrightarrow{\Omega} \mathcal{S}_*$$

$\mathrm{CAlg}(\mathrm{Sp})$ denotes the ∞ -category of E_∞ -rings and we will denote it by CAlg . The nerve $N\mathrm{CRing}$ of the category of ordinary commutative rings can be a full subcategory of CAlg . The notion of stable ∞ -category is obtained by axiomatizing the essential feature of stable homotopy theory. The ∞ -category Sp is universal among stable ∞ -categories. The derived category of an abelian category can be realized as the homotopy category of a stable ∞ -category. We may regard the theory of stable ∞ -category as a generalization of homological algebra ([JR1], [JR2], [JR3], [JR4]).

Theorem 2.1. *Let k be a commutative field. Let Sch_k denote the category of k -schemes and $\mathcal{G}_{\mathrm{Zar}}$ denote $(\mathrm{CRing}_k^{\mathrm{fin}})^{\mathrm{op}}$. There exists a fully faithful embedding*

$$N(\mathrm{Sch}_k) \rightarrow \mathrm{Sch}(\mathcal{G}_{\mathrm{Zar}}(k))$$

Let $\mathcal{G}$ be the oposite of the category of ordinary monoids. Then $\mathcal{G}$ -scheme is called $\mathbb{F}_1$ -scheme.

2.2 Spectral scheme

Definition 2.7. *Let $k \in \mathrm{CAlg}$ be an E_∞ -ring. We let $\mathcal{G}_{\mathrm{disc}}^{\mathrm{nSp}}(k)$ denote the opposite of the full subcategory of CAlg_k spanned by the compact objects ([JR1], [JR2], [JR3], [JR4]). If A is a compact commutative k -algebra, we let $\mathrm{Spec} A$ denote the corresponding object of $\mathcal{G}_{\mathrm{disc}}^{\mathrm{nSp}}(k)$. If k is connective, we let $\mathcal{G}_{\mathrm{disc}}^{\mathrm{Sp}}(k)$ denote the full subcategory of $\mathcal{G}_{\mathrm{disc}}^{\mathrm{nSp}}(k)$ spanned by the connective compact commutative k -algebras.*

Let k be an E_∞ -ring. A spectral ringed topos over k is a pair $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ where $\mathcal{X}$ is an ∞ -category and $\mathcal{O}_{\mathcal{X}}$ CAlg_k -valued sheaf on $\mathcal{X}$. A morphism $f : (\mathcal{X}, \mathcal{O}_{\mathcal{X}}) \rightarrow (\mathcal{Y}, \mathcal{O}_{\mathcal{Y}})$ is a geometric morphism of ∞ -topoi and $\alpha : f^* \mathcal{O}_{\mathcal{Y}} \rightarrow \mathcal{O}_{\mathcal{X}}$ is a morphism of CAlg_k -valued sheaves on $\mathcal{X}$. This ∞ -category of spectral ringed topoi denotes $\mathrm{RingTop}(k)$.

$$\mathrm{RingTop}(k) = {}^L\mathrm{Top}(\mathcal{G}_{\mathrm{disc}}^{\mathrm{Sp}}(k))$$

For every E_∞ -ring R there exists a locally spectrally ringed ∞ -topos $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ and a map $\theta : R \rightarrow \Gamma(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ with the following universal property: for every locally spectrally ringed ∞ -topos $(\mathcal{Y}, \mathcal{O}_{\mathcal{Y}})$, composition with θ induces a homotopy equivalence

$$\mathrm{Map}_{\mathrm{RingTop}_{\mathrm{Zar}}}((\mathcal{Y}, \mathcal{O}_{\mathcal{Y}}), (\mathcal{X}, \mathcal{O}_{\mathcal{X}})) \rightarrow \mathrm{Map}_{\mathrm{CAlg}}(R, \Gamma(\mathcal{Y}, \mathcal{O}_{\mathcal{Y}}))$$

The spectrally ringed ∞ -topos $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is uniquely determined up to equivalence and we will denote it by $\mathbf{Spec}^Z(R)$. We will refer to $\mathbf{Spec}^Z(R)$ as the spectrum of R with respect to the Zariski topology.

Definition 2.8. *A nonconnective spectral scheme is a spectrally ringed ∞ -topos $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ such that there exists a collection of objects $U_\alpha \in \mathcal{X}$ satisfying the following conditions:*

1. the canonical map $\coprod_{\alpha} U_{\alpha} \rightarrow \mathbf{1}$ is an effective epimorphism, where $\mathbf{1}$ denotes the final object of $\mathcal{X}$.
2. For each index α , there exist an E_{∞} -ring R_{α} and an equivalence of spectrally ringed ∞ -topoi

$$(\mathcal{X}/U_{\alpha}, \mathcal{O}|_{U_{\alpha}}) \simeq \mathbf{Spec}^Z(R_{\alpha})$$

We let $\mathbf{SpSch}^{nc}$ denote the full subcategory of $\mathbf{RingTop}_{Zar}$ spanned by the nonconnective spectral schemes. A spectral scheme is a nonconnective spectral scheme $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ such that $\mathcal{O}_{\mathcal{X}}$ is connective. We let $\mathbf{SpSch}$ denote the full subcategory of $\mathbf{SpSch}^{nc}$ spanned by the spectral schemes.

If R is an E_{∞} -ring, $\mathbf{Spec}^Z(R)$ can be identified with the spectrally ringed ∞ -topos

$$(\mathbf{Shv}_S(\mathbf{Spec}^Z(\pi_0 R)), \mathcal{O})$$

Here $\mathbf{Spec}^Z(\pi_0 R)$ denotes the Zariski spectrum of the commutative ring $\pi_0 R$.

Let k be an E_{∞} -ring. We define a geometry $\mathcal{G}_{Zar}^{nSp}$ as follows:

Definition 2.9.

On the level ∞ -categories, we have $\mathcal{G}_{Zar}^{nSp} = \mathcal{G}_{disc}^{nSp}$. That is, $\mathcal{G}_{Zar}^{nSp}$ is the opposite of the ∞ -category of compact objects of $\mathbf{CAlg}_k$. If A is a compact object of $\mathbf{CAlg}_k$, we let $\mathbf{Spec} A$ denote the corresponding object of $\mathcal{G}_{Zar}^{nSp}(k)$.

A morphism $f : \mathbf{Spec} A \rightarrow \mathbf{Spec} B$ in $\mathcal{G}_{Zar}^{nSp}$ is admissible if and only if there exists an element $b \in \pi_0 B$ such that f carries b to an invertible element in $\pi_0 A$ and the induced map $B[\frac{1}{b}] \rightarrow A$ is an equivalence.

A collection of admissible morphisms $\{\mathbf{Spec} B[\frac{1}{b_{\alpha}}] \rightarrow \mathbf{Spec} A\}$ generates a covering sieve on B if and only if the elements b_{α} generate the unit ideal in the commutative ring $\pi_0 B$.

Definition 2.10. Let k be an E_{∞} -ring. A nonconnective spectral k -scheme is a pair $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$, where $\mathcal{X}$ is an ∞ -topos, $\mathcal{O}_{\mathcal{X}} : \mathcal{G}_{Zar}^{nSp}(k) \rightarrow \mathcal{X}$ is an $\mathcal{G}_{Zar}^{nSp}(k)$ -structure on $\mathcal{X}$, and the pair $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is an $\mathcal{G}_{Zar}^{nSp}$. In this case we will abuse notation to identify $\mathcal{O}_{\mathcal{X}}$ with a sheaf of E_{∞} -rings on $\mathcal{X}$, which we refer to as the structure sheaf of $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$. We let $\mathbf{SpSch}^{nc}$ denote the full subcategory of $\mathbf{RingTop}(k)_{Zar}$ spanned by the nonconnective spectral schemes.

We let $\mathbf{TCAlg}$ denote the full subcategory of $\mathbf{CRing}$ spanned by commutative rings which have only terminal singularities. .

In the following theorem ([JR1], [JR2], [JR3], [JR4])

Theorem 2.2. Let k be a commutative field. Let $\mathbf{Sch}_k$ denote the category of k -schemes and $\mathcal{G}_{Zar}$ denote $(\mathbf{CRing}_k^{fin})^{op}$. There exists a fully faithful embedding

$$N(\mathbf{Sch}_k) \rightarrow \mathbf{Sch}(\mathcal{G}_{Zar}(k))$$

We let $\mathbf{TVar}_k$ denote the full subcategory of $\mathbf{Sch}_k$ spanned by varieties with only terminal singularities and we have a fully faithful embedding

$$N(\mathbf{TVar}_k) \rightarrow N(\mathbf{Sch}_k)$$

Let X be a projective variety with only terminal singularities and let $F(X)$ be a functor such that

$$F(X) = \{\mathcal{Y} | \mathcal{X} \text{ is an } \infty\text{-topos, } Y \text{ is birational to } X \text{ and is a projective variety with only terminal singularities, } \mathbf{Shv}(Y) \rightarrow \mathcal{Y} \text{ is an epimorphism}\}$$

Then there exists a limit $F(X)$ in $\mathbf{Sch}(\mathcal{G}_{Zar}(k))$ for the geometry $\mathcal{G}_{Zar}(k)$ but it suffices to show the limit $\mathcal{X}$ for a good geometry and endow it with a good functor $\mathcal{O}_{\mathcal{X}}$. Instead we suffer ourselves to do mathematics as it is.

2.3 Geometric Homotopy groups in an $(\infty, 1)$ -topos

If a locally contractible $(\infty, 1)$ -topos $([\text{Cat}])$ $\mathbb{H}$ has a site $\mathcal{C}$ with $\mathbb{H} = \text{Sh}(\infty, 1)(\mathcal{C})$ such that the objects of the site are geometrically contractible in that constant $(\infty, 1)$ -presheaves already satisfy descent over objects in $\mathcal{C}$, then the left adjoint $\Pi : \mathbb{H} \rightarrow \infty\text{Grpd}$ to LConst may be constructed $([\text{Gal}], [\text{Cat}], [\text{Cis1}], [\text{Cis2}])$. Given an $(\infty, 1)$ -topos $\mathbb{H} = \text{Sh}(\infty, 1)(\mathcal{C})$, we define the ∞ -groupoid of locally constant ∞ -stacks on an object $X \in \mathbb{H}$ to be

$$\infty\text{CovBund}(X) := \mathbb{H}(X, \text{LConst}_{\text{Core}(\infty\text{Grpd})})$$

where $\text{LConst}_{\text{Core}(\infty\text{Grpd})}$ is the constant ∞ -stack on the core ∞ -groupoid of ∞Grpd . Since $\mathbb{H}$ is a locally contractible $(\infty, 1)$ -topos in that LConst has the left adjoint $(\infty, 1)$ -functor $\Pi(-)$, then by definition of adjunction we have the equivalence

$$\infty\text{CovBund}(X) \simeq \text{Fun}(\Pi(X), \infty\text{Grpd})$$

where locally constant ∞ -stacks or ∞ -covering spaces on the one hand and $(\infty, 1)$ -functors from $\Pi(X)$ to ∞Grpd on the other. Given a morphism from X to Y for objects $X, Y \in \mathbb{H}$, we have $\Pi(X) \rightarrow \Pi(Y)$ which induces

$$\text{Fun}(\Pi(Y), \infty\text{Grpd}) \rightarrow \text{Fun}(\Pi(X), \infty\text{Grpd})$$

. If

$$\infty\text{CovBund}(Y) \rightarrow \infty\text{CovBund}(X)$$

is fully faithful, $\Pi(X) \rightarrow \Pi(Y)$ reconstructs the morphism $X \rightarrow Y$.

Apply this theory to the subcategory SpSch_{red} of SpSch_k spanned by objects locally contractible ∞ -topoi and morphisms such that

$$\infty\text{CovBund}(Y) \rightarrow \infty\text{CovBund}(X)$$

are fully faithful, where k denotes an E_∞ -ring. Let $\mathbb{H} = \text{SpSch}_{red}$, Choosing $X, Y \in \mathbb{H}$ and $f : X \rightarrow Y \in \mathbb{H}$ such that for any subobjects of X, Y and any restrictions of f are in $\mathbb{H}$ we have

$$\mathbb{H}^{epi}((\mathcal{X}, \mathcal{O}_\mathcal{X}), (\mathcal{Y}, \mathcal{O}_\mathcal{Y})) \simeq \text{Fun}^{open}(\Pi|_X, \Pi|_Y)$$

where $\Pi(X), \Pi(Y)$ are endowed with Krull topology.

Let k be an ordinary field and S a variety over k . Consider $\mathbb{H}/k$. Assume $(\mathcal{X}, \mathcal{O}_\mathcal{X})$ is a trivial product over S . Given an epimorphism

$$f : (\mathcal{X}, \mathcal{O}_\mathcal{X}) \rightarrow (\mathcal{Y}, \mathcal{O}_\mathcal{Y})$$

with the automorphism group of a general generic fibre of $(\mathcal{Y}, \mathcal{O}_\mathcal{Y})$ over S is locally algebraic scheme over k , . Then $(\mathcal{Y}, \mathcal{O}_\mathcal{Y})$ is a trivial product after base change for some generically finite extension of S .

After Daniel Dugger, Universal homotopy theories, we might generalize Kobayai-Nomizu theory for compact differentiable manifolds to the case the gros topos $\text{Sh}(\infty, 1)(\text{Diff})$ of ∞ -stacks on Diff .

3 Appendix

Consider a good geometry $\mathcal{G}$ and a rest of zeta function from which the trivial zero and pole components are removed in $\text{Ind}(\mathcal{G}^{op})$, It is irreducible over $\mathbb{Q}$ in a sense and it has continuous solutions in some part of A_∞ -ring.

References

- [JR1] Jacob Rulie, Structured Spaces, Derived Algebraic Geometry V, Available for download: Jacob Rulie's Home Page-Harvard Mathematics Department
- [JR2] Jacob Rulie, Spectral Schemes, Derived Algebraic Geometry VII, Available for download: Jacob Rulie's Home Page-Harvard Mathematics Department
- [JR3] Jacob Rulie, Higher Topos theory, Available for download: Jacob Rulie's Home Page-Harvard Mathematics Department
- [JR4] Jacob Rulie, Higher Algebra, Available for download: Jacob Rulie's Home Page-Harvard Mathematics Department
- [SM] Mac Lane, Saunders (1998). Categories for the Working Mathematician. Graduate Texts in Mathematics 5 (2nd ed.). Springer-Verlag. ISBN 0-387-98403-8.
- [B] Borceux, Francis (1994). Handbook of categorical algebra I-3. Encyclopedia of Mathematics and its Applications 50-52. Cambridge University Press.
- [Br] T. Brzezinski, R. Wisbauer (2003), Corings and Comodules, London Mathematical Society Lecture Note Series 309, ISBN 0-521-53931-5
- [A] Awodey, Steve (2006). Category Theory. Oxford Logic Guides 49. Oxford University Press. ISBN 978-0-19-151382-4
- [R] Emily Riehl (2014), Categorical Homotopy Theory, new mathematical monographs: 24, Cambridge University press, ISBN 978-1-107-04845-4
- [Cis1] D-C. Cisinski (2006), Les préfaisceaux comme modèles des types d'homotopie, Astérisque 308, Société mathématique France, ISBN 978-2-85629-225-9
- [Cis2] D-C. Cisinski (2019), Catégorie Derivables, Tome 138 Fascicule 3 Bulletin de la société mathématique de France p. 317-393.
- [Sc] D. Scappi (2013), The formal theory of Tannaka duality, 357 Astérisque Société mathématique de France, ISBN 978-2-85629-773-5
- [Cat] ncatlab.org, $(\infty, 1)$ -category theory, [https://ncatlab.org/nlab/show/\(\infty,1\)-category+theory](https://ncatlab.org/nlab/show/(\infty,1)-category+theory)
- [Gal] <https://ncatlab.org/nlab/show/Galois+theory>
- [AM] Adem, A. and Milgram, R., *Cohomology of finite groups.*, Grundlehren math. Wiss. 309, p. 317 (1991).
- [BBD] Beilinson A.A., Bernstein I.N., Deligne P., *Faisceaux pervers.*, Analyse et Topologie sur les espaces singuliers (I), Conférence de Luminy, juillet 1981, Astérisque 100 (1982).
- [Berth] Berthelot, P., *Altérations de variétés algébriques d'après A.J. DE JONG*, Séminaire Bourbaki 48, n° 815, pp. 273-311 (1997).

- [BJ] Borceux, F. and Janelidze, G. *Galois Theories.*, cambridge studies in advanced math. 72 pp.341 ISBN 0 521 80309 8 2001
- [Breen1] Breen, L., *Théorie de Schreier supérieure.*, Ann. scient. Éc. Norm. Sup., 4e série, t. 25, pp. 465-514(1992).
- [Breen2] Breen, L., *On the classification of 2-gerbes and 2-stacks*, 225 Astérisque Société Mathématique p. 160 (1994).
- [Brz] Brzezinski, T., Wisbauer, R., *Corings and Comodules*, London Mathematical Society Lecture Note Series 309, Cambridge University Press, 2003.
- [Cohn] Cohn, P.M., *Skew Fields*, Theory of general division rings, Encyclopedia of mathematics and applications 57.
- [Fuj] Fujita, T., *On Kähler fibre spaces over curves.*, J. Math.Soc. Japan 30, pp. 779-794(1978).
- [Gir] Giraud, J., *Cohomologie non abélienne.*, Grundlehren math. Wiss., Springer-Verlag Berlin Heidelberg New York, p. 467,(1971).
- [SGA] Grothendieck, A. et al., *Séminaire de géométrie algébrique du Bois-Marie*, SGA1, SGA4 I,II,III, SGA41/2, SGA5, SGA7 I,II, Lecture Notes in Mat., vols. 224,269-270-305,569,589,288-340, Springer-Verlag, New York, 1971-1977.
- [GG] Grothendieck, A., *Fondaments de la géométrie algébrique.*, Secrétariat mathématique, 11 rue Pierre Curis, Paris 5e, p. 236 (1962).
- [Dix] Grothendieck A., Giraud J., Kleiman S., Raynaud M., Tate J., *Dix exposés sur la cohomologie des schémas*, Advanced studies in pure math., vol. 3, North-Holland, Amsterdam, Paris, 1968, pp.386.
- [HS] Hirshowits, A. and Simpson, C., *Descente pour les n-champs.*, arXiv:math. AG/9807049v3 13 Mar 2001
- [I] Iitaka, S., *Introduction to birational geometry.*, Graduate Textbook in Mathematics, Springer-Verlag, p. 357 (1976).
- [Laum] Laumon, G., Moret-Bailly, L., *Champs algébriques.*, Université de Paris-sud Mathématiques, p. 94 (1992).
- [Kato] Kato, K., *Logarithmic structures of Fontaine-Illusie.*, Algebraic Analysis, Geometry and Number Theory., The Johns-Hopkins Univ. Press, Baltimore, MD, pp. 191-224(1989).
- [Kaw] Kawamata, Y., *Minimal models and the Kodaira dimension of algebraic fibre spaces.*, J. Reine Angew. Math. 363, pp. 1-46 (1985).
- [1] KKMS Kemf, G., Knudsen, F., Mumford, D., Saint-Donat, B., *Troidal embeddings I.*, Springer Lecture Notes, 339(1973).
- [Ko1] Kollár, J., *Shafarevich maps and automorphic forms.*, Princeton university press, Princeton, New Jersey pp.201 1995.
- [Ko2] Kollár, J., *Rational curves on algebraic varieties.*, Springer, Berlin-Heiderberg-Newyork-Tokyo, (1995)
- [Kon] Kontsevich, M., Rosenberg A. *Noncommutative smooth spaces.*, arXiv:math.AG/9812158v1 30Dec 1998.

- [Km1] Maehara, K., *Diophantine problems of algebraic varieties and Hodge theory in International Symposium Holomorphic Mappings, Diophantine Geometry and related Topics in Honor of Professor Shoshichi Kobayashi on his 60th birthday.*, R.I.M.S., Kyoto University October 26-30, Organizer: Junjiro Noguchi(T.I.T.), pp. 167-187 (1992).
- [Km2] Maehara, K., *Algebraic champs and Kummer coverings.*, A.C.Rep. T.I.P. Vol.18, No.1, pp.1-9(1995).
- [Km3] Maehara, K., *Conjectures on birational geometry.*, A.C.Rep. T.I.P. Vol.24, No.1, pp.1-10(2001).
- [Mats] Matsuki, K., *Introduction to the Mori Program.*, Universitext p. 468 Springer 2000
- [Mat] Matsumura, H., *On algebraic groups of birational transformations.*, Rend. Accad. Naz. Lincei, Serie VIII,34, 151-155 (1963).
- [MO] Matsumura, H. and Oort, F., *Representability of group functors, and automorphisms of algebraic schemes*, Inventiones Mathematicae, 1967 - Springer.
- [MP] Miyaoka, Y., Peternel T., *Geometry of Higher Dimensional Algebraic Varieties.*, DMV Seminar Band 26 Birkhäuser p. 213 1997
- [Mch] Mochizuki, S., *The local Pro- p Anabelian Geometry of Curves.*, Research Institute for Mathematical Sciences, Kyoto University RIMS-1097(1996).
- [Mum] Mumford D., *Selected Papers: On the classification of varieties and moduli spaces.*, Springer p. 795 2003
- [Nak] Nakayama, N., *Invariance of the plurigenera of algebraic varieties under minimal model conjectures.*, Topology 25(1986) 237-251.
- [Ro] Rosenlicht, M., *Some basic theorems on algebraic groups.*, xxxxx pp.401-443
- [RBZL] Ribes, L., Zalesskii, P., *Profinite Groups.*, Ergebnisse der Mathematik und ihrer Grenzgebiete 3.Folge Vol.40 Springer(1991).
- [Ws] Schmid, W., *Variation of Hodge structure: the singularities of the period mapping.*, Inventiones math., 22., pp. 211-319(1973).
- [Se] J-P. Serre. *Cohomologie Galoisienne*. Lecture Notes in Mathematics. , 5 4th Ed. 1973.
- [S1] Simpson, C., *Algebraic (geometric) n -stacks.*, arXiv:math. AG/9609014
- [S2] Simpson, C., *A closed model structure for n -categories, internal Hom, n -stacks and generalized Seifer-Van Kampen.*, arXiv:math: AG/9704006 v2 17 Mar 2000
- [S3] Simpson, C., *Homotopy Theory of Higher Categories, From Segal Categories to n -Categories and Beyond*, Cambridge University Press, ISBN 987-0-521-51695-2, p. 634, (2012)
- [Shatz] Shatz, S., *Profinite groups, arithmetic, and geometry.*, Annals of Math. studies, N. 67, Princeton Uni. Press, p. 252,(1972).
- [Vieh] Viehweg, E. *Quasi-projective Moduli for Polarized Manifolds.*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3.Folge.Band 30, p. 320 (1991).

[Zuo] Zuo, K., Representations of fundamental groups of algebraic varieties., Lecture Notes in Math. 1708, Springer, ISBN 3-540-66312-6.

切断をもたない種数 2 曲線束と仮想モデル・ヴェイユ群

北川真也 (岐阜工業高専)

§1 Background and Main theorem

§2 Construction

§3 Virtual Mordell-Weil groups

S : a smooth projective rational surface $/\mathbb{C}$

$\varphi : S \rightarrow \mathbb{P}^1$: a fibration whose general fibre F is a projective curve
of genus $g \geq 1$

We assume that φ is relatively minimal,

i.e., there are no (-1) -curves contained in fibres.

$\rho(S)$: the Picard number of S

(1)

In the case where $g = 1$, it is well-known that $\rho(S) = 10$. Furthermore, as a consequence of the canonical bundle formula of Kodaira, φ admits a section if and only if φ does not have any multiple fibres.

When $g \geq 2$, it can be shown that $11 \leq \rho(S) \leq 4g+6$. Furthermore, if either $\rho(S) = 4g + 6$ with $g \neq 1$ or $\rho(S) = 13$ with $g = 2$ holds, then φ always admits a section.

We restrict ourselves to the case where $g = 2$ and $\rho(S) = 12$.

Suppose that φ admits a section.

We can regard it as a horizontal curve D on S such that $D.F = 1$.

Therefore the fibres of φ contain

at least one irreducible component with multiplicity one.

(2)

Remark 1-(i). For $\sigma \in \mathbb{C} \setminus \{0, 1\}$,

$$y^2 = t \left(\frac{2}{3}x^3 - tx^2 + \frac{1}{3}t^2 \right) \left(\frac{2\sigma}{3}x^3 - \sigma tx^2 + \frac{1}{3}t^2 \right)$$

induces a rel. min. fibration $\varphi : S \rightarrow \mathbb{P}^1$ of genus two on a smooth rational surface with $\rho(S) = 12$. Furthermore, the fibre $\varphi^{-1}(0)$ is as in [NU, p. 155, 1–IV] and the irr. decomp. is the following:

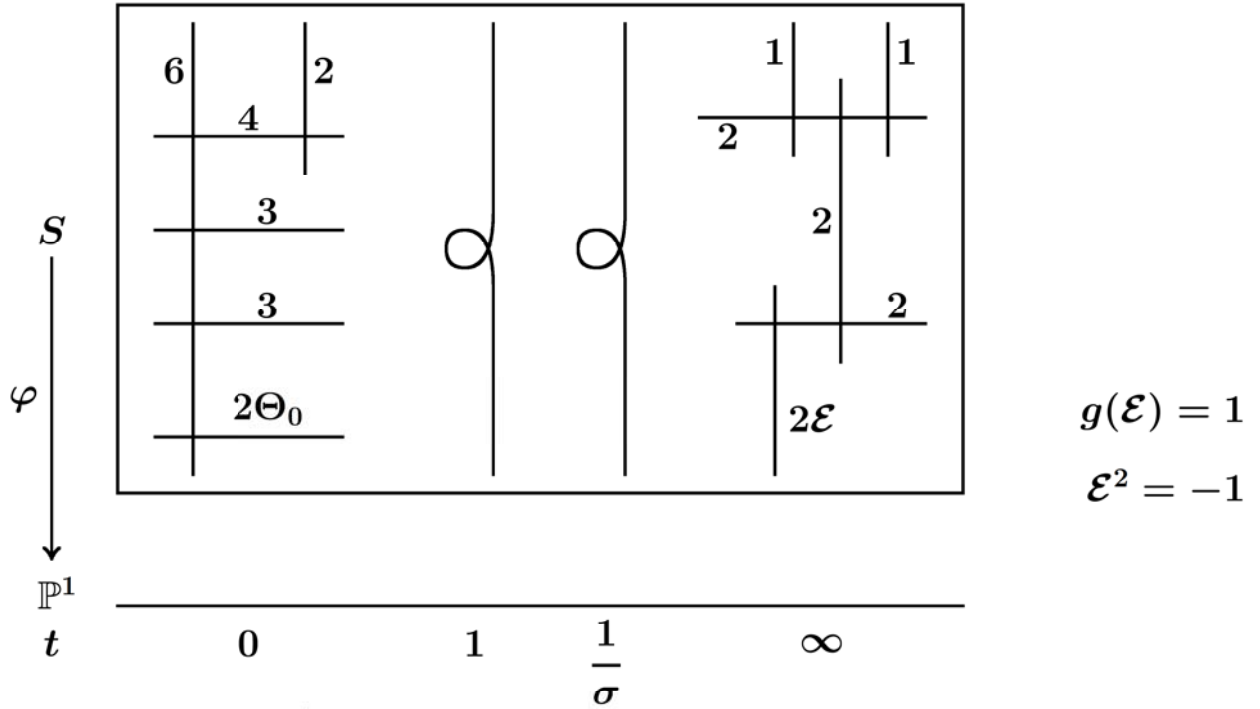
$$\varphi^{-1}(0) = 2\Theta_2 + 6\Theta_3 + 3\Theta_4 + 3\Theta_5 + 4\Theta_6 + 2\Theta_0.$$

Here Θ_0 is a (-3) -curve and the other components are (-2) -curves.

A non-existence result for sections of φ can be derived from an easy calculation as follows: Suppose that φ admits a section. We can regard it as a horizontal curve D on S such that $D \cdot \varphi^{-1}(q) = 1$ for all $q \in \mathbb{P}^1$. However, $D \cdot \varphi^{-1}(0) \geq 2$ since multiplicities of the irreducible components of $\varphi^{-1}(0)$ are at least two. We obtain a contradiction.

(3)

Remark 1-(ii). For $\sigma \in \mathbb{C} \setminus \{0, 1\}$, the induced fibration $\varphi : S \rightarrow \mathbb{P}^1$ has singular fibres as follows: $\varphi^{-1}(\infty)$ is as in [NU, p. 172, 3-II $^*_{3-0}$]



In particular, $\varphi^{-1}(q)$ is

a hyperelliptic curve of genus two for all $q \in \mathbb{P}^1 \setminus \{0, 1, 1/\sigma, \infty\}$.

(4)

A natural question arises:

If the fibres of φ contain at least one irr. comp. with multiplicity one, does φ always admit a section?

The purpose of the talk is to construct counter-examples explicitly.

For the proof of non-existence of sections,

we use the theory of the virtual Mordell-Weil groups.

Theorem 2.

Let (t, x) be local coordinates of $(\mathbb{P}^1 \setminus \{\infty\}) \times (\mathbb{P}^1 \setminus \{\infty\})$ and $pr_1 : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1$ the projection map onto the first factor.

Put $\Gamma_0 = pr_1^{-1}(0)$ and $\Gamma_\infty = pr_1^{-1}(\infty)$.

Let σ and τ be complex numbers with $\sigma \neq 0, 1$ and $\tau \neq 0, \frac{1}{2}, \frac{2}{3}, 1$.

(5)

Let $A(\gamma, \tau)$ denote, for $\gamma \in \mathbb{C} \setminus \{0\}$, the closure of the zero set of a polynomial $\gamma\tau x^3 - \gamma tx^2 - (3\tau - 2)tx + (2\tau - 1)t^2$ in t, x on $\mathbb{P}^1 \times \mathbb{P}^1$. Put $B = A(1, \tau) + A(\sigma, \tau) + \Gamma_0 + \Gamma_\infty$.

Let $\pi : \widehat{X} \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ be the finite double cover branched along B and $\mu : \widetilde{X} \rightarrow \widehat{X}$ the canonical resolution of singularities of $\widehat{X}$.

Then $pr_1 \circ \pi \circ \mu : \widetilde{X} \rightarrow \mathbb{P}^1$ is a genus two fibration.

Let $f : X \rightarrow \mathbb{P}^1$ be the relatively minimal model of $pr_1 \circ \pi \circ \mu$.

Then X is a smooth rational surface with $\rho(X) = 12$.

Furthermore, $f : X \rightarrow \mathbb{P}^1$ has no sections,

the fibres $f^{-1}(0)$ and $f^{-1}(\infty)$ are as in [NU, p. 172, 3-II₃₋₀^{*}],

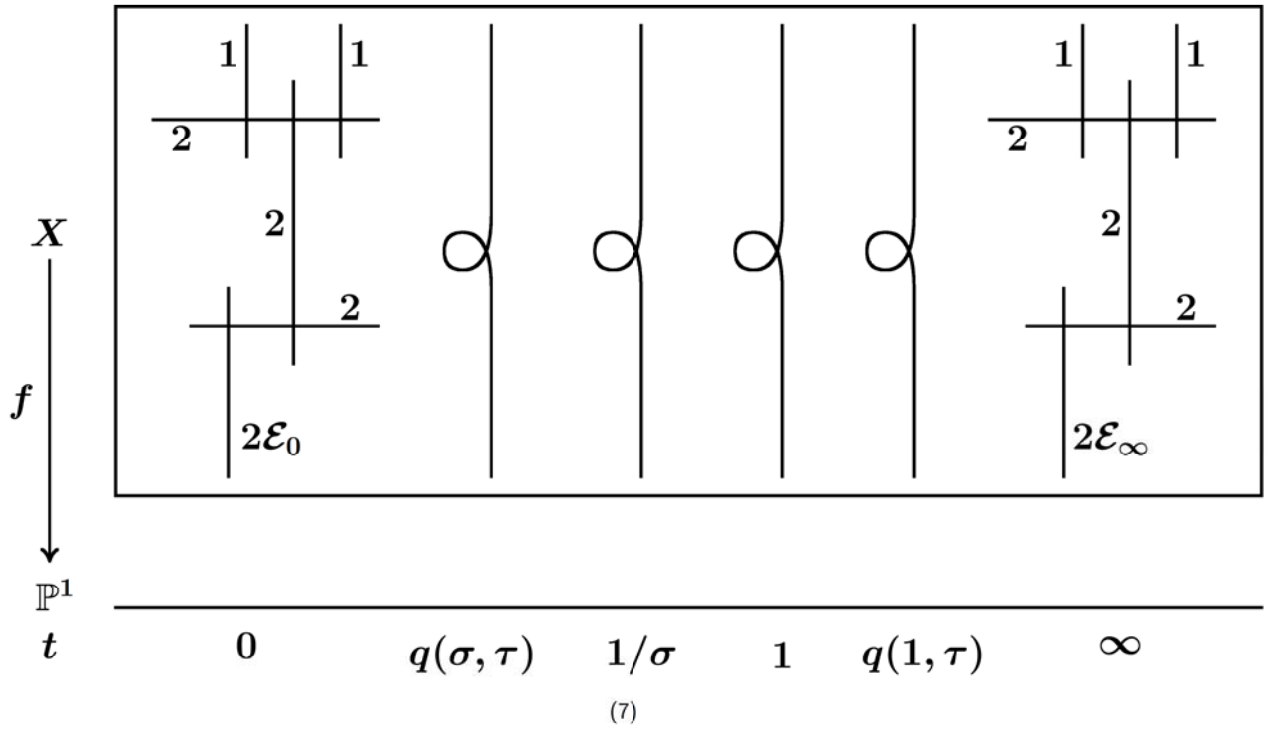
and the other fibres of f are irreducible and reduced. In particular, the fibres of f contain at least one irr. comp. with multiplicity one.

(6)

$$q(\gamma, \tau) := \frac{\tau(3\tau - 2)^3}{\gamma(2\tau - 1)} \quad \left(\tau = \frac{1}{3} \Leftrightarrow q(1, \tau) = 1 \Leftrightarrow q(\sigma, \tau) = \frac{1}{\sigma} \right)$$

If $\tau \neq \frac{1}{3}$, $q(1, \tau) \neq \frac{1}{\sigma}$ and $q(\sigma, \tau) \neq 1$, $\left(\sigma \neq 0, 1 \text{ and } \tau \neq 0, \frac{1}{2}, \frac{2}{3}, 1 \right)$

then $0, q(\sigma, \tau), 1/\sigma, 1, q(1, \tau)$ and ∞ are distinct from each other.



Organization At first we construct a genus two fibration $f : X \rightarrow \mathbb{P}^1$ as in Theorem 2 from a $\mathbb{P}^1$ -bundle $\Sigma_0 := \mathbb{P}^1 \times \mathbb{P}^1$ with a given branch divisor $B := B(\sigma, \tau)$ by the double covering method.

In Proposition 4, we show the assertions as in Theorem 2

except for non-existence of a section of f .

If f has a section, then f has at least two sections

since B does not contain a section of Σ_0 (cf. Lemma 6).

Next we consider the ruling associated to $2K_X + F$,

where K_X denotes the canonical divisor.

The degenerate fibres consist of the (-2) -curves contained in fibres of f and the (-1) -bisections of f . Here a (-1) -bisection of f means a (-1) -curve meeting F at two points.

(8)

In Proposition 7, through a birational morphism

from X to a relatively minimal model of the ruling,

we have an explicit description of the Néron-Severi group $\text{NS}(X)$.

Then we see that there is a (non-effective) divisor D with $D.F = 1$.

In fact, Corollary 8 gives us that

D and the irreducible components of the fibres of f generate $\text{NS}(X)$.

In §3, we introduce the theory of the virtual Mordell-Weil groups.

Further, Corollary 8 yields that

the virtual Mordell-Weil group of f is trivial.

As a result, a section of f is unique if it exists.

This contradicts Lemma 6. Therefore f has no sections.

This completes the proof of Theorem 2.

§2 Construction

We shall construct a smooth projective rational surface X together with a rel. min. fibration $f : X \rightarrow \mathbb{P}^1$ of genus two as in Theorem 2. Furthermore, we shall describe singular fibres of f and $\text{NS}(X)$, which coincide with the Picard group $\text{Pic}(X)$ in our situation.

Put $\Sigma_0 = \mathbb{P}^1 \times \mathbb{P}^1$.

Denote by (t, x) the inhomogeneous coordinates on Σ_0 .

Let $pr_n : \Sigma_0 \rightarrow \mathbb{P}^1$ be the projection map onto the n -th factor.

Put $\Gamma_q = pr_1^{-1}(q)$ and $\Delta_q = pr_2^{-1}(q)$ for any point $q \in \mathbb{P}^1$.

Take $\sigma \in \mathbb{C} \setminus \{0, 1\}$ and $\tau \in \mathbb{C} \setminus \{0, 1/2, 2/3, 1\}$.

Let $A(\gamma, \tau)$ denote, for $\gamma \in \mathbb{C} \setminus \{0\}$, the closure of the zero set of a polynomial $\gamma\tau x^3 - \gamma tx^2 - (3\tau - 2)tx + (2\tau - 1)t^2$ in t, x on $\mathbb{P}^1 \times \mathbb{P}^1$.

Put $B = A(1, \tau) + A(\sigma, \tau) + \Gamma_0 + \Gamma_\infty$.

(10)

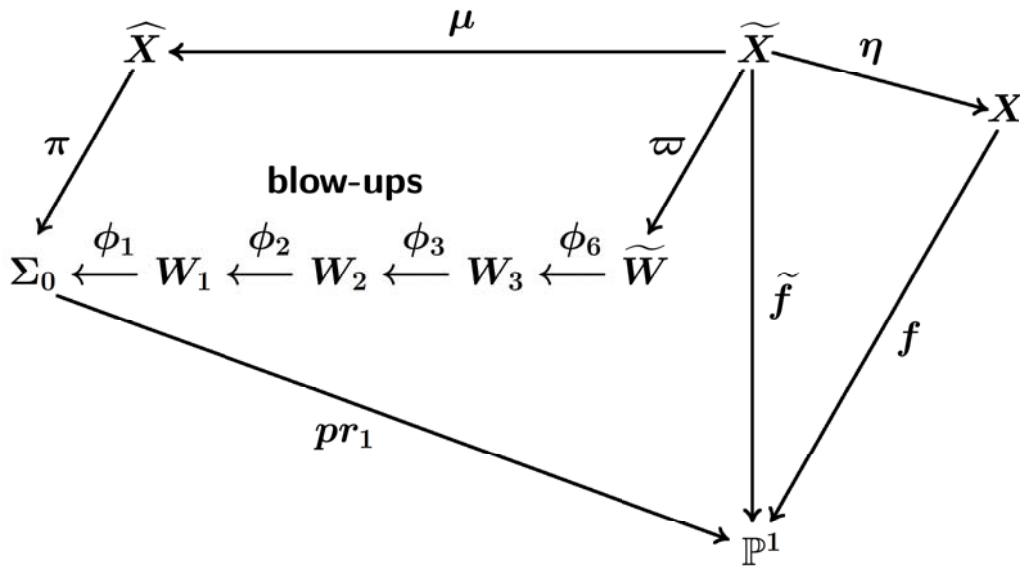
$\pi : \widehat{X} \rightarrow \Sigma_0$: the finite double cover branched along B

$\varpi : \widetilde{X} \rightarrow \widetilde{W}$: the finite double cover branched along $\widetilde{B}$

with $\text{Sing}(\widetilde{B}) = \emptyset$

$\mu : \widetilde{X} \rightarrow \widehat{X}$: the canonical resolution of singularities of $\widehat{X}$

$\tilde{\pi} := \pi \circ \mu$, $\tilde{f} := pr_1 \circ \tilde{\pi}$, $f : X \rightarrow \mathbb{P}^1$: the rel. min. model of $\tilde{f}$.



(11)

Let $\phi_1 : W_1 \rightarrow \Sigma_0$ be the blow-up at two points $(0, 0)$ and (∞, ∞) with the exceptional curves $E_{0,1}$ and $E_{\infty,1}$, i.e., $\phi_1(E_{0,1}) = (0, 0)$ and $\phi_1(E_{\infty,1}) = (\infty, \infty)$.

Let $P_{i,2}$ be the intersection point of

$E_{i,1}$ and the strict transform to W_1 of Γ_i for $i = 0, \infty$.

The strict transform $A_1(\gamma, \tau)$ to W_1 of $A(\gamma, \tau)$

passes through $P_{0,2}$ and $P_{\infty,2}$.

Next let $\phi_2 : W_2 \rightarrow W_1$ be the blow-up at two points $P_{0,2}$ and $P_{\infty,2}$ with $E_{0,2} = \phi_2^{-1}(P_{0,2})$ and $E_{\infty,2} = \phi_2^{-1}(P_{\infty,2})$.

The strict transform to W_2 of Δ_0 and that of Δ_∞

are (-1) -curves on W_2 .

Let $\phi'_2 : W_2 \rightarrow W'_1$ be the contraction of the two (-1) -curves.

(12)

The image by ϕ'_2 of the strict transform to W_2 of Γ_0 and that of Γ_∞ are (-1) -curves on W'_1 .

By contracting them, we get another $\mathbb{P}^1 \times \mathbb{P}^1$ and denote it by Σ'_0 .

Lemma 3. Let $\phi' : W_2 \rightarrow \Sigma'_0$ be the above contraction.

Denote by (v, z) the inhomogeneous coordinates on Σ'_0 .

Let $\psi : \Sigma_0 \dashrightarrow \Sigma'_0$ be the rational map given by $(v, z) = \left(\frac{t}{x^2}, \frac{t}{x} \right)$.

Then ψ is the birational map satisfying $\phi' = \psi \circ \phi_1 \circ \phi_2$.

Furthermore, the closure of the zero set of a polynomial

$\gamma(\tau - z) - (3\tau - 2)v + (2\tau - 1)vz$ in v, z on Σ'_0 for $\gamma \in \mathbb{C} \setminus \{0\}$

is isomorphic to the strict transform $A_2(\gamma, \tau)$ to W_2 of $A(\gamma, \tau)$.

In particular, $A(\gamma, \tau)$ is irreducible and tangent to $\Gamma_{1/\gamma}$

at the point given by $(t, x) = (1/\gamma, 1/\gamma)$, and B is reduced.

(13)

Proof. We obtain ψ^{-1} by setting $(t, x) = \left(\frac{z^2}{v}, \frac{z}{v}\right)$.

The indeterminacy of ψ^{-1}

consists of $(0, 0)$, (∞, ∞) and their infinitely near points.

Let $A'(\gamma, \tau)$ denote the closure of the zero set of a polynomial

$\gamma(\tau - z) - (3\tau - 2)v + (2\tau - 1)vz$ in v, z on Σ'_0 .

$\tau \neq 1 \Leftrightarrow A'(\gamma, \tau)$ is irreducible.

In fact, $A'(\gamma, \tau)$ is tangent to the closure of the zero set of

a polynomial $v - \gamma z^2$ in v, z on Σ'_0 at $(\gamma, 1)$.

Therefore $A(\gamma, \tau)$ is tangent to $\Gamma_{1/\gamma}$ at $(1/\gamma, 1/\gamma)$.

$\tau \neq 0, 1/2 \Leftrightarrow A'(\gamma, \tau)$ does not pass through $(0, 0), (\infty, \infty)$.

Thus $A'(\gamma, \tau)$ is isomorphic to $A_2(\gamma, \tau)$ through ϕ' .

In particular, $A(\gamma, \tau)$ is also irreducible and B is reduced. □

(14)

Notice that B is divisible by two in $\text{Pic}(\Sigma_0)$.

Since $\text{Pic}(\Sigma_0)$ is torsion free, $\exists! \delta \in \text{Pic}(\Sigma_0)$ s.t. $B \sim 2\delta$,

where the symbol $\sim$ means the linear equivalence of divisors.

Thus a finite double cover of Σ_0 branched along B is uniquely constructed from B up to isomorphism.

We denote it by $\pi : \widehat{X} \rightarrow \Sigma_0$.

Let us resolve singularities of $\widehat{X}$ according to Horikawa [Hor]. In fact, Γ_0 and Γ_∞ are singular fibres of type (V) as in [Hor p. 84, Definition] for all σ, τ with $\sigma \neq 0, 1$ and $\tau \neq 0, 1/2, 2/3, 1$.

Furthermore, W_2 coincide with $W^\flat$ as in [Hor p. 85, Lemma 7].

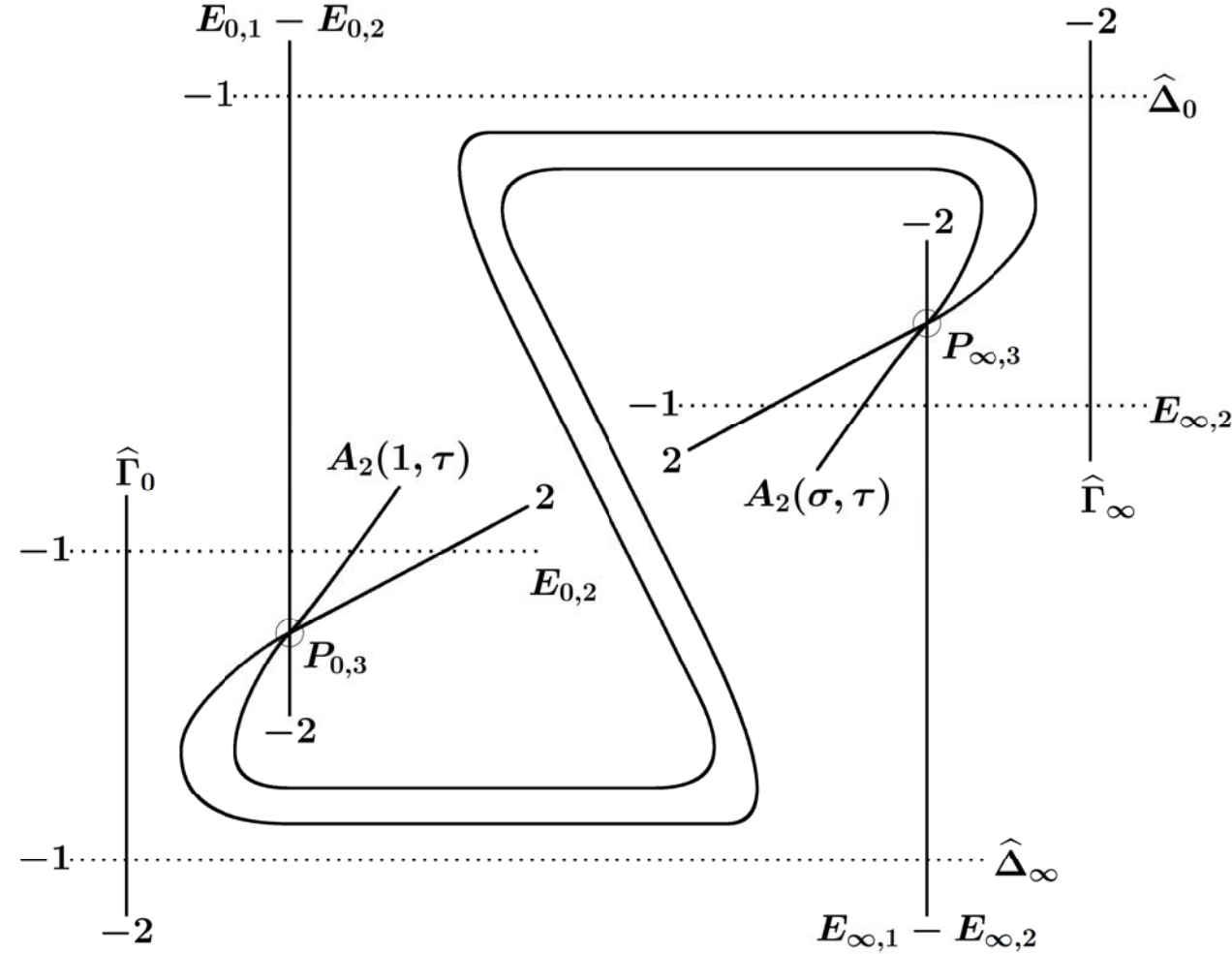
In our situation singularities of the induced branch divisor $B^\flat$ are

two simple triple points, which correspond to the point $\left(\infty, \frac{3\tau - 2}{2\tau - 1}\right)$ and the point $(0, \tau)$ on Σ'_0 through ϕ' as in Lemma 3.

(15)

On W_2

Broken lines denote curves not contained in B_2



(16)

On W_2 , in the corresp. pts, $A_2(1, \tau)$ and $A_2(\sigma, \tau)$ meet transversally.

One of the two points,

which is denoted by $P_{0,3}$, is on the strict transform of $E_{0,1}$.

$P_{\infty,3}$: the other one, which is on the strict transform of $E_{\infty,1}$.

$\phi_3 : W_3 \rightarrow W_2$: the blow-up at the two points $P_{0,3}$ and $P_{\infty,3}$

with $E_{0,3} = \phi_3^{-1}(P_{0,3})$ and $E_{\infty,3} = \phi_3^{-1}(P_{\infty,3})$.

$A_3(\gamma, \tau)$: the strict transform to W_3 of $A(\gamma, \tau)$.

Remark that $A_3(1, \tau)$ and $A_3(\sigma, \tau)$ are disjoint from each other.

$P_{i,4}$: the intersection point of $E_{i,3}$ and $A_3(1, \tau)$ for $i = 0, \infty$.

$P_{i,5}$: the intersection point of $E_{i,3}$ and $A_3(\sigma, \tau)$ for $i = 0, \infty$.

$P_{i,6}$: that of $E_{i,3}$ and the strict transform to W_3 of $E_{i,1}$.

$\phi_6 : \widetilde{W} \rightarrow W_3$: the blow-up at the six points $P_{i,j}$

with $i = 0, \infty$ and $j = 4, 5, 6$. Set $E_{i,j} = \phi_6^{-1}(P_{i,j})$.

(17)

For $i = 0, \infty$ and $k = 1, 2, 3$,

we denote by $\widehat{E}_{i,k}$ the strict transform to $\widetilde{W}$ of $E_{i,k}$.

In the same way, $\widehat{\Delta}_i$ and $\widehat{\Gamma}_i$ denote respectively that of Δ_i and Γ_i .

$A_6(\gamma, \tau)$: the strict transform to $\widetilde{W}$ of $A(\gamma, \tau)$.

For simplicity,

we denote the pull-back to $\widetilde{W}$ of them by the same symbols.

Thus we have

$$\begin{aligned}
A_6(1, \tau) &\sim 3\Delta_0 + 2\Gamma_0 - 2E_{0,1} - E_{0,2} - E_{0,3} - E_{0,4} \\
&\quad - 2E_{\infty,1} - E_{\infty,2} - E_{\infty,3} - E_{\infty,4}, \\
A_6(\sigma, \tau) &\sim 3\Delta_0 + 2\Gamma_0 - 2E_{0,1} - E_{0,2} - E_{0,3} - E_{0,5} \\
&\quad - 2E_{\infty,1} - E_{\infty,2} - E_{\infty,3} - E_{\infty,5},
\end{aligned}$$

(18)

Now, we set

$$\tilde{B} = A_6(1, \tau) + A_6(\sigma, \tau) + \hat{\Gamma}_0 + \hat{\Gamma}_\infty + \hat{E}_{0,1} + \hat{E}_{0,3} + \hat{E}_{\infty,1} + \hat{E}_{\infty,3}.$$

Since $\tilde{B}$ is smooth and divisible by two in $\text{Pic}(\tilde{W})$,

we obtain a smooth projective surface $\tilde{X}$

by the finite double cover $\varpi : \tilde{X} \rightarrow \tilde{W}$ branched along $\tilde{B}$.

Put $\tilde{\phi} = \phi_1 \circ \phi_2 \circ \phi_3 \circ \phi_6$. Then

$$\exists \mu : \tilde{X} \rightarrow \widehat{X} : \text{birational morphism s.t. } \pi \circ \mu = \tilde{\phi} \circ \varpi.$$

We call $\tilde{X}$ the canonical resolution of singularities of $\widehat{X}$.

For simplicity, we put $\tilde{\pi} = \pi \circ \mu$ and $\tilde{f} = pr_1 \circ \tilde{\pi}$.

Let us consider $\tilde{f} : \widetilde{X} \rightarrow \mathbb{P}^1$.

Recall $q(\gamma, \tau) := \frac{\tau(3\tau - 2)^3}{\gamma(2\tau - 1)}$

$$\gamma \neq 0 \quad \left(\sigma \neq 0, 1 \text{ and } \tau \neq 0, \frac{1}{2}, \frac{2}{3}, 1 \right)$$

$\Gamma_{q(\gamma, \tau)}$ is tangent to $A(\gamma, \tau)$.

We know from Lemma 3 that $\Gamma_{1/\gamma}$ does so.

By restricting $pr_1 \circ \tilde{\phi} : \widetilde{W} \rightarrow \mathbb{P}^1$ to $A_6(1, \tau)$ and to $A_6(\sigma, \tau)$,

we see that Γ_q meets B transversely at six points

$$\text{for any } q \in \mathbb{P}^1 \setminus \{0, \infty, 1, 1/\sigma, q(1, \tau), q(\sigma, \tau)\}$$

from the Riemann-Hurwitz formula.

Therefore a general fibre of $\tilde{f} : \widetilde{X} \rightarrow \mathbb{P}^1$

is a smooth projective curve of genus two.

(20)

Recall $q(\gamma, \tau) := \frac{\tau(3\tau - 2)^3}{\gamma(2\tau - 1)} \quad \left(\sigma \neq 0, 1 \text{ and } \tau \neq 0, \frac{1}{2}, \frac{2}{3}, 1 \right)$

$\tilde{f}^{-1}(q)$ is a smooth projective curve of genus two

for any $q \in \mathbb{P}^1 \setminus \{0, \infty, 1, 1/\sigma, q(1, \tau), q(\sigma, \tau)\}$.

Furthermore,

we remark that $q(1, \tau) - 1 = (3\tau - 1)^3(\tau - 1)/(2\tau - 1)$

and Γ_1 meets $A(\sigma, 1/3)$ transversely at three points.

Exactly at two points Γ_1 meets B transversely iff $q(\sigma, \tau) = 1$.

When $q(1, \tau) \neq 1$ and $q(\sigma, \tau) \neq 1$,

at four points Γ_1 meets B transversely.

Thus Γ_1 meets B transversely at least at two points.

In this way, we can check that $\Gamma_{1/\sigma}$, $\Gamma_{q(1, \tau)}$ and $\Gamma_{q(\sigma, \tau)}$ also do so.

Hence the reducible fibres of $\tilde{f}$ are $\tilde{f}^{-1}(0)$ and $\tilde{f}^{-1}(\infty)$ only.

(21)

Let e_i denote the (-1) -curve on $\widetilde{X}$ with $2e_i = \varpi^*\widehat{\Gamma}_i$ for $i = 0, \infty$.

Although e_i meets $\varpi^*\widehat{E}_{i,2}$ at one point,

e_i is disjoint from the other components of $\widetilde{f}^{-1}(i)$.

Additionally, $\varpi^*\widehat{E}_{i,2}$ is not a (-2) -curve.

Thus, after the contraction $\eta : \widetilde{X} \rightarrow X$ of e_0 and e_∞ ,

we obtain the rel. min. model $f : X \rightarrow \mathbb{P}^1$ of $\widetilde{f} : \widetilde{X} \rightarrow \mathbb{P}^1$.

Proposition 4. For $\sigma \in \mathbb{C} \setminus \{0, 1\}$ and $\tau \in \mathbb{C} \setminus \{0, 1/2, 2/3, 1\}$,

$f : X \rightarrow \mathbb{P}^1$ obtained as above is a rel. min. fibration of genus two.

The fibres $f^{-1}(0)$ and $f^{-1}(\infty)$ are as in [NU, p. 172, 3-II $^*_{3-0}$]

and the other fibres of f are irreducible and reduced.

Furthermore, X is a smooth rational surface with $\rho(X) = 12$.

(22)

Proof. Consider $A_1(1, \tau) + A_1(\sigma, \tau) + E_{0,1} + E_{\infty,1}$ on W_1 .

For $i = 0, \infty$, the strict transform to W_1 of Γ_i is a (-1) -curve.

The contraction of the two (-1) -curves translates singularities of the branch divisor into those as in [NU, p. 172, 3-II $^*_{3-0}$].

Thus, it is enough to prove that

$$\widetilde{X} \text{ is a rational surface with } \rho(\widetilde{X}) = 14.$$

Consider the projection map $pr'_1 : \Sigma'_0 \rightarrow \mathbb{P}^1$ onto the first factor.

Let Γ'_1 be the pull-back to $\widetilde{W}$ of the fibre given by $v = 1$ on Σ'_0 .

We remark that $\varpi^*\Gamma'_1$ is nef. Let us compute $\varpi^*\Gamma'_1 \cdot K_{\widetilde{X}}$.

Lemma 3 yields $\Gamma'_1 \sim 2\Delta_0 + \Gamma_0 - E_{0,1} - E_{0,2} - E_{\infty,1} - E_{\infty,2}$.

We know

$$\widetilde{B} \sim 6\Delta_0 + 6\Gamma_0 - 4(E_{0,1} + E_{0,2} + E_{\infty,1} + E_{\infty,2}) - 2 \sum_{j=3}^6 (E_{0,j} + E_{\infty,j}).$$

(23)

Hence

$$K_{\widetilde{X}} \sim \varpi^*(K_{\widetilde{W}} + \frac{1}{2}\widetilde{B}) \sim \varpi^*(\Delta_0 + \Gamma_0 - E_{0,1} - E_{0,2} - E_{\infty,1} - E_{\infty,2}),$$

$$\varpi^*\Gamma'_1 \sim \varpi^*(2\Delta_0 + \Gamma_0 - E_{0,1} - E_{0,2} - E_{\infty,1} - E_{\infty,2}).$$

For all positive integers n , we conclude that

the n -th plurigenus of $\widetilde{X}$ is zero from $\varpi^*\Gamma'_1.nK_{\widetilde{X}} = -2n < 0$.

We also see that the irregularity of $\widetilde{X}$ is zero

by considering the finite double cover ϖ

$$\left(\text{e.g., } \chi(\mathcal{O}_{\widetilde{X}}) = 2\chi(\mathcal{O}_{\widetilde{W}}) + \frac{1}{4}\widetilde{B}.K_{\widetilde{W}} + \frac{1}{8}\widetilde{B}^2 = 1 \right).$$

Therefore $\widetilde{X}$ is a rational surface by Castelnuovo's rationality criterion.

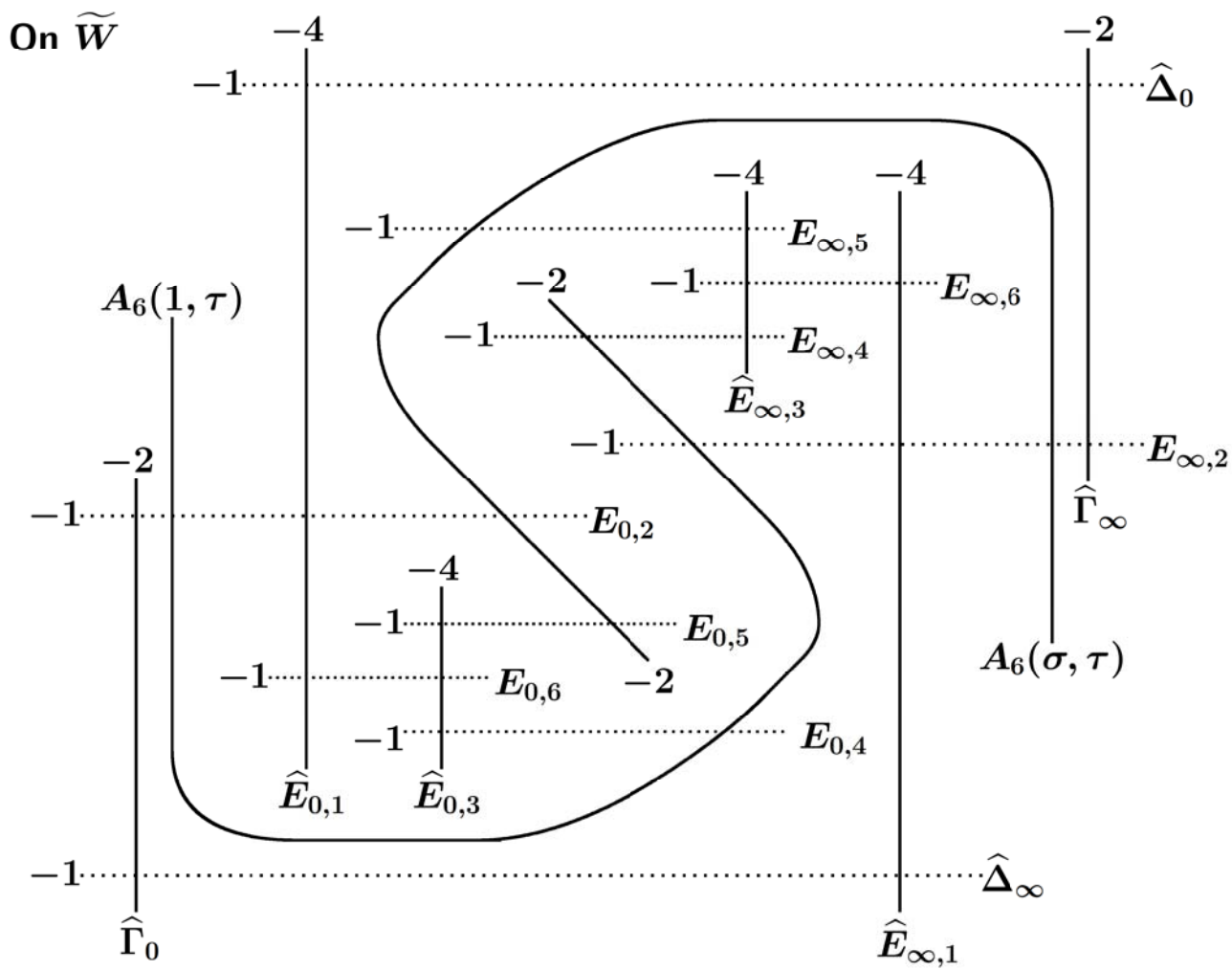
Thus $b_1(\widetilde{X}) = b_3(\widetilde{X}) = 0$ and $b_2(\widetilde{X}) = \rho(\widetilde{X})$,

where $b_n(\widetilde{X})$ denotes the n -th Betti number of $\widetilde{X}$.

This and Noether's formula provide $\rho(\widetilde{X}) = 10 - K_{\widetilde{X}}^2$.

So $\rho(\widetilde{X}) = 14$ follows. □

(24)



(25)

Corollary 5. For $i = 0, \infty$ and $j = 1, 3$,

let $\Theta_{i,j}$ denote the (-2) -curve with $2\eta^*\Theta_{i,j} = \varpi^*\widehat{E}_{i,j}$.

Let $\Theta_{i,j}$ be the (-2) -curve which is identified with $\varpi^*E_{i,j}$ through η for $i = 0, \infty$ and $j = 4, 5, 6$.

Put $\Theta_{i,2} = \eta(\varpi^*\widehat{E}_{i,2})$ for $i = 0, \infty$.

Then $\Theta_{i,2}$ is an elliptic curve with

$$\Theta_{i,2} \cdot \Theta_{i,1} = -\Theta_{i,2}^2 = 1 \text{ for } i = 0, \infty.$$

For $i = 0, \infty$,

$$\Theta_{i,4} \cdot \Theta_{i,3} = \Theta_{i,5} \cdot \Theta_{i,3} = \Theta_{i,3} \cdot \Theta_{i,6} = \Theta_{i,6} \cdot \Theta_{i,1} = 1.$$

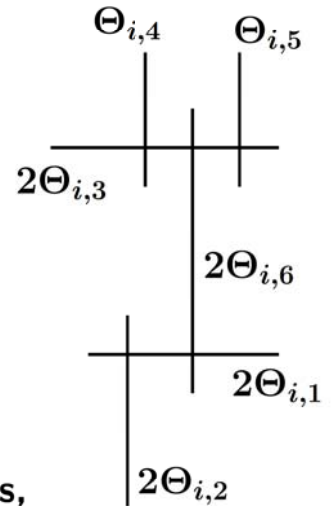
For the other pairs of irr. components of the fibres,

two components are disjoint from each other.

The irr. decomp. of the reducible fibre $f^{-1}(i)$, $i = 0, \infty$ is as follows:

$$f^{-1}(i) = \Theta_{i,4} + \Theta_{i,5} + 2\Theta_{i,3} + 2\Theta_{i,6} + 2\Theta_{i,1} + 2\Theta_{i,2}.$$

(26)



Lemma 6. Let $f : X \rightarrow \mathbb{P}^1$ be a fibration as in Proposition 4.

If there exists a section of f , then f has at least two sections.

Proof. Suppose that there exists a section of f ,

which can be regarded as a horizontal curve D_1 on X .

Let $\widetilde{D}_1$ be the strict transform by $\eta : \widetilde{X} \rightarrow X$ of D_1 .

Then the image C by $\tilde{\pi} : \widetilde{X} \rightarrow \Sigma_0$ of $\widetilde{D}_1$ is a section of $pr_1 : \Sigma_0 \rightarrow \mathbb{P}^1$.

Here we recall the irreducible decomposition of B :

$$B = A(1, \tau) + A(\sigma, \tau) + \Gamma_0 + \Gamma_\infty.$$

In particular, B does not contain C as an irreducible component.

Hence we obtain another section $\widetilde{D}_2$ of $\tilde{f}$ as the other component

$$\left(\tilde{\pi}^* C - \widetilde{D}_1 \right) \text{ from the irreducible decomposition of } \tilde{\pi}^* C.$$

So we have another section of f as the image by η of $\widetilde{D}_2$. □

(27)

Proposition 7. Let $f : X \rightarrow \mathbb{P}^1$ be a fibration as in Proposition 4 and $\Theta_{i,j}$ the irr. components of the reducible fibres as in Corollary 5. Then there exists a birational morphism $\nu : X \rightarrow \mathbb{P}^2$ such that the pull-back to X of a line ℓ on $\mathbb{P}^2$ and that of (-1) -curves e_h , $h = 1, 2, \dots, 11$ contracted by ν satisfy the following:

$$F \sim 7\ell - 3e_1 - 2 \sum_{h=2}^{11} e_h$$

$$\begin{aligned} \Theta_{0,2} &= -K_X + e_2, & \Theta_{\infty,2} &= -K_X + e_3, \\ \Theta_{0,4} &= \ell - e_1 - e_8 - e_{10}, & \Theta_{\infty,4} &= \ell - e_1 - e_9 - e_{11}, \\ \Theta_{0,1} &= e_4 - e_2, & \Theta_{\infty,1} &= e_5 - e_3, \\ \Theta_{0,6} &= e_6 - e_4, & \Theta_{\infty,6} &= e_7 - e_5, \\ \Theta_{0,3} &= e_8 - e_6, & \Theta_{\infty,3} &= e_9 - e_7, \\ \Theta_{0,5} &= e_{10} - e_8, & \Theta_{\infty,5} &= e_{11} - e_9. \end{aligned}$$

(28)

Proof. Let e_1 denote the (-1) -curve with $2\eta^*e_1 = \varpi^*A_6(1, \tau)$.

Since $\Gamma_1.A_6(1, \tau) = 3$ on $\widetilde{W}$, we have $F.e_1 = 3$.

The images by η of $\varpi^*\widehat{\Delta}_0$ and $\varpi^*\widehat{\Delta}_\infty$

are two disjoint (-1) -curves on X , which meet F at two points.

Put $e_2 = \eta\left(\varpi^*\widehat{\Delta}_0\right)$ and $e_3 = \eta\left(\varpi^*\widehat{\Delta}_\infty\right)$.

We also remark that $e_2.e_1 = e_3.e_1 = 0$,

since $\widehat{\Delta}_0.A_6(1, \tau) = \widehat{\Delta}_\infty.A_6(1, \tau) = 0$.

We know $\varpi^*\Gamma'_1.K_{\widetilde{X}} = -2$ in the proof of Proposition 4.

By the adjunction formula we verify that $pr'_1 : \Sigma'_0 \rightarrow \mathbb{P}^1$ induces

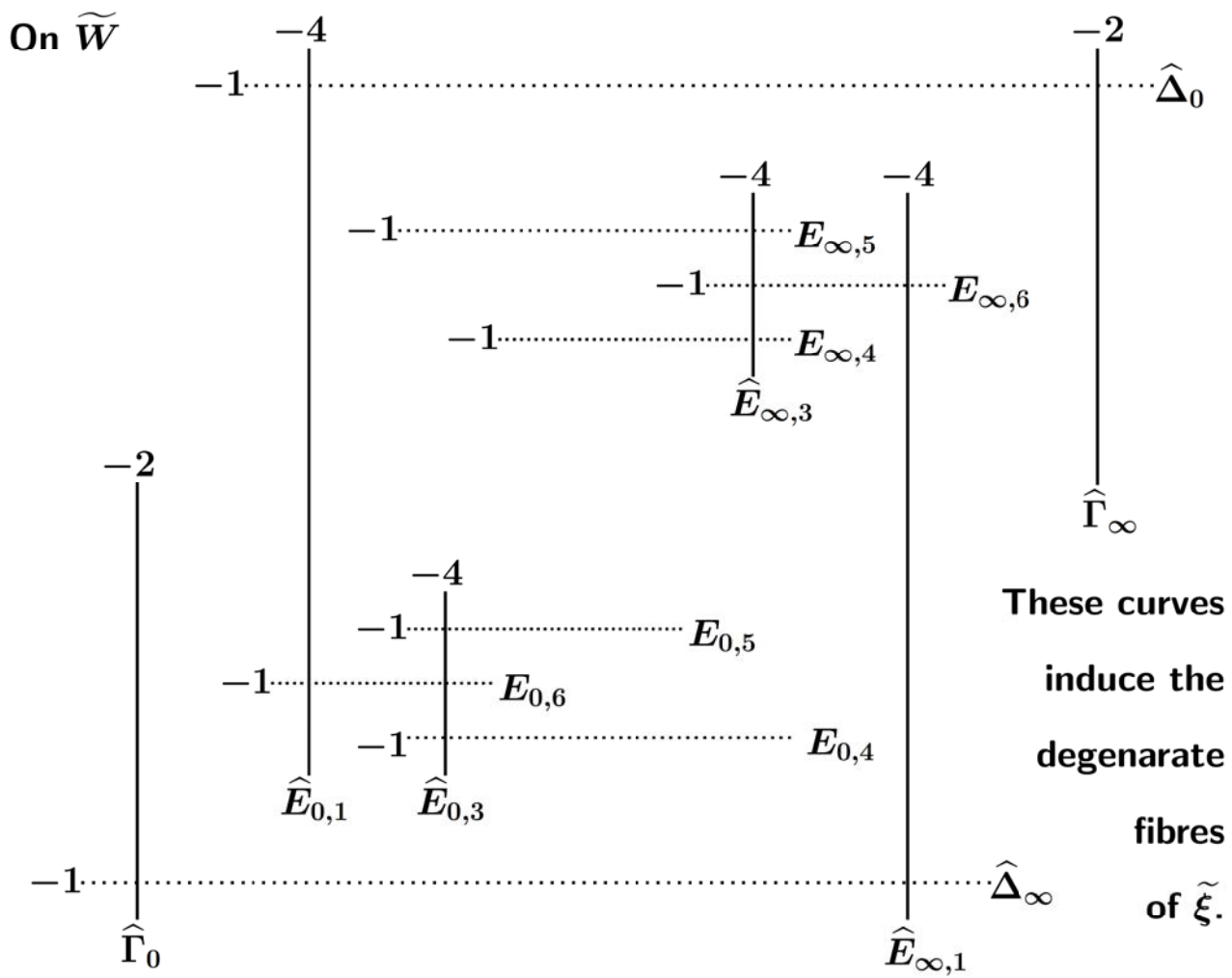
a ruling $\widetilde{\xi} : \widetilde{X} \rightarrow \mathbb{P}^1$ through $\psi \circ \widetilde{\pi} : \widetilde{X} \rightarrow \Sigma'_0$.

The degenerate fibres of $\widetilde{\xi}$ are $\widetilde{\xi}^{-1}(0)$ and $\widetilde{\xi}^{-1}(\infty)$ only,

since the fibres of pr'_1 except for $pr'^{-1}_1(0)$ and $pr'^{-1}_1(\infty)$

do not pass through the intersection points of $A'(1, \tau)$ and $A'(\sigma, \tau)$.

(29)



(30)

$\tilde{\xi}^{-1}(i)$ contains e_i for each $i = 0, \infty$ as an irreducible component.

Hence there is a unique ruling $\xi : X \rightarrow \mathbb{P}^1$ such that $\tilde{\xi} = \xi \circ \eta$.

Furthermore, $\xi^{-1}(\infty)$ consists of $\Theta_{0,j}, j = 1, 3, 4, 5, 6$ and e_2 .

$\xi^{-1}(0)$ consists of $\Theta_{\infty,j}, j = 1, 3, 4, 5, 6$ and e_3 .

Notice that $e_1 \cdot \Theta_{0,4} = e_1 \cdot \Theta_{\infty,4} = 1$ and

the other components are disjoint from e_1 .

Let $\nu_1 : X \rightarrow \Sigma_1$ be the birational morphism contracting e_2, e_3 and

eight (-2) -curves $\Theta_{i,1}, \Theta_{i,6}, \Theta_{i,3}, \Theta_{i,5}$ with $i = 0, \infty$,

which are the strict transforms of eight (-1) -curves.

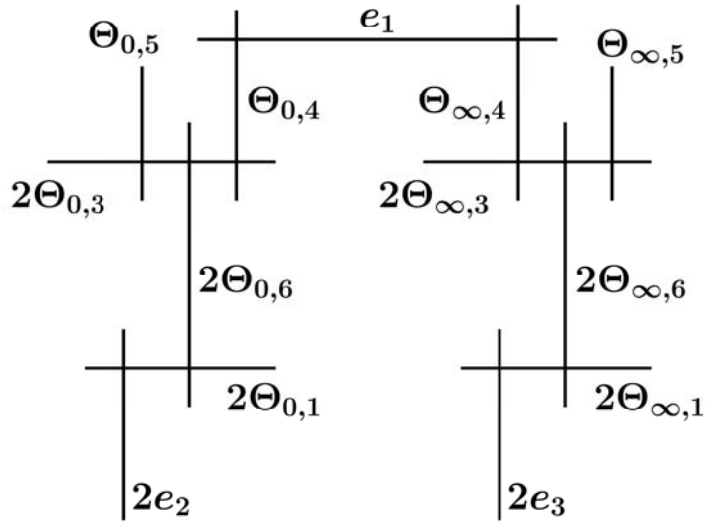
Here Σ_1 is a relatively minimal model of $\xi : X \rightarrow \mathbb{P}^1$.

We remark that the image of e_1 is the minimal section of Σ_1 .

Let $\nu_0 : \Sigma_1 \rightarrow \mathbb{P}^2$ be the contraction and put $\nu = \nu_0 \circ \nu_1$.

(31)

From the configuration of e_2, e_3 and eight (-2) -curves $\Theta_{i,1}, \Theta_{i,6}, \Theta_{i,3}, \Theta_{i,5}$ with $i = 0, \infty$, we can denote the pull-backs to X of the eight (-1) -curves by $e_h, h = 4, 5, \dots, 11$ so that $e_4 = \Theta_{0,1} + e_2$,



$$e_5 = \Theta_{\infty,1} + e_3, \quad e_6 = \Theta_{0,6} + e_4, \quad e_7 = \Theta_{\infty,6} + e_5, \quad e_8 = \Theta_{0,3} + e_6, \\ e_9 = \Theta_{\infty,3} + e_7, \quad e_{10} = \Theta_{0,5} + e_8 \quad \text{and} \quad e_{11} = \Theta_{\infty,5} + e_9.$$

Recall that the images by ν_1 of $\Theta_{0,4}$ and $\Theta_{\infty,4}$ are fibres of Σ_1 .

We have $\Theta_{0,4} = \ell - e_1 - e_8 - e_{10}$ and $\Theta_{\infty,4} = \ell - e_1 - e_9 - e_{11}$,

where ℓ denotes the pull-back to X of a line on $\mathbb{P}^2$.

(32)

Next we recall that $\varpi^* \hat{\Delta}_\infty = \eta^* e_3 - e_0$ and

$$\begin{aligned}
K_{\widetilde{X}} &\sim \varpi^* \left(K_{\widetilde{W}} + \frac{1}{2} \widetilde{B} \right) \\
&\sim \varpi^* (\Delta_\infty + \Gamma_0 - E_{0,1} - E_{0,2} - E_{\infty,1} - E_{\infty,2}) \\
&\sim \varpi^* (\Delta_\infty - E_{\infty,1}) - \varpi^* E_{\infty,2} + \varpi^* (\Gamma_0 - E_{0,1} - E_{0,2}) \\
&\sim \varpi^* \hat{\Delta}_\infty - \varpi^* E_{\infty,2} + \varpi^* \hat{\Gamma}_0 \\
&\sim (\eta^* e_3 - e_0) - \varpi^* E_{\infty,2} + 2e_0.
\end{aligned}$$

Hence we have $\varpi^* E_{\infty,2} \sim -K_{\widetilde{X}} + \eta^* e_3 + e_0 \sim \eta^* (-K_X + e_3) - e_\infty$.

Therefore we get $\Theta_{\infty,2} = -K_X + e_3$.

In the same way, we see $\Theta_{0,2} = -K_X + e_2$. Furthermore, we show

$$\begin{aligned}
F &\sim f^{-1}(i) = 2\Theta_{i,2} + 2\Theta_{i,1} + 2\Theta_{i,6} + 2\Theta_{i,3} + \Theta_{i,4} + \Theta_{i,5} \\
&\sim -2K_X + \ell - e_1 \\
&\sim 7\ell - 3e_1 - 2 \sum_{h=2}^{11} e_h.
\end{aligned}$$

□

(33)

Corollary 8. Put $D = e_1 - e_{11}$. Then

$$\mathrm{NS}(X) \simeq \mathbb{Z}D \oplus \bigoplus_{j=1}^6 \mathbb{Z}\Theta_{0,j} \oplus \bigoplus_{j=1}^6 \mathbb{Z}\Theta_{\infty,j}.$$

Proof. It is well-known that $\mathrm{NS}(X) \simeq \mathbb{Z}\ell \oplus \bigoplus_{h=1}^{11} \mathbb{Z}e_h$.

Thus we only have to represent ℓ and e_h 's

as $\mathbb{Z}$ -linear combinations of D and $\Theta_{i,j}$'s from Proposition 7.

D and the irr. components of the reducible fibres except for $\Theta_{\infty,5}$ generate ℓ and e_1 as follows:

$$\begin{aligned} \ell = & 7D + 16\Theta_{0,1} + 13\Theta_{0,2} + 22\Theta_{0,3} + 14\Theta_{0,4} + 11\Theta_{0,5} + 19\Theta_{0,6} \\ & - 13\Theta_{\infty,1} - 16\Theta_{\infty,2} - 7\Theta_{\infty,3} - 4\Theta_{\infty,4} - 10\Theta_{\infty,6}, \\ e_1 = & 3D + 6\Theta_{0,1} + 5\Theta_{0,2} + 8\Theta_{0,3} + 5\Theta_{0,4} + 4\Theta_{0,5} + 7\Theta_{0,6} \\ & - 5\Theta_{\infty,1} - 6\Theta_{\infty,2} - 3\Theta_{\infty,3} - 2\Theta_{\infty,4} - 4\Theta_{\infty,6}. \end{aligned}$$

(34)

Furthermore, Proposition 7 immediately yields that

$$\begin{aligned}
e_{11} &= e_1 - D, \quad e_9 = \ell - e_1 - e_{11} - \Theta_{\infty,4}, \quad e_7 = e_9 - \Theta_{\infty,3}, \\
e_5 &= e_7 - \Theta_{\infty,6}, \quad e_3 = e_5 - \Theta_{\infty,1}, \quad e_2 = e_3 + \Theta_{0,2} - \Theta_{\infty,2}, \\
e_4 &= e_2 + \Theta_{0,1}, \quad e_6 = e_4 + \Theta_{0,6}, \quad e_8 = e_6 + \Theta_{0,3}, \quad e_{10} = e_8 + \Theta_{0,5}.
\end{aligned}$$

Hence, we see that

e_h , $h = 2, 3, \dots, 11$ can be the $\mathbb{Z}$ -linear combinations inductively.

Therefore D , $\Theta_{0,1}, \Theta_{0,2}, \dots, \Theta_{0,6}$, $\Theta_{\infty,1}, \Theta_{\infty,2}, \Theta_{\infty,3}, \Theta_{\infty,4}$ and $\Theta_{\infty,6}$ form $\mathbb{Z}$ -basis of $\text{NS}(X)$. □

§3 Virtual Mordell-Weil groups

We shall introduce the theory of the virtual Mordell-Weil groups, which is used to complete the proof of Theorem 2.

S : a smooth projective rational surface $/\mathbb{C}$

$\varphi : S \rightarrow \mathbb{P}^1$: a rel. min. fibration whose general fibre F is

a projective curve of genus $g \geq 2$

We denote by n_q

the number of irreducible components of $\varphi^{-1}(q)$ for any $q \in \mathbb{P}^1$.

In [Viet, p. 101, Def. 0.2], the virtual Mordell-Weil rank r of φ ,

which does not necessarily admit a section, is defined as

$$r = \rho(S) - 2 - \sum_{q \in \mathbb{P}^1} (n_q - 1).$$

(36)

For example, when $\varphi : S \rightarrow \mathbb{P}^1$ is a fibration as in Proposition 4,

we know that $\rho(S) = 12$ and $n_0 = n_\infty = 6$ with $n_q = 1$

for all $q \in \mathbb{P}^1 \setminus \{0, \infty\}$, which lead to $r = 0$.

Let V be the subgroup of $\text{NS}(S)$ generated by

the irreducible components of the fibres of φ .

The primitive closure $\widehat{V}$ is defined as $\widehat{V} = V \otimes \mathbb{Q} \cap \text{NS}(S)$.

Let us observe that $\widehat{V}/V$ can be regarded as

the virtual Mordell-Weil group of φ with $r = 0$.

Assume that there exists on S a divisor D with $D.F = 1$.

When φ admits a section, we can regard it as the above D .

Set $T_D = \mathbb{Z}D \oplus V \subset \text{NS}(S)$, and put $\widehat{T}_D = T_D \otimes \mathbb{Q} \cap \text{NS}(S)$.

Then, for all D with $D.F = 1$, the quotient groups of $\widehat{T}_D$ by T_D are isomorphic to each other and to $\widehat{V}/V$ as follows.

(37)

Lemma 9. The natural projection $T_D \rightarrow V$ induces an isomorphism

$$\hat{T}_D/T_D \simeq \hat{V}/V \text{ naturally.}$$

Proof. Let $\Theta_{q,j}$ be an irreducible component of a reducible fibre $\varphi^{-1}(q)$ for $j = 1, 2, \dots, n_q$. Take any $E \in \hat{T}_D$.

We have $E = \alpha D + \sum \beta_{q,j} \Theta_{q,j}$ for some $\alpha, \beta_{q,j} \in \mathbb{Q}$ by definition.

In fact, $\alpha = E.F$ must be an integer.

In particular, $\sum \beta_{q,j} \Theta_{q,j} = E - \alpha D \in \text{NS}(S)$. Thus, $\sum \beta_{q,j} \Theta_{q,j} \in \hat{V}$.

In this way, while $D.F = 1$, the natural projection $\hat{T}_D \rightarrow \hat{V}$ of the primitive closures is well-defined.

Consider the composition $\hat{T}_D \rightarrow \hat{V} \rightarrow \hat{V}/V$, which is a surjective
homomorphism of groups.

Its kernel is equal to T_D . So $\hat{T}_D/T_D \simeq \hat{V}/V$ follows. $\square$

(38)

Via φ , we can regard S as a smooth projective curve of genus g
defined over the rational function field $\mathbb{K} = \mathbb{C}(\mathbb{P}^1)$.

We assume that it has a $\mathbb{K}$ -rational point O .

Let $\mathcal{J}_\varphi/\mathbb{K}$ be the Jacobian variety of the generic fibre $\mathcal{F}/\mathbb{K}$ of φ .

The Mordell-Weil group of φ is the group of $\mathbb{K}$ -rational points $\mathcal{J}_\varphi(\mathbb{K})$.

It is a finitely generated abelian group.

The rank of the group is equal to r .

There is a natural one-to-one correspondence between

the set of $\mathbb{K}$ -rational points $\mathcal{F}(\mathbb{K})$ and the set of sections of φ .

For $P \in \mathcal{F}(\mathbb{K})$, we denote by (P) the section corresponding to P

which is regarded as a horizontal curve on S .

In particular, (O) corresponding to the origin O of $\mathcal{J}_\varphi(\mathbb{K})$

is called the zero section.

(39)

In [Sh, p. 362, Theorem 3], we have the natural isomorphism of groups $\mathcal{J}_\varphi(\mathbb{K}) \simeq \text{NS}(S)/T_{(O)}$.

By definition, the torsion part $\mathcal{J}_\varphi(\mathbb{K})_{\text{tor}}$ is isomorphic to $\hat{T}_{(O)}/T_{(O)}$.

From Lemma 9, we conclude $\mathcal{J}_\varphi(\mathbb{K})_{\text{tor}} \simeq \hat{V}/V$.

Let $f : X \rightarrow \mathbb{P}^1$ be a fibration as in Proposition 4. We recall $r = 0$. Furthermore, if f admits a section, then we see that the Mordell-Weil group of f is trivial from Corollary 8 and Lemma 9. Hence, we have the following.

Lemma 10.

Suppose that f admits a section. Then it is the unique section of f .

Proof of Theorem 2. We only have to show that f has no sections.

The assertion follows from Lemmas 6 and 10. □

(40)

Derivations having divergence zero

長峰孝典

2016 年 8 月 27 日

1 序章

R を整域, A を R を部分環にもつ整域とする. $Q(A)$ で A の商体を表す. 写像 $D : A \rightarrow A$ が **R -導分 (R -derivation)** であるとは, $f, g \in A$ と $r \in R$ に対して以下の 3 条件をみたすときを言う.

- (1) $D(f + g) = D(f) + D(g)$.
- (2) $D(rf) = rD(f)$.
- (3) $D(fg) = fD(g) + gD(f)$.

R -導分 D に関する基本的な性質を以下にまとめる.

- (P1) $A^D := \{f \in A \mid D(f) = 0\}$ は A の R を含む部分環である. 特に A が体のとき A^D は A の部分体である.
- (P2) $f/g \in Q(A)$ に対して

$$\tilde{D}(f/g) := \frac{D(f)g - fD(g)}{g^2}$$

と定めると $\tilde{D}$ は $Q(A)$ における R -導分で, $Q(A)^{\tilde{D}} \cap A = A^D$ をみたす. $\tilde{D}$ を導分 D の $Q(A)$ への延長と呼ぶ.

- (P3) R の標数を 0 とする. このとき A^D は A において代数的に閉じている.
- (P4) D が**局所冪零導分 (locally nilpotent derivation)** であるとは, 任意の $f \in A$ に対して $D^n(f) = 0$ をみたす非負整数 $n \in \mathbb{Z}_{\geq 0}$ が存在するときを言う.
- (P5) A を R 上の n 変数多項式環 $R[x_1, x_2, \dots, x_n]$ とする. このとき,

$$\operatorname{div}(D) := \sum_{i=1}^n \frac{\partial D(x_i)}{\partial x_i}$$

と定め, $\operatorname{div}(D)$ を導分 D の**発散 (divergence)** という.

- (P6) $A = R[x_1, x_2, \dots, x_n]$ とする. このとき, D が**三角導分 (triangular derivation)** であるとは, 各 $i = 1, 2, \dots, n$ に対して $D(x_i) \in R[x_1, x_2, \dots, x_{i-1}]$ をみたすときを言う.

(P7) $A = R[x_1, x_2, \dots, x_n]$ とする. このとき, D が三角導分なら局所冪零導分である.

(P8) R を $\mathbb{Q}$ を含む整域, A を R 上の n 変数多項式環とする. このとき, D が局所冪零なら $\text{div}(D) = 0$ である.

本稿では以下の問題を起点として発散が 0 となる導分の核について考察する.

問題 1.1 (Hilbert の第 14 問題)

k を体, $k(x_1, x_2, \dots, x_n)$ を k 上の n 変数の有理関数体, L を $k(x_1, x_2, \dots, x_n)$ の部分体で k を含むものとする. このとき $L \cap k[x_1, x_2, \dots, x_n]$ は k 代数として有限生成か?

この問題は, 多項式環 $k[x_1, x_2, \dots, x_n]$ の部分 k 代数の有限生成性について問うものである. この問題は, n が 2 以下の場合に肯定的であることを Zariski [15] が示した. しかし, n が 3 以上の場合には反例が知られている. 最初の反例は 1958 年に Nagata [10] により発見された.

さて, この問題を多項式環上の導分の言葉で記述することを考えよう. D を多項式環 $k[x_1, x_2, \dots, x_n]$ 上の k -導分, $\tilde{D}$ を導分 D の k 上の n 変数有理関数体 $k(x_1, x_2, \dots, x_n)$ への延長とし, $L := k(x_1, x_2, \dots, x_n)^{\tilde{D}}$ とおく. このとき, L は k を含む $k(x_1, x_2, \dots, x_n)$ の部分体で, $L \cap k[x_1, x_2, \dots, x_n] = k[x_1, x_2, \dots, x_n]^D$ である. 従って Hilbert の第 14 問題の特別な場合として, 以下の問題が考えられる.

問題 1.2 (導分に関する Hilbert の第 14 問題)

k を体, D を多項式環上の k -導分とする. このとき $k[x_1, x_2, \dots, x_n]^D$ は k 代数として有限生成か?

この問題は n が 3 以下の場合には肯定的であることが Zariski の結果から従う. 一方, n が 4 以上の場合には反例が知られている. 特に $n = 2, 3$ の場合には Nowicki-Nagata [13] や Miyanishi [8] により, 興味深い以下の結果が証明された.

定理 1.3 (Nowicki-Nagata, Miyanishi)

k を標数 0 の体, D を $k[x_1, x_2, \dots, x_n]$ 上の k -導分で $k[x_1, x_2, \dots, x_n]^D \neq k$ であり, 零写像でないものとする. このとき,

- (1) $k[x_1, x_2]^D = k[h]$ をみたす多項式 $h \in k[x_1, x_2] \setminus k$ が存在する. つまり, $k[x_1, x_2]^D$ は k 上の 1 変数の多項式環に同型である ([13]).
- (2) D を局所冪零導分とすると, $k[x_1, x_2, x_3]^D$ は k 上の 2 変数の多項式環に同型である ([8]).

定理 1.3 は $n = 2$ の場合に, Berson [1] や El Kahoui [4] により, UFD 上の多項式環の場合に一般化されている. 以下がその主張である.

定理 1.4 (Berson, El Kahoui)

R を標数 0 の UFD, D を $R[x_1, x_2]$ 上の R -導分で $R[x_1, x_2]^D \neq R$ であり, 零写像でないものとする. このとき, $R[x_1, x_2]^D = k[h]$ をみたす多項式 $h \in R[x_1, x_2] \setminus R$ が存在する.

しかしながら, 定理 1.4 は一般の整域上では成立しない. Maubach [7] により次のような例が与えられている.

例 1.5 (Maubach)

k を標数 0 の体, $R := k[t^2, t^3]$ とする. このとき $R[x, y]$ における R -導分を $D = t^2 \frac{\partial}{\partial x} + t^3 \frac{\partial}{\partial y}$ と定めると, $R[x, y]^D = R[ft^2, f^2t^2, f^3t^2, \dots, f^nt^2, \dots]$ となる. ただし $F = tx - y \notin R[x, y]$ とおく.

上の例における R -導分 D は (P6) より三角導分であり, さらに (P7) により局所冪零導分で, 特に $\text{div}(D) = 0$ である. しかし, このような性質の良い導分であっても, その核は R 代数として有限生成ではない.

本稿では, 例 1.5 のような現象に注目し, 有理数体を含む整域上 2 変数多項式環における, 発散が 0 となる導分に関する結果を述べる.

2 整閉多項式と導分の核について

この章では, R を整域 A を R 上の n 変数多項式環 $R[x_1, x_2, \dots, x_n]$ とし, R の商体を $Q(R)$ で表わす.

定義 2.1 $f \in A \setminus R$ をとる.

- (1) f が**整閉多項式 (closed polynomial)** であるとは, 環 $R[f]$ が A において整閉となることを言う.
- (2) f が**弱整閉多項式 (weakly closed polynomial)** であるとは, $R[f] \subset R[g]$ かつ $Q(R)[g] \cap A = R[g]$ をみたすような整閉多項式 $g \in A \setminus R$ が存在するときを言う.

例 2.2 (1) 互いに素な自然数 $r, s \in \mathbb{Z}_{\geq 1}$ に対して, $x^r y^s \in R[x, y]$ は整閉多項式で, $Q(R) \cap R[x, y] = R[x^r y^s]$ をみたす.

- (2) $R' := k[x]$ とおく. ただし k は体とする. このとき, $g = xy \in R'[y]$ は整閉多項式だが, $Q(R')[g] \cap R'[y] \subsetneq R'[g]$ である.

- (3) R を UFD とする. このとき, 全ての定数でない多項式は弱整閉多項式である.

- (4) $R_t := k[t^2, t^3]$ とおく. ただし k は標数が 0 の体とする. このとき,
 $h := t^2x - t^3y \in R_t[x, y]$ は弱整閉多項式ではない.

また, 以下の Russell-Sathaye [14] による結果は, $Q(R)[f] \cap A = R[f]$ をみたす多項式 $f \in A \setminus R$ が十分多く存在することを意味している.

命題 2.3 (Russell-Sathaye)

R を整域, $f \in A = R[x_1, x_2, \dots, x_n] \setminus R$ を定数でない多項式で $f(0, 0, \dots, 0) = 0$ をみたすものとする. ここで, $c(f)$ を f の各単項式の係数で生成される R のイデアルとする. このとき, $c(f) = R$ ならば $Q(R)[f] \cap A = R[f]$ が成り立つ.

この命題は $Q(R)[f] \cap A = R[f]$ をみたす多項式 $f \in A \setminus R$ の簡単な構成方法も与えている. 例えば, 多項式 f のある単項式の係数が R の単元であるようにすれば, $Q(R)[f] \cap A = R[f]$ をみたす多項式 f が構成できる.

定義 2.4 $F = (f_1, f_2, \dots, f_{n-1}) \in A^{n-1}$ に対して, R -導分 D_F を以下で定める. 各 $g \in A$ に対して, $D_F(g) := \det J(f_1, f_2, \dots, f_{n-1}, g)$ と定める. ただし, $J(f_1, f_2, \dots, f_{n-1}, g)$ は $(f_1, f_2, \dots, f_{n-1}, g)$ の $(x_1, x_2, \dots, x_n)$ に関するヤコビ行列である. この R -導分 D_F をヤコビアン型の R -導分と呼ぶ.

標数 0 の整域 R 上の 2 変数多項式環 $R[x, y]$ において, 整閉多項式とヤコビアン型の導分は深い関係がある.

定理 2.5 (Kojima-N)

R を標数 0 の整域, $f \in R[x, y] \setminus R$ を定数でない多項式で, $Q(R)[f] \cap R[x, y] = R[f]$ をみたすものとする. このとき以下同値である.

- (1) f は整閉多項式である.
- (2) f に関するヤコビアン型の導分 D_f に関して, $R[x, y]^{D_f} = R[f]$ が成り立つ.

この定理 2.5 は Nowicki [11] の体上の場合に得られている結果を一般の整域上に拡張したものである ([6]). また, この結果は整域上の整閉多項式の一つの特徴づけになっているだけでなく, 定理 1.4 の部分的な拡張になっている. 定理 2.5 を, より精密にした結果を以下に述べる.

定理 2.6 R を標数 0 の整域, $f \in R[x, y] \setminus R$ を定数でない多項式とする. このとき以下同値である.

- (1) f が弱整閉多項式である.
- (2) f に関するヤコビアン型の導分 D_f に関して, $R[x, y]^{D_f} = R[g]$ をみたす多項式 $g \in R[x, y]$ が存在する.

R 上の 2 変数の多項式環 $R[x, y]$ において, 多項式 $f \in R[x, y] \setminus R$ によるヤコビアン型の導分 D_f は以下のように書ける.

$$D_f = -\frac{\partial f}{\partial y} \frac{\partial}{\partial x} + \frac{\partial f}{\partial x} \frac{\partial}{\partial y}.$$

従って, $\operatorname{div}(D_f) = -\frac{\partial}{\partial x}(f_y) + \frac{\partial}{\partial y}(f_x) = 0$ となり, ヤコビアン型の導分の発散は 0 となることがわかる. 一方で, 以下の事実は整域 R が $\mathbb{Q}$ を含むとき, $R[x, y]$ における発散が 0 になる導分の性質を記述している.

命題 2.7 R を $\mathbb{Q}$ を含む整域, D を $R[x, y]$ における発散が 0 の R -導分とする. このとき, $D = D_f$ かつ, $f(0, 0) = 0$ となる多項式 $f \in R[x, y]$ が唯一つ存在する. この多項式 f を D -多項式と呼ぶ.

定理 2.6 と命題 2.7 を合わせると次の結果を得る.

定理 2.8 R を $\mathbb{Q}$ を含む整域, D を $R[x, y]$ における発散が 0 の R -導分, $f \in R[x, y]$ を D -多項式とする. このとき以下同値である.

- (1) f が弱整閉多項式である.
- (2) $R[x, y]^D = R[g]$ をみたす多項式 $g \in R[x, y]$ が存在する.

この定理は, $\mathbb{Q}$ -整域 R 上の発散が 0 となる導分のクラスに対して, 定理 1.4 の一般化を与えるものである. ここで, 例 1.5 の導分 $D = t^2 \frac{\partial}{\partial x} + t^3 \frac{\partial}{\partial y}$ をもう一度考察してみる. 例 1.5 において $R = k[t^2, t^3]$ は $\mathbb{Q}$ を含む整域であり, $\operatorname{div}(D) = 0$ をみたす. また, この導分 D に関する D -多項式は $h := t^2x - t^3y$ であるが, 例 2.2 (4) でみたように, h は弱整閉多項式ではない.

3 証明

この章では, 1 章, 2 章で述べた内容で, 主結果及びその周辺に関するものの証明を行う. この章を通して, $R^{[n]}$ や $k^{[n]}$ はそれぞれ R 上, k 上の n 変数多項式環を表すものとする.

この章の証明では以下の結果を用いる.

定理 3.1 (Kojima-N)

R を整域, $f \in R^{[n]} \setminus R$ を $Q(R)[f] \cap R^{[n]} = R[f]$ をみたすものとする. このとき以下の条件 (1) と (2) は同値である.

- (1) f は整閉多項式である.
- (2) $Q(R)[f]$ は集合 $M(n, Q(R)) = \{Q(R)[g] \mid g \in Q(R)^{[n]} \setminus Q(R)\}$ における極大元である.

さらに R の標数が 0 のとき, 以下の条件 (3) と条件 (1), (2) は同値である.

- (3) $R[f]$ は, ある R -導分 D によって $R[f] = (R^{[n]})^D$ と表せる.

3.1 導分の諸性質について

[(P8) の証明]

D を $R^{[n]} = R[x_1, x_2, \dots, x_n]$ 上の局所冪零導分とする. ここで, R 上の n 変数多項式環に新しい変数 T を追加し, $n+1$ 変数多項式環 $R^{[n+1]} = R[x_1, x_2, \dots, x_n, T]$ を考える. また, $\tilde{D}$ を $\tilde{D}(x_i) = D(x_i), \tilde{D}(T) = 0$ として, $R^{[n+1]}$ における導分を定義する. $\tilde{D}$ の定め方により, $\tilde{D}$ も局所冪零導分である. 従って $T\tilde{D}$ もまた局所冪零導分となる. ここで,

$$F := \exp T\tilde{D} = \sum_{i=0}^{\infty} \frac{1}{i!} (T\tilde{D})^i$$

と定めると, F は $R^{[n+1]}$ における R 上の自己同型となる. また, $F(x_i) = x_i + D(x_i)T + \frac{1}{2}D^2(x_i)T^2 + \dots, F(T) = T, (i = 1, 2, \dots, n)$ であるので $1 \leq i, j \leq n$ に対して,

$$(1) \quad \frac{\partial F(x_i)}{\partial x_j} = \delta_{i,j} + \frac{\partial D(x_i)}{\partial x_j} T + \dots,$$

$$(2) \quad \frac{\partial F(T)}{\partial x_j} = 0, \frac{\partial F(T)}{\partial T} = 1$$

となる, ただし, $\delta_{i,j}$ はクロネッカーのデルタである. 従って, F から定まるヤコビ行列 $J(F)$ は

$$\begin{pmatrix} 1 + \frac{\partial D(x_1)}{\partial x_1} T + g_{11} & \frac{\partial D(x_1)}{\partial x_2} T + g_{12} & \cdots & \frac{\partial D(x_1)}{\partial x_n} T + g_{1n} & * \\ \frac{\partial D(x_2)}{\partial x_1} T + g_{21} & 1 + \frac{\partial D(x_2)}{\partial x_2} T + g_{22} & \cdots & \frac{\partial D(x_2)}{\partial x_n} T + g_{2n} & * \\ \vdots & & \ddots & \vdots & \vdots \\ \frac{\partial D(x_n)}{\partial x_1} T + g_{n1} & 1 + \frac{\partial D(x_n)}{\partial x_2} T + g_{n2} & \cdots & 1 + \frac{\partial D(x_n)}{\partial x_n} T + g_{nn} & * \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

となる. ただし $g_{ij} \in R^{[n+1]}$ は $\text{ord}_T(g_{ij}) \geq 2$ となる多項式である. ここで, $\det(J(F))$ における T の係数をみると,

$$\frac{\partial D(x_1)}{\partial x_1} + \frac{\partial D(x_2)}{\partial x_2} + \cdots + \frac{\partial D(x_n)}{\partial x_n} = \text{div}(D)$$

である. ところで, F は $R^{[n+1]}$ における自己同型となるので, $\det J(F) \in R^*$ である. 従って, $\text{div}(D) = 0$ を得る.

3.2 例 2.2 (3) の証明

R を UFD とし, $f \in R^{[n]} \setminus R$ をとる. $K := Q(R)$ とおく. まず, $K[f]$ を含む $M(n, K)$ の極大元が存在することを示す. $K[f]$ が $M(n, K)$ の極大元

でないとする. すると, $K[f] \subsetneq K[g]$ なる $g \in K^{[n]} \setminus K$ が存在する. ある R の 0 でない元 $c \in R \setminus \{0\}$ により $cg \in R^{[n]}$ とでき, $K[g] = K[cg]$ が成り立つので $g \in R^{[n]} \setminus R$ としてよい. また, 一般性を失わずに f, g は定数項を持たないとしてよい. $f \in K[g]$ より, ある多項式 $u(t) \in K[t]$ を用いて $f = u(g)$ と書ける. この両辺の次数を比較して, $\deg f = \deg u \deg g$ を得る. もし $\deg u = 1$ であるとする, $f = ag, a \in K^*$ と書けが, $K[f] = K[g]$ となり仮定に反する. よって $\deg u \geq 2$ となり $\deg f > \deg g$ を得る. $\deg f$ は有限の値なのでこの議論を有限回繰り返すことで $K[f]$ を含む極大元を得る.

$K[f]$ を含む極大元 $K[g]$ をとる. 上と同様の議論により $g \in R^{[n]} \setminus R$ としてよい. ここで, $c(g) \in R \setminus \{0\}$ を多項式 g の各係数の最大公約元とする. $K[g] = K[c(g)^{-1}g]$ なので $c(g) \in R^*$ としてよい. 従って命題 2.3 より, $K[g] \cap R^{[n]} = R[g]$ が成り立つ. さらに,

$$R[f] \subset (K[f] \cap R^{[n]}) \subset (K[g] \cap R^{[n]}) = R[g]$$

となり, $R[f] \subset R[g]$ をみたす. また, 定理 3.1 より g は整閉多項式である. 従って, f は弱整閉多項式である.

3.3 命題 2.3 の証明

以下の命題は命題 2.3 を, UFD 上に制限した場合の主張である. 本稿では, 命題 2.3 の証明は行わない.

命題 3.2 R を UFD とする. $f \in R^{[n]} \setminus R$ に対して, 各単項式の係数の最大公約元を $c(f) \in R$ で表わす. このとき, $f(0, 0, \dots, 0) = 0$ とすると, 以下同値である.

- (1) f が $Q(R)[f] \cap R^{[n]} = R[f]$ をみたす.
- (2) $c(f) \in R^*$ となる.

[命題 3.2 の証明]

$K := Q(R)$ とおく. また, $c(f^*) \in R^*$ をみたす多項式 $f^* \in R^{[n]}$ を用いて $f = c(f)f^*$ と表す. この表示は R の単元倍を除いて一意である. まず, $c(f) \in R^*$ の場合を考える. $g \in K[f] \cap R^{[n]}$ をとる. $g \in K[f]$ より, $u_0, u_1, \dots, u_m \in K$ を用いて

$$g = u_m f^m + u_{m-1} f^{m-1} + \dots + u_1 f + u_0$$

と書ける. また, $r \in R \setminus \{0\}$ を $ru_i \in R, (i = 0, 1, \dots, m)$ となるようにとる. $g \in R^{[n]}$ で $f(0, 0, \dots, 0) = 0$ より, $u_0 = g(0, 0, \dots, 0) \in R$ であるので,

$$r(g - u_0) = f(ru_m f^{m-1} + ru_{m-1} f^{m-2} + \dots + ru_1) \in K[f] \cap R^{[n]}$$

である. ここで, $g_1 := ru_m f^{m-1} + ru_{m-1} f^{m-2} + \cdots + ru_1 \in R^{[n]}$ とおく. すると, $c(g_1) = r \cdot c(f)^{-1} c(g - u_0) \in rR$ となる. 従って, $g_1 \in rR^{[n]}$ となり, $ru_1 = g_1(0, 0, \dots, 0) \in rR$ である. よって $u_1 \in R$ を得る. 以下, 帰納的な議論によって $u_0, u_1, \dots, u_m \in R$ を得る. これは $g \in R[f]$ を意味する. 従って, $K[f] \cap R^{[n]} = R[f]$ が成り立つ.

次に $c(f) \notin R^*$ の場合を考える. $f^* \notin R[f]$ より, R 上では $R[f] \subsetneq R[f^*]$ で, K 上では $K[f] = K[f^*]$ である. ここで, 前半の議論より, $K[f^*] \cap R^{[n]} = R[f^*]$ が成り立つ. 以上より,

$$R[f] \subsetneq R[f^*] = (K[f^*] \cap R^{[n]}) = (K[f] \cap R^{[n]})$$

が成り立ち, 命題の同値性が示された.

この命題により, 以下がわかる.

系 3.3 R を UFD とする. $f, g \in R^{[n]} \setminus R$ が $f(0, 0, \dots, 0) = g(0, 0, \dots, 0) = 0$ かつ $R[f] \subset R[g]$ をみたすとする. このとき f が $Q(R)[f] \cap R^{[n]} = R[f]$ をみたせば, g も $Q(R)[g] \cap R^{[n]} = R[g]$ をみたす.

[系 3.3 の証明] $g \in R[f]$ より, $u_0, u_1, \dots, u_m \in R$ を用いて

$$g = f(u_m f^{m-1} + u_{m-1} f^{m-2} + \cdots + u_1)$$

と書ける. よって, $c(g) = c(f)c(u_m f^{m-1} + u_{m-1} f^{m-2} + \cdots + u_1)$ となる. 命題 3.2 より $c(f) \in R^*$ なので $c(g) \in R^*$ となり g も $Q(R)[g] \cap R^{[n]} = R[g]$ をみたす.

3.4 定理 2.6 の証明

まず次の補題を示す.

補題 1 R を整域, $f, g \in R[x, y] \setminus R$ を $R[f] \subset R[g]$ をみたすものとする. このとき, $R[x, y]^{D_f} = R[x, y]^{D_g}$ が成り立つ.

[補題の証明] $f \in R[g]$ より, ある多項式 $u(t) \in R[t]$ を用いて $f = u(g)$ と書ける. このとき, $f_x = u'(g)g_x, f_y = u'(g)g_y$ と表せる (ただし, u' は u の t に関する微分である). よって,

$$D_f = -f_y \frac{\partial}{\partial x} + f_x \frac{\partial}{\partial y} = u'(g)(-g_y \frac{\partial}{\partial x} + g_x \frac{\partial}{\partial y}) = u'(g)D_g$$

が成り立つ. $f \notin R$ より, $u'(g) \neq 0$. 従って $R[x, y]^{D_f} = R[x, y]^{D_g}$.

定理 2.6 の証明を始める. $K := Q(R)$ とおく. f が弱整閉多項式なら整閉多項式で $K[g] \cap R[x, y] = R[g]$ かつ $R[f] \subset R[g]$ となる $g \in R[x, y] \setminus R$ が

存在する. 上の補題と, 定理 2.5 を用いると, $R[x, y]^{D_f} = R[x, y]^{D_g} = R[g]$ となる.

逆に, $R[x, y]^{D_f} = R[g]$ となる $g \in R[x, y] \setminus R$ があつたとする. $\tilde{D}$ を D_F の $K[x, y]$ への延長とする. このとき, $\tilde{D}(g) = D_F(g) = 0$ より $K[g] \subset K[x, y]^{\tilde{D}}$ であるので

$$R[g] \subset (K[g] \cap R[x, y]) \subset (K[x, y]^{\tilde{D}} \cap R[x, y]) = R[x, y]^{D_f}$$

よって, $K[g] \cap R[x, y] = R[g]$ が成り立つ. 多項式 g の整閉性は定理 3.1 より従う. 故に, f は弱整閉多項式である.

3.5 命題 2.7 の証明

$p := D(x)$, $q := D(y)$ とおき,

$$p = \sum [m, n]_p x^m y^n, \quad q = \sum [m, n]_q x^m y^n$$

と表す. ただし, $[m, n]_p, [m, n]_q \in R$. このとき,

$$\begin{aligned} \frac{\partial p}{\partial x} &= \sum m [m, n]_p x^{m-1} y^n = \sum m [m, n-1]_p x^{m-1} y^{n-1}, \\ \frac{\partial q}{\partial y} &= \sum n [m, n]_q x^m y^{n-1} = \sum n [m-1, n]_q x^{m-1} y^{n-1} \end{aligned}$$

である. $0 = \operatorname{div}(D) = \frac{\partial p}{\partial x} + \frac{\partial q}{\partial y}$ より, $\frac{\partial p}{\partial x} = -\frac{\partial q}{\partial y}$ であるので, $m, n \geq 1$ に対して, $-\frac{1}{n}[m, n-1]_p = \frac{1}{m}[m-1, n]_q$ を得る. ここで $f := \sum [m, n]_f x^m y^n$

とおく. ただし, $[m, n]_f = \begin{cases} 0 & (m = n = 0) \\ \frac{1}{m}[m-1, 0]_q & (m \geq 1, n = 0) \\ -\frac{1}{n}[m, n-1]_p & (m \geq 0, n \geq 1) \end{cases}$ と定める.

このとき,

$$f = \sum_{m \geq 1, n=0} \frac{1}{m} [m-1, 0]_q x^m + \sum_{m, n \geq 1} -\frac{1}{n} [m, n-1]_p x^m y^n$$

であるので, $f_x = q$, $f_y = -p$ となり, $D = D_f$ かつ, $f(0, 0) = 0$ である.

3.6 定理 2.8 の証明

この定理は, 定理 2.6 と命題 2.7 から直ちに得られる.

参考文献

- [1] J. Berson, Derivations on polynomial rings over a domain, Master's thesis, University of Nijmegen, The Netherlands, 1999.
- [2] J. Berson, A. van den Essen and S. Maubach, Derivations having divergence zero on $R[x, y]$, *Israel J. Math.*, **124** (2001), 115–124.
- [3] A. van den Essen, Polynomial automorphisms and the Jacobian conjecture, *Progress in Math.*, **190** (2000), Birkhäuser, Boston.
- [4] M. El Kahoui, Constants of derivations in polynomial rings over unique factorization domains, *Proc. Amer. Math. Soc.*, **132** (2004), 2537–2541.
- [5] M. Kato and H. Kojima, Closed polynomials in polynomial rings over unique factorization domains, *Comm. Algebra*, **43** (2015), 1935–1938.
- [6] H. Kojima and T. Nagamine, Closed polynomials in polynomial ring over integral domain, *J. Pure Appl. Algebra*, **219** (2015), 5493–5499.
- [7] S. Maubach, Polynomial endomorphism and kernels of derivations, Doctor's thesis, University of Nijmegen, The Netherlands, 2003.
- [8] M. Miyanishi, Regular subrings of a polynomial ring, *Osaka J. Math.* **17** (1980) 329–338.
- [9] T. Nagamine, Derivations having divergence zero and closed polynomials over domains, *J. Algebra*, **462** (2016), 67–76.
- [10] M. Nagata, On the fourteenth problem of Hilbert, in *Proceedings of the International Congress of Mathematicians, 1958*, Cambridge Univ. Press, London, New York, 1960, 459–462.
- [11] A. Nowicki, On the equation $J(f, g) = 0$ for polynomials in $k[x, y]$, *Nagoya Math. J.*, **109** (1988), 151–157.
- [12] A. Nowicki, Polynomial derivations and their rings of constants, N. Copernicus University, Torun, (1994).
- [13] A. Nowicki and M. Nagata, Rings of constants for k -derivations in $k[x_1, \dots, x_n]$, *J. Math. Kyoto Univ.*, **28** (1988), 111–118.
- [14] P. Russell and A. Sathaye, On finding and cancelling variables in $k[X, Y, Z]$, *J. Algebra*, **57** (1979), 151–166.
- [15] O. Zariski, Intérpretations algébriques-géométriques du quatorzième problème de Hilbert, *Bell. Sci. Mth.* **78** (1954), 155–168.

メルセンヌ素数とその派生数の一般化に関する研究

津山工業高等専門学校 電気電子工学科 2 年

桐山 翔伍

1. 研究の動機

中学の頃から数学，特に整数に関して興味があった．高専で数学クラブに入って約数の話題になり，整数に関する議論をしていくうちに，18 という数の約数 $\{1,2,3,6,9,18\}$ について，約数を2つずつ $1\ 2\ |\ 3\ 6\ |\ 9\ 18$ というように区切り，それら2つの数をそれぞれ足してみると，

$$1 + 2 = 3, \quad 3 + 6 = 9 = 3^2, \quad 9 + 18 = 27 = 3^3$$

という構造があることに気付いた，さらに，約数の中の6,18に関して，

$$6 = 2 \times 3, \quad 18 = 2 \times 3^2$$

が成り立っていることに気が付いた．そこで， $2 \times 3^3 = 54$, $2 \times 3^4 = 162, \dots$ を調べると，これらも同様な構造をもつことがわかった．つまり，6,18,54,162,486などの 2×3^k の数の約数の構造も，約数を2つずつに区切りそれら2つの数をそれぞれ足してみると，必ず $3^1, 3^2, \dots, 3^k$ となっていたのである．

$$\begin{array}{c} \underbrace{1\ 2}_3 \mid \underbrace{3\ 6}_{3^2} \\ \underbrace{1\ 2}_3 \mid \underbrace{3\ 6}_{3^2} \mid \underbrace{9\ 18}_{3^3} \\ \underbrace{1\ 2}_3 \mid \underbrace{3\ 6}_{3^2} \mid \underbrace{9\ 18}_{3^3} \mid \underbrace{27\ 54}_{3^4} \\ \underbrace{1\ 2}_3 \mid \underbrace{3\ 6}_{3^2} \mid \underbrace{9\ 18}_{3^3} \mid \underbrace{27\ 54}_{3^4} \mid \underbrace{81\ 162}_{3^5} \\ \underbrace{1\ 2}_3 \mid \underbrace{3\ 6}_{3^2} \mid \underbrace{9\ 18}_{3^3} \mid \underbrace{27\ 54}_{3^4} \mid \underbrace{81\ 162}_{3^5} \mid \underbrace{243\ 486}_{3^6} \end{array}$$

この観点に立って，約数を適当に区切った和が $4^1, 4^2, \dots, 4^k$ となっているものや $5^1, 5^2, \dots, 5^k$ となっているものがあるのかどうかを調べていった．その結果， 4^k に関する構造や 5^k に関する構造を持つものはなくて，次は $7^1, 7^2, \dots, 7^k$ の構造をもつものがあり，それは28,196,1372,9604,67228,などの $2^2 \times 7^k$ の数であった．

28,196,1372,9604,67228,などの $2^2 \times 7^k$ の数の約数の構造は，下の図のように約数を3つずつに区切りそれら3つの数をそれぞれ足してみると， $7^1, 7^2, \dots, 7^k$ となっていたのである．

$$\begin{array}{c} \underbrace{1\ 2\ 4}_7 \mid \underbrace{7\ 14\ 28}_{7^2} \\ \underbrace{1\ 2\ 4}_7 \mid \underbrace{7\ 14\ 28}_{7^2} \mid \underbrace{49\ 98\ 196}_{7^3} \\ \underbrace{1\ 2\ 4}_7 \mid \underbrace{7\ 14\ 28}_{7^2} \mid \underbrace{49\ 98\ 196}_{7^3} \mid \underbrace{343\ 686\ 1372}_{7^4} \\ \underbrace{1\ 2\ 4}_7 \mid \underbrace{7\ 14\ 28}_{7^2} \mid \underbrace{49\ 98\ 196}_{7^3} \mid \underbrace{343\ 686\ 1372}_{7^4} \mid \underbrace{2401\ 4802\ 9604}_{7^5} \\ \underbrace{1\ 2\ 4}_7 \mid \underbrace{7\ 14\ 28}_{7^2} \mid \underbrace{49\ 98\ 196}_{7^3} \mid \underbrace{343\ 686\ 1372}_{7^4} \mid \underbrace{2401\ 4802\ 9604}_{7^5} \mid \underbrace{16807\ 33614\ 67228}_{7^6} \end{array}$$

さらに研究を行ってみると，次は $2^4 \times 31^k$ という数が見つかり，この数の約数の構造は，約数を5つずつに区切りそれら5つの数を足してみると， $31^1, 31^2, \dots, 31^k$ となっていた．そしてその次は， $2^6 \times$

127^k という数であり、この数の約数の構造は、約数を7つずつに区切りそれら7つの数をそれぞれ足してみると、 $127^1, 127^2, \dots, 127^k$ となっていたのである。

このような約数の構造は、3, 7, 31, 127といった素数に関係していることから、数学クラブの先生にこのことを説明したところ、それはメルセンヌ素数といわれる数であることを聞かされた。

定義 1. メルセンヌ素数は、 $M_n = 2^{n+1} - 1$ において、 n に1, 2, 3, ...を代入したとき M_n が素数となるものをいう。

また、 $M_n = 1 + 2 + \dots + 2^n$ であることもわかり、上で研究してきた数が、メルセンヌ素数 M_n とそれから得られる $D_k = 2^n(M_n)^k$ というタイプの数を扱っていたことがわかった。さらにメルセンヌ素数は完全数というものにも関連することがわかった。

定義 2. 完全数 x とは、 x を除く約数の総和 $\tau(x)$ が x に等しくなるものである。すなわち、 $x = \tau(x)$ である。

たとえば、メルセンヌ素数3に関する数 $6 = 2 \times 3$ を例にとると、 $\tau(6) = 1 + 2 + 3 = 6$ であるので、6は完全数である。メルセンヌ素数7に関する数 $28 = 2^2 \times 7$ も $\tau(28) = 1 + 2 + 4 + 7 + 14 = 28$ より完全数である。

以上のことから、これらのことにとっても興味を覚え、 $D_k = 2^n \times (M_n)^k$ をメルセンヌ素数 M_n に関する第 k 派生数と呼び、それを応用する研究を行うことにした。そして研究の結果、詳細は5節で述べるが、定理1、定理2、定理3という3つの定理を得ることができ、さらにこれらの結果から一般的な完全数と強完全数という概念を定義することができ、新たな研究の領域を発見した。

2. メルセンヌ素数 M_n の第 k 派生数について

まず、メルセンヌ素数 M_n に関する第 k 派生数というものを定義する。

定義 3. メルセンヌ素数 M_n とそれから得られる $D_k = 2^n(M_n)^k$ をメルセンヌ素数 M_n に関する第 k 派生数と呼ぶ。

たとえば、6は $6 = 2^1 \times 3$ よりメルセンヌ素数3に関する第1派生数 D_1 であり、18は $18 = 2^1 \times 3^2$ よりメルセンヌ素数3に関する第2派生数 D_2 である。28は $28 = 2^2 \times 7$ よりメルセンヌ素数7に関する第1派生数 D_1 であり、196は $196 = 2^2 \times 7^2$ よりメルセンヌ素数7に関する第2派生数 D_2 である。

メルセンヌ素数 M_n に関する第 k 派生数 D_k の約数を小さい順に並べて、最初の $n+1$ 個の約数を第1パート、その次の $n+1$ 個の約数を第2パート、さらに次の $n+1$ 個の約数を第3パート、以下同様にして第 $k+1$ パートまでを考える。たとえば、196の約数の第1パートは1, 2, 4であり、第2パートは7, 14, 28、第3パートは49, 98, 196である。

$$\begin{array}{c|c|c} 1 & 2 & 4 \\ \hline 7 & 7^2 & 7^3 \end{array}$$

次のことが成り立つ。

命題 1. メルセンヌ素数 M_n に関する第 k 派生数 D_k の約数を小さい順に並べたとき、第 j パートの約数の和は $(M_n)^j$ である。

(証明) D_k の約数の第 1 パートの和は

$$1 + 2 + \cdots + 2^n = M_n$$

であり、第 2 パートの和は

$$M_n + 2M_n + \cdots + 2^n M_n = M_n(1 + \cdots + 2^n) = (M_n)^2$$

である。数学的帰納法により第 j パートの和は

$$\begin{aligned} & (M_n)^{j-1} + 2(M_n)^{j-1} + \cdots + 2^n(M_n)^{j-1} \\ &= (M_n)^{j-1}(1 + 2 + \cdots + 2^n) = (M_n)^j \end{aligned}$$

となり、証明された。(証明終)

次に、今後の研究に必要な D_k の約数の部分和である $\tau(D_k)$ を定義する。

定義 4. メルセンヌ素数 M_n に関する第 k 派生数 D_k の約数の D_k を除く第 k パートと第 $k+1$ パートの和を $\tau(D_k)$ とする。命題 1 を用いて言い換えると

$$\tau(D_k) = (M_n)^k + (M_n)^{k+1} - D_k$$

とする。

たとえば、メルセンヌ素数 7 に関する $D_1=28$, $D_2=196$, $D_3=1372$ はそれぞれ次のようになる。

$$\underbrace{1 \ 2 \ 4}_7 \left| \underbrace{7 \ 14 \ 28}_{7^2} \right| \underbrace{49 \ 98 \ 196}_{7^3} \left| \underbrace{343 \ 686 \ 1372}_{7^4} \right|$$

$$D_1=28 \text{ の場合: } \tau(28) = 7^1 + 7^2 - 28 = 7 + 49 - 28 = 28$$

$$D_2=196 \text{ の場合: } \tau(196) = 7^2 + 7^3 - 196 = 49 + 343 - 196 = 196$$

$$D_3=1372 \text{ の場合: } \tau(1372) = 7^3 + 7^4 - 1372 = 343 + 2401 - 1372 = 1372$$

上の例から分かるように、 D_k の約数の部分和に関しては、 $D_k = \tau(D_k)$ が成り立つのである。そして、特に第 1 派生数 D_1 は次のことがいえた。

命題 2. メルセンヌ素数 M_n に関する第 1 派生数 D_1 は完全数である。

(証明) 定義 2 より $D_1 = 2^n M_n$ であり、定義 4 より $\tau(D_1) = M_n + (M_n)^2 - D_1$ であるので

$$\begin{aligned} \tau(D_1) &= M_n(1 + M_n - 2^n) = M_n(1 + 1 + 2 + \cdots + 2^n - 2^n) \\ &= M_n(1 + 1 + 2 + \cdots + 2^{n-1}) = M_n(1 + 2^n - 1) = 2^n M_n = D_1 \quad (\text{証明終}) \end{aligned}$$

[注意 1] 明らかにメルセンヌ素数 M_n に関する第 1 派生数 D_1 は偶数であり、オイラーによると偶数の完全数は D_1 に限ることが証明されている。さらに「奇数の完全数が存在するかどうか」は未解決問題となっている(高木[T]参照)。

定義 5. x 以外の約数をいくつか足して x になるとき、数 x を**擬似完全数**という。

たとえば、18 の場合 $3 + 6 + 9 = 18$, 54 の場合 $9 + 18 + 27 = 54$ であるので、18 と 54 は擬似完全数である。18 と 54 はメルセンヌ素数3の第2派生数と第3派生数である。一般的に次のことが証明できた。

命題 3. メルセンヌ素数 M_n に関する第 k 派生数 D_k は疑似完全数である.

(証明) $\tau(D_k) = (M_n)^k + (M_n)^{k+1} - D_k$ であり, $\tau(D_k) = D_k$ となっていれば D_k は疑似完全数である. $D_k = 2^n(M_n)^k$ より

$$\begin{aligned}\tau(D_k) &= (M_n)^k + (M_n)^{k+1} - 2^n(M_n)^k = (M_n)^k(1 + M_n - 2^n) = (M_n)^k(1 + 1 + 2 + \cdots + 2^n - 2^n) \\ &= (M_n)^k(1 + 1 + 2 + \cdots + 2^{n-1}) = (M_n)^k(1 + 2^n - 1) = (M_n)^k 2^n = D_k\end{aligned}$$

よって, メルセンヌ素数 M_n に関する第 k 派生数 D_k は疑似完全数である. (証明終)

命題 4. メルセンヌ素数 M_n に関する第1派生数 D_1 の約数の逆数和 S_1 は2に等しい.

(証明) $D_1 = 2^n M_n$ より,

$$\begin{aligned}S_1 &= 1 + \frac{1}{2} + \cdots + \frac{1}{2^n} + \frac{1}{M_n} + \cdots + \frac{1}{2^n M_n} = \frac{1 + 2 + \cdots + 2^n + M_n + \cdots + 2^n M_n}{2^n M_n} = \frac{\tau(D_1) + 2^n M_n}{2^n M_n} \\ &= \frac{2^n M_n + 2^n M_n}{2^n M_n} = 2\end{aligned}$$

よって, 第1派生数 D_1 の約数の逆数和 S_1 は2に等しい. (証明終)

次に, 疑似完全数としての第 k 派生数 D_k の約数の逆数和について研究した.

命題 5. メルセンヌ素数 M_n に関する第 k 派生数 D_k の約数の第 k パートと第 $k+1$ パートの数の逆数和 S_k は以下である.

$$S_k = \frac{2}{(M_n)^{k-1}}$$

(証明) $D_1 = 2^n M_n$ より,

$$\begin{aligned}S_k &= \frac{1}{M_n^{k-1}} + \frac{1}{2(M_n)^{k-1}} + \cdots + \frac{1}{2^n(M_n)^{k-1}} + \frac{1}{(M_n)^k} + \cdots + \frac{1}{2^n(M_n)^k} \\ &= \frac{1 + 2 + \cdots + 2^n + M_n + \cdots + 2^n M_n}{2^n(M_n)^k} = \frac{\tau(D_1) + 2^n M_n}{2^n(M_n)^k} = \frac{2^n M_n + 2^n M_n}{2^n(M_n)^k} = \frac{2}{(M_n)^{k-1}}\end{aligned}$$

よって, D_k の約数の第 k パートと第 $k+1$ パートの数の逆数和 S_k は $\frac{2}{(M_n)^{k-1}}$ になる. (証明終)

3. これまでの完全数に関する研究

上に述べた本研究で扱っているメルセンヌ素数 M_n に関する第 k 派生数は, $M_n = 1 + 2 + \cdots + 2^n$ を基礎にした研究であると考えることができる. そうすると, ${}^3M_n = 1 + 3 + \cdots + 3^n$ や ${}^5M_n = 1 + 5 + \cdots + 5^n$ などから同様な研究ができないかと思えた. そのことを数学クラブの先生に申し出たところ, それはメルセンヌ素数や完全数を一般化する方向の研究とみることができるので, そのような論文を調べようという指示があった. この立場からのこれまでの研究を MathSciNet という数学の論文検索サービスで調べてみると, T.Yamada[Y]の研究, A.Bege 等[B]の研究が見つかった.

T.Yamada[Y]の研究や A.Bege 等[B]の研究は, ある数 N の約数の和を $\sigma(N)$ としたとき, N が完全数ならば $\sigma(N) = 2N$ であるが, $\sigma(\sigma(N)) = 2N$ とした場合の研究を行っていた. そしてそれをさらにそれぞれの立場から一般化の試みがなされた研究であり, 本研究の方向性とは異なっていた.

また、最近、飯高[I]の研究が出版された。これは本研究の方向性に近いものではあったが、厳密には異なる研究となっている。

以上のことから、本研究はこれまで扱われてこなかった領域であるのではないかと考え、この研究を進めることをきめた。

4. 素数3に関するメルセンヌ素数 3M_n の第 k 派生数

本研究においてこれまでメルセンヌ素数 M_n から第 k 派生数 D_k に関する5つの命題を発見し証明した。しかし、整数に関する本を見ていると、得られた結果は良く知られているものであった。しかし証明のアプローチが異なるので、それを重視して、 ${}^3M_n = 1 + 3 + \cdots + 3^n$ や ${}^5M_n = 1 + 5 + \cdots + 5^n$ などを用いて同様な研究ができないかと考えた。そこでこの節では、 ${}^3M_n = 1 + 3 + \cdots + 3^n$ を用いた研究について述べていく。

まず、 ${}^3M_n = 1 + 3 + 3^2 + \cdots + 3^n$ と置く。このとき、等比数列の計算により ${}^3M_n = \frac{3^{n+1}-1}{2}$ が得られることを注意しておく。

定義 6. ${}^3M_n = \frac{3^{n+1}-1}{2}$ が素数になるとき、 3M_n を3-メルセンヌ素数とよぶ。

たとえば、 ${}^3M_2 = \frac{3^{2+1}-1}{2} = 13$ となり、これは3-メルセンヌ素数である。

定義 7. 3-メルセンヌ素数 3M_n と、それから得られる $D_k = 3^n \times ({}^3M_n)^k$ を3-メルセンヌ素数 3M_n に関する第 k 派生数と呼ぶ。

たとえば、117, 1521 を例にとると、 $117 = 3^2 \times (13)^1$ であり ${}^3M_2 = 13$ であるので、117 は3-メルセンヌ素数 ${}^3M_2 = 13$ に関する第1派生数 D_1 である。また、 $1521 = 3^2 \times (13)^2$ であるので、1521は3-メルセンヌ素数 ${}^3M_2 = 13$ に関する第2派生数 D_2 である。

3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k の約数を小さい順に並べたとき、そのパートの構造は、例えば ${}^3M_2 = 13$ に関する第2派生数 $D_2 = 1521$ については以下のようになっていた。

$$\underbrace{1 \ 3 \ 9}_{13} \mid \underbrace{13 \ 39 \ 117}_{13^2} \mid \underbrace{169 \ 507 \ 1521}_{13^3}$$

次の命題 6 は、命題 1 に対応する約数のパートの構造に関するものであり、それを証明することができた。

命題 6. 3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k の約数の第 j パートの約数の和は $({}^3M_n)^j$ である。

(証明) D_k の約数の第 1 パートの和は

$$1 + 3 + \cdots + 3^n = {}^3M_n$$

であり、第 2 パートの和は

$${}^3M_n + 3 \cdot {}^3M_n + \cdots + 3^n \cdot {}^3M_n = {}^3M_n(1 + \cdots + 3^n) = ({}^3M_n)^2$$

である。数学的帰納法により第 j パートの和は

$$\begin{aligned} & ({}^3M_n)^{j-1} + 3({}^3M_n)^{j-1} + \cdots + 3^n({}^3M_n)^{j-1} \\ &= ({}^3M_n)^{j-1}(1 + 3 + \cdots + 3^n) = ({}^3M_n)^j \end{aligned}$$

となり，証明された．（証明終）

定義 8. 3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k の D_k を除く第 k パートと第 $k+1$ パートの和を $\tau(D_k)$ とする．命題 6 を用いて言い換えると

$$\tau(D_k) = ({}^3M_n)^k + ({}^3M_n)^{k+1} - D_k$$

とする．

さらに，3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k に関する次の公式も発見した．

命題 7. 3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k について以下が成り立つ．

$$D_k = 2\tau(D_k) - ({}^3M_n)^k$$

（証明） 定義 7 より $D_k = 3^n \times ({}^3M_n)^k$ であり，命題 6 より $\tau(D_k) = ({}^3M_n)^k + ({}^3M_n)^{k+1} - D_k$ であるので，

$$\begin{aligned} \tau(D_k) &= ({}^3M_n)^k + ({}^3M_n)^{k+1} - 3^n \times ({}^3M_n)^k = ({}^3M_n)^k(1 + {}^3M_n - 3^n) \\ &= ({}^3M_n)^k(1 + 1 + 3 + \cdots + 3^{n-1}) = ({}^3M_n)^k \left(1 + \frac{(3^n - 1)}{2}\right) = ({}^3M_n)^k + \frac{({}^3M_n)^k(3^n - 1)}{2} \end{aligned}$$

である．よって $\tau(D_k) = ({}^3M_n)^k + \frac{({}^3M_n)^k(3^n - 1)}{2}$ であり，これより，

$$2\tau(D_k) - ({}^3M_n)^k = ({}^3M_n)^k + ({}^3M_n)^k(3^n - 1) = ({}^3M_n)^k + 3^n \times ({}^3M_n)^k - ({}^3M_n)^k = 3^n \times ({}^3M_n)^k = D_k$$

（証明終）

3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k の逆数和に関しても次の結果を得ることができた．

命題 8. 3-メルセンヌ素数 3M_n に関する第 k 派生数 D_k の第 k パートと第 $k+1$ パートの数の逆数和 S_k は以下になる．

$$S_k = \frac{1 + {}^3M_n}{3^n ({}^3M_n)^{k-1}}$$

特に， $S_1 = \frac{1 + {}^3M_n}{3^n}$ である．

（証明） $D_1 = 3^n ({}^3M_n)$ ， $\tau(D_1) = ({}^3M_n) + ({}^3M_n)^2 - D_1$ より，

$$\begin{aligned} S_k &= \frac{1}{({}^3M_n)^{k-1}} + \frac{1}{3({}^3M_n)^{k-1}} + \cdots + \frac{1}{3^n ({}^3M_n)^{k-1}} + \frac{1}{({}^3M_n)^k} + \cdots + \frac{1}{3^n ({}^3M_n)^k} \\ &= \frac{1 + 3 + \cdots + 3^n + {}^3M_n + \cdots + 3^n ({}^3M_n)}{3^n ({}^3M_n)^k} = \frac{\tau(D_1) + D_1}{3^n ({}^3M_n)^k} = \frac{({}^3M_n) + ({}^3M_n)^2 - D_1 + D_1}{3^n ({}^3M_n)^k} \\ &= \frac{({}^3M_n) + ({}^3M_n)^2}{3^n ({}^3M_n)^k} = \frac{1 + {}^3M_n}{3^n ({}^3M_n)^{k-1}} \end{aligned}$$

よって、 D_k の第 k パートと第 $k+1$ パートの数の逆数和 S_k は $\frac{1+{}^3M_n}{3^n({}^3M_n)^{k-1}}$ になる。(証明終)

[注意 2] 命題 5 と命題 8 の結果も非常に類似したものである。それは、命題 5 における公式 $S_k = \frac{2}{(M_n)^{k-1}}$ を

$M_n = 2^{n+1} - 1$ で書き直すと、 $S_k = \frac{1+M_n}{2^n(M_n)^{k-1}}$ となるからである。

5. 素数 p に関するメルセンヌ素数 pM_n の第 k 派生数について

前節までに素数2と3に関するメルセンヌ素数の第 k 派生数に関する8つの命題を発見し証明した。これらの研究を踏まえて、より一般的な研究を行った。

${}^pM_n = 1 + p + p^2 + \cdots + p^n$ と置く。このとき、等比数列の計算により ${}^pM_n = \frac{p^{n+1}-1}{p-1}$ が得られる。

定義 9. ${}^pM_n = \frac{p^{n+1}-1}{p-1}$ が素数になるとき、 pM_n を p -メルセンヌ素数とよぶ。

定義 10. p -メルセンヌ素数 pM_n と、それから得られる $D_k = p^n \times ({}^pM_n)^k$ を p -メルセンヌ素数 pM_n に関する第 k 派生数と呼ぶ。

p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の約数を小さい順に並べたとき、第 j パートの構造に関する次の定理を証明した。

定理 1. p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の約数の第 j パートの約数の和は $({}^pM_n)^j$ である。

(証明) D_k の約数の第1パートの和は

$$1 + p + \cdots + p^n = {}^pM_n$$

であり、第2パートの和は

$${}^pM_n + p({}^pM_n) + \cdots + p^n({}^pM_n) = {}^pM_n(1 + \cdots + p^n) = ({}^pM_n)^2$$

である。数学的帰納法により第 j パートの和は

$$\begin{aligned} & ({}^pM_n)^{j-1} + p({}^pM_n)^{j-1} + \cdots + p^n({}^pM_n)^{j-1} \\ &= ({}^pM_n)^{j-1}(1 + p + \cdots + p^n) = ({}^pM_n)^j \end{aligned}$$

となり、証明された。(証明終)

定義 11. p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の約数の D_k を除く第 k パートと第 $k+1$ パートの和を $\tau(D_k)$ とする。定理1を用いて言い換えると

$$\tau(D_k) = ({}^pM_n)^k + ({}^pM_n)^{k+1} - D_k$$

とする。

次に、 p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k に関する次の公式を証明した。

定理 2. p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k について以下が成り立つ.

$$D_k = (p-1)\tau(D_k) - (p-2)({}^pM_n)^k$$

(証明) 定義 10 より $D_k = p^n \times ({}^pM_n)^k$ であり, 定義 11 より $\tau(D_k) = ({}^pM_n)^k + ({}^pM_n)^{k+1} - D_k$ であるので,

$$\begin{aligned}\tau(D_k) &= {}^pM_n^k + ({}^pM_n)^{k+1} - p^n({}^pM_n)^k = ({}^pM_n)^k(1 + {}^pM_n - p^n) \\ &= ({}^pM_n)^k(1 + 1 + p + \cdots + p^{n-1}) = ({}^pM_n)^k \left(1 + \frac{(p^n - 1)}{p - 1}\right) = ({}^pM_n)^k + \frac{({}^pM_n)^k(p^n - 1)}{p - 1}\end{aligned}$$

である. よって $\tau(D_k) = ({}^pM_n)^k + \frac{({}^pM_n)^k(p^n - 1)}{p - 1}$ であり, これより,

$$\begin{aligned}(p-1)\tau(D_k) &= (p-1)({}^pM_n)^k + ({}^pM_n)^k(p^n - 1) = (p-1)({}^pM_n)^k + p^n({}^pM_n)^k - ({}^pM_n)^k \\ &= (p-2)({}^pM_n)^k + p^n({}^pM_n)^k\end{aligned}$$

これより

$$(p-1)\tau(D_k) - (p-2)({}^pM_n)^k = p^n({}^pM_n)^k = D_k$$

よって, $D_k = (p-1)\tau(D_k) - (p-2)({}^pM_n)^k$ である. (証明終)

p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の逆数和に関しても次の結果を証明した.

定理 3. p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の第 k パートと第 $k+1$ パートの数の逆数和 S_k は以下である.

$$S_k = \frac{1 + {}^pM_n}{p^n({}^pM_n)^{k-1}}$$

特に, $S_1 = \frac{1 + {}^pM_n}{p^n}$ である.

(証明) $D_1 = p^n({}^pM_n)$, $\tau(D_1) = ({}^pM_n) + ({}^pM_n)^2 - D_1$ より,

$$\begin{aligned}S_k &= \frac{1}{({}^pM_n)^{k-1}} + \frac{1}{p({}^pM_n)^{k-1}} + \cdots + \frac{1}{p^n({}^pM_n)^{k-1}} + \frac{1}{({}^pM_n)^k} + \cdots + \frac{1}{p^n({}^pM_n)^k} \\ &= \frac{1 + p + \cdots + p^n + {}^pM_n + \cdots p^n({}^pM_n)}{p^n({}^pM_n)^k} = \frac{\tau(D_1) + D_1}{p^n({}^pM_n)^k} = \frac{({}^pM_n) + ({}^pM_n)^2 - D_1 + D_1}{p^n({}^pM_n)^k} \\ &= \frac{({}^pM_n) + ({}^pM_n)^2}{p^n({}^pM_n)^k} = \frac{1 + {}^pM_n}{p^n({}^pM_n)^{k-1}}\end{aligned}$$

よって, p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の約数の逆数和 S_k は $\frac{1 + ({}^pM_n)}{p^n({}^pM_n)^{k-1}}$ になる. (証明終)

6. 素数 p に関する完全数について

定理 2 によって, p -メルセンヌ素数 pM_n に関する第 1 派生数 D_1 の公式

$$D_1 = (p-1)\tau(D_1) - (p-2){}^pM_n$$

を得たが、これは $p = 2$ のとき $D_1 = \tau(D_1)$ を満たすため、上の式は完全数の一般化であると考えることができる。そこで、次のことを定義し研究を進めた。

定義 1 2. 素数 p に関する完全数 x とは、

$$x = (p - 1)\tau(x) - (p - 2)^p M_n$$

をみたすものとする。

さらに、 x の約数の逆数和 S が適当な自然数 a で $p^a S$ が自然数となるとき、 x を素数 p に関する強完全数と呼ぶ。

[注意 3] 命題 2 の注意 1 において、「奇数の完全数が存在するかどうか」は未解決問題となっていることを述べたが、 $p \geq 3$ のとき、素数 p に関する完全数 x は全て奇数であることは上の定義からすぐにわかる。

[注意 4] 定理 2 と定理 3 から、 p -メルセンヌ素数 ${}^p M_n$ に関する第1派生数 D_1 は素数 p に関する強完全数である。

さて、 $p = 3$ に関する完全数 x は $x = 2\tau(x) - {}^3 M_n$ であるが、 $1 \leq x \leq 10^5$ の範囲でコンピューターを用いて調査した結果、3-メルセンヌ素数 ${}^3 M_n$ の第1派生数 D_1 以外に、1809と18549が見つかった。これらの分析結果は以下である。

(1) $p = 3$ に関する完全数1809について

まず、 $S = \frac{40 \times 67}{3^3 \times 67}$ であるため、1809は強完全数ではない。次に1809の完全数としての約数の構造を調べると、以下のようにになっていた。

$$\underbrace{1 \ 3 \ 9 \ 27}_{40} \mid \underbrace{67 \ 201 \ 603 \ 1809}_{40 \times 67} \mid$$

ここにある67は素数であるが、 $67 = \frac{5 \times 3^3 - 1}{2}$ という関係式を持っているため3-メルセンヌ素数 ${}^3 M_n$ ではない。しかし、 $1809 = 3^3 \times 67$ であり、1809の約数の第 1 パートの合計は40、そして第 2 パートの合計は 40×67 となっており、3-メルセンヌ素数 ${}^3 M_n$ の第1派生数 D_1 と類似の構造をもっていることがわかる。

(2) $p = 3$ に関する完全数18549について

まず、 $S = \frac{121 \times 229}{3^4 \times 229}$ であるため、18549は強完全数ではない。次に18549の完全数としての約数の構造は以下のようにになっていた。

$$\underbrace{1 \ 3 \ 9 \ 27 \ 81}_{121} \mid \underbrace{229 \ 687 \ 2061 \ 6183 \ 18549}_{121 \times 229} \mid$$

ここにある229も素数であるが、 $229 = \frac{17 \times 3^3 - 1}{2}$ という関係式を持っているため3-メルセンヌ素数 ${}^3 M_n$ ではない。しかし、これについても $18549 = 3^4 \times 229$ であり、18549の約数の第 1 パートの合計は121、そして第 2 パートの合計は 121×229 となっており、やはり 3-メルセンヌ素数 ${}^3 M_n$ の第1派生数 D_1 と類似の構造をもっていた。

このことから、現在、 p -メルセンヌ素数 pM_n の第1派生数 D_1 以外の素数 p に関する完全数 x に強く興味をもっており、この研究を進めるにあたり、次に述べる重み q 付きの p -メルセンヌ素数という概念が重要であると考えている。

定義 13. 素数 p に対して、素数 w がある自然数 a とある素数 q により

$$w = \frac{q \times p^a - 1}{p - 1}$$

となつてるとき、 w を重み q の p -メルセンヌ素数といい、 ${}^{q \times p}M_a$ とかく。

たとえば、 $p = 3$ のときに $w = 67, 229$ とすると、それぞれ以下のようになる。

$$67 = \frac{5 \times 3^3 - 1}{2}, \quad 229 = \frac{17 \times 3^3 - 1}{2}$$

これより、67は重み5の3-メルセンヌ素数 ${}^{5 \times 3}M_3$ 、229は重み17の3-メルセンヌ素数 ${}^{17 \times 3}M_4$ である。

重み q 付きの p -メルセンヌ素数を用いた素数 p に関する完全数 x については、現在研究中である。

また、素数 p に関する強完全数については、『 p -メルセンヌ素数 pM_n の第1派生数 D_1 以外には存在しないだろう』という仮説を立てている。

7. 今後の研究計画

今後の研究計画を以下のように立てている。

- (1) p -メルセンヌ素数 pM_n に関する第1派生数 D_1 以外で、素数 p に関する完全数 x の研究を、重み q の p -メルセンヌ素数のアプローチから進める。
- (2) p -メルセンヌ素数 pM_n に関する第1派生数 D_1 以外には存在しないのではないかという予想を証明する。
- (3) p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k の数列の研究をする。すなわち、 p -メルセンヌ素数 pM_n に関する第 k 派生数 D_k から得られた無限数列

$$1, p, p^2, \dots, p^n, {}^pM_n, p {}^pM_n, \dots, ({}^pM_n)^k, p({}^pM_n)^k, \dots, p^n({}^pM_n)^k, \dots$$

に関する研究をすることで、完全数の研究の新たな方向性が見つかると考えている。

参考文献

- [B] A.Bege, K.Forgarasi, Generalized perfect numbers, Acta Univ. Sapientiae, Mathematica, 1, 1 (2009) pp73-82
- [Y] T. Yamada, Unitary super perfect numbers, Math. Pannon. 19 (2008), no. 1, pp37-47.
- [I] 飯高茂, 数学の研究をはじめよう(I), 現代数学社, (2016)
- [T] 高木貞治, 初等整数論講義第2版, 共立出版, (1971)

研究レポート

三元整数環のピタゴラス数の分類

津山工業高等専門学校

矢部 佳史

(電子制御工学科 4 年)

1. はじめに

本研究の目的は、三元整数環 M_3 のピタゴラス数の分類である。三元整数 M_3 とは、四元数[H]に習って書くと、 M_3 は集合 $\{xi + yj + kz | x, y, z \in \mathbb{Z}\}$ で $i^2 = i, k^2 = k, ij = jk = j, j^2 = ji = ki = ik = kj = 0$ をみたすものとすることができる。しかし、これは2次整数行列環の部分環とみることもでき、

$$M_3 = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\}$$

である。以下、我々は三元整数 M_3 を上行列として扱い、 M_3 の元を M_3 数と呼ぶ。また、 M_3 数の中で行列式が ± 1 であるものは単元と呼ぶ。

さて、自然数のピタゴラス数 (a, b, c) は、 $a^2 + b^2 = c^2$ をみたすもので、これは2つのパラメータ s と t ($s > t$) を用いて

$$a = s^2 - t^2, \quad b = 2st, \quad c = s^2 + t^2$$

と表わされることはよく知られている。特に a, b, c の最大公約数が1であるときを原始ピタゴラス数というが、このとき s と t は、 s と t のどちらか一方は偶数で、もう片方は奇数であることが必要十分条件である。また、自然数のピタゴラス数はピタゴラス行列

$$P = \begin{pmatrix} -1 & -2 & 2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}$$

を用いると、すべての原始ピタゴラス数が $(3, 4, 5)$ から得られることが知られている[Ko]。この意味で $(3, 4, 5)$ は原始ピタゴラス数のオリジンと考えることができる。さらにこれに関連して橘は[Ta]の中で複素ピタゴラス数のオリジンに関する研究を行い、相対的なオリジンというペアが無数に存在していることを示し、さらにその構造について論じた。以上のことから、我々は整数環やガウス整数環以外の環で、特に非可換環でのピタゴラス数はこういったものであるのか、それに興味を覚えた。

本研究では、三元整数環 M_3 においてピタゴラス数を定義し、その研究を行う。

【定義1】 A, B, C を M_3 数とする。 (A, B, C) が(M_3 数の)ピタゴラス数であるとは、 A, B, C の(1,1)成分と(2,2)成分は正で

$$A^2 + B^2 = C^2$$

をみたすものをいう。

(注) (A, B, C) がピタゴラス数であるならば、 A, B, C の(1,1)成分の3つの数と、(2,2)成分の3つの数は自然数のピタゴラス数である。

以下、本研究においては、 M_3 数のピタゴラス数に可約と既約という概念を与え、 M_3 数のピタゴラス数の分類を試みる。

2. $(2+3)$ 型の M_3 数

以下において、 (A, B, C) はピタゴラス数とし、 $A = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}$, $C = \begin{pmatrix} c_1 & c_2 \\ 0 & c_3 \end{pmatrix}$ として、 M_3 数 A, B, C を表記する。

さて、 $A = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$ が $a_1 = a_2 + a_3$ をみたすとき、 A を $(2+3)$ 型の M_3 数と呼ぶ。以下の命題が成り立つ。

【命題 1】 A, B, C を $(2+3)$ 型の M_3 数とし、さらに (a_1, b_1, c_1) と (a_3, b_3, c_3) は自然数のピタゴラス数とする。このとき (A, B, C) はピタゴラス数である。

(証明). $A^2 = \begin{pmatrix} a_1^2 & a_2(a_1 + a_3) \\ 0 & a_3^2 \end{pmatrix}$ であり、 A は $(2+3)$ 型であるので $(1,2)$ 成分を計算する

と、 $a_2(a_1 + a_3) = (a_1 - a_3)(a_1 + a_3) = a_1^2 - a_3^2$ である。同様に B^2 の $(1,2)$ 成分は $b_2(b_1 + b_3) = b_1^2 - b_3^2$ であり、 C^2 の $(1,2)$ 成分は $c_2(c_1 + c_3) = c_1^2 - c_3^2$ である。したがって、

$$A^2 + B^2 = \begin{pmatrix} a_1^2 + b_1^2 & a_1^2 + b_1^2 - (a_3^2 + b_3^2) \\ 0 & a_3^2 + b_3^2 \end{pmatrix} = \begin{pmatrix} c_1^2 & c_1^2 - c_3^2 \\ 0 & c_3^2 \end{pmatrix} = C^2$$

であるので、 (A, B, C) はピタゴラス数である。Q.E.D.

(例 1)

$$A = \begin{pmatrix} 3 & -7 \\ 0 & 10 \end{pmatrix}, B = \begin{pmatrix} 4 & -20 \\ 0 & 24 \end{pmatrix}, C = \begin{pmatrix} 5 & -21 \\ 0 & 26 \end{pmatrix}$$

とすると、 A, B, C は $(2+3)$ 型の M_3 数であり、そして (A, B, C) は M_3 数のピタゴラス数である。□

ところで、上の例の A, B, C はそれぞれ

$$A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & -2 \\ 0 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 4 & -8 \\ 0 & 12 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 5 & -8 \\ 0 & 13 \end{pmatrix}$$

と分解する。そこで $A' = \begin{pmatrix} 3 & -2 \\ 0 & 5 \end{pmatrix}$, $B' = \begin{pmatrix} 4 & -8 \\ 0 & 12 \end{pmatrix}$, $C' = \begin{pmatrix} 5 & -8 \\ 0 & 13 \end{pmatrix}$ とおくと

$$A'^2 + B'^2 = C'^2$$

が成り立つため、 (A', B', C') はピタゴラス数であることがわかる。

上の例に限らず $d_1 = \gcd(a_1, b_1, c_1)$, $d_3 = \gcd(a_3, b_3, c_3)$ とおいたとき $d_1 > 1$ または $d_3 > 1$ の場合のデータを調べると、ほとんどの場合に同様な分解が起こっていた。

3. 可約と既約な M_3 数のピタゴラス数の定義

M_3 数のピタゴラス数に可約と既約という概念を定義する。

【定義 2】 A, B, C をピタゴラス数とする。このとき、単元でないある M_3 数 D によって、
 $A = DA'$ かつ $B = DB'$ かつ $C = DC'$ 、または $A = A'D$ かつ $B = B'D$ かつ $C = C'D$ のどちらかで A, B, C が M_3 数で分解し、さらに $A'^2 + B'^2 = C'^2$ が成り立つとき (A, B, C) は可約であるという。そして、 D を (A, B, C) の可約係数という。
 可約でないピタゴラス数を既約であるという。

(注) (a_1, b_1, c_1) と (a_3, b_3, c_3) が自然数の原始ピタゴラス数であるとき、 M_3 数のピタゴラス数 (A, B, C) は既約である。このような既約なピタゴラス数 (A, B, C) を原始的であるという。

以下において、ピタゴラス数 (A, B, C) は原始的でないものとする。

(例 2) M_3 数のピタゴラス数

$$A = \begin{pmatrix} 3 & 7 \\ 0 & 10 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 20 \\ 0 & 24 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 21 \\ 0 & 26 \end{pmatrix}$$

は、 $\gcd(3, 4, 5) = 1$, $\gcd(10, 24, 26) = 2$ であるので、 A, B, C をそれぞれ

$$A = \begin{pmatrix} 1 & s \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 7-5s \\ 0 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & s \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 4 & 20-12s \\ 0 & 12 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & s \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 5 & 21-13s \\ 0 & 13 \end{pmatrix}$$

と分解する。そして、

$$A' = \begin{pmatrix} 3 & 7-5s \\ 0 & 5 \end{pmatrix}, \quad B' = \begin{pmatrix} 4 & 20-12s \\ 0 & 12 \end{pmatrix}, \quad C' = \begin{pmatrix} 5 & 21-13s \\ 0 & 13 \end{pmatrix}$$

とおくと、このとき $A'^2 + B'^2 = C'^2$ を解くと、 $s = 1$ である。すなわち、 (A, B, C) は可約なピタゴラス数である。□

(例 3) M_3 数のピタゴラス数

$$A = \begin{pmatrix} 8 & 1 \\ 0 & 15 \end{pmatrix}, \quad B = \begin{pmatrix} 6 & 8 \\ 0 & 8 \end{pmatrix}, \quad C = \begin{pmatrix} 10 & 5 \\ 0 & 17 \end{pmatrix}$$

を考える. $\gcd(8,6,10) = 2$, $\gcd(15,8,17) = 1$ であるので, A, B, C をそれぞれ

$$A = \begin{pmatrix} 4 & 1-4t \\ 0 & 15 \end{pmatrix} \begin{pmatrix} 2 & t \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 8-3t \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 2 & t \\ 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 5-5t \\ 0 & 17 \end{pmatrix} \begin{pmatrix} 2 & t \\ 0 & 1 \end{pmatrix}$$

と分解する. そして,

$$A' = \begin{pmatrix} 4 & 1-4t \\ 0 & 15 \end{pmatrix}, \quad B' = \begin{pmatrix} 3 & 8-3t \\ 0 & 8 \end{pmatrix}, \quad C' = \begin{pmatrix} 5 & 5-5t \\ 0 & 17 \end{pmatrix}$$

とおく. このとき $A'^2 + B'^2 = C'^2$ を解くと, $t = 3$ である. すなわち, (A, B, C) は可約なピタゴラス数である. $\square$

4. 可約なピタゴラス数の判定

可約なピタゴラス数を判定するために, 次のことを定義する.

【定義 3】 M_3 数 A が単元でないある M_3 数 D によって $A = A'D = DA'$ と分解されるとき, A は D で可換に分解されるという. さらに, ピタゴラス数 (A, B, C) で, A, B, C はそれぞれ単元でないある M_3 数 D で可換に分解されるとき, (A, B, C) は D での分解が可換であるという.

【命題 2】 (A, B, C) を原始的でない $(2+3)$ 型のピタゴラス数とすると, (A, B, C) は D での分解が可換であり, さらに (A, B, C) は可約である.

(証明) $A = \begin{pmatrix} a_1 & a_1 - a_3 \\ 0 & a_3 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_1 - b_3 \\ 0 & b_3 \end{pmatrix}$, $C = \begin{pmatrix} c_1 & c_1 - c_3 \\ 0 & c_3 \end{pmatrix}$ とし, $a_1 = d_1 a'_1$, $b_1 = d_1 b'_1$, $c_1 = d_1 c'_1$ さらに $a_3 = d_3 a'_3$, $b_3 = d_3 b'_3$, $c_3 = d_3 c'_3$ とする. このとき, $D = \begin{pmatrix} d_1 & d_1 - d_3 \\ 0 & d_3 \end{pmatrix}$, さらに $A' = \begin{pmatrix} a'_1 & a'_1 - a'_3 \\ 0 & a'_3 \end{pmatrix}$, $B' = \begin{pmatrix} b'_1 & b'_1 - b'_3 \\ 0 & b'_3 \end{pmatrix}$, $C' = \begin{pmatrix} c'_1 & c'_1 - c'_3 \\ 0 & c'_3 \end{pmatrix}$ と置くと,

$$A = DA' = A'D, \quad B = DB' = B'D, \quad C = DC' = C'D$$

であり, 明らかに $A'^2 + B'^2 = C'^2$ が成り立つ. Q.E.D.

ピタゴラス数の既約性の研究において, 以下の命題は明らかなものであるが重要である.

【命題 3】 (A, B, C) は原始的でないピタゴラス数で, かつ D での分解が可換である, すなわち

$$A = A'D = DA', B = B'D = DB', C = C'D = DC'$$

であるとする. このとき (A, B, C) は可約である.

(証明) $A^2 + B^2 = C^2$ より $A'DA'D + B'DB'D = C'DC'D$ であり, 可換性より $A'^2 D^2 + B'^2 D^2 = C'^2 D^2$ が成り立つ. D には逆行列が存在するので, $A'^2 + B'^2 = C'^2$ が成り立つ.

Q.E.D.

命題 3 の対偶を考えると, 「 (A, B, C) が既約ならば, A, B, C の中には単元でないある M_3 数 D によって可換に分解されないものがある」となる. このことから, A, B, C がそれぞれ単元でないにある M_3 数 D によって可換に分解されることを判断できる量について研究した.

【命題 4】 $A = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$ とし $D = \begin{pmatrix} d_1 & d_2 \\ 0 & d_3 \end{pmatrix}$ (ただし $a_1 \neq 0, a_3 \neq 0, d_1 \neq 0, d_3 \neq 0$) とする. さらに $a_1 = d_1 a'_1$ かつ $a_3 = d_3 a'_3$ (ただし $d_1 \neq d_3$) であるとする. このとき

$$u_a = a_1 + \frac{a'_1 - a'_3}{d_1 - d_3} d_3$$

と置くと, $d_2 = a_2 / u_a$ が成り立つことと, A が D によって可換に分解されることは同値である.

(証明) $D = \begin{pmatrix} d_1 & d_2 \\ 0 & d_3 \end{pmatrix}$ とし. $A'D = DA'$ とする. $A'D = DA'$ の (1,2) 成分をみると

$$d_1 a'_2 + d_2 a'_3 = a'_1 d_2 + d_3 a'_2 \quad (3.1)$$

が成り立つ. したがって

$$a'_2 = \frac{a'_1 - a'_3}{d_1 - d_3} d_2$$

である. 一方 $a_2 = a'_1 d_2 + d_3 a'_2$ より

$$a_2 = \left(a'_1 + \frac{a'_1 - a'_3}{d_1 - d_3} d_3 \right) d_2 = u_a d_2$$

である. 逆に $d_2 = a_2 / u_a$ が成り立つためには (3.1) でなくてはならない. すなわち $A'D = DA'$ である. Q.E.D.

(A, B, C) を原始的でないピタゴラス数とし, さらに A, B, C はそれぞれ単元でないにある M_3 数 D で可換に分解されるものとする. このとき, 命題 2 で定義された量 u_a, u_b, u_c に

関して

$$\frac{a_2}{u_a} = \frac{b_2}{u_b} = \frac{c_2}{u_c}$$

が成り立つ場合が重要である．ここで

$$u_a = a_1 + \frac{a'_1 - a'_3}{d_1 - d_3} d_3, \quad u_b = b_1 + \frac{b'_1 - b'_3}{d_1 - d_3} d_3, \quad u_c = c_1 + \frac{c'_1 - c'_3}{d_1 - d_3} d_3$$

である．以上のことから次の定理が得られる．

【定理 1】 (A, B, C) を原始的でないピタゴラス数とする．さらに $d_1 = \gcd(a_1, b_1, c_1)$, $d_3 = \gcd(a_3, b_3, c_3)$ とする．以下が成り立つ．

- (1) $d_1 \neq d_3$ でかつ $\frac{a_2}{u_a} = \frac{b_2}{u_b} = \frac{c_2}{u_c} = d$ で d が整数ならば (A, B, C) は可約である．
 (2) $d_1 = d_3$ ならば (A, B, C) は可約である．

(証明) $d_1 \neq d_3$ ならば命題 3 から明らかであるので, $d_1 = d_3$ の場合を示す．

$$\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} = \begin{pmatrix} d_1 & d_2 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a'_1 & a'_2 \\ 0 & a'_3 \end{pmatrix}$$

として, (1,2)成分を計算すると $a_2 = d_1 a'_2 + d_2 a'_1$ であり,

$$\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} = \begin{pmatrix} a'_1 & a'_2 \\ 0 & a'_3 \end{pmatrix} \begin{pmatrix} d_1 & d_2 \\ 0 & d_1 \end{pmatrix}$$

として, (1,2)成分を計算しても $a_2 = d_2 a'_1 + d_1 a'_2$ である．したがって, $A = A'D = DA'$ が成り立つ．同様にして, $B = B'D = DB', C = C'D = DC'$ が成り立つ．命題 2 より (A, B, C) は可約である．Q.E.D.

(例 4) ピタゴラス数

$$A = \begin{pmatrix} 3 & 13 \\ 0 & 16 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 8 \\ 0 & 12 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 15 \\ 0 & 20 \end{pmatrix}$$

を考える． $d_1 = 1, d_3 = 4$ であり, $a_1 = a'_1 = 3, b_1 = b'_1 = 4, c_1 = c'_1 = 5, a'_3 = 4, b'_3 = 3, c'_3 = 5$ である．したがって

$$u_a = 3 + \frac{3-4}{1-4} \times 4 = \frac{13}{3}, \quad u_b = 4 + \frac{4-3}{1-4} \times 4 = \frac{8}{3}, \quad u_c = 3 + \frac{5-5}{1-4} \times 4 = 5$$

より

$$d_2 = \frac{a_2}{u_a} = \frac{b_2}{u_b} = \frac{c_2}{u_c} = 3$$

である．したがって, (A, B, C) は可約である．実際, A, B, C の分解は

$$A = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 0 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 0 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

であり, $\begin{pmatrix} 3 & 1 \\ 0 & 4 \end{pmatrix}^2 + \begin{pmatrix} 4 & -1 \\ 0 & 3 \end{pmatrix}^2 = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}^2$ が成り立つ. $\square$

(例 5) ピタゴラス数

$$A = \begin{pmatrix} 6 & -1 \\ 0 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 8 & 2 \\ 0 & 8 \end{pmatrix}, \quad C = \begin{pmatrix} 10 & 1 \\ 0 & 10 \end{pmatrix}$$

を考えると, 定理 1 より (A, B, C) は可約なピタゴラス数である. 実際, A, B, C の分解は

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ 0 & 5 \end{pmatrix}$$

であり, $\begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix}^2 + \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix}^2 = \begin{pmatrix} 5 & -2 \\ 0 & 5 \end{pmatrix}^2$ が成り立つ. $\square$

5. 反射的なピタゴラス数

【定義 4】 (A, B, C) を原始的でないピタゴラス数とする. ある自然数 d があって, $a_3 = da_1$, $b_3 = db_1$, $c_3 = dc_1$ または $a_1 = da_3$, $b_1 = db_3$, $c_1 = dc_3$ であるとき, (A, B, C) を反射的であるという. このとき d を **反射係数** という.

(例 6) 反射的なピタゴラス数

$$A = \begin{pmatrix} 3 & 1 \\ 0 & 12 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 3 \\ 0 & 16 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 3 \\ 0 & 20 \end{pmatrix}$$

を考える. $d_1 = 1$, $d_3 = 4$, $a_1 = a'_1 = 3$, $b_1 = b'_1 = 4$, $c_1 = c'_1 = 5$, $a'_3 = 3$, $b'_3 = 4$, $c'_3 = 5$ である.

$$u_a = 3 + \frac{3-3}{1-4} \times 4 = 3$$

より $\frac{a_2}{u_a} = \frac{1}{3}$ である. しかし, A, B, C は

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 5 & -1 \\ 0 & 5 \end{pmatrix}$$

と分解でき, $\begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix}^2 + \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix}^2 = \begin{pmatrix} 5 & -1 \\ 0 & 5 \end{pmatrix}^2$ が成り立つ. そして,

$$A \neq \begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 3 & -5 \\ 0 & 12 \end{pmatrix}, \quad B \neq \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 16 \end{pmatrix},$$

$$C \neq \begin{pmatrix} 5 & -1 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 0 & 20 \end{pmatrix}$$

である. $\square$

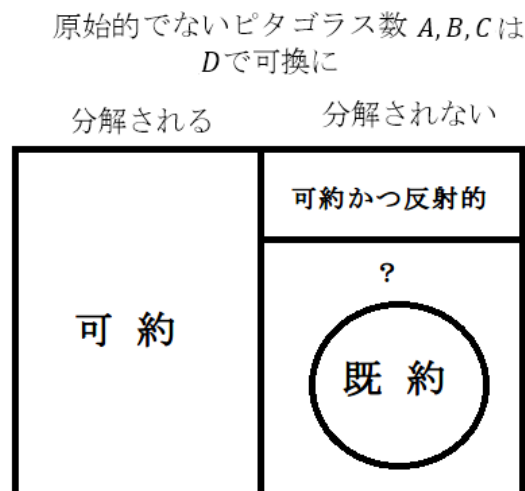
【命題 5】 (A, B, C) を原始的でない反射的なピタゴラス数とすると, (A, B, C) は可約である.

(証明) (A, B, C) は既約であると仮定と仮定する, さらに $\gcd(a_1, b_1, c_1) = 1$ を仮定してもよい. $A = DA', B = DB', C = DC'$ とすると, (A, B, C) が既約であることより, D は単元である. これは反射係数が $d = 1$ であることを意味するこれは (A, B, C) が原始的であることを意味し, 矛盾である. Q.E.D.

6. これまでのまとめと予想

我々の目的はピタゴラス数が与えられたとき, それが既約であるか可約であるかを判断することである. これまでの議論から, (A, B, C) が原始的なピタゴラス数であれば必ず既約なるため, 原始的でないピタゴラス数について詳細に研究してきた.

そして (A, B, C) が D での分解が可換であるならば, (A, B, C) は可約であることがわかった. また, (A, B, C) が D での分解が可換であることの十分条件として命題 4 を得て, そこから可約の条件である定理 1 を得た. それでは命題 4 の条件をみたさないものはどういったタイプのものであるか. この問題に対してその後研究を行った. その結果, 反射係数が 1 より大きい反射的なピタゴラス数の存在が見つかった. そしてそれは D での分解が可換に分解されないのであるが, 可約である. 以上のことをまとめたものが以下の図である.



我々はこれまでの数値的データによる研究から以下の予想を立てている.

【予想】 (A, B, C) を原始的でない反射的なピタゴラス数とし, さらに (A, B, C) は D での分解が可換でないと仮定する. このとき, (A, B, C) が反射的でなければ (A, B, C) は既約である.

7. 双対的なピタゴラス数

我々の目的は, M_3 数のピタゴラス数を分類することである. そのために本研究では既約なものと可約なものに分類することを目的とした. もしこの分類が完成すれば, 次は, 例えば「既約なピタゴラス数の集合はどのような構造になっているのか」ということがテーマになる. その一つの手がかりとして双対的なピタゴラス数という概念を定義する.

【命題 6】 (A, B, C) をピタゴラス数とする. そして適当な M_3 数 D によって, $A = DA'$, $B = DB'$, $C = DC'$ と分割する. このとき, $\tilde{A} = A'D$, $\tilde{B} = B'D$, $\tilde{C} = C'D$ と置くと, $(\tilde{A}, \tilde{B}, \tilde{C})$ はまたピタゴラス数となる.

(証明) $A^2 + B^2 = C^2$ より $DA'DA' + DB'DB' = DC'DC'$ であり, D には逆行列が存在するので, $A'DA' + B'DB' = C'DC'$ を得る. 右から D を掛けることで, $A'DA'D + B'DB'D = C'DC'D$ を得る. したがって, $\tilde{A}^2 + \tilde{B}^2 = \tilde{C}^2$ が成り立ち, $(\tilde{A}, \tilde{B}, \tilde{C})$ はまたピタゴラス数となる. Q.E.D.

【定義 5】 $(\tilde{A}, \tilde{B}, \tilde{C})$ を (A, B, C) の D 双対なピタゴラス数という.

(例 7) 例 6 で扱った反射的なピタゴラス数

$$A = \begin{pmatrix} 3 & 1 \\ 0 & 12 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 3 \\ 0 & 16 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 3 \\ 0 & 20 \end{pmatrix}$$

は,

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 5 & -1 \\ 0 & 5 \end{pmatrix}$$

であり,

$$\tilde{A} = \begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 3 & -5 \\ 0 & 12 \end{pmatrix}, \quad \tilde{B} = \begin{pmatrix} 4 & -1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 16 \end{pmatrix},$$

$$\tilde{C} = \begin{pmatrix} 5 & -1 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 0 & 20 \end{pmatrix}$$

と置くと, $(\tilde{A}, \tilde{B}, \tilde{C})$ は (A, B, C) の D 双対なピタゴラス数である. $\square$

8. さらなる展開

現在, ピタゴラス数の研究に平行して, 3乗ピタゴラス数というものを定義して研究を行っている.

【定義 6】 (A, B, C, D) が $(M_3$ 数の) 3 乗ピタゴラス数であるとは, A, B, C, D の $(1,1)$ 成分と $(2,2)$ 成分は正で

$$A^3 + B^3 + C^3 = D^3$$

をみたすものをいう.

自然数におけるこの種の研究は, オイラーやハーディー, ラマヌジャンなどの研究が知られている. しかし, 部分的にはその構造は明らかにされてきてはいるが, 全容を現す結果は未だ得られていない[WM]. 我々は自然数の結果を睨みながら, M_3 数上での研究を行うことで, M_3 数特有の構造が浮かび上がるのではないかと期待している. さらに k 乗ピタゴラス数が同様に定義し, 一般的な研究を行うことも考えている.

参考文献

- [Ho] 堀源一郎, ハミルトンと四元数, 海鳴社, 2007 年
- [Ko] 小林吹代, ピタゴラス数を生み出す行列のはなし, ベレ出版, 2008 年
- [Ta] 橘智子, 複素ピタゴラス数の構造について, 津山代数幾何シンポジウム 2012 報告集, pp202-211(2013 年 2 月),
http://www.tsuyama-ct.ac.jp/matsuda/AlgeGeo/algegeo_index.html
- [WM] Diophantine Equation—3rd Powers, Wolfram MathWorld,
<http://mathworld.wolfram.com/DiophantineEquation3rdPowers.html>