

代数学ミニシンポジウム 2017 in 倉敷

報告集

高専代数学幾何学研究会編

(世話役：松田修，山中聡)

2017 年 11 月

はじめに

本論文集は，2017 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 2017 in 倉敷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 27 年度津山高専校長裁量経費（教育研究活動経費）「空間認知と解読という視点を基礎として，より抽象的概念の理解に向かわせる高等数学教育へのニューアプローチ」（代表：松田修）の援助を受けました．

2017 年 11 月 松田修，山中聡

代数学ミニシンポジウム 2017

日時：2017 年 9 月 22 日（金）～9 月 23 日（土）

場所：倉敷市民会館，第 1 会議室

世話人：松田修，山中聡

プログラム

22 日（金）

9:30－11:00

桐山翔伍（津山高専 3 年），松田修（津山高専） 「素数 p に関する完全数について」

加田紘大（津山高専 2 年），松田修（津山高専） 「ルーローの多角形について」

圓山夏生（津山高専 2 年），松田修（津山高専） 「 $\mathbf{Z}/m\mathbf{Z}$ からつくるグラフの曲面への埋め込みについて」

11:10－12:00

飯高茂 「超完全数の世界」

13:30－14:20

前原和寿 「Galois theory and Langlands program」

14:30－15:20

長峰孝典（新潟大学） 「On automorphisms and coordinates in polynomial rings」

15:40－16:30

小島秀雄（新潟大） 「 $\mathbf{Q}$ ホモロジー射影平面上の単尖点有理曲線について」

16:40－17:30

福岡慶明（高知大） 「偏極多様体の随伴束の大域切断のなす次元に関する話題」

17:40－18:10

山中聡（津山高専） 「環拡大の森田同値」

23 日（土）

9:00－9:30

島倫太郎（海城中 3），清水琢也（海城中 3），川崎真澄（海城中高数学科）

「Ratio of real roots of quadratic equations (joint work with Seishin highschool in Kurashiki)」

9:40－10:30

北川真也（岐阜高専） 「モーデル・ヴェイユ群が自明な最大ピカール数の有理曲面のトリゴナル曲線束」

10:40－11:30

月岡透（東海大） 「射影空間の直積をブローアップして得られる弱ファノ多様体について」

目次

ハイパー完全数と スーパー完全数 (飯高 茂)	1
Galois Theory and Langlands Program 前原和寿)	26
ON SOME PROPERTIES OF COORDINATES (長峰孝典)	49
モデル・ヴェイユ群が自明な最大ピカル数の有理曲面のトリゴナル曲線束 (北川真也)	60
素数 p を基礎にした完全数の研究 (桐山翔伍)	76
正多角形から得られるルーロー図形の研究 (加田紘大)	86
$\mathbb{Z}/m\mathbb{Z}$ からつくるグラフの曲面への埋め込みについて (圓山夏生)	97
Rational unicuspidal curves on $\mathbb{Q}$ -homology projective planes whose complements have logarithmic Kodaira dimension $-\infty$ (小島秀雄生)	104
偏極多様体の随伴束の大域切断のなす次元に関する話題 (福間慶明)	107
環拡大の森田同値 (山中聡)	134

ハイパー完全数と スーパー完全数 倉敷市民会館にて

飯高 茂

平成 29 年 11 月 9 日

目 次

1	スーパー完全数	3
1.1	スーパー完全数の定義	3
1.2	スーパー完全数についてオイラーの定理の類似	3
2	スーパー完全数の m だけ平行移動	4
2.1	$m = 0$ のとき	4
2.2	$m = 2$ のとき	5
3	素数解 p	6
4	スーパーオイラー完全数 II 型	8
4.1	m : 偶数の場合	8
5	高橋君との研究交流	9
5.1	m : 奇数の場合	9
6	m: 奇数の場合	10
6.1	$m = -1$ の場合	10
6.2	$m = 1 - 4k$ の場合	11
6.3	オイラー余関数	11
6.4	$m = -3$: の場合	12
6.5	$m = -7$: の場合	13
6.6	$m = -1 - 4k$ のとき	13
6.7	検証	15
7	$m = -1 - 2t$ で、解が無限にあるとき	18
8	混合スーパー完全数	20
8.1	$\sigma(a) - \varphi(a)$	20
8.2	$\varphi(a) - \sigma(a)$	23

1 スーパー完全数

D.Suryanarayana は 1969 年にスーパー完全数 (superperfect numbers) を定義して基本定理を確立した. (Suryanarayana, D. "Super Perfect Numbers." Elem. Math. 24, 16-17, 1969.)

1.1 スーパー完全数の定義

$a = 2^e$ とおくと $\sigma(a) = 2^{e+1} - 1$ となる. これを素数と仮定し q とおく. αq はユークリッドの完全数.

$\sigma(q) = q + 1 = 2^{e+1} = 2a$ になるので中抜きして

$$\sigma(q) = 2a.$$

$q = \sigma(a)$ を左辺に代入すると,

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

が成り立つ. 記号 $\sigma^2(a) = \sigma(\sigma(a))$ を用いると $\sigma^2(a) = 2a$ と書き直せる.

一般にこれを満たす a をスーパー完全数と呼ぶ.

ここでもオイラーの定理 (偶数完全数は ユークリッドの完全数になる) の類似が成り立つ.

1.2 スーパー完全数についてオイラーの定理の類似

定理 1.

$$\sigma^2(a) = 2a$$

を満たす a は偶数のとき 2^{p-1} とかける. ここで $q = 2^p - 1$ はメルセンヌ素数.

Proof.(By Iitaka)

偶数の仮定により, $e > 0$ があり $a = 2^e L$, (L : 奇数) と書ける.

$N = 2^{e+1} - 1$ とおくと $\sigma(a) = N\sigma(L)$.

1). $L = 1$

$a = 2^e$ により $\sigma(a) = N$. $\sigma^2(a) = \sigma(N)$. $\sigma^2(a) = 2a = N + 1$ によれば $\sigma(N) = N + 1$. それゆえ N は素数. $N = 2^{e+1} - 1$ はメルセンヌ素数.

2). $L > 2$

$N > 1$ なので, $\sigma(L)$ は $\sigma(a) = N\sigma(L)$ の真の約数. よって $1, \sigma(L), N\sigma(L)$ は相異なる約数ゆえに

$$\sigma^2(a) \geq 1 + \sigma(L) + N\sigma(L).$$

$\sigma^2(a) = 2a$ なので $2a \geq 1 + \sigma(L) + N\sigma(L)$.

$2a = 2^{e+1}L = (N+1)L$ によれば

$$(N+1)L \geq 1 + \sigma(L) + N\sigma(L) \geq 1 + (N+1)L.$$

これは矛盾.

オイラーの証明と類似している.

2 スーパー完全数の m だけ平行移動

m だけ平行移動 m した狭義の完全数 α は定義により $q = 2^{e+1} - 1 + m$ が素数になる
とき $\alpha = 2^e q$ と書ける.

$a = 2^e$ および $N = 2^{e+1} - 1$ とおくと, $N = \sigma(a)$, $q = N + m = \sigma(a) + m$, $q + 1 = 2a + m$
を満たす.

q : 素数 により

$$\sigma(q) = q + 1.$$

この式の左辺 $= \sigma(q) = \sigma(\sigma(a) + m)$. 右辺 $= q + 1 = 2a + m$

かくて

$$\sigma(\sigma(a) + m) = 2a + m.$$

これを平行移動 m のスーパー完全数の方程式といいこの解 a を平行移動 m のスーパー
完全数という.

命題 1. $a = 2^e$ が平行移動 m のスーパー完全数ならば $q = 2^{e+1} - 1 + m$ は素数となる.

とくに $2^e q$ は平行移動 m の狭義の完全数になる.

Proof.

式 $\sigma(\sigma(a) + m) = 2a + m$ に $a = 2^e$ を代入すると

$$\sigma(2^{e+1} - 1 + m) = 2^{e+1} + m.$$

$k = 2^{e+1} - 1 + m$ とおくと, $\sigma(k) = k + 1$. よって, k : 素数.

注意 1. 実例にあたると, a が偶数の仮定だけでも $a = 2^e$ が導ける可能性がある.

2.1 $m = 0$ のとき.

$m = 0$ のときパソコンで計算してみる.

偶数完全数解は 2 のべき, すなわち $a = 2^e$ であることはすでに示された.

パソコンで計算してみても奇数の解は見つからない.

完全数の場合奇数の完全数があるか? という問題があるが 2000 年以上にわたって未
解決.

スーパー完全数の場合も奇数のスーパー完全数あるかが問われている. この場合も難問
かもしれないし, 案外解けるかもしれない.

表 1: $\sigma^2(a) = 2a$

a	素因数分解	$2a - 1$ (メルセンヌ素数)
16	2^4	31
64	2^6	127
4096	2^{12}	8191
65536	2^{16}	131071
262144	2^{18}	524287

2.2 $m = 2$ のとき.

$m = 2$ のとき, パソコンで計算してみると驚天動地の世界が現れた.

表 2: $\sigma(\sigma(a) + 2) = 2a + 2$

a	素因数分解	$2a + 1$ (Fermat 素数あり)
1	2^0	$3 = 2 + 1$
2	2^1	$5 = 2^2 + 1$
8	2^3	$17 = 2^4 + 1$
11	11	
41	41	
65	$5 * 13$	
107	107	
128	2^7	$257 = 2^8 + 1$
149	149	
881	881	
959	$7 * 137$	
2141	2141	
14363	$53 * 271$	
21119	$7^2 * 431$	
32768	2^{15}	$65537 = 2^{32} + 1$
238895	$5 * 47779$	
967679	$23 * 42073$	

表を眺めた結果

- a が偶数なら 2 のべきになり, $2a + 1$ にはフェルマ素数が並ぶ.
- a が奇数の場合は, 11, 41, 107 などの素数が出る一方, 65, 959 などの合成数が並ぶ.

3 素数解 p

$\sigma(\sigma(a)+m) = 2a+m$ に素数の解 p があるとする. すると定義より $\sigma(p+1+m) = 2p+m$ を満たす.

与えられた m に対し上式の解となる素数 p を探した.

$$m = 2 \text{ のとき, } \sigma(p+3) = 2p+2$$

$$p = 11, 41, 107, 149, 881, 2141, 8381, 18629, 116621 \text{ (petit Fermat 素数)}$$

i). 最初の解 $p = 11$. $b = p+1+m = p+3 = 14 = 2Q$. とおくとき $Q = 7$. ここで $Q = 7$ を伏せておき,

$$p+3 = 2Q, a = p = 2Q-3. \sigma(\sigma(a)+m) = \sigma(2Q) = 3(Q+1), 2a+2 = 4Q-6+2 = 4Q-4$$

なので $3(Q+1) = 4Q-4$. これより $Q = 7; a = 2Q-3 = 14-3 = 11$

$$\text{ii). } p = 41 \quad p+1+2 = 4 \cdot 11 = 4Q. \quad \sigma(4Q) = 7(Q+1) = 7Q+7, 7Q+7 = 2a+2 = 2(4Q-3)+2 = 8Q-4. Q = 11.$$

$$\text{iii). } p = 107. \quad p+1+2 = 10 \cdot 11 = 10Q. \quad \sigma(10Q) = 18Q+18. \quad a = 10Q-3. 2a+2 = 20Q-4.$$

$$18Q+18 = 20Q-4 \text{ より } Q = 11, a = p = 10Q-3 = 110-3 = 107.$$

$$\text{iv). } p+3 = RQ, Q : \text{素数}, R, Q : \text{互いに素とする. } \sigma(p+3) = \sigma(RQ) = \sigma(R)(Q+1), 2p+2 = 2(RQ-3)+2 = 2RQ-4.$$

$$\text{これより, } \sigma(R)(Q+1) = 2RQ-4, \sigma(R)+4 = (2R-\sigma(R))Q.$$

$$R = 2^\varepsilon \text{ のとき, } R' = \sigma(R) = 2^{\varepsilon+1} - 1. 2R - \sigma(R) = 1 \text{ ゆえに, } Q = 2^{\varepsilon+1} + 3.$$

これが素数でかつ, $2^\varepsilon Q - 3$ が素数 p のとき解になる.

$Q = 2^\varepsilon + 3$ は 4 だけ平行移動したメルセンヌ素数,

$2^\varepsilon Q$ は 4 だけ平行移動した完全数.

表 3: $\sigma(p+3) = 2p+2$

ε	$R = 2^\varepsilon$	$R' = 2R - 1$	$Q = 2^\varepsilon + 3$	$p = RQ - 3$	factor
1	2	3	7	11	O
2	4	7	11	41	O
3	8	15	19	149	O
4	16	31	35	557	35 no prm
5	32	63	67	2141	O
6	64	127	131	8381	$17^2 \cdot 29$
7	128	255	259	33149	259 no prm
8	256	511	515	131837	515 no prm
9	512	1023	1027	525821	$149 \cdot 3529$
10	1024	2047	2051	2100221	2051 no prm

$$m = 4$$

$\sigma(p+5) = 2p+4$ を満たす.

$$p = 47, 587.$$

$$m = -2$$

$$p = 7, 29, 497, 8129$$

$$m = -4$$

$$p = 23, 107, 467, 653, 1955, 130307, 522755$$

これらの素数は居場所を探して彷徨っているようだ.

4 スーパーオイラー完全数 II 型

$\sigma(a)$ の代わりにオイラー関数 $\varphi(a)$ を用いて平行移動 m のスーパーオイラー完全数 II 型を定義してみよう.

$q_0 = 2^e + 1 + m$ は素数とする. $a = 2^e$ とおく.

$a = 2\varphi(a)$ により $q_0 = 2\varphi(a) + 1 + m$. 代入して $\varphi(q_0) = \varphi(2\varphi(a) + 1 + m)$.

q_0 は素数だから $\varphi(q_0) = q_0 - 1$.

一方, $q_0 - 1 = a + m$. これらを組み合わせると,

$$\varphi(2\varphi(a) + 1 + m) = a + m.$$

これを スーパーオイラー完全数 II 型の定義式といい, この解をスーパーオイラー II 型完全数という.

4.1 m :偶数の場合

$\varphi(2\varphi(a) + 1 + m) = a + m$ において, m を偶数と仮定する. オイラー関数は自然数について定義されるので, $x = 2\varphi(a) + 1 + m \geq 1$.

一般に $\varphi(x)$ は $x > 2$ なら偶数なので,

$x = 2\varphi(a) + 1 + m \geq 2$ は偶数なので a も偶数. よって奇数の L によって $a = 2^e L$ と書ける.

1) $x = 2\varphi(a) + 1 + m > 1$ とする. $\varphi(x) \leq x - 1 = 2\varphi(a) + m$.

$$a + m = \varphi(2\varphi(a) + 1 + m) = \varphi(x) \leq x - 1 = 2\varphi(a) + m$$

$$2^e L + m = a + m \leq x - 1 = 2\varphi(a) + m = 2^e \varphi(L) + m.$$

$L \leq \varphi(L)$ により, $L = 1, a = 2^e$. $x = 2\varphi(a) + 1 + m = 2^e + 1 + m$,

$$\varphi(x) = \varphi(2\varphi(a) + 1 + m) = a + m = 2^e + m = Q - 1.$$

ゆえに $x = 2^e + 1 + m$ は素数.

2) $x = 2\varphi(a) + 1 + m = 1$ とする.

$$2\varphi(a) + m = 0.$$

$\varphi(2\varphi(a) + 1 + m) = a + m$ により, $1 = a + m$. $2\varphi(a) + m = 0$ なので $2\varphi(a) = -m = a - 1$.

ところで, $2\varphi(a) = a - 1$ を満たす a は存在しない, という予想がある. そこでこれを仮説として使う.

したがって, $x = 2\varphi(a) + 1 + m = 1$ となる場合はないと理解する. この仮説を用いた結果次の定理ができた.

定理 2. m を偶数と仮定する. $\varphi(2\varphi(a) + 1 + m) = a + m$ の解は $a = 2^e$, ここで, $Q = 2^e + 1 + m$ は素数.

ここで, $m = 0$ なら $Q = 2^e + 1$ はフェルマ素数.
 $m = -2$ なら $Q = 2^e - 1$ はメルセンヌ素数.

5 高橋君との研究交流

2017 年 8 月下旬から当時小学校 4 年生の高橋洋翔君との研究交流が始まった. ここでは高橋君を T を筆者を I と書く. (T は 10 歳の数学少年, I は 75 歳の後期高齢者).

1. 2017 年 8 月 25 日. T は I に数学の研究になる課題を教えてほしいと要望.
2. 8 月 27 日. I は葉書を出して. $\varphi(2\varphi(a) + 1) = a + 1$ の解 a は何かを問う.
3. 2 日後 T は 解は 2^e . ここで $2^e + 1$ は素数と返書.
4. I は葉書を出して, 未解決の問題なので難問と添え書きして $\varphi(2\varphi(a) - 2) = -3$ の解を問う.
5. T は 解は 双子素数の兄の方であると証明をつけて ipad で返書.
6. 2 日後 I は 葉書を出して一般に m : 負の奇数のとき $\varphi(2\varphi(a) + 1 + m) = a + m$, の解などを問う.
7. 9 月 2 日 T は 多くの課題と結果を書きならべ, $m = -1$ のとき $\varphi(2\varphi(a)) = a - 1$ の解は 2 とフェルマ素数と予想するが未証明と ipad で返書
8. それを受けて I は $m = -1$: のとき解はないとしていた誤りに気づき, 正しい証明を作り mail で伝えた.

以下はこのような流れの中でできた結果についてふれる.

5.1 m : 奇数の場合

$\varphi(2\varphi(a) + 1 + m) = a + m$ の解を求める.

m を奇数と仮定する. 一般に $x > 2$ なら $\varphi(x)$ は 偶数なので a も奇数.

命題 2. m を奇数 $2N - 1$ とする. $m \geq -1$ の場合は $\varphi(2\varphi(a) + 1 + m) = a + m$ の解があるとき, 1) $N = 0$ のとき $m = -1, a = 2$, またはフェルマ素数, 2) $N = 1$ のとき $x = 1, a = 1$ になる.

Proof.

$2\varphi(a) + 1 + m = 2(\varphi(a) + N)$ によって

$$\varphi(2(\varphi(a) + N)) = a + 2N - 1.$$

$b = \varphi(a) + N$ とおくとき $\varphi(2b) = a + 2N - 1$.

$b = \varphi(a) + N = 2^e L$ (L : 奇数) の形に書いて

$L > 2$ のとき, $L - \varphi(L) \geq 1$ により

$$\begin{aligned}
 a + 2N - 1 &= \varphi(2b) \\
 &= 2^\varepsilon \varphi(L) \\
 &\leq 2^\varepsilon (L - 1) \\
 &= \varphi(a) + N - 2^\varepsilon \\
 &\leq a - 1 + N - 2^\varepsilon.
 \end{aligned}$$

これより

$$a + 2N - 1 \leq a - 1 + N - 2^\varepsilon.$$

$N \leq -2^\varepsilon \leq -1$. よって $m \leq -3$.

$L = 1$ のとき, $b = \varphi(a) + N = 2^\varepsilon$.

一方, $2^\varepsilon = \varphi(2b) = a + 2N - 1$, により

$$a + 2N - 1 = 2^\varepsilon = \varphi(a) + N$$

$a > 1$ ならば

$$a - \varphi(a) + 2N - 1 = N + 1 - 2N = 1 - N.$$

ゆえに $N = 0, a - \varphi(a) = 1$.

$b = 2^\varepsilon = \varphi(a) + N = a - 1$.

ゆえに, $a = 1 + b = 1 + 2^\varepsilon$ は素数なのでこれが奇数ならフェルマ素数. $\varepsilon = 0$ のとき, $a = 2$. したがって, $a = 2$, またはフェルマ素数

$a = 1$ ならば $a + 2N - 1 = \varphi(a) + N$ に代入すれば, $2N = 1 + N$. よって, $N = 1$.

6 m : 奇数の場合

$\varphi(2\varphi(a) + 1 + m) = a + m$ の研究を行う.

6.1 $m = -1$ の場合

$\varphi(2\varphi(a)) = a - 1$ のときは $a = 2$ またはフェルマ素数 となることを高橋洋翔は予想した.

幸い証明できた (Iitaka)

Proof.

$a = 2$ は解. そこで $a \geq 3$ としてよい.

$\varphi(a)$ は偶数なので, $\varphi(a) = 2^\varepsilon L, (L : \text{奇数})$ としてよい.

$2\varphi(a) = 2^{\varepsilon+1}L$ により $\varphi(2\varphi(a)) = 2^{\varepsilon}\varphi(L)$.

1). $L > 2$.

$$\begin{aligned} a-1 &= \varphi(2\varphi(a)) \\ &= 2^{\varepsilon}\varphi(L) \\ &\leq 2^{\varepsilon}(L-1) \\ &= 2^{\varepsilon}L - 2^{\varepsilon} \\ &= \varphi(a) - 2^{\varepsilon}. \end{aligned}$$

よって,

$$a-1 \leq \varphi(a) - 2^{\varepsilon} \leq a-1 - 2^{\varepsilon}.$$

ゆえに, $0 \leq -2^{\varepsilon}$ となり矛盾.

2). $L = 1$.

$\varphi(a) = 2^{\varepsilon}$. $\varphi(2\varphi(a)) = a-1$ に代入すると, $\varphi(2\varphi(a)) = 2^{\varepsilon}$ によれば $2^{\varepsilon} = a-1$. したがって, $a = 2^{\varepsilon} + 1$. これはフェルマ素数.

6.2 $m = 1 - 4k$ の場合

高橋洋翔のプリントにしたがい, $m = 1 - 4k, (k > 0)$ とする.

$\varphi(2\varphi(a) + 2 - 4k) = a + 1 - 4k$ となる.

$b = \varphi(a) + 1 - 2k$ とおくと, これは奇数 ($a > 2$).

$b > 1$ なら $\varphi(b) \leq b-1$ によって,

$$a+1-4k = \varphi(2\varphi(a) + 2 - 4k) = \varphi(2b) = \varphi(b) \leq b-1 = \varphi(a) - 2k. \quad (1)$$

中抜きして

$$a+1-4k \leq \varphi(a) - 2k.$$

$$co\varphi(a) = a - \varphi(a) \leq 2k - 1.$$

$co\varphi(a) = 1, 2, \dots, 2k-1$ となるが, $k=1$ の場合を扱う.

6.3 オイラー余関数

一般に $co\varphi(a) = a - \varphi(a)$ と定めオイラー余関数と呼ぶ. $a > 1$ なら $co\varphi(a) \geq 1$. 次の結果はやさしいが有用.

1. $\text{co}\varphi(a) = 1$ なら a は素数. 逆も正しい
2. $\text{co}\varphi(a) = 2$ なら $a = 4$.
3. $\text{co}\varphi(a) = 3$ なら $a = 9$.
4. $\text{co}\varphi(a) = 4$ なら $a = 8, 10$.
5. $\text{co}\varphi(a) = 5$ なら $a = 25$.

6.4 $m = -3$: の場合

a). $k = 1$ の場合. (この場合を最初に解決したのは高橋洋翔氏)
 定義式は $\varphi(2\varphi(a) - 2) = a - 3$ となる.
 $\text{co}\varphi(a) = a - \varphi(a) \leq 2k - 1 = 1$ により $\text{co}\varphi(a) = 1$ なので a :素数. $b = \varphi(a) - 1 = a - 2$.
 $a - 3 = \varphi(b)$ より, $b - 1 = a - 3 = \varphi(b)$. すなわち, b も素数. $(a, a - 2)$ は双子素数で
 a は兄という.
 $b = 1$ の場合は, $1 = b = \varphi(a) - 1$. このとき $a = 4$.
 次の結果にまとめる.
 $a = 4$ は確かに解. $a = 2 + p$ とし p, a はともに素数とする.
 $2\varphi(a) - 2 = 2(a - 1) - 2 = 2a - 4 = 2p$ になり $\varphi(2p) = p - 1 = a - 3$.
 こうして双子素数の解が確認できた.

表 4: 双子素数

a	$a - 2$
5	3
7	5
13	11
19	17
31	29
43	41
61	59
73	71

定理 3 (Hiroto Takahashi). $\varphi(2\varphi(a) - 2) = a - 3$ となる条件は $a = 4$ または双子素数の兄.

双子素数の特徴付けと見るとこれは美しい定理と言ってよい.

6.5 $m = -7$: の場合

b). $k = 2, m = -7$

条件は $\varphi(2\varphi(a) - 6) = a - 7$ となる. したがって $a > 7$.

$$\text{co}\varphi(a) = a - \varphi(a) \leq 2k - 1 = 3.$$

このとき $\text{co}\varphi(a) = 1, 2, 3$ となるので順次調べる.

1) $\text{co}\varphi(a) = 3, a = 9$ になり, これは解.

2) $\text{co}\varphi(a) = 2, a = 4$ になり解ではない.

3) $\text{co}\varphi(a) = 1, a$ は素数.

$b = \varphi(a) + 1 - 2k = \varphi(a) - 3$. 最初に $b = 1$ とすると, $\varphi(a) = 4$. このとき $a = 8, 10, a = 8$ のみ解.

$b > 1$ として以下考える.

$$b = \varphi(a) + 1 - 2k = a - 4.$$

$a - 7 = \varphi(2\varphi(a) - 6) = \varphi(2b) = \varphi(b)$ によれば, $\varphi(b) = a - 7 = b - 3$. すなわち $\text{co}\varphi(b) = 3$. よって, $b = 9$. したがって $a = 13$.

定理 4. $m = -7$ のとき $\varphi(2\varphi(a) - 6) = a - 7$ となる条件は $a = 2^3, 3^2, 13$.

6.6 $m = -1 - 4k$ のとき

$m = -1 - 4k$ のときは条件式は $\varphi(2\varphi(a) - 4k) = a - 1 - 4k$ となる.

$b = \varphi(a) - 2k$ とおくとこれは偶数 ($a > 2$), $\varphi(2b) = a - 1 - 4k$ となる. b を素因数分解して, $b = 2^\varepsilon Q, Q$: 奇数とする.

$$\varphi(2^{\varepsilon+1}Q) = a - 1 - 4k.$$

i). $Q = 1$ のとき.

$$\varphi(a) - 2k = b = 2^\varepsilon, \varphi(2^{\varepsilon+1}) = 2^\varepsilon = a - 1 - 4k.$$

$$a = 1 + 4k + 2^\varepsilon, \text{ かつ } \varphi(a) = 2^\varepsilon + 2k$$

$$\text{これによつて } \text{co}\varphi(a) = a - \varphi(a) = 2k + 1.$$

a). $k = 1; m = -5$.

$$\text{co}\varphi(a) = 2k + 1 = 3. \text{ すると, } a = 9. 9 = a = 1 + 4k + 2^\varepsilon = 5 + 2^\varepsilon.$$

$$2^\varepsilon = 4 \text{ になり, } \varepsilon = 2, b = 4.$$

b). $k = 2; m = -9, \varphi(2\varphi(a) - 8) = a - 9. \text{co}\varphi(a) = 2k + 1 = 5. \text{ すると, } a = 25. \text{ これは解.}$

ii). $Q > 2. \varphi(Q) \leq Q - 1, b = \varphi(a) - 2k$ を使う.

$$\begin{aligned}
a - 1 - 4k &= \varphi(2^{\varepsilon+1}Q) \\
&= 2^\varepsilon \varphi(Q) \\
&\leq 2^\varepsilon (Q - 1) \\
&= 2^\varepsilon Q - 2^\varepsilon \\
&= b - 2^\varepsilon.
\end{aligned}$$

$$a - 1 - 4k \leq b - 2^\varepsilon = \varphi(a) - 2k - 2^\varepsilon.$$

$b = \varphi(a) - 2k$ によつて, $b = \varphi(a) - 2k$, $\varphi(2b) = a - 1 - 4k$ であり

$$a - 1 - 4k \leq \varphi(a) - 2k - 2^\varepsilon.$$

$a > 2$ のとき, $\varphi(a) \leq a - 1$ を用いて

$$a - 1 - 4k \leq \varphi(a) - 2k - 2^\varepsilon \leq a - 12k - 2^\varepsilon.$$

中抜きして

$$a - 1 - 4k \leq a - 1 - 2k2^\varepsilon.$$

これより $-4k \leq -2k - 2^\varepsilon$; $k \geq 2^{\varepsilon-1}$.

以後 $k = 1$ とする. $m = 5$. 上の評価式により, $k = 1 \geq 2^{\varepsilon-1}$. すなわち, $\varepsilon - 1 = 0$.

$a - 5 = a - 1 - 4k \leq b - 2^\varepsilon = b - 2 = \varphi(a) - 4$ により $a - 5 \leq b - 2 = \varphi(a) - 4 \leq a - 5$.

ゆえに, $a - 5 = b - 2$, $\varphi(a) = a - 1$. $b = a - 3$ かつ a は素数.

$\varphi(2b) = a - 1 - 4k = a - 5 = b - 2$, $\varphi(2b) = \varphi(4Q) = 2\varphi(Q)$.

$2\varphi(Q) = \varphi(2b) = a - 5 = b - 2 = 2Q - 2$ が得られて, $\varphi(Q) = Q - 1$. ゆえに Q も素数で, $a = 3 + 2Q$ も素数になった.

a	$a - 3$	$Q = (a - 3)/2$
13	10	5
17	14	7
29	26	13
37	34	17
41	38	19
61	58	29
89	86	43
97	94	47

さて逆に奇素数 a をとる. $a - 3$ は偶数なのでこれを 2 で割ると素数 p . $a = 2p + 3$, $2a - 6 = 4p$. $2\varphi(a) - 4 = 2(a - 3) = 4p$.

そこで $\varphi(2a - 6) = \varphi(4p) = 2(p - 1) = a - 5$.

$p, a = 2p + 3$ がともに素数となる場合は無限にあるかもしれない. かくして双子素数と類似した素数の対についてこれらが無限にあるか, という問題ができた.

このような (a, p) を年の差カップルと呼ぶことに異論はないでしょう.

$k = 2, m = -9$ の場合も興味深い.

高橋洋翔氏は 2017 年 9 月 3 日の ipad での私信で

(v) $m = -1 - 2^e$ のとき $\varphi(2\varphi(a) + 1 + m) = a + m$ の解は無限にありそう (未証明) と書いた.

彼はそれに先立つ 8 月 28 日ごろ, $m = -3$ のとき 解が 4 と双子素数の兄の方になることを証明していた.

$m = -5$ と $m = -9$ のとき 解が 双子素数と類似の形になることが分かった. しかし個別研究はともかく, これから一般論を作るのは困難であろう, と私は考えていた.

しかし, 高橋洋翔氏の第 v のテーゼが気になったので調べたところこれらの解は超双子素数になることがわかった.

双子素数 と同様に 超双子素数も無限にあると信じれば解が無限にありそう, という彼の感想はまさに正鵠を得たものと言える.

6.7 検証

命題 3. p と $a = 2^e p + 2^e + 1$ がともに素数なら a は $m = -1 - 2^{e+1}$ のとき $\varphi(2\varphi(a) + 1 + m) = a + m$ の解

Proof.

$a = 2^e p + 2^e + 1$ は素数なので $\varphi(a) = 2^e p + 2^e = 2^e(p + 1)$.

$2\varphi(a) + 1 + m = 2^{e+1}(p + 1) - 2^{e+1} = 2^{e+1}p$ なので $\varphi((2\varphi(a) + 1 + m)) = 2^e(p - 1)$

一方, $a + m = 2^e p + 2^e + 1 - 1 - 2^{e+1} = 2^e(p - 1)$.

よって $\varphi(2\varphi(a) + 1 + m) = a + m$ が確認された.

表 5: $\varphi(2\varphi(a) + 1 + m) = a + m$

$m = -3$		$m = -5$			$m = -9$		
a	$a - 2$	a	$a - 3$	$b/2$	a	$a - 5$	$b/4$
5	3	13	10	5	17	12	3
7	5	17	14	7	73	68	17
13	11	29	26	13	97	92	23
19	17	37	34	17	193	188	47
31	29	41	38	19	241	236	59
43	41	61	58	29	337	332	83
61	59	89	86	43	409	404	101
73	71	97	94	47	433	428	107
103	101	109	106	53	457	452	113
109	107	137	134	67	601	596	149
139	137	149	146	73	673	668	167
151	149	181	178	89	769	764	191
181	179	197	194	97	937	932	233
193	191	229	226	113	1009	1004	251
199	197	257	254	127	1033	1028	257
$4 = 2^2$		$9 = 3^2$			$25 = 5^2$		

表 6: $\varphi(2\varphi(a) + 1 + m) = a + m$ 続き

$m = -17$			$m = -33$			$m = -65$		
a	$a - 9$	$b/8$	a	$a - 17$	$b/16$	a	$a - 33$	$b/32$
97	88	11	97	80	5	193	160	5
113	104	13	193	176	11	257	224	7
193	184	23	673	656	41	449	416	13
241	232	29	769	752	47	577	544	17
257	248	31	1153	1136	71	641	608	19
337	328	41	2113	2096	131	769	736	23
353	344	43	2689	2672	167	1217	1184	37
433	424	53	3169	3152	197	1409	1376	43
577	568	71	4129	4112	257	2689	2656	83
593	584	73	4513	4496	281	3137	3104	97
641	632	79	4993	4976	311	3329	3296	103
21=3*7			65=5*13			209=11*19		
25=5*5			289 = 17 ²			961 = 31 ²		
49=7*7								

7 $m = -1 - 2t$ で、解が無限にあるとき

$m = -1 - 2t$ のとき $\varphi(2\varphi(a) + 1 + m) = a + m$ の解が無限にあるとする.

$b = \varphi(a) - t$ とおくと $2b = 2\varphi(a) + 1 + m$. $b = 2^\varepsilon Q$, (Q :奇数) とおくと $2b = 2^{\varepsilon+1}Q$ となり, $\varphi(2\varphi(a) + 1 + m) = a + m$ に代入すると

$$2^{\varepsilon+1}\varphi(Q) = a + m = a - 1 - 2t$$

よって,

$$a = 2t + 1 + 2^\varepsilon\varphi(Q).$$

さらに

$$\varphi(a) = t + b = t + 2^{\varepsilon+1}Q.$$

この式を引いて

$$\text{co}\varphi(a) = a - \varphi(a) = 1 + t - 2^\varepsilon\text{co}\varphi(Q).$$

よって $\text{co}\varphi(a) \leq 1 + t$.

a が素数でないなら $\text{co}\varphi(a) \geq 2$. このとき評価式 $\text{co}\varphi(a) \geq \sqrt{a}$ が成り立つ.

これより, $1 + t \geq \sqrt{a}$. $(1 + t)^2 \geq a$ となり解は有限個.

したがって解が無限にあるとの仮定によって, a が素数になり, $\text{co}\varphi(a) = 1$.

$$1 = \text{co}\varphi(a) = 1 + t - 2^\varepsilon\text{co}\varphi(Q).$$

よって,

$$t = 2^\varepsilon\text{co}\varphi(Q).$$

$$a - 1 = \varphi(a) = t + 2^\varepsilon Q.$$

により a に無限に解があれば Q にも無限に解がある.

$t = 2^\varepsilon\text{co}\varphi(Q)$ において, $\frac{t}{2^\varepsilon} = \text{co}\varphi(Q)$.

Q が素数でない, すなわち $\text{co}\varphi(Q) > 1$ なら $\text{co}\varphi(Q) > \sqrt{Q}$.

$$\left(\frac{t}{2^\varepsilon}\right)^2 \geq Q.$$

Q は有限個の解になり仮定に反する. よって $\text{co}\varphi(Q) = 1$. すなわち, Q は素数. $t = 2^\varepsilon\text{co}\varphi(Q) = 2^\varepsilon$.

$$\varphi(a) = t + b = t + 2^\varepsilon Q$$

に以上の式を入れて

$$a - 1 = t + 2^\varepsilon Q.$$

$\alpha = 1 + t = 1 + 2^\varepsilon, \beta = 2^\varepsilon$ とおくとき

a, Q は素数, $a = 1 + t + 2^\varepsilon Q = \alpha + \beta Q$ を満たす.

これらは超双子素数と呼ばれる.

1. $\alpha = 2, \beta = 1$ なら双子素数.
2. $\alpha = 1, \beta = 2$ ならソフィージェルマンの素数.
3. $\alpha = 3, \beta = 2$ なら $m = -3$ のときの解.
4. $\alpha = 1 + 2^\varepsilon, \beta = 2^\varepsilon$ なら $m = -1 - 2 \cdot 2^\varepsilon$ のときの解.

8 混合スーパー完全数

$\sigma(a)$ と $\varphi(a)$ を組み合わせたらどうだろう, と高橋氏がつぶやいたのでこれをヒントにして混合スーパー完全数を次のように導入した.

8.1 $\sigma(a) - \varphi(a)$

$a = 2^e, q = 2^e + 1 + m$ は素数とする.

$\varphi(a) = 2^{e-1}, 2\varphi(a) = 2^e = a$ なので $q = 2\varphi(a) + 1 + m = 2^e + 1 + m$,

q :素数 なので,

$\sigma(q) = q + 1, q + 1 = 2^e + 2 + m = a + 2 + m$.

これに, $q = 2\varphi(a) + 1 + m$ を代入すると,

$$\sigma(2\varphi(a) + m + 1) = a + m + 2.$$

これを平行移動 m の第 1 種の混合スーパー完全数の方程式といいこの解を第 1 種の混合スーパー完全数という.

表 7: $P = 2, m = -4$

a	$(a) = \text{factor}$
3	$(3) = 3$
8	$(8) = 2^3$
16	$(16) = 2^4$
32	$(32) = 2^5$
64	$(64) = 2^6$
130	$(130) = 2 * 5 * 13$
512	$(512) = 2^9$
800	$(800) = 2^5 * 5^2$

解 $(130) = 2 * 5 * 13$ は不協和音である.

表 8: $P = 2, m = -2$

a	$(a) = \text{factor}$
4	$(4) = 2^2$
8	$(8) = 2^3$
24	$(24) = 2^3 * 3$
32	$(32) = 2^5$
128	$(128) = 2^7$

解 $(24) = 2^3 * 3$ は不協和音である.

表 9: $P = 2, m = 0$

a	$(a) = \text{factor}$
2	$(2) = 2$
4	$(4) = 2^2$
16	$(16) = 2^4$
256	$(256) = 2^8$
322	$(322) = 2 * 7 * 23$

表 10: $P = 2, m = 2$

a	$(a) = \text{factor}$
2	$(2) = 2$
4	$(4) = 2^2$
8	$(8) = 2^3$
16	$(16) = 2^4$
36	$(36) = 2^2 * 3^2$
64	$(64) = 2^6$
128	$(128) = 2^7$

解 $(36) = 2^2 * 3^2$ は不協和音である.

8.2 $\varphi(a) - \sigma(a)$

$a = 2^e, q = 2^{e+1} + 1 + m$ は素数とすると $q - 1 = 2a + m$.

$N = 2^{e+1} - 1$ とおくと $\sigma(a) = N$,

$q = 2^{e+1} + 1 + m = N + 2 + m = \sigma(a) + 2 + m$.

q :素数 なので, $\varphi(q) = q - 1$.

$\varphi(q) = \varphi(\sigma(a) + 2 + m), q - 1 = 2a + m$. なので

$$\varphi(\sigma(a) + 2 + m) = 2a + m.$$

これを平行移動 m の第 2 種の混合スーパー完全数の方程式といいこの解を第 2 種の混合スーパー完全数という.

表 11: $P = 2, m = -4$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(4) = 2^2$	4
$(8) = 2^3$	8
$(16) = 2^4$	16
$(32) = 2^5$	32
$(256) = 2^8$	256
$(512) = 2^9$	512
$(2048) = 2^{11}$	2048
$(8192) = 2^{13}$	8192

表 12: $P = 2, m = -3$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(2) = 2$	2

表 13: $P = 2, m = -2$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(2) = 2$	2
$(4) = 2^2$	4
$(16) = 2^4$	16
$(64) = 2^6$	64
$(4096) = 2^{12}$	4096
$(65536) = 2^{16}$	65536

$m = -1$ のとき解はない

表 14: $P = 2, m = 0$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(2) = 2$	2
$(8) = 2^3$	8
$(128) = 2^7$	128
$(32760) = 2^3 * 3^2 * 5 * 7 * 13$	32760
$(32768) = 2^{15}$	32768

$m = 1$ のとき解はない

表 15: $P = 2, m = 2$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(2) = 2$	2
$(2) = 2$	4
$(4) = 2^2$	4
$(8) = 2^3$	8
$(32) = 2^5$	32
$(64) = 2^6$	64
$(2048) = 2^{11}$	2048
$(16384) = 2^{14}$	16384
$(32768) = 2^{15}$	32768

$m = 3$ のとき解はない

表 16: $P = 2, m = 4$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(4) = 2^2$	4
$(16) = 2^4$	16
$(1024) = 2^{10}$	1024

$m = 5$ のとき解はない

表 17: $P = 2, m = 6$ 第二種混合スーパー完全数

$(a) = \text{factor}$	
$(2) = 2$	2
$(8) = 2^3$	8
$(32) = 2^5$	32
$(128) = 2^7$	128
$(512) = 2^9$	512

表 18: $P = 2, m = 2$

a	$(a) = \text{factor}$
2	$(2) = 2$
4	$(4) = 2^2$
8	$(8) = 2^3$
16	$(16) = 2^4$
36	$(36) = 2^2 * 3^2$
64	$(64) = 2^6$
128	$(128) = 2^7$

9 ウルトラ完全数

高橋洋翔は スーパー完全数 をヒントにして次のような新種の完全数を定義した. ここで
はウルトラ完全数という.

$\sigma^3(a) = \sigma(\sigma(\sigma(a)))$ とおく. $\sigma^3(a) = 4a - 1$ をウルトラ完全数の方程式, この解をウル
トラ完全数という.

$a = 2^e, (q = 2a - 1 : \text{素数})$ のとき, a はウルトラ完全数になる.

m だけ平行移動したウルトラ完全数

$a = 2^e, (q = 2a - 1 + m : \text{素数})$ のとき, a を m だけ平行移動したウルトラ完全数と
いう.

$a = 2^e$ に対して, $N = 2^{e+1} - 1, \sigma(a) = N = 2a - 1 = q - m$ なので

$q = N + m = \sigma(a) + m.$

$\sigma(q) = q + 1$ なので $\sigma(q) = \sigma(\sigma(a) + m), q + 1 = 2a + m.$

$$\sigma(q) = \sigma(\sigma(a) + m) = 2a + m.$$

$\sigma(2a) = 4a - 1, 2a = \sigma(\sigma(a) + m) - m$ なので

$$\sigma(\sigma(\sigma(a) + m) - m) = 4a - 1.$$

この式を m だけ平行移動したウルトラ完全数の方程式, この解 a を m だけ平行移動したウルトラ完全数という.

Galois Theory and Langlands Program

Kazuhisa Maehara at Kurashiki

November 16, 2017

Abstract

We generalize the Galois theory to the non algebraic case. The category the set of whose objects are projective algebraic varieties up to birational equivalence and whose morphisms are separable dominant rational maps can be controlled by the category the set of whose objects are algebraically closed subgroups of a topological group that we define in this paper and whose morphisms are inclusions. Next we explain one of the conjectures of Langlands program and give a chance to prove it.

1 Galois Theory

We refer to Ch.5 in N.Bourbaki "Éléments de Mathématique Algèbre Chapitres 4 à 7" for the sake of the reader in this section([B1]).

Definition 1.1. 1. A field is algebraically closed if every algebraic extension of the field is trivial.

2. Let K be a field. An algebraically closed and algebraic over K is called an algebraic closure of K .

3. A field is separably closed if every algebraic separable extension of the field is trivial.

4. A separably closed and algebraic over K is called a separable closure of K .

Theorem 1.1. Let K be a field. There exists an algebraic closure of K ; if Ω and Ω' are algebraic closures, there exists a K -isomorphism of Ω onto Ω' .

Corollary 1.1. Let K and K' be two fields, Ω an algebraic closure of K and Ω' an algebraic closure of K' . There exists an isomorphism $u : K \rightarrow K'$ if and only if there exists an isomorphism of Ω onto Ω' which extends u .

Proposition 1.1. Let Ω be an algebraically closed field of K

1. The algebraic separable closure Ω^s of K in Ω is a separable closure of K .

2. If E and E' are two separable closures, there exists a K -isomorphism of E onto E' .

Theorem 1.2. Every extension E of a field K admits a transcendental basis. In other word every extension of K is an algebraic extension of a pure extension of K .

Theorem 1.3. Let E be an extension of K . Every transcendental basis has the same cardinality.

Proposition 1.2. Let Ω_K be an algebraically closed extension of a field K , E and F two subextensions of Ω_K and u a K -isomorphism of E onto F . There exists a K -automorphism v of Ω_K which extends u if and only if Ω_K has the same transcendent degrees over E and F .

$$\begin{array}{ccc}
\Omega_K & \xrightarrow{v} & \Omega_K \\
\uparrow & & \uparrow \\
E & \xrightarrow{u} & F \\
\uparrow & & \uparrow \\
K & \xrightarrow{=} & K
\end{array}$$

Proof. Necessary condition is obvious. Suppose Ω has the same transcendent degree with respect to E and F . Choose transcendent bases B and C of E and F over K , respectively. Since B and C are equipotent, u can be extended to a K -isomorphism u' between $E(B)$ and $F(C)$. Since Ω is an algebraic closure of $E(B)$ and $F(C)$, respectively, u' can be extended to an automorphism v of Ω . $\square$

Corollary 1.2. *Let Ω_K be an algebraically closed extension of a field K and E a subextension of Ω_K . Each K -automorphism of E can be extended to a K -automorphism of Ω_K .*

Theorem 1.4. *Let N be a Galois extension of K and Γ the Galois group. Let $\mathcal{K}$ be the set of subextensions of N and $\mathcal{G}$ the set of closed subgroups of Γ . For each subgroup $\Delta \subseteq \Gamma$, $K(\Delta)$ denotes the invariant field by Δ and for each field $E \in \mathcal{K}$, $g(E)$ denotes the E -automorphism group of N . Then $\Delta \mapsto K(\Delta)$ is the bijection from $\mathcal{G}$ onto $\mathcal{K}$ and $E \mapsto g(E)$ is the inverse bijection from $\mathcal{K}$ onto $\mathcal{G}$. N/E is a Galois extension. $\text{Gal}(N/E)$ is a closed subgroup of $\text{Gal}(N/K)$, which has an induced topology of $\text{Gal}(N/K)$.*

Proposition 1.3. *Let N be a quasi-Galois extension of K . N_r denote the invariant field by the K -automorphisms of N and N_s denote the separable algebraic closure of K in N . Then*

1. N_r is the radical closure of K in N .
2. N_s is the Galois extension of K and each K -automorphism of N_s can be extended uniquely to an N_r -automorphism of N .
3. The fields N_r and N_s are linearly disjoint over K and $N = K(N_r \cup N_s)$, $N = N_r \otimes_K N_s$.

Definition 1.2. • *A is an etale algebra over K if A is K -isomorphic to an algebra K^n . If E is a finite extension of K , E is an etale algebra over K if and only if E is separable over K . v.35*

- *A is a reduced commutative algebra if A is isomorphic to a subalgebra of a product of fields.*
- *A is an separable commutative algebra over K if $A \otimes_K L$ is reduced for any extension L of K .*
- *A is a reduced commutative algebra of finite over K if A is K -isomorphic to $L_1 \times \cdots \times L_n$, where L_i is an extension of finite degree of K for $1 \leq i \leq n$.*

Proposition 1.4. • *Every pure extension is seaparable.*

- *Let E be a field, G an automorphism of E and K the invariant subfield of E by G . Then E is a separable extension of K .*
- *Let L be an extension of a field K . If L is separable over K , every subextension of L is separable over K . Inversely, if each subextension of finite type of L is separable over K , then L is separable over K .*

- Let L be an extension of K and M an extension of L . If M is separable over L and if L is separable over K , then M is separable over K . Note that even if M is separable over K , M is not necessarily separable over L .
- Let F be an algebraic extension of K and E a subextension of F . F is separable if and only if F is separable over E and E is separable over K .

Let N/K and N'/K' be Galois extensions.

Consider the following commutative square:

$$\begin{array}{ccc} N & \xrightarrow{v} & N' \\ \uparrow & & \uparrow \\ K & \xrightarrow{u} & K' \end{array}$$

There exists a continuous homomorphism that we explain explicitly

$$\text{Gal}(N/K) \longleftarrow \text{Gal}(N'/K')$$

$$*g \longleftarrow g$$

Let F/K be a Galois extension and $F/E/K$ a subextension of E .

One then has a continuous injective homomorphism called Inflation:

$$\text{Gal}(F/E) \longrightarrow \text{Gal}(F/K) \quad \text{injection}$$

When E/K is moreover a Galois extension, then one has a continuous surjective homomorphism called Restriction;

$$\text{Gal}(F/K) \longrightarrow \text{Gal}(E/K) \quad \text{surjection}$$

Suppose

$$v^{-1}(K') = K, N' = K'(v(N))$$

Then one has a continuous isomorphism called Translation:

$$\text{Gal}(N/K) \longrightarrow \text{Gal}(N'/K') \quad \text{identity}$$

$$\begin{array}{ccc} & & N' \\ & & \uparrow \\ N & \longrightarrow & K'(v(N)) \\ \uparrow & & \uparrow \\ v^{-1}(K') & \longrightarrow & K' \\ \uparrow & & \\ K & & \end{array}$$

$$\text{Gal}(N'/K') \xrightarrow{\text{restriction}} \text{Gal}(K'(v(N))/K') \xrightarrow{\text{translation}} \text{Gal}(N/v^{-1}K') \xrightarrow{\text{inflation}} \text{Gal}(N/K)$$

A V 68 Th.5 Bourbaki

Theorem 1.5. *Let N be a Galois extension of K and $N' = K'(N)$ an extension of K' . Assume $K = K' \cap N$. Then the extension N' of K' is Galois and the canonical homomorphism $K' \otimes_K N' \rightarrow N'$ is an isomorphism onto N' . We have a translation isomorphism:*

$$\text{Gal}(N'/K') \simeq \text{Gal}(N/K)$$

Let K be a field and Ω_K^s a separably closed extension of K with infinite separant transcendent degree over K . Let Γ be the automorphism group of Ω_K^s which consists of all the automorphisms of Ω_K^s fixing K . A transcendent extension separably closed over K is said to be LGalois extension of K and its K -automorphism group LGalois group. Let $\text{LGal}(\Omega_K^s/K)$ be LGalois group. One equips Ω_K^s with discrete topology and the set $(\Omega_K^s)^{\Omega_K^s}$ of mappings from Ω_K^s to itself with product topology, topology of simple convergence in Ω_K^s .

Let $x_1, \dots, x_n$ be separant transcendent elements over K for Ω_K^s and $K(x_1, \dots, x_n)$ a pure transcendent extension of K . Let Λ be the set of subextension of Ω_K^s such that they are extensions of finite type over K , say, $K(x_1, \dots, x_n)$. For $\sigma \in \Gamma$ and $E \in \Lambda$, $U_E(\sigma)$ denotes the set of $\tau \in \Gamma$ which has the same restriction on E that σ has. Thus $U_E(\sigma)_{E \in \Lambda}$ forms a base of filter of neighbourhood of $\sigma \in \Gamma$. Let A be a part of Γ . A is open if and only if for any $\sigma \in A$ there exists an $E \in \Lambda$ such that $U_E(\sigma) \subseteq A$. The algebraic closure $\bar{A}$ of A consists of $\sigma \in \Gamma$ such that for any field $E \in \Lambda$ in the algebraic closure of the A -invariant field $((\Omega_K^s)^A)$ in Ω_K^s , there exists $\tau \in A$ such that $\tau \in U_E(\sigma)$. Hence the invariant fields of A and $\bar{A}$ are to be identified. Note that the algebraic closure of A and the maximal fixed group of $((\Omega_K^s)^A)$ are identical. Let ϵ be the unit of Γ . Let Λ' be the set of LGalois subextension of Ω_K^s of finite type over K . The set Λ' is cofinal in Λ and the family of $(U_E(\epsilon))_{E \in \Lambda'}$ is a base of filter of neighbourhood of ϵ in Γ . For $E \in \Lambda'$, the set $U_E(\epsilon)$ is the kernel of the restriction homomorphism $\text{LGal}(\Omega_K^s/K) \rightarrow \text{LGal}(E/K)$:

$$1 \rightarrow U_E(\epsilon) \rightarrow \text{LGal}(\Omega_K^s/K) \rightarrow \text{LGal}(E/K) \rightarrow 1$$

One has $U_E(\sigma) = \sigma U_E(\epsilon) = U_E(\epsilon)\sigma$ for $\sigma \in \Gamma$ and $E \in \Lambda'$. Since $U_E(\epsilon)$ is a normal subgroup of Γ for every $E \in \Lambda'$ and since the family $(U_E(\epsilon))_{E \in \Lambda'}$ is a base of neighbourhood of ϵ , the topology of Γ is compatible with the structure of group. In other words, $(\sigma, \tau) \rightarrow \sigma\tau^{-1}$ of $\Gamma \times \Gamma \rightarrow \Gamma$ is continuous. If $\tau \in \cap_{E \in \Lambda} U_E(\sigma)$ and if there exists $x \in \Omega_K^s$ such that $\sigma(x) \neq \tau(x)$, then there exists $E \in \Lambda$ such that $\sigma(x) \neq \tau(x)$ for $x \in E$. Note that we should have defined a concept analogous with quasi-Galois.

Proposition 1.5. $\cap_{E \in \Lambda} U_E(\sigma) = \{\sigma\}$ *The topology is separated.*

Each fibre of the projection of the graph

$$\Gamma \subset (\Omega_K^s)^{\Omega_K^s}$$

is Ω_K^s . If u is adherent to Γ , then for each couple (x, y) of Ω_K^s , there exists $\sigma \in \Gamma$ such that

$$u(x) = \sigma(x) \quad u(y) = \sigma(y) \quad u(x+y) = \sigma(x+y) \quad u(xy) = \sigma(xy)$$

Since σ is a homomorphism, one has

$$u(x+y) = u(x) + u(y), \quad u(xy) = u(x)u(y)$$

On the same argument, $u(x) = x$ for $x \in K$. Hence u is a homomorphism and Ω_K^s is separably closed over K . Thus u is a K -automorphism of Ω_K^s , so $u \in \Gamma$. Hence Γ is closed in $(\Omega_K^s)^{\Omega_K^s}$. Note that every field is the increasing filtrant union of the subfields of finite type over the prime field. Recall the following proposition.

Proposition 1.6. *Let E be an extension of a field K and B a base of transcendence of E over K . E is of finite type over K if and only if B is finite and the degree $[E : K(B)]$ is finite.*

Let L be a LGalois extension of K and L_i an increasing filtrant family of subextensions of L . Assume L_i are LGalois extensions of K and assume $L = \cup_i L_i$. For each $i \in I$ Γ_i denotes LGalois group $\text{LGal}(L_i/K)$. For $i < j$ in I one has $L_i \subset L_j$ and one has the restriction

$$\phi_{ij} : \Gamma_j \rightarrow \Gamma_i$$

which are continuous homomorphisms. The family (Γ_i, ϕ_{ij}) is a projective system of topological groups.

$$\begin{array}{ccc} & \Gamma & \\ \lambda_i \swarrow & & \searrow \lambda_j \\ \Gamma_i & \xleftarrow{\phi_{ij}} & \Gamma_j \end{array}$$

Here (λ_i) is a family of continuous homomorphisms. There exists a homomorphism $\lambda : \Gamma \rightarrow \lim_i \Gamma_i$ by definition of projective limit. Let $u = (u_i)_{i \in I}$ be an element of $\lim_i \Gamma_i$. For $i \in I$ u_i is a K -automorphism of L_i and u_i is the restriction of u_j to L_i for $i < j$. Since $L = \cup_i L_i$, there exists a unique element $\sigma \in \Gamma$ such that $\sigma(x) = u_i(x)$ for $x \in L_i$. Thus λ is a bijection. We say an LGal group is a pro-Cremona group.

Proposition 1.7.

$$\Gamma \simeq \lim_i \Gamma_i$$

Fundamental Theorem of LGalois theory:

Theorem 1.6. *Let L be a LGalois extension of K and Γ its LGalois group. Let $\mathcal{K}$ be the set of subextensions E of L such that L/E are separable and $\mathcal{G}$ the set of closed subgroup of Γ . For each subgroup $\Delta \in \mathcal{G}$, $k(\Delta)$ denotes the invariant field of L by Δ and for $E \in \mathcal{K}$ $g(E)$ denotes the group of E -automorphism of L . Then $\Delta \rightarrow k(\Delta)$ is a bijection of $\mathcal{G}$ to $\mathcal{K}$. $E \rightarrow g(E)$ is an inverse bijection of $\mathcal{K}$ to $\mathcal{G}$. For $E \in \mathcal{K}$, $\text{LGal}(L/E)$ is an algebraically closed subgroup of $\text{LGal}(L/K)$ with an induced topology. For a subgroup Δ of Γ , Let E be the invariant field of Δ . Then the LGalois group of E is the closure of Δ in Γ . Let $\mathcal{M}$ be the set of subextensions of L such that if $u : E \simeq E'$ then transcendent degrees of L over E and E' should be the same. Let $E, F \in \mathcal{M}$.*

$$\text{Hom}_K^{\text{sep}}(E, F) \simeq \text{Hom}^{\text{al.close inc}}_{\text{LGal}(L/K)}(\text{LGal}(L/F), \text{LGal}(L/E))$$

where the left homomorphisms are field separable injections and the right homomorphism are continuous algebraically closed inclusions. Note that we consider an fixed algebraically closed field containing all fields in the category of fields and on the other hand an fixed topological group LGalois group containing all topological group LGalois groups in the category of LGalois groups. In $\text{Hom}_K^{\text{sep}}(E, F)$, E is to be abstract, in $\text{Hom}^{\text{al.close inc}}_{\text{LGal}(L/K)}(\text{LGal}(L/F), \text{LGal}(L/E))$ $\text{LGal}(L/E)$ is to be abstract.

Proof. Let a field $E \in \mathcal{K}$. When $[L : E] < \infty$, it comes from usual Galois theory, we assume $[L : E] = \infty$. Let $G_E = g(E)$ be the algebraic closure of a subgroup of Γ which makes E invariant and E' the fixed field by G_E . Clearly, $E \subseteq E'$. Let L_E be the algebraic closure of E in L and $G_E^{L_E}$ the restriction of G_E on L_E . Note that $\text{rest} : G_E \rightarrow G_E^{L_E}$ is surjective. In L_E we have $E = E'|_{L_E}$ by virtue of Galois theory. If E' is algebraic over E , $E'|_{L_E} = E'$. If E' is not algebraic over E , then there exists transcendent elements in E' over E . However, they are not invariant by the definition of LGalois group. Thus $E' = E$. Next let Δ be a group in $\mathcal{G}$ and $k(\Delta)$ the fixed field by Δ . Let $G = g(k(\Delta))$ be the algebraic closure of the group which makes $k(\Delta)$ invariant. Δ is contained in G . Since Δ is closed, $\Delta = G$.

We show the last statement. Given an extension F of E in $\mathcal{M}$, there exists an injection

$$\mathrm{LGal}(L/F) \rightarrow \mathrm{LGal}(L/E)$$

Conversely, given

$$u : \mathrm{LGal}(L/F) \rightarrow \mathrm{LGal}(L/E)$$

one has a closed subgroup $u(\mathrm{LGal}(L/F))$ in $\mathrm{LGal}(L/E)$. Hence one has an invariant field F' of $u(\mathrm{LGal}(L/F))$. There exists an isomorphism $u^* : F' \rightarrow F$ since LGal groups are isomorphic. By hypothesis, u^* can be extended to a K -automorphism $v^* : L \rightarrow L$. Hence for $x \in F'$ one has $\sigma(v^*(x)) = v^*(x)$ for $\sigma \in \mathrm{LGal}(L/F)$. Thus $\sigma \rightarrow (v^*)^{-1}\sigma v^*$ gives u . Hence one has

$$F \xrightarrow{(v^*)^{-1}} F' \xrightarrow{\text{inc}} E$$

If F and F' do not have the same equipotents of any separant transcendent bases over K , $\mathrm{LGal}(L/F)$ and $\mathrm{LGal}(L/F')$ are not isomorphic since a transcendent element has conjugates as all transcendent elements of L over K , the set of which is equipotent to that of L . Thus F and F' have separant transcendent bases A and B which are equipotent. Since $K(A)$ and $K(B)$ are isomorphic, the separable closures of them are also isomorphic. Hence the isomorphism of $\mathrm{LGal}(L/F)$ and $\mathrm{LGal}(L/F')$ induces that of their absolute Galois groups $\mathrm{Gal}(\bar{F}^s/F)$ and $\mathrm{Gal}(\bar{F}'^s/F')$. Hence F and F' are isomorphic. $\square$

The category whose objects are subfields of a fixed separably closed field of a ground field such that it is separable over each subfield and whose morphisms are separable inclusions is equivalent to the category whose objects are algebraically closed subgroups of an automorphism group of a fixed separably closed field over a ground field and whose morphisms are inclusions.

Let K be a field and Ω_K^s a separably closed extension of K with infinite transcendental degree over K . Let Γ be the automorphism group of Ω_K^s which consists of all the automorphisms of Ω_K^s fixing K .

Let $\mathrm{LGal}(\Omega_K^s/K)$ be LGal group.

Let $K(X)$, $K(Y)$ be function fields separable over K and $\mathrm{LGal}(\Omega_K^s/K(X))$ $\mathrm{LGal}(\Omega_K^s/K(X))$ LGal groups.

Let $\sigma \in \mathrm{LGal}(\Omega_K^s/K(X))$ and $u : K(Y) \rightarrow K(X)$ an isomorphism over K . Then there exists an automorphism $v : \Omega_K^s \rightarrow \Omega_K^s$ which extends u . Then

$$\begin{array}{ccc} \Omega_K^s & \xrightarrow{v} & \Omega_K^s \\ \uparrow & & \uparrow \\ K(Y) & \xrightarrow{u} & K(X) \\ \sigma(u(x)) & = & u(x) \\ \mathrm{LGal}(\Omega_K^s/K(X)) & \longrightarrow & \mathrm{LGal}(\Omega_K^s/K(Y)) \end{array}$$

$$\begin{array}{ccc} \sigma & \longrightarrow & v^{-1}\sigma v \\ \Omega_K^s & \xrightarrow{v} & \Omega_K^s \\ \uparrow & & \uparrow \\ K(Y) & \xrightarrow{u} & K(X) \\ \uparrow & & \uparrow \\ K(Y) & \xrightarrow{u} & K(X) \end{array}$$

Let $K(\bar{X})^s$ be the separable closure of $K(X)$ in Ω_K^s . There exists a surjective homomorphism restriction

$$\mathrm{LGal}(\Omega_K^s/K(X)) \rightarrow \mathrm{Gal}(\overline{K(X)}^s/K(X))$$

Given a homomorphism $K(Y) \subset K(X)$ between separable function fields over K , we have the commutative square

$$\begin{array}{ccccc}
\mathrm{LGal}(\Omega_K^s/K(X)) & \xrightarrow{\text{inflation}} & \mathrm{LGal}(\Omega_K^s/K(Y)) & & \\
\downarrow \text{restriction} & & \downarrow \text{restriction} & & \\
\mathrm{Gal}(\overline{K(X)}^s/K(X)) & \longrightarrow & \mathrm{Gal}(\overline{K(Y)}^s/K(Y)) & & \\
\downarrow \text{restriction} & \nearrow \text{inflation} & & & \\
\mathrm{Gal}(\overline{K(Y)}^s/K(X) \cap \overline{K(Y)}^s) & & & & \\
& & \mathrm{LGal}(\Omega_K^s/\overline{K(S)}^s(Y_{\bar{\eta}})) \longrightarrow \mathrm{Gal}(\overline{K(S)}^s(Y_{\bar{\eta}})/\overline{K(S)}^s(Y_{\bar{\eta}})) & & \\
& & \downarrow & & \downarrow \\
\mathrm{LGal}(\Omega_K^s/K(X)) \xrightarrow{\text{inflation}} \mathrm{LGal}(\Omega_K^s/K(Y)) & \longrightarrow & \mathrm{Gal}(\overline{K(Y)}^s/K(Y)) & & \\
& \searrow & \downarrow & & \\
& & \mathrm{LGal}(\Omega_K^s/K(S)) \longrightarrow \mathrm{Gal}(\overline{K(S)}^s/K(S)) & & \\
& & \downarrow & & \\
& & \mathrm{Gal}(\overline{K(S)}^s/K(S)) & &
\end{array}$$

Note that $K(S) = \overline{K(S)}^s \cap K(Y)$ and that

$$\mathrm{Gal}(\overline{K(Y)}^s/K(Y)) \xrightarrow{\text{restriction}} \mathrm{Gal}(\overline{K(S)}^s/K(S)).$$

There exists a commutative square such that the vertical left side automorphism $\sigma \mapsto v^{-1}\sigma v$ gives the vertical automorphism of affine schemes:

$$\begin{array}{ccc}
\mathrm{LGal}(\Omega_K^s/\overline{K(S)}^s(Y_{\bar{\eta}})) & \longrightarrow & \mathrm{Spec}(\overline{K(S)}^s(Y_{\bar{\eta}})) \\
\downarrow \simeq & & \downarrow \simeq \\
\mathrm{LGal}(\Omega_K^s/\overline{K(S)}^s(Y_{\bar{\eta}})) & \longrightarrow & \mathrm{Spec}(\overline{K(S)}^s(Y_{\bar{\eta}}))
\end{array}$$

Choose a lifting of the left side vertical automorphism $\sigma \mapsto u^{-1}\sigma u$ to give an automorphism of vertical middle terms $\sigma \mapsto v^{-1}\sigma v$:

$$\begin{array}{ccccc}
\mathrm{Gal}(\overline{K(S)}^s/K(S)) & \longrightarrow & \mathrm{LGal}(\Omega_K^s/\overline{K(S)}^s(Y_{\bar{\eta}})) & \longrightarrow & \mathrm{Spec}(\overline{K(S)}^s(Y_{\bar{\eta}})) \\
\downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq \\
\mathrm{Gal}(\overline{K(S)}^s/K(S)) & \longrightarrow & \mathrm{LGal}(\Omega_K^s/\overline{K(S)}^s(Y_{\bar{\eta}})) & \longrightarrow & \mathrm{Spec}(\overline{K(S)}^s(Y_{\bar{\eta}}))
\end{array}$$

V.66 corollary 6. v.69 corollary 2([B1])

Proposition 1.8. *Let N be a Galois extension of K , E_1 and E_2 two subextension of N and Γ_1 and Γ_2 the Galois groups of N over E_1 and E_2 , respectively. The following conditions are equivalent:*

1. $\Gamma = \text{Gal}(L/K)$ is a direct product of Γ_1 and Γ_2 .
2. The extensions of E_1 and E_2 are Galois over K and one has $E_1 \cap E_2 = K$,

$$K(E_1 \cup E_2) = N$$

The canonical homomorphism

$$E_1 \otimes_K E_2 \rightarrow N$$

is an isomorphism.

And apply faithful flat descent. v.70 lemme3

Proposition 1.9. *Let A be a K -algebra, M_1 and M_2 two A -module of finite rank over K . Suppose that there exists an extension L of K such that the modules $L \otimes_K M_1$ and $L \otimes_K M_2$ over $L \otimes_K A$ are an isomorphism. Then the modules M_1 and M_2 are an isomorphism.*

v.14 proposition 7([B1])

Proposition 1.10. *Let E and F be two extensions of K in an algebraically closed field Ω over K . If E and F are linearly disjoint over K , every subextension of E and every subextension of F are linearly disjoint over K .*

In case K is algebraically closed;

If

$$\text{Gal}(\overline{K(Y)}/K(Y)) = \text{Gal}(\overline{K(S)}/K(S)) \times \text{Gamma}$$

where Gamma is a group. then one has the following statements applying the proposition above, replacing $K = K(Y)$, $E_1 = K(Y)(\overline{K(S)})$, $E_2 = K(Y)(\overline{K(Y_{\bar{\eta}})})$.

$$K(Y) = K(S, Y_{\bar{\eta}})$$

$$K(Y)(\overline{K(S)}) \cap K(Y)(\overline{K(Y_{\bar{\eta}})}) = K(Y)$$

$$K(Y)(\overline{K(S)}) \cup K(Y)(\overline{K(Y_{\bar{\eta}})}) = \overline{K(Y)}$$

$$\overline{K(Y)} = E_1 \otimes_{K(Y)} E_2$$

Hence E_1 and E_2 are linearly disjoint over $K(Y)$. Thus $K(Y)(Y_{\bar{\eta}})$ and $K(Y)(S)$ are linearly disjoint over $K(Y)$. Therefore, $K(Y_{\bar{\eta}})$ and $K(S)$ are linearly disjoint over K by faithful flat descentness. One has

$$K(Y) = K(S) \otimes_K K(Y_{\bar{\eta}})$$

Translation diagramm:

$$\begin{array}{ccccc}
\overline{K(Y_{\bar{\eta}})} & \xrightarrow{v} & K(Y)(\overline{K(Y_{\bar{\eta}})}) & \longrightarrow & \overline{K(Y)} \\
\uparrow & & \uparrow & & \uparrow \\
K(Y_{\bar{\eta}}) & \xrightarrow{u} & K(Y) & \longrightarrow & K(Y)(\overline{K(S)}) \\
\uparrow & & \uparrow u' & & \uparrow w \\
K & \longrightarrow & K(S) & \longrightarrow & \overline{K(S)}
\end{array}$$

Since

$$v^{-1}K(Y) = K(Y_{\bar{\eta}}), \quad w^{-1}K(Y) = K(S)$$

one has

$$\text{Gal}(/K(Y_{\bar{\eta}})) \simeq \text{Gal}(N/E_2)$$

$$\text{Gal}(/K(S)) \simeq \text{Gal}(N/E_1)$$

Given a group G with identity element e , a subgroup H , and a normal subgroup $N \triangleleft G$; then the following statements are equivalent:

1. G is the product of subgroups, $G = NH$, where the subgroups have trivial intersection, $N \cap H = \{e\}$.
2. For every $g \in G$, there are unique $n \in N$ and $h \in H$, such that $g = nh$.
3. For every $g \in G$, there are unique $h \in H$ and $n \in N$, such that $g = hn$.
4. The natural embedding $i : H \rightarrow G$ and the natural projection $\pi : G \rightarrow G/N$ composed, $\pi \circ i$, is an isomorphism between H and the quotient group G/N .
5. There exists a homomorphism $G \rightarrow H$ that is the identity on H and whose kernel is N .

If these statements hold, we define G to be a semidirect product of N and H , written $G = N \rtimes H$

$$(n_1 h_1)(n_2 h_2) = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = (n_1 n_2^{h_1} h_1 h_2)$$

Here

$$H \rightarrow \text{Aut}(N) : n \mapsto h n h^{-1} = n^h$$

SGA1 203 corollary 1.7

Proposition 1.11. *Let K be an algebraically closed field, X and Y two connected schemes over K . Suppose that X is proper over K and that Y is locally noetherian. Let a and b be geometric points of X and Y with values the same algebraically closed extension of K , the geometric point of $c = (a, b)$ of $X \times_K Y$. The homomorphism $\pi_1(X \times_K Y, c) \rightarrow \pi_1(X, a) \times \pi_1(Y, b)$ is induced by the homomorphisms on the fundamental groups associated to two projections $X \times_K Y \rightarrow X$ and $X \times_K Y \rightarrow Y$ and this homomorphism is an isomorphism.*

Let K be an algebraically closed field, X_0 and S varieties over K . Let $X = X_0 \times_K S$. Then $K(X) = K(X_0) \otimes_K K(S)$. Thus $K(X_0)$ and $K(S)$ are linearly disjoint over K . Therefore every set of separable algebraic elements over $K(X_0)$ and every set of separable algebraic elements over $K(S)$ are linearly disjoint over K .

1. The two extensions are Galois;

$$K(X) \left(\overline{K(S)}^s \right) / K(X)(S)$$

$$K(X) \left(\overline{K(X_0)}^s \right) / K(X)(X_0)$$

- 2.

$$K(X) \left(\overline{K(X_0)}^s \right) \cap K(X) \left(\overline{K(S)}^s \right) = K(X)$$

- 3.

$$K(X) \left(\overline{K(X_0)}^s \cup \overline{K(S)}^s \right) = \overline{K(X)}$$

Translation diagramm:

$$\begin{array}{ccccc}
\overline{K(X_0)}^s & \xrightarrow{v} & K(X)(\overline{K(X_0)}^s) & \longrightarrow & \overline{K(X)}^s \\
\uparrow & & \uparrow & & \uparrow \\
K(X_0) & \xrightarrow{u} & K(X) & \longrightarrow & K(X)(\overline{K(S)}^s) \\
\uparrow & & \uparrow u' & & \uparrow w \\
K & \longrightarrow & K(S) & \longrightarrow & \overline{K(S)}^s
\end{array}$$

Thus

$$\mathrm{Gal}(\overline{K(X)}^s/K(X)) \simeq \mathrm{Gal}(\overline{K(X_0)}^s/K(X_0)) \times \mathrm{Gal}(\overline{K(S)}^s/K(S))$$

$\mathrm{LGal}(\Omega_K^s/K(X))$ has a normal subgroup $\mathrm{Gal}(\overline{K(X)}^s/K(X))$. If $\mathrm{Gal}(\overline{K(X)}^s/K(X))$ is a direct product $\mathrm{Gal}(\overline{K(X_0)}^s/K(X_0)) \times \mathrm{Gal}(\overline{K(S)}^s/K(S))$, then $\mathrm{LGal}(\omega_K^s/K(X))$ is also a direct product $\mathrm{LGal}(\overline{K(X_0)}^s/K(X_0)) \times \mathrm{Gal}(\overline{K(S)}^s/K(S))$. Indeed, if it is not a direct product, it would be a proper semi-direct product. And $\mathrm{Gal}(\overline{K(S)}^s/K(S))$ would non trivially act on $\mathrm{Gal}(\overline{K(X_0)}^s/K(X_0))$. However it is a direct product $\mathrm{Gal}(\overline{K(X_0)}^s/K(X_0)) \times \mathrm{Gal}(\overline{K(S)}^s/K(S))$. The action is trivial. Hence $\mathrm{LGal}(\Omega_K^s/K(X))$ is a direct product.

Theorem 1.7. (*K.Ueno Conjecture*) Let K be an algebraically closed field, S a variety over K , X and Y two varieties over S . Suppose $X = X_0 \times_K S$ and $f : X \rightarrow Y$ a separable dominant rational map over S and that the general generic fibre $Y_{\bar{\eta}}$ of Y/S is a variety of κ non negative. Then $\mathrm{var}(Y/S) = 0$.

Proof. By hypothesis the homomorphism of absolute Galois groups associated to the field homomorphism of the dominant rational map between the rational function fields of X and Y over S

$$\mathrm{Gal}(\overline{K(X)}^s/K(X)) \rightarrow \mathrm{Gal}(\overline{K(Y)}^s/K(Y))$$

over $\mathrm{Gal}(\overline{K(S)}^s/K(S))$ gives a pro-finite group section of $\mathrm{Gal}(\overline{K(Y)}^s/K(Y))$ over $\mathrm{Gal}(\overline{K(S)}^s/K(S))$. Next we consider the cartesian square

$$\begin{array}{ccc}
\mathrm{Gal}(\overline{K(Y)}^s/K(Y)) & \longleftarrow & G \\
\downarrow & & \downarrow \\
\mathrm{Gal}(\overline{K(S)}^s/K(S)) & \longleftarrow & 1
\end{array}$$

G is the pullback of $\mathrm{Gal}(\overline{K(Y)}^s/K(Y))$ along the homomorphism $1 \rightarrow \mathrm{Gal}(\overline{K(S)}^s/K(S))$. G is identified to be a normal subgroup of $\mathrm{Gal}(\overline{K(Y)}^s/K(Y))$. The topological group homomorphism $\mathrm{Gal}(\overline{K(Y)}^s/K(Y)) \rightarrow \mathrm{Gal}(\overline{K(S)}^s/K(S))$ is surjective since Y/S is a connected morphism, $K(S)$ is algebraically closed in $K(Y)$. By hypothesis, this surjection has a topological homomorphic section. Thus the topological group $\mathrm{Gal}(\overline{K(Y)}^s/K(Y))$ is a semi-direct product of G with an image of the section σ of $\mathrm{Gal}(\overline{K(S)}^s/K(S))$. Let (g, s) be a couple of elements where g is in G and s is in $\sigma(\mathrm{Gal}(\overline{K(S)}^s/K(S)))$. The product is as follows

$$g_1 s_1 g_2 s_2 = g_1 s_1 g_2 s_1^{-1} s_1 s_2 = g_1 g_2^{s_1} s_1 s_2$$

Hence

$$g \mapsto g^s$$

is a bi-continuous topological automorphism of G . Therefore it comes from an automorphism of $\text{Spec}K(Y_{\bar{\eta}})$. We have a homomorphism of topological groups.

$$\sigma(\text{Gal}(\overline{K(S)})^s / K(S)) \rightarrow \text{AutSpec}K(Y_{\bar{\eta}})$$

The automorphism group of $\text{Spec}K(Y_{\bar{\eta}})$ has an abelian variety as a neutral component. The factor group by a neutral component is a discrete group with countable cardinality. Replacing S by a K -variety S' which comes from a generically finite morphism $S' \rightarrow S$, $\sigma(\text{Gal}(\overline{K(S')})^s / K(S'))$ becomes small enough. Then one has a representation

$$\sigma(\text{Gal}(\overline{K(S')})^s / K(S')) \rightarrow \text{Aut}^0 \text{Spec}K(Y_{\bar{\eta}})$$

which has a compact profinite subgroup of an abelian variety. Thus it is a finite group. Replacing S' by S'' again, we have a trivial representation

$$\sigma(\text{Gal}(\overline{K(S'')})^s / K(S'')) \rightarrow \text{Aut}^0 \text{Spec}K(Y_{\bar{\eta}})$$

Thus

$$\text{Gal}(\overline{K(Y'')})^s / K(Y'') = G \times \sigma(\text{Gal}(\overline{K(S'')})^s / K(S''))$$

where $Y'' = Y(S'')$. Hence Y'' is birationally isomorphic to a product $S'' \times_K Y_{\bar{\eta}}$. □

In case K is not algebraically closed.

Consider the exact sequence

$$1 \rightarrow \Gamma_{\bar{S}} \rightarrow \text{Gal}(\overline{K(\bar{S})})^s / K(S) \rightarrow \text{Gal}(\overline{K})^s / K \rightarrow 1$$

One has the exact sequence

$$1 \rightarrow H^1(\text{Gal}(\overline{K})^s / K, (G \rightarrow \text{Aut}(G))) \rightarrow H^1(\text{Gal}(\overline{K(\bar{S})})^s / K(S), (G \rightarrow \text{Aut}(G))) \rightarrow H^1(\Gamma_{\bar{S}}, (G \rightarrow \text{Aut}(G))) \rightarrow$$

We have an extension to be considered in the midterm which sends to the right term where it is a neutral element. Thus we find an extension in the right term where we denote it by F . Pulling back it we have a desired extension in the middle term where it represents a fibre product

$$\begin{array}{ccccc} F & \longleftarrow & F \times_K S \simeq Y & \longleftarrow & Y_0 \times_{\bar{K}} \bar{S} \\ \downarrow & & \downarrow & & \downarrow \\ K & \longleftarrow & S & \longleftarrow & \bar{S} \end{array}$$

If the center of the profinite group G is free, we can explain it explicitly. We have the exact sequence

$$1 \rightarrow H^1(\Gamma_K, \text{Out}(G)) \rightarrow H^1(\text{Gal}(\overline{K(\bar{S})})^s / K(S), \text{Out}(G)) \rightarrow H^1(\Gamma_{\bar{S}}, \text{Out}(G)) \rightarrow$$

where the extension associated to a fibre Y/S is in the middle term cohomology which vanishes in the right hand

cohomology to give rise to an extension in the right hand cohomology:

$$\begin{array}{ccc}
 & & 1 \\
 & & \downarrow \\
 & & G \\
 & & \downarrow \\
 & & \text{Aut}(G) \\
 & & \downarrow \\
 & & \text{Out}(G) \\
 & & \downarrow \\
 & & 1 \\
 \\
 1 & \downarrow & \\
 \text{Gal}(\overline{K(S_{\bar{K}})}^s / K(S_{\bar{K}})) & \searrow & \text{Aut}(G) \\
 \downarrow & & \downarrow \\
 \text{Gal}(\overline{K(S)}^s / K(S)) & \longrightarrow & \text{Out}(G) \\
 \downarrow & \nearrow & \downarrow \\
 \text{Gal}(\overline{K}^s / K) & & 1 \\
 \downarrow & & \\
 1 & &
 \end{array}$$

It is a universal exact sequence:

$$1 \rightarrow G \rightarrow \text{Aut}(G) \rightarrow \text{Out}(G) \rightarrow 1$$

We have an extension of profinite groups over Γ_K by

$$\begin{array}{ccc}
 1 & & 1 \\
 \downarrow & & \downarrow \\
 G & \longrightarrow & G \\
 \downarrow & & \downarrow \\
 \text{Aut}(G) \times_{\text{Out}(G)} \text{Gal}(\overline{K}^s / K) & \longrightarrow & \text{Aut}(G) \\
 \downarrow & & \downarrow \\
 \text{Gal}(\overline{K}^s / K) & \longrightarrow & \text{Out}(G) \\
 \downarrow & & \downarrow \\
 1 & & 1
 \end{array}$$

, which is associated to a variety F/K . Then

$$\begin{array}{ccccc}
1 & & & & 1 \\
\downarrow & & & & \downarrow \\
G & \xrightarrow{\quad\quad\quad} & G & & \\
\downarrow & & \downarrow & & \\
\text{Aut}(G) \times_{\text{Out}(G)} \text{Gal}(\overline{K(S)}^s / K(S)) & \xrightarrow{\quad\quad\quad} & \text{Aut}(G) & & \\
\downarrow & & \downarrow & & \\
\text{Gal}(\overline{K(S)}^s / K(S)) & \xrightarrow{\quad\quad\quad} & \text{Gal}(\overline{K}^s / K) & \longrightarrow & \text{Out}(G) \\
\downarrow & & & & \downarrow \\
1 & & & & 1
\end{array}$$

$\text{Aut}(G) \times_{\text{Out}(G)} \text{Gal}(\overline{K(S)}^s / K(S))$ is associated to a variety $F \times_K S$, which is originally a given variety Y .

Note: 81 EGA IV 2 Let X, Y be schemes over a field k and K/K' an extension over k . We have injections.

$$\text{Hom}_{K'}(X_{K'}, Y_{K'}) \rightarrow \text{Hom}_K(X_K, Y_K)$$

$$\text{Aut}_{K'}(X_{K'}) \rightarrow \text{Aut}_K(X_K)$$

For example let $\mathbb{Q}$ be the natural rational field and $\mathbb{C}$ the field of the complex numbers. Then the lattice of the closed subgroups of the topological group $\text{Aut}_{\mathbb{Q}}(\mathbb{C})$ determines the intermediate fields between $\mathbb{Q}$ and $\mathbb{C}$. Consider all the function fields of the complex varieties and arithmetic varieties. They are all contained in $\mathbb{C}$.

In case that given function fields of varieties in the intermediate fields, we make use of a strategy for LGalois theory. For example consider the next theorem again:

Theorem 1.8. (*K.Ueno Conjecture*) Let K be an algebraically closed field, S a variety over K , X and Y two varieties over S . Suppose $X = X_0 \times_K S$ and $f : X \rightarrow Y$ a separable dominant rational map over S and that the general generic fibre $Y_{\bar{\eta}}$ of Y/S is a variety of κ non negative. Then $\text{var}(Y/S) = 0$.

Proof. Let Γ be the absolute Galois group of the function field of S and G the absolute LGalois group of the function field of the general generic fibre $Y_{\bar{\eta}}$ of Y/S . Then the automorphism group of $Y_{\bar{\eta}}$ of Y/S is contained in the automorphism group of the absolute LGalois group with section over Γ . Hence we have the next diagram:

$$H^1(\Gamma, \text{Aut}_{\Gamma}(G)) \longrightarrow H^1(\Gamma, (G \rightarrow \text{Aut}_{\Gamma}(G)))$$

After changing Γ , the distinguished element of $H^1(\Gamma, \text{Aut}_{\Gamma}(G))$ vanishes by the repeated argument and so the image of the element in $H^1(\Gamma, (G \rightarrow \text{Aut}_{\Gamma}(G)))$ vanishes too. Hence we obtain the conclusion. $\square$

This plays an essential role for the proof of Iitaka-Viehweg conjecture. Furthermore, we have an Iitaka-Viehweg formula:

$$\kappa(X) \geq \kappa(X_{\bar{\eta}}) + \kappa(S)$$

$$\kappa(\omega_{X/S}) \geq \kappa(X_{\bar{\eta}}) + \text{var}(X/S)$$

for a separable fibre space X/S .

We shall enlarge the concept of LGalois groups of an algebraic field over a field to the automorphism groups between formally smooth (resp. smooth) morphisms of schemes and obtain the concept of (resp. non commutative) schemes in point of view of topological groups by patching. We shall obtain an analogue of Kodaira-Spencer(resp.Grauert) deformation theory for smooth schemes (resp. reduced algebraic spaces) and moreover for schemes of positive characteristics.

Definition 1.3. *Let k be a field, X a k -scheme and x a point of X . We say that X is geometrically reduced or separable at the point x over k if for any extension k' of k and any point x' of $X' = X \otimes_k k'$ over x X is reduced at x' , i.e., $\mathcal{O}_{X',x'}$ is reduced.*

2 Langlands Program

We refer to [G] in this section. Notation: K is an algebraic number field, i.e., $K/\mathbb{Q}$ is a finite field extension. We write v for a place of K , i.e., a representative of an equivalence class of non trivial valuations. A finite (non-Archimedean) valuation is written as $v < \infty$ and an infinite(Archimedean) valuation as $v \mid \infty$. We write P_∞ for the finite set of all infinite places of K and P for a finite subset of all places of K , which contains P_∞ . Furthermore we write K_v for the completion of K with respect to the valuation v . If the valuation v is discrete, then we write $\mathcal{O}_v$ for the valuation ring of K_v . We write $\mathfrak{m}_v$ for the maximal ideal of $\mathcal{O}_v$. If this is a principal ideal, then we write π_v for a uniformizing element. By fixing a suitable constant $C > 1$, there is a one-to-one identification of valuations and absolute values:

The valuation v is assigned the absolute value $|\cdot|_v$, which is defined as: $|x|_v := \begin{cases} C^{-v(x)} & , \text{ if } x \neq 0 \\ 0 & , \text{ if } x = 0 \end{cases} \quad \forall x \in K$.

Conversely, the absolute value $v_{|\cdot|}$, which is defined as: $v_{|\cdot|}(x) := -\log_C(|x|) \quad \forall x \in K^\times$.

Definition 2.1. *The set of the finite adeles of an algebraic number field K , named $\mathbb{A}_{K,fin}$, is defined as the restricted product of K_v concerning the $\mathcal{O}_v$, which means $\mathbb{A}_{K,fin} := \widehat{\prod_{v \nmid \infty}^{\mathcal{O}_v} K_v}$.*

This means, that the set of the finite adeles contains all $(x_v)_v \in \prod_{v \nmid \infty} K_v$, so that $x_v \in \mathcal{O}_v$ for almost all v . Addition and multiplication are defined component-wise. In this way $\mathbb{A}_{K,fin}$ is a ring. The topology is the restricted product topology. That means that the topology is generated by the so-called restricted open rectangles, which have the following form: $U = \prod_{v \in E} U_v \times \prod_{v \notin E} \mathcal{O}_v$, where E is a finite subset of the set of all places of K , containing P_∞ and $U_v \subset K_v$ is open. In the following, we will use the term finite adele ring of K as a synonym for $\mathbb{A}_{K,fin}$.

Definition 2.2. *The adele ring of an algebraic number field K , named $\mathbb{A}_K$, is defined as the product of the set of the finite adeles with the product of the completions at the infinite valuations. These are $\mathbb{R}$ or $\mathbb{C}$, their number is finite.*

That means $\mathbb{A}_K := \mathbb{A}_{K,fin} \times \prod_{v \mid \infty} K_v = \widehat{\prod_{v \nmid \infty}^{\mathcal{O}_v} K_v} \times \prod_{v \mid \infty} K_v$.

We define addition and multiplication component-wise. As a result, the adele ring is a ring. The elements of the adele ring are called adeles of K . In the following, we write $\mathbb{A}_K = \widehat{\prod_v K_v}$, although this is generally not a restricted product.

Given a vector space L over K , a general linear group $\mathrm{GL}_n(L)$ can act a vector space L^n . When L is the separably closure with infinite separant transcendent basis of K , an etale extension of L is L^n . Let A_K denote an adele of K . We have a representation

$$\mathrm{GL}_n(A_K) \rightarrow \mathrm{GL}_n(L) \rightarrow \mathrm{LGal}(L^n/K)$$

The Langlands correspondence in number theory is a conjectural correspondence between

1. n -dimensional complex linear representations of the Galois group $\mathrm{Gal}(\bar{K}/K)$ of a given number field K , and
2. The automorphic representations of a n -dimensional general linear group $\mathrm{GL}_n(\mathbf{A}_K)$ with coefficients in the ring of adeles of K , arising within the representations given by functions on the double coset space $\mathrm{GL}_n(K) \backslash \mathrm{GL}_n(\mathbf{A}_K) / \mathrm{GL}_n(\mathcal{O})$ where $\mathcal{O} = \prod_p \mathcal{O}_p$ is the ring of integers of all formal cmpletions of K .

Let G be a reductive algebraic group over a number field K and $\mathbf{A}$ denote the adeles of K . Let Z denote the center of G and let ω be a continuous unitary character from $Z(K) \backslash Z(\mathbf{A})^\times$ to $\mathbb{C}^\times$. Fix a Haar measure on $G(\mathbf{A})$ and $L_0^2(G(K) \backslash G(\mathbf{A}), \omega)$ denote the Hilbert space of measurable complex-valued function, f , on $G(\mathbf{A})$ satisfying

1.

$$f(\gamma g) = f(g) \text{ for all } \gamma \in G(K)$$

2.

$$f(gz) = f(g)\omega(Z) \text{ for all } z \in Z(\mathbf{A})$$

3.

$$\int_{Z(\mathbf{A})G(K) \backslash G(\mathbf{A})} |f(g)|^2 dg < \infty$$

4.

$$\int_{U(K) \backslash U(\mathbf{A})} f(ug) du = 0$$

This is called the space of cusp forms with central character ω on $G(\mathbf{A})$. A function occurring in such a space is called a cuspidal function. This space is a unitary representation of the group $G(\mathbf{A})$ where the action of $g \in G(\mathbf{A})$ on a cuspidal function ϕ is given

$$(R_0(g)\phi)(x) = \phi(xg)$$

for $x \in G(K) \backslash G(\mathbf{A})$. The space of cusp forms with center character ω decoposes into a direct sum of Hilbert spaces

$$L_0^2(G(K) \backslash G(\mathbf{A}), \omega) = \bigoplus_{(\pi, V_\pi)}^\wedge m_\pi V_\pi$$

where the sum runs over the irreducible subrepresentations of $L_0^2 G(K) \backslash G(\mathbf{A}), \omega$ and m_π are positive integers. A cuspidal represetation of $G(\mathbf{A})$ is such a subrepresentation (π, V) for some ω .

Conjecture 2.1. (Langlands) ([G]) Suppose E is a finite Galois extension of F with Galois group $G = \mathrm{Gal}(E/F)$ and $\sigma : G \rightarrow \mathrm{GL}_n(\mathbb{C})$ is an irreducible representation of G . Then there exists an automorphic cuspidal representation π_σ on GL_n over F such that

$$L(s, \pi_\sigma) = L(s, \sigma)$$

2.1 Artin L-functions

Note that the image of the absolute Galois group into a linear algebraic group is finite. So it suffices to consider a finite Galois extension of K in some sense. Suppose K is a number field and E is a finite Galois extension of K with Galois group $G = \text{Gal}(E/K)$. A representation of G is a homomorphism σ of G into $\text{GL}(V)$, the group of invertible linear transformations of a complex vector space of dimension n . Given a finite place $\mathcal{P}$ of K , we say a prime $\mathcal{B}$ of $\mathcal{O}_E$ lies over $\mathcal{P}$ if $\mathcal{B}$ appears in the factorization of $\mathcal{P}\mathcal{O}_E$ into prime ideals of $\mathcal{O}_E$. Given such a pair $\mathcal{B}/\mathcal{P}$, the following local objects are defined, each depending on $\mathcal{B}$ only up to conjugation in G :

1. The decomposition group $D_{\mathcal{B}} = \{g \in G : g(\mathcal{B}) = \mathcal{B}\}$;
2. The inertia group

$$I_{\mathcal{B}} = \{g \in D_{\mathcal{B}} : g(x) = x \bmod \mathcal{B} \text{ for all } x \in \mathcal{O}_E\};$$

3. The Frobenius automorphism $\text{Fr}_{\mathcal{B}}$ generating the cyclic group $D_{\mathcal{B}}/I_{\mathcal{B}} \simeq \text{Gal}(\mathcal{O}_E/\mathcal{B} : \mathcal{O}_K/\mathcal{P})$. When $I_{\mathcal{B}} = \{1\}$, we call $\mathcal{P}$ unramified in E . In this case, $\text{Fr}_{\mathcal{B}}$ represents a conjugacy class in G . Since almost all $\mathcal{P}$ are unramified in this sense and since knowledge of $\text{Fr}_{\mathcal{B}}$ completely determines the factorization type of such $\mathcal{P}$, it is natural to focus attention on these $\text{Fr}_{\mathcal{B}}$.

Returning to our representation $\sigma : G \rightarrow \text{GL}(V)$, let $V_{\mathcal{B}}$ denote the subspace of V formed by vectors invariant by $\sigma(I_{\mathcal{B}})$. Then $\sigma(\text{Fr}_{\mathcal{B}})$ is defined unambiguously on $V_{\mathcal{B}}$ and the Euler factor

$$L_{\mathcal{P}}(\sigma, s) = [\det(I - \sigma(\text{Fr}_{\mathcal{B}})(N\mathcal{P})^{-s})|_{V_{\mathcal{B}}}]^{-1}$$

depends only on $\mathcal{P}$, not $\mathcal{B}$ with $N\mathcal{P}$ the cardinality of the field $\mathcal{O}_E/\mathcal{P}$. Now we can define Artin's L-function attached to σ by the product

$$L(\sigma, s) = L_{E/K}(\sigma, s) = \prod_{\mathcal{P}} L_{\mathcal{P}}(\sigma, s)$$

convergent for $\text{Re}(s) > 1$.

2.2 Automorphic L-function

Proposition 2.1. *The functor from the category of étale schemes to the category of sets equipped with an action of the absolute Galois group is an equivalence of categories.*

$$\mathbf{Sch}_{et} \longrightarrow \text{Gal}(k_s/k) - \text{Set}$$

$$X \longrightarrow X(k_s)$$

Let K be an algebraic number field. Let G be an algebraic reduced étale group scheme over K . For any valuation v we have an isomorphism

$$\iota_v : \bar{K}_v \simeq \mathbb{C}$$

and an isomorphism

$$\text{Gal}([K]_{\bar{K}_v}/K) \simeq \text{Gal}([K]_{\bar{K}_w}/K) \simeq \text{Gal}([K]_{\mathbb{C}}/K)$$

for another valuation w . Note that $\text{Fr}_{\mathcal{B}} \in \text{Gal}([K]_{\mathbb{C}}/K)$. Given a representation

$$\sigma : \text{Gal}([K]_{\bar{K}_v})/K \rightarrow G(\mathbb{C}) \text{ with action of } \mathbb{C}$$

or equivalently

$$\sigma : \text{Gal}([K]_{\bar{K}_v})/K \rightarrow G([K]_{\bar{K}_v}) \text{ with action of } [K]_{\bar{K}_v}$$

one obtains a representation to a étale group scheme

$$\sigma : \text{Gal}([K]_{\bar{K}_v})/K \rightarrow G$$

and hence applying K_v

$$\sigma : \text{Gal}([K]_{\bar{K}_v})/K \rightarrow G(\bar{K}_v)$$

We infer that

$$\text{Fr}_v \in \text{Aut}_{\mathcal{O}_K}(\mathcal{O}_{K_v}) \rightarrow \sigma(\text{Fr}_v) \in G(\mathcal{O}_{K_v})$$

We begin with L-functions defined by local data but the function defined in this way is not easy to prove an analytic continuation, functional equation and the convergence. Given a positive integer N and a finite set of bad primes, let Ψ_p be a GL_N matrix for a prime $p \notin S$, where p is in the primes in a number field. Then we have an L-function attached to the local data $\{\Psi_p\}$ defined by

$$L(s, \{\Psi_p\}) = \prod_{p \notin S} \frac{1}{\det(1_N - p^{-s} \Psi_p)}$$

Note that it is sufficient for Ψ_p to be determined up to conjugacy classes. In the case of Riemann's zeta, the set S is void and $\Psi_p = 1$. In the case of Dirichlet L-functions for a Dirichlet character χ modulo F , we take $S = \{p : p|F\}$ and the local data at $p \notin S$ is $\Psi_p = \chi(p)$. To define automorphic L-functions, we give how to attach local data Ψ_p to an irreducible unitary representation π of a reductive adèle group $G(A_K)$ but it is independent of the fact π is automorphic. Since the local group G_v where v runs over primes of the algebraic number field K , are known to be Type I, any irreducible unitary representation π of $G(A_K)$ factors over primes into a completed restricted tensor product:

$$\pi \simeq \bigotimes_v^{\wedge'} \pi_v$$

where π_v is an irreducible unitary representation of G_v uniquely determined up to isomorphism. In particular, this factorization can apply to an irreducible unitary representation π_ϕ generated by a square integrable cusp form ϕ . Let K_v be a 'good' maximal compact subgroup of G . Recall that an irreducible unitary representation of G_v is a spherical representation if it has a non zero K_v -fixed vector, when there is a one dimensional space of K_v -fixed vectors in the representation space. Note that for all but finitely many primes v , the local representations π_v are spherical. Let the set S of bad primes be at least large enough to contain the finite set of primes v for which π_v is non spherical. Let G be a reductive linear group over an ultrametric local field k . Let P be a minimal parabolic subgroup of G with unipotent radical N and choice of Levi component of M . When $G = \text{GL}(n, \mathbb{Q}_p)$, P is upper triangle matrices, N is elements of P with 1's diagonal components and M the diagonal matrices. Let K be a 'good' maximal compact subgroup of G . Let $\mathcal{H}_{G,K}$ denote the spherical Hecke algebra defined as

$\mathcal{H}_{G,K}$ is the left and right K -invariant complex valued functions on G .

Endow G with a right Haar measure so that the measure of K is 1, which is also a left Haar measure. $\mathcal{H}_{G,K}$ is a convolution algebra with the convolution product

$$(\psi * \varphi)(g) = \int_G \psi(gh^{-1}) \varphi(h) dh$$

where dh is the Haar measure.

Elementary representation theory says that the isomorphism class of a spherical representation is completely determined by the representation of the spherical Hecke algebra on the one dimensional space of spherical vectors on the representation. Since the space of spherical vectors is just one dimensional, automorphisms are complex scalars. Hence to describe a spherical representation π is to describe a $\mathbb{C}$ -algebra homomorphism

$$\mathcal{H}_{G,K} \rightarrow \mathbb{C}$$

Let δ_P be the modular function of P . It means that for a right Haar measure μ_P on P we have

$$\mu_P(pE) = \mu_P(pEp^{-1}) = \delta_P(p) \cdot \mu_P(E)$$

for any $p \in P$ and measurable $E \subset P$. The Satake transform $S(\varphi)$ of a function $\varphi \in \mathcal{H}_{G,K}$ is defined by the integral formula

$$(S\varphi)(m) = \delta_P(m)^{-\frac{1}{2}} \int_N \varphi(nm) dn = \delta_P(m)^{-\frac{1}{2}} \int_N \varphi(mn) dn$$

dn denotes a Haar measure on N normalized so that

$$\text{characteristic function of } K \longrightarrow \text{characteristic function of } K \cap M$$

Let $\mathcal{H}_{M,K \cap M}$ be the spherical Hecke algebra of the reductive group M which is a fixed Levi component of the parabolic P . The Weyl group of M in G is

$$W = \text{the normalizer of } M \text{ in } G / \text{the centralizer of } M \text{ in } G$$

Satake's theorem says that the Satake transform S gives an isomorphism from the spherical Hecke algebra $\mathcal{H}_{G,K}$ of G to the Weyl group invariant elements $\mathcal{H}_{M,K \cap M}^W$ of the spherical Hecke algebra $\mathcal{H}_{M,K \cap M}$ of M . Now generally the spherical Hecke algebra $\mathcal{H}_{M,K \cap M}$ of M is of the form

$$\mathbb{C}[z_1, z_1^{-1}, z_2, z_2^{-1}, \dots, z_n, z_n^{-1}]$$

for indeterminates z_i , where n is the split rank of G . For example, the split rank of $\text{GL}(n, \mathbb{Q}_p)$ is n . Note that the spherical Hecke algebra of the Levi component of a minimal parabolic is a commutative Noetherian ring. The Weyl group W acts in such a manner that the full spherical Hecke algebra of M is integral over the W -invariant elements. Therefore $\mathcal{H}_{M,K \cap M}^W$ is a commutative Noetherian ring. Thus the spherical Hecke algebra $\mathcal{H}_{G,K}$ is a commutative Noetherian ring. For example, in the case of $\text{GL}(n, \mathbb{Q}_p)$, the Weyl group W is the symmetric group S_n and it acts on

$$\mathcal{H}_{M,K \cap M} \simeq \mathbb{C}[z_1, z_1^{-1}, z_2, z_2^{-1}, \dots, z_n, z_n^{-1}]$$

by permutation of these indeterminates z_i . Thus the W -fixed subalgebra is

$$\mathcal{H}_{M,K \cap M}^W \simeq \mathbb{C}[z_1, z_1^{-1}, z_2, z_2^{-1}, \dots, z_n, z_n^{-1}]^W \simeq \mathbb{C}[s_1, s_2, \dots, s_n, s_n^{-1}]$$

It is generated by the elementary symmetric polynomials $s_1, s_2, \dots, s_n$ in the z_i , together with the monomial s_n^{-1} . The integrality assures that any algebra homomorphism

$$\lambda : \mathcal{H}_{G,K} \simeq \mathcal{H}_{M,K \cap M}^W \rightarrow \mathbb{C}$$

extends to an algebra homomorphism

$$\tilde{\lambda} : \mathcal{H}_{M,K \cap M} \rightarrow \mathbb{C}$$

By an identification

$$\mathcal{H}_{M,K \cap M} \simeq \mathbb{C}[z_1, z_1^{-1}, z_2, z_2^{-1}, \dots, z_n, z_n^{-1}]$$

we have the images

$$\tilde{\lambda}(z_1), \tilde{\lambda}(z_2), \dots, \tilde{\lambda}(z_n)$$

which are the Satake parameters associated to λ . For each prime v of the algebraic number field we arrange the Satake parameters into a suitable diagonal matrix Φ_v : in case of $\text{GL}(n, \mathbb{Q}_p)$ with Satake parameters $\tilde{\lambda}(z_1), \tilde{\lambda}(z_2), \dots, \tilde{\lambda}(z_n)$, we can take

$$\Phi_p = \begin{pmatrix} \tilde{\lambda}(z_1) & & & \\ & \tilde{\lambda}(z_2) & & \\ & & \ddots & \\ & & & \tilde{\lambda}(z_n) \end{pmatrix} \quad (1)$$

Then the standard L-function attached to the local data Φ_v coming from the Satake parameters is

$$L(s, \pi, \{\Phi_v\}) = \prod_{v \notin S} \frac{1}{\det(1 - q_v^{-s} \Phi_v)}$$

where q_v is the order of the residue class field for v , and S is the finite set of primes where the local representation is not spherical. This also omits archimedean primes.

Suppose π is an irreducible unitary representation of $G(\mathbf{A}_K)$ in some space H_π . Then π can be factored as a restricted direct product $\pi = \otimes \pi_v$, with each π_v an irreducible representation of $G_v = \text{GL}(K_v)$. In particular, for almost all v , π_v is unramified; this means that its space H_v contains a one-dimensional space of vectors which are left fixed by the group of operators $\pi(g_v)$, $g_v \in \text{GL}(\mathcal{O}_v)$, with $\mathcal{O}_v = \{x \in K_v : |x|_v \leq 1\}$. The product $\otimes_v \pi_v$ is restricted in the sense that the space consists of vectors $w = \otimes w_v$ with the property that w_v is $\text{GL}(\mathcal{O}_v)$ -fixed for almost all v . Thus the representation $\pi(g)$ is well defined by the formula

$$\pi(g)w = \prod_v \pi_v(g_v)w_v$$

since $\pi(g_v)$ belongs to $\text{GL}(\mathcal{O}_v)$ for almost all v . If there exists an isomorphism A between H_π and some subspace V_π of L_0^2 the Hilbert space of square-integrable functions $G(K) \backslash G(\mathbf{A}_K)$ such that $A\pi(g) = R(g)A$ for all g in $G(\mathbf{A}_K)$, then we say π is equivalent to some subrepresentation of R_0 .

References

- [B1] N.Bourbaki, *Éléments de Mathématique Algèbre Chapitres 4 à 7*, Springer-Verlag Berlin Heidelberg pp. 422 (2007).
- [G] Gelbart, S., *An elementary introduction to the Langlands program*, Americal Mathematical Society. Bulletin.(1984) New Series, 10(2): 177-219, ISSN 0002-9904
- [BG] Bernstein, J., Gelbart, S. *An Introduction to the Langlands Program*, Birkhäuser, (2003) Boston ISBN 3-7643-3211-5.
- [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 plurigena 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.

ON SOME PROPERTIES OF COORDINATES

TAKANORI NAGAMINE

ABSTRACT. In this paper, we study some properties of coordinates in the polynomial ring by introducing some concepts which are weaker than coordinates. In particular, in the polynomial ring in two variables over an algebraically closed field of characteristic zero, we show some relations between polynomials and their fibers on $\mathbb{A}^2$.

1. INTRODUCTION

Let k be a field of characteristic zero and $k^{[n]} = k[x_1, \dots, x_n]$ be the polynomial ring in n variables over k . A polynomial $f \in k^{[n]}$ is called a *coordinate* if there exists polynomials $f_2, \dots, f_n \in k^{[n]}$ such that $k[f, f_2, \dots, f_n] = k^{[n]}$. We say that f is a *generically univariate* if there exists a coordinate $g \in k^{[n]}$ such that $k[f] \subset k[g]$. In general, it is difficult to decide whether f is a coordinate or not. In the case where $n = 2$, there are some criteria for a polynomial $f \in k^{[2]}$ to be a coordinate. The following theorem is proved by S. Abhyankar and T. Moh ([1]).

Theorem 1.1. (Abhyankar-Moh embedding theorem) *Let $f \in k^{[2]}$ be a polynomial. Then f is a coordinate if and only if $k^{[2]}/(f) \simeq k^{[1]}$.*

On the other hand, we can understand a polynomial is a coordinate or not, by the notations of derivations. Let A be a k -domain and let $D : A \rightarrow A$ be a k -derivation. D is called a *locally nilpotent derivation* if for any $a \in A$, there exists an integer $N(a) \geq 1$ such that $D^N(a) = 0$ for $N \geq N(a)$. We denote A^D by the kernel of D .

For a polynomial $f \in k^{[2]} = k[x, y]$, we define a k -derivation Δ_f by

$$\Delta_f := -\frac{\partial f}{\partial y} \frac{\partial}{\partial x} + \frac{\partial f}{\partial x} \frac{\partial}{\partial y}.$$

The following theorem gives a criterion for a polynomial $f \in k^{[2]}$ to be a coordinate.

Theorem 1.2. (cf. [3, Proposition 2.1]) *Let $f \in k^{[2]} \setminus k$ be a non-constant polynomial. Then the following conditions are equivalent:*

- (i) *f is a coordinate.*

Date: March 30, 2017.

Key words and phrases. Closed polynomials, Coordinates, Derivations.

(ii) Δ_f is a locally nilpotent derivation and $1 \in (f_x, f_y)$.

As we can see Theorem 1.2, it is important to decide whether Δ_f is locally nilpotent or not. The following gives an answer for this question.

Proposition 1.3. (cf. [4, Corollary 4.7]) *Let $f \in k^{[2]} \setminus k$ be a non-constant polynomial. Then the following conditions are equivalent:*

- (i) f is a generically univariate.
- (ii) Δ_f is a locally nilpotent derivation.

In this paper, we study some properties of coordinates in the polynomial ring by introducing some concepts which are weaker than coordinates. In Section 2, we introduce some concepts which are weaker than coordinates and show some relations between these concepts and their fibers on $\mathbb{A}^2$. The main result of this section is Theorem 2.5. This theorem gives some geometric characterizations of these concepts. In Section 3, we study algebraically closed subrings of an integral domain. The main result of this section is Theorem 3.4, which is a generalization of [5, Theorem 3.1]. Finally, in Section 4, we give some examples of concepts which are introduced in Section 2.

2. FIBERS AND SUBALGEBRAS OF THE POLYNOMIAL RINGS

Let k be a field and let A be a k -domain. We denote $Q(A)$ by the quotient field of A . A subring B of A is called *algebraically closed* in A if for every polynomial $f(T) \in B[T]$ with coefficients in B , every root of $f(T)$ belonging to A also belongs to B . We say that B is *factorially closed* in A if for all $a, b \in A \setminus \{0\}$, $ab \in B$ implies that a and b belong to B .

Lemma 2.1. *Let B be a subring of A . Then the following assertions hold true.*

- (1) *If B is factorially closed in A , then it is algebraically closed in A .*
- (2) *B is algebraically closed in A if and only if B is integrally closed in A and $Q(B) \cap A = B$.*

Proof. Omitted. □

In the rest of this section, we consider the case where A is the polynomial ring. Let $k^{[n]}$ be the polynomial ring in n variables over k . A polynomial $f \in k^{[n]} \setminus k$ is called a *closed polynomial* if $k[f]$ is integrally closed in $k^{[n]}$. We say also f is a *factorially closed polynomial* if $k[f]$ is factorially closed in $k^{[n]}$. We use the notation “coordinate” and “generically univariate” in the same sense as in Section 1 over a field with any characteristic.

Lemma 2.2. *Let $f \in k^{[n]} \setminus k$ be a non-constant polynomial. Then the following two conditions are equivalent:*

- (i) $k[f]$ is algebraically closed in $k^{[n]}$.
- (ii) $k[f]$ is integrally closed in $k^{[n]}$.

Proof. (i) $\Rightarrow$ (ii) is clear. (ii) $\Rightarrow$ (i) follows from $k(f) \cap k^{[n]} = k[f]$ and Lemma 2.1 (2). $\square$

By the above lemma, we say simply a polynomial f is *closed* if $k[f]$ is integrally closed or algebraically closed in $k^{[n]}$.

Next, we consider whether $f \in k^{[n]} \setminus k$ is a generically univariate or not. We denote $\overline{k[f]}$ by the algebraic closure of $k[f]$ in $k^{[n]}$. Then $\overline{k[f]}$ is a Dedekind subring of $k^{[n]}$ containing k . It follows from [10, Theorem 8] that there exists $g \in k^{[n]} \setminus k$ such that $\overline{k[f]} = k[g]$ and $g(0, \dots, 0) = 0$. Further such a polynomial g is unique up to multiplication by non-zero elements of k . Then the following holds true.

Lemma 2.3. *With the above notations, the following two conditions are equivalent:*

- (i) f is a generically univariate.
- (ii) g is a coordinate.

Proof. The part “(ii) $\Rightarrow$ (i)” is clear. So, we prove the part “(i) $\Rightarrow$ (ii)”. Suppose that f is a generically univariate. Then there exists a coordinate $u \in k^{[n]}$ such that $k[f] \subset k[u]$. Since $k[g] \subset k[u]$ and $k[g]$ is algebraically closed in $k^{[n]}$, $k[g] = k[u]$. So g is a coordinate. $\square$

These four concepts “variable”, “generically univariate”, “factorially closed polynomial” and “closed polynomial” have some relations as below.

Proposition 2.4. *Let $f \in k^{[n]} \setminus k$ be a non-constant polynomial. Then the following assertions hold true.*

- (1) *If f is a variable, then it is a generically univariate and a factorially closed polynomial.*
- (2) *If f is a factorially closed polynomial, then it is closed.*
- (3) *f is a variable if and only if it is a generically univariate and closed.*

Proof. (1) is clear. (2) follows from Lemma 2.2. The “only if” part of (3) follows from (1) and (2). The “if” part of (3) follows from Lemma 2.3. $\square$

In the rest of this section, we assume further that k is an algebraically closed field of characteristic zero and $n = 2$. Let $f \in k^{[2]} \setminus k$ be a

non-constant polynomial. We consider the morphism $\Phi_f : \operatorname{Spec} k^{[2]} \rightarrow \operatorname{Spec} k[f]$ associated to the inclusion $k[f] \hookrightarrow k^{[2]}$. Here, we denote $\Phi_f^{-1}(P)$ by a fiber of Φ_f at a close point $P \in \operatorname{Spec} k[f]$ and note that $\Phi_f^{-1}(P) = \operatorname{Spec}(k[x, y]/(f - \lambda))$, where $\lambda \in k$ and $(f - \lambda)$ is the ideal corresponding to P . The fiber $\Phi_f^{-1}(P)$ is irreducible and reduced if and only if the polynomial $f - \lambda$ is irreducible. The following is the main result in this section.

Theorem 2.5. *Let k be an algebraically closed field of characteristic zero, let $f \in k^{[2]} \setminus k$ be a non-constant polynomial and let $\Phi_f : \operatorname{Spec} k^{[2]} \rightarrow \operatorname{Spec} k[f]$ be the morphism associated to the inclusion $k[f] \hookrightarrow k^{[2]}$. Let m be the degree of field extension $Q(\overline{k[f]})$ over $k(f)$. Then the following assertions hold true.*

- (1) *f is factorially closed if and only if every fiber of Φ_f is irreducible and reduced.*
- (2) *f is a generically univariate if and only if*

$$\Phi_f^{-1}(P) = \sum_{i=1}^r m_i F_i,$$

where $F_i \simeq \mathbb{A}^1$ for $1 \leq i \leq m$ and $\sum_{i=1}^r m_i = m$, for any closed point $P \in \operatorname{Spec} k[f]$.

Proof. We set $k^{[2]} = k[x, y]$.

(1). Suppose that f is factorially closed. If there exists $\lambda \in k$ such that $f - \lambda$ is reducible, then $f - \lambda = gh$ for some $g, h \in k[x, y] \setminus k$. Since $\deg g$ and $\deg h$ are less than $\deg(f - \lambda)$, g and h do not belong to $k[f - \lambda]$. This is a contradiction. Hence every fiber of Φ_f is irreducible and reduced.

Conversely, we suppose that every fiber of Φ_f is irreducible and reduced. We may assume that f is irreducible. It follows from [2, Theorem 1.1 (1)] that f is closed. So, $k[x, y]^{\Delta_f} = k[f]$ by [8, Theorem 2,1].

On the other hand, since $k[x, y]$ is UFD, $\Delta_f = gD$ for some $g \in k[x, y] \setminus \{0\}$ and an irreducible derivation D . Since $k[f] = k[x, y]^{\Delta_f} = k[x, y]^D$, $k(f) \subset k(x, y)^{\tilde{D}}$, where $\tilde{D}$ is the natural extension of D to $k(x, y)$. It follows from [6, Lemma 2.4 (2)] that the abelian monoid $X_D(k[x, y])$ contains no abelian subgroup other than (0) . Therefore, by using [6, Lemma 1.5 (1)], we see that $k[f]$ is factorially closed in $k[x, y]$, which implies that f is a factorially closed polynomial.

(2). In order to show the equivalence, we need some arguments. By the argument preceding Lemma 2.3, we can write as $\overline{k[f]} = k[g]$ for some non-constant polynomial $g \in k[x, y] \setminus k$. Now, we consider the morphism $\Psi : \operatorname{Spec} k[g] \rightarrow \operatorname{Spec} k[f]$ with respect to the inclusion $k[f] \hookrightarrow k[g]$. Let

$m \geq 1$ be the degree of field extension $k(g)$ over $k(f)$. Then for any closed point $P \in \operatorname{Spec} k[f]$,

$$\Psi^{-1}(P) = \sum_{i=1}^r m_i Q_i,$$

where each Q_i is a distinct closed point of $\operatorname{Spec} k[g]$ and $\sum_{i=1}^r m_i = m$. Therefore

$$\Phi_f^{-1}(P) = \Phi_g^{-1}\left(\sum_{i=1}^r m_i Q_i\right) = \sum_{i=1}^r m_i \Phi_g^{-1}(Q_i).$$

If f is a generically univariate, then g is a coordinate, by Lemma 2.3. It follows from Theorem 1.1 that $\Phi_g^{-1}(Q_i)$ is isomorphic to $\mathbb{A}^1$ for any $1 \leq i \leq r$. Therefore we have the assertion.

Conversely, in order to prove the assertion, it is sufficient to prove that g is a coordinate. Since g is closed, it follows from [2, Theorem 1.1] that there exists $Q_0 \in \operatorname{Spec} k[g]$ such that $\Phi_g^{-1}(Q_0)$ is irreducible and reduced. Put $P := \Psi(Q_0) \in \operatorname{Spec} k[f]$. By the assumption, $\Phi_f^{-1}(P) = \sum_{i=1}^r m_i F_i$ with $F_i \simeq \mathbb{A}^1$, where $\sum_{i=1}^r m_i = m$. Since $\Phi_g^{-1}(Q_0) \subset \Phi_f^{-1}(P)$ and $\Phi_g^{-1}(Q_0)$ is irreducible, there exists $1 \leq i \leq r$ such that $\Phi_g^{-1}(Q_0) \subset F_i \simeq \mathbb{A}^1$. Since the dimension of $\Phi_g^{-1}(Q_0)$ is one, $\Phi_g^{-1}(Q_0) F_i \simeq \mathbb{A}^1$. Therefore, by using Theorem 1.1 again, we see that g is a coordinate. $\square$

3. ALGEBRAICALLY CLOSED SUBALGEBRAS

Let R be an integral domain and let A be an R -domain. We denote $Q(R)$ by the quotient field of R . We denote the set of R -subalgebras of A whose transcendental degree over R equals r by $S(r, A)$, that is,

$$S(r, A) := \{B \mid B \text{ is an } R\text{-subalgebra of } A \text{ with } \operatorname{tr.deg}_R B = r\}.$$

Here, this set $S(r, A)$ is ordered by partial inclusion.

In order to state the main result in this section, we prepare two lemmas below. We set $K := Q(R)$ and $A_K := K \otimes_R A$. The following lemmas state that some conditions on R -subalgebras of A are invariant by the extension of the scalar K .

First, we discuss about integrally closed subring in A or A_K .

Lemma 3.1. *Let B be an R -subalgebra of A such that $Q(B) \cap A = B$. Then the following two conditions are equivalent:*

- (i) B is integrally closed in A .
- (ii) B_K is integrally closed in A_K .

Proof. (i) $\Rightarrow$ (ii). Suppose that B is integrally closed in A . If $\alpha \in A_K$ is integral over B_K , then there exist $\beta_1, \dots, \beta_m \in B_K$ such that

$$\alpha^m + \beta_1 \alpha^{m-1} + \cdots + \beta_{m-1} \alpha + \beta_m = 0.$$

We choose elements $a, b \in R \setminus \{0\}$ with $a\alpha \in A$ and $b\beta_i \in B$ for any $1 \leq i \leq m$ and set $c := ab \in R$. Then we have

$$(c\alpha)^m + c\beta_1(c\alpha)^{m-1} + \cdots + c^{m-1}\beta_{m-1}(c\alpha) + c^m\beta_m = 0.$$

Since $c\alpha \in A$ and $c^i\beta_i \in B$, $c\alpha$ is integral over B , and so $c\alpha \in B$. Hence $\alpha \in B_K$.

(ii) $\Rightarrow$ (i). Suppose that B_K is integrally closed in A_K . If $a \in A$ is integral over B , then it is also integral over B_K as an element of A_K . By (ii), a is an element of B_K . Hence $a \in B_K \cap A \subset Q(B) \cap A = B$. Therefore B is integrally closed in A . $\square$

By Lemma 3.1, we have the following. Its proof is the same as that of Lemma 3.1.

Corollary 3.2. *Let B be an R -subalgebra of A . Then the following two conditions are equivalent:*

- (i) B is algebraically closed in A .
- (ii) B_K is algebraically closed in A_K .

Lemma 3.3. *Suppose that the characteristic of R equals zero and A is finitely generated over R . For an R -subalgebra B of A , the following two conditions are equivalent:*

- (i) There exists an R -derivation D of A such that $A^D = B$.
- (ii) $Q(B) \cap A = B$ and there exists a K -derivation D_K of A_K such that $(A_K)^{D_K} = B_K$.

Proof. We may assume that A is generated by $a_1, \dots, a_r \in A$ over R .

(i) $\Rightarrow$ (ii). Let D be an R -derivation on A such that $A^D = B$. Since B is the kernel of derivation D , it follows from Remark ?? (1) that B is algebraically closed in A . Hence $Q(B) \cap A = B$ by Proposition 2.1 (2). We denote D_K by the natural extension of D to A_K , that is, $D_K(a_i) := D(a_i)$ for $1 \leq i \leq n$. It is clear that B_K is contained in $(A_K)^{D_K}$. On the other hand, if $\alpha \in (A_K)^{D_K}$, then $\lambda\alpha \in A$ for some $\lambda \in R \setminus \{0\}$ and

$$0 = \lambda D_K(\alpha) = D_K(\lambda\alpha) = D(\lambda\alpha).$$

Therefore $\lambda\alpha \in A^D = B$, and so $\alpha \in B_K$.

(ii) $\Rightarrow$ (i). Conversely, we suppose that there exists a K -derivation D_K on A_K with $(A_K)^{D_K} = B_K$ and $Q(B) \cap A = B$. We can choose a non-zero element $\lambda \in R \setminus \{0\}$ such that $\lambda D_K(a_i) \in A$ for $1 \leq i \leq n$. Now, we define an R -derivation D of A by $D := \lambda D_K$. This is a desired one. Indeed, since $B \subset B_K \cap A \subset Q(B) \cap A = B$, $B = B_K \cap A$. By the construction of D , we see that D is the restriction of λD_K on A . We note

also $(A_K)^{\lambda D_K} = (A_K)^{D_K} = B_K$. Hence $A^D = (A_K)^{\lambda D_K} \cap A = B_K \cap A$. From the above argument, we have $A^D = B$. $\square$

The following is the main result in this section.

Theorem 3.4. *Let R be an integral domain and let A be an R -domain. For an element B of $S(r, A)$, the following conditions are equivalent:*

- (i) B is algebraically closed in A .
- (ii) B is integrally closed in A and $Q(B) \cap A = B$.
- (iii) B is a maximal element of $S(r, A)$.

Moreover, if the characteristic of R equals zero and A is finitely generated over R , then the above conditions are equivalent to the condition (iv).

- (iv) There exists an R -derivation D of A such that $A^D = B$.

Proof. The part “(i) $\Leftrightarrow$ (ii)” follows from Proposition 2.1 (2).

(i) $\Rightarrow$ (iii). Let C be any element of $S(r, A)$ containing B . Since B and C have same transcendental degree, the ring extension C over B is algebraic. Hence $B = C$, which implies B is a maximal element of $S(r, A)$.

(iii) $\Rightarrow$ (i). We denote $\bar{B}$ by the algebraic closure of B in A . Then $\bar{B}$ is an element of $S(r, A)$. Since $B \subset \bar{B}$ and B is a maximal element of $S(r, A)$, $B = \bar{B}$. So B is algebraically closed in A .

Next, in order to prove the rest of this theorem, we assume further that the characteristic of R equals zero and A is finitely generated over R . We set $K := Q(R)$.

(ii) $\Rightarrow$ (iv). By Lemma 3.1, B_K is integrally closed in A_K . Since K is a field, it follows from [9, Theorem 5.4] that there exists a K -derivation D_K of A_K such that $(A_K)^{D_K} = B_K$. By Lemma 3.3 and the assumption on B , we have an R -derivation D of A satisfying $A^D = B$.

(iv) $\Rightarrow$ (ii). Suppose that there exists an R -derivation D on A with $A^D = B$. By Lemma 3.3, $Q(B) \cap A = B$ and there exists a K -derivation D_K of A_K such that $(A_K)^{D_K} = B_K$. Since K is a field, it follows from [9, Theorem 5.4] that B_K is integrally closed in A_K . Therefore B is integrally closed in A by Lemma 3.1. $\square$

In Theorem 3.4, we consider the case where A is the polynomial ring $R^{[n]}$ in n variables over R and $r = 1$. Then we get a part of [5, Theorem 3.1] as a corollary of Theorem 3.4.

4. EXAMPLES

By using Theorem 2.5, we give some examples of factorially closed polynomials and closed polynomials in the case where $n = 2$.

Proposition 4.1. *Let k be a field of characteristic zero and let $f \in k[x, y] \setminus k$ be a non-constant polynomial of degree $d \geq 2$. The following two conditions are equivalent:*

- (i) $\deg \bar{f} = d - 1$, where $\bar{f} := \gcd(f_x, f_y)$.
- (ii) There exists $\lambda \in k \setminus \{0\}$ such that $k[f] \subset k[x + \lambda y]$.

In particular, if the above conditions hold, then f is a generically univariate but is not closed, and the algebraic closure of $k[f]$ in $k[x, y]$ is equal to $k[x + \lambda y]$.

Proof. (i) $\Rightarrow$ (ii). Suppose that $\deg \bar{f} = d - 1$. First of all, we consider the homogeneous decomposition of f_x and f_y . Let $f = f_d + \cdots + f_0$ be the homogeneous decomposition of f . The following give the homogeneous decomposition of f_x and f_y :

$$\begin{cases} f_x = \frac{\partial f_d}{\partial x} + \cdots + \frac{\partial f_1}{\partial x}. \\ f_y = \frac{\partial f_d}{\partial y} + \cdots + \frac{\partial f_1}{\partial y}. \end{cases}$$

Since $\deg \bar{f} = d - 1$, there exists $\lambda \in k \setminus \{0\}$ such that $\lambda f_x = f_y$. Indeed, we write $f_x = p\bar{f}$ and $f_y = q\bar{f}$ for some $p, q \in k[x, y]$. Then we have

$$d - 1 \leq \deg \bar{f} + \deg p = \deg f_x \leq d - 1.$$

Hence $\deg p = 0$, which means that p is a non-zero constant. q is also a non-zero constant. By putting $\lambda := q/p \in k \setminus \{0\}$, we have $\lambda f_x = f_y$.

By comparing the homogeneous decomposition of f_x and f_y , we have $\lambda \partial f_e / \partial x = \partial f_e / \partial y$ for $1 \leq e \leq d$. Now, we represent $f_e \neq 0$ as

$$f_e = \sum_{i=0}^e [e - i, i] x^{e-i} y^i,$$

where $[e - i, i] \in k$. Then we have the following:

$$\begin{cases} \frac{\partial f_e}{\partial x} = \sum_{i=0}^{e-1} (e - i) [e - i, i] x^{e-(i+1)} y^i. \\ \frac{\partial f_e}{\partial y} = \sum_{i=1}^e i [e - i, i] x^{e-i} y^{i-1} = \sum_{i=0}^{e-1} (i + 1) [e - (i + 1), i + 1] x^{e-(i+1)} y^i. \end{cases}$$

So, we have

$$\lambda(e - i) [e - i, i] = (i + 1) [e - (i + 1), i + 1]$$

for $0 \leq i \leq e-1$. Since $f_e \neq 0$, $[e, 0] \neq 0$. Here, we can show easily that the following equation holds for $0 \leq i \leq e-1$:

$$[e - (i+1), i+1] = \binom{e}{i+1} \lambda^{i+1} [e, 0].$$

By using this equation, we have

$$\begin{aligned} f_e &= \sum_{i=0}^e [e-i, i] x^{e-i} y^i = [e, 0] x^e + \sum_{i=0}^{e-1} [e-(i+1), i+1] x^{e-(i+1)} y^{i+1} \\ &= [e, 0] x^e + \sum_{i=0}^{e-1} \binom{e}{i+1} \lambda^{i+1} [e, 0] x^{e-(i+1)} y^{i+1} \\ &= [e, 0] \sum_{i=0}^e \binom{e}{i} x^{e-i} (\lambda y)^i \\ &= [e, 0] (x + \lambda y)^e \in k[x + \lambda y]. \end{aligned}$$

Then $f = \sum_{e=0}^d f_e \in k[x + \lambda y]$, and hence $k[f] \subset k[x + \lambda y]$.

(ii) $\Rightarrow$ (i). Since $k[f] \subset k[x + \lambda y]$, there exists $u(T) \in k[T]$ of degree $d = \deg f$ with $f = u(x + \lambda y)$. Then $f_x = u'(x + \lambda y)$ and $f_y = \lambda u'(x + \lambda y)$, where $u'(T) = du(T)/dT$. Then $u'(x + \lambda y) \mid \bar{f}$, and so we have

$$d - 1 = \deg u'(x + \lambda y) \leq \deg \bar{f} \leq d - 1.$$

Therefore $\deg \bar{f} = d - 1$. □

Corollary 4.2. *Let $f \in k[x, y] \setminus k$ be a non-constant polynomial of prime degree. Then the following two conditions are equivalent:*

- (i) f is closed.
- (ii) $\deg \bar{f} < \deg f - 1$.

Proof. (i) $\Rightarrow$ (ii). If $\deg \bar{f} = \deg f - 1$, then f is not closed by Proposition 4.1. The part “(ii) $\Rightarrow$ (i)” follows from [7, Theorem 3.6]. □

In the rest of this section, we discuss about factorially closedness of polynomials.

We prove the following lemma. In this lemma, we consider the case where the polynomial ring in n variables over an arbitrary integral domain. Let R be an integral domain and let $R^{[n]}$ be the polynomial ring in n variables over R . We denote the quotient field of R by K . Let R' be an integral domain containing R . A polynomial $f \in R^{[n]}$ is called *factorially closed over R'* (resp. *algebraically closed over R'*) if $R'[f]$ is factorially closed (resp. algebraically closed) in $R^{[n]} \otimes_R R'$.

Lemma 4.3. *Let $f \in R^{[n]} \setminus R$ be a non-constant polynomial. Then the following assertions hold true.*

- (1) *The following two conditions are equivalent:*
- (i) *f is factorially closed over R .*
 - (ii) *f is factorially closed over K .*
- (2) *If there exist a field L such that L over K is Galois extension and f is factorially closed over L , then f is factorially closed over K .*

Proof. (1) (i) $\Rightarrow$ (ii). We choose two polynomials $g, h \in R^{[n]} \otimes_R K = K^{[n]}$ with $gh \in K[f]$. Without loss of generality, we may assume that $g, h \in R^{[n]}$. Since $gh \in K[f]$, there exist $a_0, \dots, a_m \in R$ and $b_0, \dots, b_m \in R \setminus \{0\}$ such that

$$gh = \frac{a_0}{b_0}f^m + \frac{a_1}{b_1}f^{m-1} + \dots + \frac{a_{m-1}}{b_{m-1}}f + \frac{a_m}{b_m}.$$

Putting $b := \prod_{i=0}^m b_i$ and $c_i := b(a_i/b_i) \in R$ for $0 \leq i \leq m$, we have

$$bgh = c_0f^m + c_1f^{m-1} + \dots + c_{m-1}f + c_m \in R[f].$$

Since f is factorially closed over R , we have $g, h \in R[f] \subset K[f]$.

(ii) $\Rightarrow$ (i). We choose two polynomials $g, h \in R^{[n]}$ with $gh \in R[f]$. Since $gh \in K[f]$ and f is factorially closed over K , $g \in K[f] \cap R^{[n]}$ and $h \in K[f] \cap R^{[n]}$.

So, it is sufficient to prove that $R[f] = K[f] \cap R^{[n]}$. Since f is factorially closed over K , it is also algebraically closed over K . By Corollary 3.2, f is also algebraically closed over R . Then we have

$$R[f] \subset (K[f] \cap R^{[n]}) \subset (K(f) \cap R^{[n]}) = R[f],$$

and so $R[f] = K[f] \cap R^{[n]}$.

(2). Let G be the Galois group of L over K . Here, G acts on a polynomial of $L^{[n]}$ by acting on its coefficients. Then we can see easily that $L[f]^G = K[f]$, where $L[f]^G = \{u \in L[f] \mid \sigma(u) = u, \text{ for any } \sigma \in G\}$.

In order to show that f is factorially closed over K , we choose two polynomials $g, h \in K^{[n]} \setminus \{0\}$ with $gh \in K[f]$. Since $K[f] \subset L[f]$ and f is factorially closed over L , g and h belong to $L[f]$. Note that $L[f] \cap K^{[n]} = L[f]^G = K[f]$. Hence we have $g, h \in K[f]$. $\square$

We give an example of factorially closed polynomials below.

Example 4.4. Let R be an integral domain of characteristic zero and $R[x, y]$ be the polynomial ring in two variables over R . Let $h(x, y) := f(x) + g(y) \in R[x, y]$, where $f, g \in R[T]$ and, $\deg_x f(x)$ and $\deg_y g(y)$ are relatively prime. Then h is factorially closed over R (of cause h is algebraically closed over R).

Proof. We denote K by the quotient field of R . Let L be an algebraically closure of K . For any element of $\lambda \in L$, $h - \lambda$ is irreducible as an

element of $L[x, y]$. By Theorem 2.5 (1), h is factorially closed over L . Since the field extension L over K is Galois, h is factorially closed over K by Lemma 4.3 (2). By using Lemma 4.3 (1), we see that h is also factorially closed over R . $\square$

ACKNOWLEDGMENTS

The author is sincerely grateful to Professor Hideo Kojima for his hearty guidance and valuable comments on this research.

REFERENCES

- [1] S. S. Abhyankar and T. T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math., **276** (1975), 148–166.
- [2] I. V. Arzhantsev and A. P. Petravchuk, Closed polynomials and saturated subalgebras of polynomial algebras, Ukrainian Math. J., **59** (2007), 1783–1790.
- [3] J. Berson and A. van den Essen, An algorithm to find a coordinate's mate, J. Sym. Comp., **36** (2003), 835–843.
- [4] G. Freudenburg, Algebraic theory of locally nilpotent derivations, Encyclopaedia Math. Sci., 136, Springer, Berlin, 2006.
- [5] H. Kojima and T. Nagamine, Closed polynomials in polynomial rings over integral domains, J. Pure Appl. Algebra, **219** (2015), 5493–5499.
- [6] M. Miyanishi, Vector fields on factorial schemes, J. Algebra, **173** (1995), 144–165.
- [7] T. Nagamine, Derivations having divergence zero and closed polynomials over domains, J. Algebra, **462** (2016), 67–76.
- [8] A. Nowicki, On the equation $J(f, g) = 0$ for polynomials in $k[x, y]$, Nagoya Math. J., **109** (1988), 151–157.
- [9] A. Nowicki, Rings and fields of constants for derivations in characteristic zero, J. Pure Appl. Algebra, **96** (1994), 47–55.
- [10] A. Zaks, Dedekind subrings of $k[x_1, \dots, x_n]$ are rings of polynomials, Israel J. Math., **9** (1971), 285–289.

(T. Nagamine) GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, NIIGATA UNIVERSITY, 8050 IKARASHININOCHO, NISHI-KU, NIIGATA 950-2181, JAPAN
E-mail address: t.nagamine14@m.sc.niigata-u.ac.jp

モデル・ヴェイユ群が自明な最大ピカール数の有理曲面の トリゴナル曲線束

北川真也 (Cheng Gong と Jun Lu との共同研究)

[Kit] S. Kitagawa, Extremal hyperelliptic fibrations on rational surfaces,
Saitama Math. J. 30 (2013), 1–14.

[GKL] C. Gong, S. Kitagawa and Jun Lu,
Extremal trigonal fibrations on rational surfaces, in preperation.

§1 用語と記号

§2 先行結果

§3 主結果

§4 証明の概略

§1 用語と記号

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

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

We assume that f is relatively minimal,

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

Via f , we can regard X 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 $\mathcal{J}_f/\mathbb{K}$ be the Jacobian variety of the generic fibre $\mathcal{F}/\mathbb{K}$ of f .

The Mordell-Weil group of f is the group of $\mathbb{K}$ -rational points $\mathcal{J}_f(\mathbb{K})$.

It is a finitely generated abelian group.

$r(f) := \text{rk}\mathcal{J}_f(\mathbb{K})$: the Mordell-Weil rank of f .

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 f .

For $P \in \mathcal{F}(\mathbb{K})$, we denote by (P) the section corresponding to P

which is regarded as a horizontal curve on X .

In particular, (O) corresponding to the origin O of $\mathcal{J}_f(\mathbb{K})$

is called the zero section.

$\text{NS}(X)$: Néron-Severi group of X , $\rho(X)$: Picard number of X .

Let V be the subgroup of $\text{NS}(X)$ generated by

the irreducible components of the fibres of f .

Set $T_{(O)} = \mathbb{Z}(O) \oplus V \subset \text{NS}(X)$

We have the natural isomorphism of groups

$$\mathcal{J}_f(\mathbb{K}) \simeq \text{NS}(X)/T_{(O)}$$

in [Shi1, p. 214, Theorem 1.3] and [Shi2, p. 362, Theorem 3].

In [Shi1, p. 214, Theorem 1.3] and [Shi2, p. 362, Theorem 3],

we have the natural isomorphism of groups

$$\mathcal{J}_f(\mathbb{K}) \simeq \text{NS}(X)/T_{(O)}.$$

We denote by n_q

the number of irreducible components of $f^{-1}(q)$ for any $q \in \mathbb{P}^1$.

As a corollary, we have

$$r(f) = \rho(X) - 2 - \sum_{q \in \mathbb{P}^1} (n_q - 1). \quad (\star)$$

[Shi1] T. Shioda, On the Mordell-Weil lattices, Comment. Math. Univ. St. Pauli 39 (1990), 211–240.

[Shi2] T. Shioda, Mordell-Weil lattices for higher genus fibration over a curve, in New trends in algebraic geometry, Cambridge Univ. Press (1996), 359–373.

For the case $g = 1$, the theory of the Mordell-Weil lattices are sufficiently developed by Oguiso and Shioda in [OS]. In their work, the lattice E_8 played very important role as the predominant frame. For example, it was shown that the Mordell-Weil group is trivial if and only if there exists a singular fibre of type II^* in the sense of Kodaira whose dual graph contains E_8 as a subgraph. The lattice E_8 also appears in another application by Shioda [Shi3] to describe a hierarchy of deformations of rational double points.

[OS] K. Oguiso and T. Shioda, The Mordell-Weil lattice of a rational elliptic surface, *Comment. Math. Univ. St. Paul.* 40 (1991), 83–99.

[Shi3] T. Shioda, Mordell-Weil lattices of type E_8 and deformation of singularities, *Lecture Notes in Math.* 1468, Springer, Berlin (1991), 177–202.

In what follows, we assume $g \geq 2$.

Since X is rational, $b_1(X) = b_3(X) = 0$ and $b_2(X) = \rho(X)$,

where $b_n(X)$ denotes the n -th Betti number of X .

This and Noether's formula provide $\rho(X) = 4g + 6 - (K_X + F)^2$, where K_X denotes the canonical divisor of X .

The adjoint divisor $(K_X + F)$ is nef from [KK, p. 181, Lemma 1.1].

Thus we have that $\rho(X) \leq 4g + 6$.

[KK] S. Kitagawa and K. Konno, Fibred rational surfaces with extremal Mordell-Weil lattices, *Math. Z.* 251 (2005), 179–204.

Lemma 1 ([KK, p. 182, Lemma 1.2]). Let C be an irreducible curve on X such that $(K_X + F).C = 0$. If $(K_X + F)^2 > 0$, then C is a non-singular rational curve satisfying one of the following:

- (1) C is a (-2) -curve contained in a fibre.
- (2) C is a (-1) -section, i.e., a (-1) -curve with $F.C = 1$.

Suppose that there is a (-1) -curve E with $(K_X + F).E = 0$ and let $\mu_1 : X \rightarrow X_1$ be its contraction.

Since $F.E = 1$, $F_1 := (\mu_1)_*F$ is non-singular on X_1 .

Furthermore, we have $\mu_1^*(K_{X_1} + F_1) = K_X + F$.

If there is a (-1) -curve E_1 with $(K_{X_1} + F_1).E_1 = 0$, then,

by contracting it, we get the pair (X_2, F_2) with F_2 non-singular and $K_{X_2} + F_2$ pulls back to $K_X + F$.

We can continue the procedure until we arrive at a pair (X_n, F_n) such that we cannot find a (-1) -curve E_n with $(K_{X_n} + F_n).E_n = 0$.

We put $Y := X_n$ and $G := F_n$.

If $\mu : X \rightarrow Y$ denotes the natural map, then $\mu^*(K_Y + G) = K_X + F$ and $G = \mu_*F$ is a non-singular curve isomorphic to F .

The original fibration $f : X \rightarrow \mathbb{P}^1$ corresponds to a pencil $\Lambda_f \subset |G|$ with at most simple (but not necessarily transversal) base points.

When $(K_X + F)^2 > 0$, $K_X + F$ is nef and big.

This implies that, Y is the minimal resolution of singularities of the surface $\text{Proj}(R(X, K_X + F))$, which has at most rational double points by Lemma 1, where $R(X, K_X + F) = \bigoplus_{n \geq 0} H^0(X, n(K_X + F))$.

Therefore, such a model is uniquely determined.

We call the pair (Y, G) the reduction of (X, F) .

Now, for a non-negative integer d , we put

$$\Sigma_d = \{((X_0 : X_1 : X_2), (Y_0 : Y_1)) | X_1 Y_1^d = X_2 Y_0^d\} \subset \mathbb{P}^2 \times \mathbb{P}^1$$

and call it Hirzebruch surface of degree d .

The restriction of the second projection to Σ_d gives

a structure of $\mathbb{P}^1$ -bundle. We also remark that $\Sigma_0 \simeq \mathbb{P}^1 \times \mathbb{P}^1$.

Conversely, any $\mathbb{P}^1$ -bundle over $\mathbb{P}^1$ is isomorphic to Σ_d for some d .

We often consider on the Zariski open subset defined by $X_0 Y_0 \neq 0$ and take $(x, y) = (X_1/X_0, Y_1/Y_0)$ as an affine coordinate.

Let $\Delta_{[d]}$ be a minimal section of Σ_d defined by $x = 0$ and

$\Gamma_{[d]}$ the fibre defined by $y = 0$.

Then we have that $\Delta_{[d]}^2 = -d$, $\Gamma_{[d]}^2 = 0$ and $\Delta_{[d]} \cdot \Gamma_{[d]} = 1$.

§2 先行結果 Saito and Sakakibara [SS, Thm 2.8] show $r(f) \leq 4g + 4$.

Theorem 2 ([SS, Thm 4.1]). Let X be a smooth rational surface and $f : X \rightarrow \mathbb{P}^1$ a relatively minimal fibration of genus $g \geq 2$. Assume that $r(f) = 4g + 4$. Then $f : X \rightarrow \mathbb{P}^1$ is obtained as a blowing up of an irreducible pencil of hyperelliptic curves on Σ_d with $0 \leq d \leq g$.

[SS] M.-H. Saito and K.-I. Sakakibara, On Mordell-Weil lattices of higher genus fibrations on rational surfaces, J. Math. Kyoto Univ. 34 (1994), 859–871.

[Vie] K. Viet Nguyen, On certain Mordell-Weil lattices of hyperelliptic type on rational surfaces, J. Math. Sci. (New York) 102 (2000), 3938–3977.

Theorem 3 ([SS, Thm 4.1], [Vie, Thm 2.4] and [Kit, Thm 2.2]).

Let X be a smooth rational surface and $f : X \rightarrow \mathbb{P}^1$ a relatively minimal fibration of genus $g \geq 2$.

Assume that $\rho(X) = 4g + 6$.

Then there exists a birational morphism $\mu : X \rightarrow \Sigma_d$ with $d \leq g + 1$ such that the following conditions (i), (ii) hold.

- (i) μ_*F is linearly equivalent to $(2\Delta_{[d]} + (g + d + 1)\Gamma_{[d]})$.
- (ii) The pull-back to X of a (-1) -curve contracted by μ intersects with F at just one point.

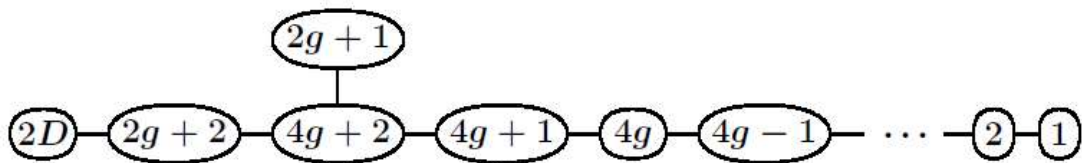
In particular, f has at least one (-1) -section and F is a hyperelliptic curve.

Theorem 4 ([Kit, Thm 3.1]). Let X be a smooth rational surface and $f : X \rightarrow \mathbb{P}^1$ a relatively minimal fibration of genus $g \geq 2$.

Assume that $\rho(X) = 4g + 6$.

Then the following conditions are equivalent to each other.

- (1) The Mordell-Weil group of f is trivial.
- (2) f has a reducible fibre whose dual graph is as follows:



Here $2D$ is a $(-g-1)$ -curve whose multiplicity in the reducible fibre is 2 and the numbers within the circles denote the multiplicities of (-2) -curves in the reducible fibre.

(3a) $f : X \rightarrow \mathbb{P}^1$ can be obtained from Σ_g by eliminating the base points of the following pencil Λ : Take a curve $H_{[g],0}$ satisfying the following three conditions.

- (i) $H_{[g],0} \sim 2\Delta_{[g]} + (2g + 1)\Gamma_{[g]}$.
- (ii) $H_{[g],0}$ is smooth at the intersection point of $\Gamma_{[g]}$ with $\Delta_{[g]}$.
- (iii) $H_{[g],0}$ is tangent to $\Gamma_{[g]}$ at the above intersection point.

Then the pencil Λ is generated by $H_{[g],0}$ and $(2\Delta_{[g]} + (2g + 1)\Gamma_{[g]})$.

(3b) $f : X \rightarrow \mathbb{P}^1$ can be obtained from Σ_g by eliminating the base points of the following pencil Λ :

$$tx^2y^{2g+1} = y + x^2 + \sum_{i=1}^2 \sum_{j=1}^{ig+1} c_{i,j} x^i y^j,$$

where $c_{i,j}$ are complex numbers

and t is a parameter of the pencil Λ .

When F is a non-hyperelliptic curve, Viet and Saito [VS, Thm 1.1] show $r(f) \leq 3g + 6$.

Theorem 5 ([VS, Thm 1.2]). Let X be a smooth rational surface and $f : X \rightarrow \mathbb{P}^1$ a relatively minimal fibration of genus $g \geq 3$. Assume that $r(f) = 3g + 6$ and F is a non-hyperelliptic curve. Then $f : X \rightarrow \mathbb{P}^1$ can be obtained as a blow-up of an irreducible pencil of plane quintics or trigonal curves on Σ_d with $0 \leq d \leq g/3$, $d \equiv g \pmod{2}$.

[VS] K. Viet Nguyen and M.-H. Saito, On Mordell-Weil lattices for non-hyperelliptic fibrations of surfaces with zero geometric genus and irregularity. *Izv. Ross. Akad. Nauk Ser. Mat.* 66 (2002), 137–154

Theorem 6 ([VS, Proposition 3.2] and [KK, p. 188]).

Let X be a smooth rational surface and

$f : X \rightarrow \mathbb{P}^1$ a relatively minimal fibration whose general fibre

F is a trigonal curve of genus $g \geq 3$.

Let (Y, G) denote the reduction of (X, F) .

Assume that $\rho(X) = 3g + 8$.

Then $Y = \Sigma_d$ and $G \sim 3\Delta_{[d]} + (1 + (g + 3d)/2)\Gamma_{[d]}$

for some d such that $d \equiv g \pmod{2}$ and $0 \leq d \leq (g + 2)/3$.

In particular, f has at least one (-1) -section,

though f has at most $(3g + 6)$ (-1) -sections.

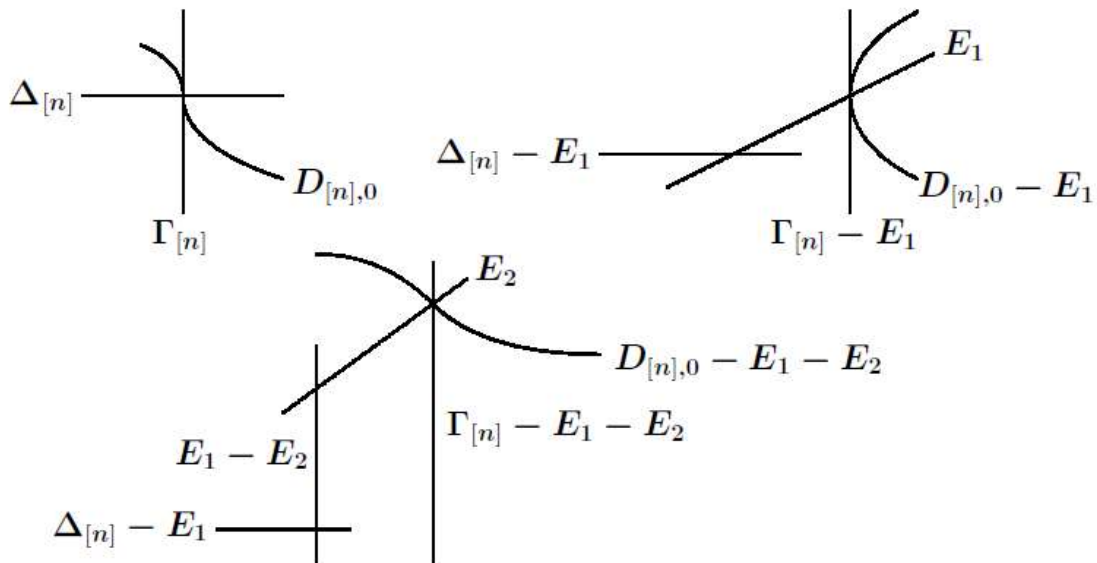
§3 主結果

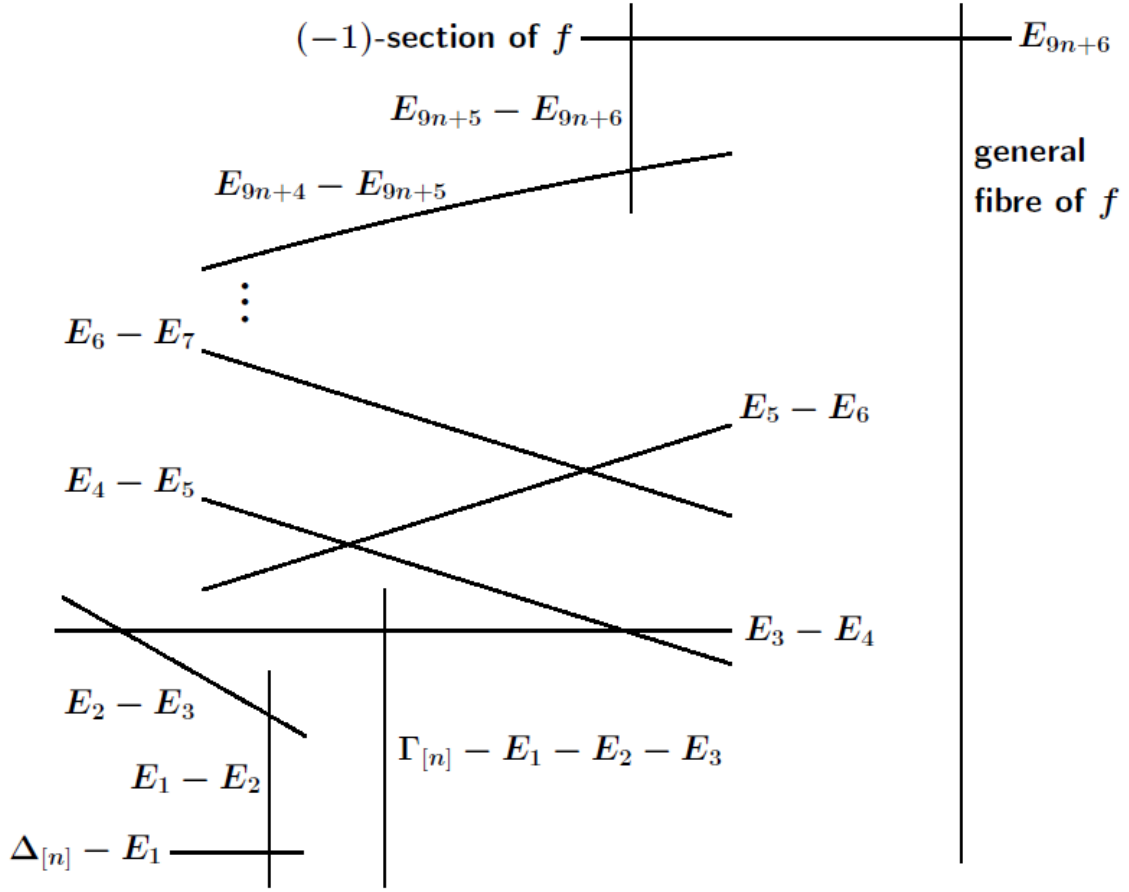
Example 7. Let Λ be a pencil defined by $tx^3y^{3n+1} = y + x^3$ on Σ_n and

$D_{[n],0}$ a curve defined by $y + x^3 = 0$. Then $D_{[n],0} \sim 3\Delta_{[n]} + (3n+1)\Gamma_{[n]}$

and the curves defined by $tx^3y^{3n+1} = y + x^3$ are trigonal curves of

genus $g = 3n$ except when $t = 0, \infty$. Blow-ups at base points of Λ .





$$\begin{aligned}
& \mathbb{Z}(\Delta_{[n]} - E_1) \oplus \mathbb{Z}(\Gamma_{[n]} - E_1 - E_2 - E_3) \oplus \bigoplus_{i=1}^{9n+5} \mathbb{Z}(E_i - E_{i+1}) \oplus \mathbb{Z}E_{9n+6} \\
& \simeq \mathbb{Z}\Delta_{[n]} \oplus \mathbb{Z}\Gamma_{[n]} \oplus \bigoplus_{i=1}^{9n+6} \mathbb{Z}E_i \\
& \simeq \text{NS}(X).
\end{aligned}$$

Thus the irreducible components of the reducible fibre over $t = \infty$ and the (-1) -section E_{9n+6} of f generate $\text{NS}(X)$. Therefore the Mordell-Weil group of f is trivial by [Shi2, p. 362, Theorem 3].

Proposition 8. Let n be a positive integer,

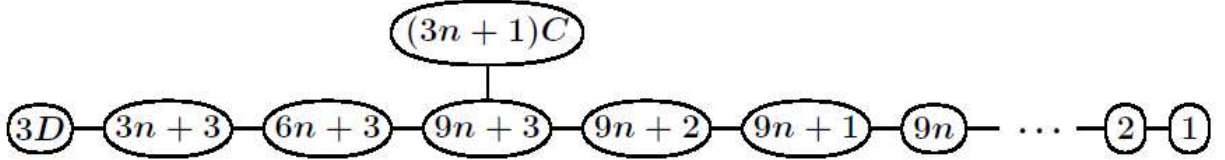
X a smooth rational surface and

$f : X \rightarrow \mathbb{P}^1$ a rel. min. trigonal fibration of genus $g = 3n$.

Assume that $\rho(X) = 3g + 8$.

Then the following conditions are equivalent to each other.

(1) f has a reducible fibre whose dual graph is as follows:



Here $(3n+1)C$ is a (-3) -curve whose multiplicity in the reducible fibre is $(3n+1)$, $3D$ is a $(-n-1)$ -curve whose multiplicity in the reducible fibre is 3 and the numbers within the circles denote the multiplicities of (-2) -curves in the reducible fibre.

(2a) $f : X \rightarrow \mathbb{P}^1$ can be obtained from Σ_n by eliminating the base points of the following pencil Λ : Take a curve $D_{[n],0}$ satisfying the following three conditions.

- (i) $D_{[n],0} \sim 3\Delta_{[n]} + (3n+1)\Gamma_{[n]}$.
- (ii) $D_{[n],0}$ is smooth at the intersection point of $\Gamma_{[n]}$ with $\Delta_{[n]}$.
- (iii) $D_{[n],0}$ has a contact of order 3 with $\Gamma_{[n]}$ through the above intersection point.

Then the pencil Λ is generated by $D_{[n],0}$ and $(3\Delta_{[n]} + (3n+1)\Gamma_{[n]})$.

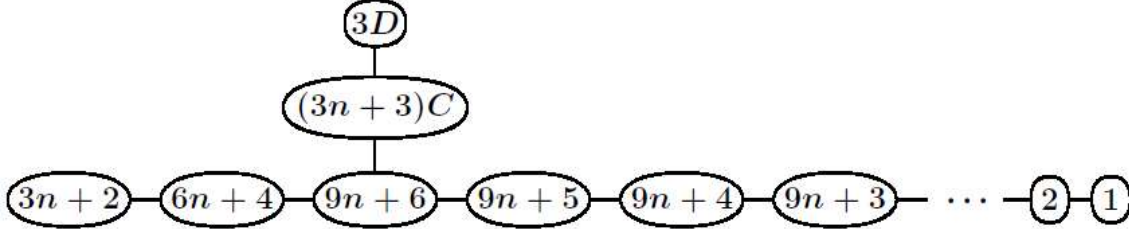
(2b) $f : X \rightarrow \mathbb{P}^1$ can be obtained from Σ_n by eliminating the base points of the following pencil Λ :

$$tx^3y^{3n+1} = y + x^3 + \sum_{i=1}^3 \sum_{j=1}^{in+1} c_{i,j} x^i y^j.$$

Proposition 9. Let n be a positive integer, X a smooth rational surface with $\rho(X) = 3g + 8$ and $f : X \rightarrow \mathbb{P}^1$ a rel. min. trigonal fibration of genus $g = 3n + 1$.

Then the following conditions are equivalent to each other.

(1) f has a reducible fibre whose dual graph is as follows:



Here $(3n+3)C$ is a (-3) -curve whose multiplicity in the reducible fibre is $(3n+3)$, $3D$ is a $(-n-1)$ -curve whose multiplicity in the reducible fibre is 3 and the numbers within the circles denote the multiplicities of (-2) -curves in the reducible fibre.

(2a) $f : X \rightarrow \mathbb{P}^1$ can be obtained from Σ_{n+1} by eliminating the base points of the following pencil Λ : Take a curve $D_{[n+1],0}$ satisfying the following three conditions.

- (i) $D_{[n+1],0} \sim 3\Delta_{[n+1]} + (3n+3)\Gamma_{[n+1]}$.
- (ii) $D_{[n+1],0}$ is smooth at $(x, y) = (\infty, 0)$.
- (iii) $D_{[n+1],0}$ has a contact of order 3 with $\Gamma_{[n+1]}$ through $(\infty, 0)$.

Then the pencil Λ is generated by $(3\Delta_{[n+1]} + (3n+3)\Gamma_{[n+1]})$ and $D_{[n+1],0}$.

(2b) $f : X \rightarrow \mathbb{P}^1$ can be obtained from Σ_{n+1} by eliminating the base points of the following pencil Λ :

$$tx^3y^{3n+3} = 1 + x^3y + \sum_{i=1}^3 \sum_{j=1}^{i(n+1)} c_{i,j} x^i y^j,$$

where $c_{i,j}$ are complex numbers such with $c_{3,1} \neq -1$.

Corollary 10. Let $f : X \rightarrow \mathbb{P}^1$ be as in Propositions 8 and 9. Then the Mordell-Weil group of f is trivial.

Theorem 11.

Let X be a smooth rational surface and $f : X \rightarrow \mathbb{P}^1$ a relatively minimal trigonal fibration of genus $g \geq 3$. Assume that $\rho(X) = 3g + 8$. If $g - 2$ is divisible by three,

then the Mordell-Weil group of f is non-trivial.

If g is a multiple of three and the Mordell-Weil group of f is trivial, then f is as in Proposition 8.

If $g - 1$ is a multiple of three and that, then f is as in Proposition 9.

Conversely, the Mordell-Weil groups of fibrations as in Propositions 8 and 9 are trivial.

§4 証明の概略 Recall Theorem 6: Let X be a smooth rational surface and $f : X \rightarrow \mathbb{P}^1$ a relatively minimal fibration whose general fibre F is a trigonal curve of genus $g \geq 3$. Assume that $\rho(X) = 3g + 8$. Let (Y, G) denote the reduction of (X, F) .

Then $Y = \Sigma_d$ and $G \sim 3\Delta_{[d]} + (1 + (g + 3d)/2)\Gamma_{[d]}$

for some d such that $d \equiv g \pmod{2}$ and $0 \leq d \leq (g + 2)/3$.

Put $n = [g/3]$, where $[g/3]$ denotes the greatest integer not exceeding $g/3$. We remark that $\Gamma_{[d]}.G = 3$ and $0 \leq d \leq n + 1$,

$$\Delta_{[d]}.G = \frac{g + 2 - 3d}{2} = \begin{cases} 1 + \frac{3(n - d)}{2} \geq 1, & \text{when } g = 3n, \\ \frac{3(n + 1 - d)}{2} \geq 0, & \text{when } g = 3n + 1, \\ 2 + \frac{3(n - d)}{2} \geq 2, & \text{when } g = 3n + 2. \end{cases}$$

(再掲) Put $n = [g/3]$, where $[g/3]$ denotes the greatest integer not exceeding $g/3$. Let (Σ_d, G) be the reduction of (X, F) . We remark that $\Gamma_{[d]}.G = 3$ and $d \equiv g \pmod{2}$, $0 \leq d \leq n + 1$,

$$\Delta_{[d]}.G = \frac{g + 2 - 3d}{2} = \begin{cases} 1 + \frac{3(n-d)}{2} \geq 1, & \text{when } g = 3n, \\ \frac{3(n+1-d)}{2} \geq 0, & \text{when } g = 3n + 1, \\ 2 + \frac{3(n-d)}{2} \geq 2, & \text{when } g = 3n + 2. \end{cases}$$

Therefore, we have the following

Corollary 12. Let D an irreducible reduced curve on Σ_d .

Then the following holds.

$D.G = 0$ if and only if $D = \Delta_{[n+1]}$ with $d = n + 1$ and $g = 3n + 1$.

$D.G = 1$ if and only if $D = \Delta_{[n]}$ with $d = n$ and $g = 3n$.

$D.G = 2$ if and only if $D = \Delta_{[n]}$ with $d = n$ and $g = 3n + 2$.

Sketch of Proof of Theorem 11. Assume that $\rho(X) = 3g + 8$. Let F denote a general fibre of f . Let $\mu : (X, F) \rightarrow (Y, G)$ be the reduction. Theorem 6 gives us $Y = \Sigma_d$ and $G \sim 3\Delta_{[d]} + (1 + (g + 3d)/2)\Gamma_{[d]}$. Assume that the Mordell-Weil group of f is trivial. Then a section of f is unique. We shall denote the (-1) -section of f by E_{3g+6} . Therefore, in the process of contracting by μ , we may assume that the point corresponding to E_{i+1} is an infinitely near point of that to E_i for $i = 1, 2, \dots, 3g + 5$. We recall that $\Delta_{[d]}$, $\Gamma_{[d]}$ and E_i , $i = 1, 2, \dots, 3g + 6$ form $\mathbb{Z}$ -basis of $\text{NS}(X)$. Since $(3g + 5)$ (-2) -curves $E_i - E_{i+1}$, $i = 1, 2, \dots, 3g + 5$ are connected, a reducible singular fibre F_∞ of f contains all of them. However, they do not generate F_∞ . From $\rho(X) = 3g + 8$ and the equation $(\star)$ of the Mordell-Weil rank, the number of reducible fibres of f is at most two.

We suppose that f has a reducible fibre F_1 other than F_∞ . Let $\Theta_{1,0}$ be the identity component of F_1 . From $(\star)$, we show that F_1 has exactly one component $\Theta_{1,1}$ other than $\Theta_{1,0}$. Since $\Theta_{1,1}$ is disjoint from the zero section $(O) = E_{3g+6}$ and also from the $(3g+5)$ irreducible components $(E_i - E_{i+1})$ of the other reducible fibre F_∞ , we can regard $\Theta_{1,1}$ as an irreducible curve on Σ_d through μ . Thus, $\Theta_{1,1}.G = \Theta_{1,1}.F = 0$ through μ . Therefore, from Corollary 12 we conclude that $\Theta_{1,1}$ must be identified with the minimal section $\Delta_{[d]}$ of Σ_d with $d = n+1$ and $g = 3n+1$. Similarly, F_∞ also has exactly one component $\Theta_{\infty,1}$ other than the $(3g+5)$ irreducible components $(E_i - E_{i+1})$. Furthermore, the image of $\Theta_{\infty,1}$ on Σ_{n+1} is linearly equivalent to $3\Delta_{[n+1]} + (3n+3)\Gamma_{[n+1]}$ by Theorem 6.

From these,

$$\begin{aligned} T &\simeq \mathbb{Z}\Theta_{1,1} \oplus \mathbb{Z}\Theta_{\infty,1} \oplus \bigoplus_{i=1}^{3g+5} \mathbb{Z}(E_i - E_{i+1}) \oplus \mathbb{Z}(O) \\ &\simeq \mathbb{Z}\Delta_{[n+1]} \oplus (3n+3)\mathbb{Z}\Gamma_{[n+1]} \oplus \bigoplus_{i=1}^{3g+6} \mathbb{Z}E_i. \end{aligned}$$

This contradicts the assumption that the Mordell-Weil group of f is trivial by [Shi2, p. 362, Theorem 3].

In this way, F_∞ is the unique reducible fibre of f .

From $\rho(X) = 3g+8$ and $(\star)$,

the number of irreducible components of F_∞ is $3g+7$.

Put $\Theta_{3g+5-i} = E_i - E_{i+1}$, $i = 1, 2, \dots, 3g+5$.

We denote the two components other than them by $\Theta_{3g+6}, \Theta_{3g+5}$. We remark that μ does not contract Θ_{3g+6} and Θ_{3g+5} .

Let D_1 and D_2 , respectively, be the image of Θ_{3g+6} and Θ_{3g+5} on Σ_d .

Since $\bigoplus_{i=0}^{3g+4} \mathbb{Z}\Theta_i \oplus \mathbb{Z}(O) \simeq \bigoplus_{i=1}^{3g+6} \mathbb{Z}E_i$, by [Shi2, p. 362, Theorem 3] we have

$$\mathbb{Z}D_1 \oplus \mathbb{Z}D_2 \simeq \mathbb{Z}\Delta_{[d]} \oplus \mathbb{Z}\Gamma_{[d]}. \quad (\heartsuit)$$

If one of the two curves D_1 and D_2 is a trisection of Σ_d , which means a horizontal curve meeting a fibre of Σ_d at three points, then the other one must be a fibre of Σ_d .

Therefore, $\mathbb{Z}D_1 \oplus \mathbb{Z}D_2 \simeq 3\mathbb{Z}\Delta_{[d]} \oplus \mathbb{Z}\Gamma_{[d]}$, which contradicts $(\heartsuit)$.

Thus, at least one of them is a section of Σ_d .

In what follows, we assume that D_1 is a section of Σ_d . In particular, $D_1 \sim \Delta_{[d]} + \gamma\Gamma_{[d]}$ for some non-negative integer γ and is smooth. For $h = 0, 1, \dots, 3g+4$ and $j = 3g+5, 3g+6$, we know $\Theta_h \cdot \Theta_j \geq 0$ and $F \cdot \Theta_j = (O) \cdot \Theta_j = 0$.

Hence we have

$$\begin{aligned} \Theta_{3g+6} &= \Delta_0 + \gamma\Gamma - E_1 - E_2 - \dots - E_{D_1 \cdot G}, \quad D_1 \cdot G \leq 3g+5, \\ \Theta_{3g+5} &= \alpha\Delta_0 + \beta\Gamma - \sum_{i=1}^{3g+5} \delta_i E_i, \quad 2 \geq \alpha \geq \delta_1 \geq \delta_2 \geq \dots \geq \delta_{3g+5} \geq 0, \\ \sum_{i=1}^{3g+5} \delta_i &= D_2 \cdot G, \\ \delta_{D_2 \cdot G + 1} &= 0 \text{ for some non-negative integers } \alpha, \beta. \end{aligned}$$

Therefore we have

$$0 \leq \Theta_{3g+6} \cdot \Theta_{3g+5} = \begin{cases} D_1 \cdot D_2 - \sum_{i=1}^{D_2 \cdot G} \delta_i = D_1 \cdot D_2 - D_2 \cdot G & \text{if } D_2 \cdot G \leq D_1 \cdot G, \\ D_1 \cdot D_2 - \sum_{i=1}^{D_1 \cdot G} \delta_i \leq D_1 \cdot D_2 - D_1 \cdot G & \text{otherwise.} \end{cases}$$

Thus,

$$\min\{D_1 \cdot G, D_2 \cdot G\} \leq D_1 \cdot D_2 \quad (\diamond)$$

is a necessary condition for the Mordell-Weil group of f to be trivial.

At first, we concentrate on the case where $\Gamma_{[d]}.D_2 = 1$.

Then we may assume that $G = D_1 + 2D_2$

since suffixes can be exchanged each other if necessary.

When $D_2.G \leq D_1.G$,

we have $D_1.D_2 + 2D_2^2 = D_2.G \leq D_1.D_2$ from $(\diamond)$.

This implies $D_2^2 \leq 0$. Thus $D_2 = \Delta_{[d]}$.

However, $\mathbb{Z}D_1 \oplus \mathbb{Z}D_2 \simeq \mathbb{Z}\Delta_{[d]} \oplus \left(1 + \frac{g+3d}{2}\right) \mathbb{Z}\Gamma_{[d]}$,
which contradicts $(\heartsuit)$.

When $D_1.G \leq D_2.G$,

we have $D_1^2 + 2D_1.D_2 = D_1.G \leq D_1.D_2$ from $(\diamond)$.

This and $D_1.D_2 \geq 0$ imply $D_1^2 \leq 0$.

Hence $D_1 = \Delta_{[d]}$, which also leads a contradiction to $(\heartsuit)$.

Therefore, the case where $\Gamma_{[d]}.D_2 = 1$ does not occur.

By an argument similar to the previous case, we can show that the case where $\Gamma_{[d]}.D_2 = 2$ does not occur.

At last, we consider the case where $\Gamma_{[d]}.D_2 = 0$.

Then D_2 must be a fibre of Σ_d .

This implies that $D_1.D_2 = 1$ and $D_2.G = 3$.

From $(\diamond)$, we have $D_1.G \leq 1$.

Therefore, from Corollary 12 we conclude that $\gamma = 0$ and

$$(D_1.G, g, d) = (1, 3n, n), (0, 3n+1, n+1). \quad \square$$

研究レポート（研究論文）

素数 p を基礎にした完全数の研究

津山工業高等専門学校電気電子工学科 3 年
桐山翔伍

1. はじめに

昨年の JSEC2016 において「メルセンヌ素数とその派生数に関する研究」[K1]を発表した。この研究において、私はこれまでに知られている完全数をより一般的に扱った「素数 p を基礎にした完全数」という数を定義することに成功した。

完全数 a とは $\tau(a)$ を a を除いた約数の和としたとき、 $a = \tau(a)$ となる数のことである。私は昨年の研究において、通常の6, 28, 496, 8128, ... といった完全数は、「素数2を基礎にした完全数」ではないかと考えた。なぜならこれらは全て、2のべき乗の和 $(1 + 2 + \dots + 2^n)$ から得られるメルセンヌ素数に関係しているからである。例えば、完全数6は $6 = 2 \times 3$ であり、これは $3 (= 1 + 2)$ というメルセンヌ素数に関係し、完全数28は $2^2 \times 7$ であり、これは $7 (= 1 + 2 + 2^2)$ というメルセンヌ素数と関係している。そしてこれ以降の完全数も調べてみた限り、全て $2^n \times (\text{メルセンヌ素数})$ という形になっていたのである。

メルセンヌ素数が2のべき乗の和から得られるのであれば、3のべき乗の和 $(1 + 3 + \dots + 3^n)$ から得られるメルセンヌ素数、5のべき乗の和 $(1 + 5 + \dots + 5^n)$ から得られるメルセンヌ素数、より一般に素数 p のべき乗の和 $(1 + p + \dots + p^n)$ から得られるメルセンヌ素数というものを考えれば、これに関係した素数 p を基礎にした完全数という数があるのではないだろうかと思い、研究を行ったのである。詳細は次節にて述べるが、昨年の研究において素数 p を基礎にした完全数を定義することに成功した。そして今年は、この素数 p を基礎にした完全数の特徴をつきとめることにチャレンジした。

2. 昨年の研究

昨年行った研究の中から、今年行った研究に関連する部分を簡単に説明する。

まず素数2のべき乗の和から得られるメルセンヌ素数 ${}^2M_n$ 、すなわち、

$${}^2M_n = 1 + 2 + 2^2 + \dots + 2^{n-1}$$

となる素数 ${}^2M_n$ を考える。そして、

$$a = 2^{n-1} \times {}^2M_n$$

と置く。このとき、 $\tau(a)$ を a 以外の約数の和とすると

$$a = \tau(a)$$

が成り立つ。すなわち、このようにして得られた数 a は全て完全数であることが分かった。

そこで、素数3のべき乗の和から得られるメルセンヌ素数 ${}^3M_n$ を定義してみた。すなわち

$${}^3M_n = 1 + 3 + 3^2 + \dots + 3^{n-1}$$

という素数 ${}^3M_n$ である。そして、

$$a = 3^{n-1} \times {}^3M_n$$

なる数を研究したところ,

$$a = 2\tau(a) - {}^3M_n$$

という法則が成り立つことに気がついた. さらに素数 5 のべき乗の和から得られるメルセンヌ素数 ${}^5M_n$ を,

$${}^5M_n = 1 + 5 + \cdots + 5^{n-1}$$

という素数 ${}^5M_n$ とし,

$$a = 5^{n-1} \times {}^5M_n$$

を研究してみた. その結果,

$$a = 4\tau(a) - 3 \times {}^5M_n$$

という法則を発見した.

そこで一般に, 素数 p のべき乗の和から得られるメルセンヌ素数

$${}^pM_n = 1 + p + p^2 + \cdots + p^{n-1}$$

を定義し, ${}^pM_n$ を p メルセンヌ素数と呼ぶことにした. そして

$$a = p^{n-1} \times {}^pM_n \quad (1)$$

なる数を研究したところ

$$a = (p-1)\tau(a) - (p-2) {}^pM_n \quad (2)$$

が成り立つことを突きとめ, これを証明した. この a は ${}^pM_n$ と p^{n-1} の積から得られるため, ${}^pM_n$ 派生数と呼ぶことにした.

私は, 等式(2)が成り立つ数は, ${}^pM_n$ 派生数以外にもあるのではないかと思った. そこで, 以下を定義し研究を進めた.

定義 (${}^pM_n$ 完全数)

p を素数, ${}^pM_n$ を p メルセンヌ素数とする. このとき a が ${}^pM_n$ 完全数であるとは, a が

$$a = (p-1)\tau(a) - (p-2) {}^pM_n$$

を満たすときをいう.

(注意 1) $p \geq 3$ のとき, ${}^pM_n$ 完全数は奇数である.

3. 今回の研究方針

これまで扱われていた完全数については, 歴史的な結果がある. それは, 紀元前にユークリッドが予想し, 18 世紀にオイラーが証明した次の定理である.

定理 (ユークリッド・オイラー)

$M_n = 1 + 2 + \dots + 2^{n-1}$ とし, $a = 2^{n-1}M_n$ を考える. このとき M_n が素数ならば, a は完全数である. 逆に, 偶数 (2 の倍数) の完全数はこのような形に限る.

今回の研究においては, 上の定理(ユークリッド・オイラー)を, ${}^pM_n$ 完全数について書きかえることを目標にした.

4. $p = 3, 5, 7$ の場合の ${}^pM_n$ 完全数の研究

本研究の目標は, 定理(ユークリッド・オイラー)を, ${}^pM_n$ 完全数に書き換えることである. そのために $p = 3, 5, 7$ の場合の, 特に ${}^pM_n$ 派生数以外の ${}^pM_n$ 完全数を, フリーソフト wxMaxima を使い, 10^6 までの範囲でコンピュータを用いて調査した.

$p = 3$ の場合, ${}^3M_n$ 完全数については, ${}^3M_3 = 13$ のとき ${}^pM_n$ 派生数以外の ${}^pM_n$ 完全数として 1809 と 18549 が見つかった. これらの数を分析すると,

$$1809 = 3^3 \times 67, \quad 18549 = 3^4 \times 229$$

となっており, 1809 は素数 67 に, 18549 は素数 229 を因数として持つことが分かった. $p = 5, 7$ については, ${}^pM_n$ 派生数以外の素数 p に関する ${}^pM_n$ 完全数は見つからなかった. そこで, 本研究の目標としている定理(ユークリッド・オイラー)を見直すと, ${}^pM_n$ 完全数 a を p の倍数である $a = p^{d-1}Q$ という形のものに限り調査すればよいのではないかと考えた.

しかし, ${}^pM_n$ 完全数 a の定義から, $p \geq 3$ のとき a は奇数であるが, だからといって, a を p の倍数だけに限定することはできない. そこで, もう少し一般にして $a = p_1^{d-1}Q$ (ただし p_1, Q は素数) という形で考えた方が適切であると判断した. そして, $p = 3, 5, 7$ のときの ${}^pM_n$ 完全数 $a = p_1^{d-1}Q$ のデータを $1 \leq d \leq 20$ の範囲で調査した.

① $p = 3$ の場合: ${}^3M_n$ 完全数 $a = p_1^{d-1}Q$ のデータ (${}^3M_n = \frac{3^n - 1}{2}$, $2 \leq n \leq 7$)

n	${}^3M_n$	d	p_1	Q	完全数 a
3	13	3	3	13	$3^2 \times 13$
		4	3	67	$3^3 \times 67$
		5	3	229	$3^4 \times 229$
		8	3	6547	$3^7 \times 6547$
		17	3	129140149	$3^{16} \times 129140149$
		19	3	1162261453	$3^{18} \times 1162261453$
7	1093	7	3	1093	$3^6 \times 1093$
		11	3	176053	$3^{10} \times 176053$
		17	3	129139069	$3^{16} \times 129139069$

- ② $p = 5$ の場合 : ${}^5M_n$ 完全数 $a = p_1^{d-1}Q$ のデータ (${}^5M_n = \frac{5^n-1}{4}$, $2 \leq n \leq 7$)

n	${}^5M_n$	d	p_1	Q	完全数 a
3	31	3	5	31	$5^2 \times 31$
		7	5	78031	$5^6 \times 78031$
7	19531	3	3	8363	$3^2 \times 8363$
		7	5	19531	$5^6 \times 19531$

- ③ $p = 7$ の場合 : ${}^7M_n$ 完全数 $a = p_1^{d-1}Q$ のデータ (${}^7M_n = \frac{7^n-1}{6}$, $2 \leq n \leq 7$)

n	${}^7M_n$	d	p_1	Q	完全数 a
5	2801	5	7	2801	$7^4 \times 2801$
		6	7	103643	$7^5 \times 103643$

5. データの考察

p メルセンヌ素数 ${}^pM_n$ とは

$${}^pM_n = 1 + p + p^2 + \cdots + p^{n-1}$$

であった. これを p 進表示で考えると, 1が n 個並んだ数

$${}^pM_n = 11 \cdots 1$$

を意味する. この観点から ${}^pM_n$ 完全数 a を考察してみようと考えた. そして, 前節で得られた ${}^pM_n$ 完全数 $a = p_1^{d-1}Q$ (ただし p_1, Q は素数) の表を見て, 素数 Q を p 進表示してみた. 以下がその結果である.

- ① $p = 3$ の場合 : ${}^3M_n$ 完全数 $a = p_1^{d-1}Q$ の素因数 Q の 3進表示のデータ

n	${}^3M_n$	d	p_1	Q	Q の 3進表示
3	13	3	3	13	111
		4	3	67	2111
		5	3	229	22111
		8	3	6547	2222111
		17	3	129140149	222222222222111
		19	3	1162261453	22222222222222111
7	1093	7	3	1093	1111111
		11	3	176053	2221111111
		17	3	129139069	2222222221111111

② $p = 5$ の場合 : ${}^5M_n$ 完全数 $a = p_1^{d-1}Q$ の素因数 Q の5進表示のデータ

n	${}^5M_n$	d	p_1	Q	Q の5進表示
3	31	3	5	31	111
		7	5	78031	4444111
7	19531	4	3	8363	231423
		7	5	19531	1111111

③ $p = 7$ の場合 : ${}^7M_n$ 完全数 $a = p_1^{d-1}Q$ の素因数 Q の7進表示のデータ

n	${}^7M_n$	d	p_1	Q	Q の7進表示
5	2801	5	7	2801	11111
		6	7	103643	611111

p 進表示された Q には、次のような特徴がある.

- (1) ${}^5M_n$ 完全数における $a = 3^2 \times 8363$ 以外は, $p_1 = p$ である.
- (2) $p_1 = p$ の場合, Q を p 進表示で考えると, Q は d 桁の数であり, 1と $p-1$ という数だけで構成されている. そして, 下 n 桁まで 1 が並び, $n+1$ 桁から d 桁まで $p-1$ が並ぶ.

6. 主結果

${}^pM_n$ 完全数 $a = p_1^{d-1}Q$ (ただし p_1, Q は素数)においては, $p_1 = p$ の場合に重要なデータが得られた. すなわち, $a = p^{d-1}Q$ のときの素数 Q の p 進表示に特徴が現れた. この特徴を 10進表示で考えると,

$$Q = {}^pM_n + p^n(p-1){}^pM_{d-n} \quad (\text{ただし, } d \geq n)$$

となる. これを元に次を定義した.

定義 (擬 p メルセンヌ数)

d, n を自然数 $d \geq n$ とする. このとき ${}^pK_{d,n}$ を

$${}^pK_{d,n} = {}^pM_n + p^n(p-1){}^pM_{d-n}$$

とし, これを**擬 p メルセンヌ数**と呼ぶ.

特に, ${}^pK_{d,n}$ が素数のとき, ${}^pK_{d,n}$ を**擬 p メルセンヌ素数**という.

(注意 2) 擬 p メルセンヌ数の定義により, ${}^pK_{d,n}$ はその形から p 進表示すると, n 桁までが 1 が並び $n+1$ 桁から d 桁までが $p-1$ という数が並ぶことが分かる.

(注意 3) ${}^pK_{d,n} = (p-1)M_d - (p-2)M_n$ でもある.

(注意 4) $p = 2$ のとき, 注意 2 より ${}^2K_{d,n} = {}^2M_d$ である. すなわち, 擬 p メルセンヌ数はメルセンヌ数である.

以上の準備のもとで, 以下に今回の研究で得られた定理を述べる.

定理 1 ${}^pM_n$ を p メルセンヌ素数, ${}^pK_{d,n}$ を擬 p メルセンヌ素数とし, $a = p^{d-1} {}^pK_{d,n}$ とおく. このとき, a は ${}^pM_n$ 完全数である.

定理 1 の証明には, 高本[Ta]の P. 13 にある次の命題 1 を使う必要があった.

命題 1. $S(x)$ を x の約数の和とする. もし a と b が互いに素なら, $S(ab) = S(a)S(b)$ となる.

定理 1 の証明に命題 1 を使うため, ${}^pM_n$ 完全数 a の定義を $S(a)$ で書きかえておく. ${}^pM_n$ 完全数の定義より

$$a = (p-1)\tau(a) - (p-2) {}^pM_n$$

であり, $\tau(a) = S(a) - a$ であるので

$$a = (p-1)(S(a) - a) - (p-2) {}^pM_n$$

である. よって,

$$pa = (p-1)S(a) - (p-2) {}^pM_n \quad (3)$$

を得る.

(定理 1 の証明) (3) が成り立つことを示す. p^{d-1} と ${}^pK_{d,n}$ は互いに素であるので命題 1 より

$$S(a) = S(p^{d-1})S({}^pK_{d,n}) = \frac{p^d - 1}{p - 1} (1 + {}^pK_{d,n})$$

である. したがって,

$$\begin{aligned} (p-1)S(a) &= (p^d - 1)(1 + {}^pK_{d,n}) = p^d - 1 + pa - {}^pK_{d,n} \\ &= (p-1) {}^pM_d + pa - {}^pK_{d,n} \end{aligned}$$

である. ${}^pK_{d,n} = (p-1) {}^pM_d - (p-2) {}^pM_n$ (注意 3) より,

$$pa = (p-1)S(a) - (p-2) {}^pM_n$$

となり, a は ${}^pM_n$ 完全数である. (証明終)

7. 定理 1 の逆に関する考察

定理(ユークリッド・オイラー)に対応する定理 1 の逆が成り立つかを解決することが, 重

要な課題となった.

問題 1. p の倍数である ${}^pM_n$ 完全数は $a = p^{d-1} {}^pK_{n,d}$ に限るか.

以下, 問題 1 について考察する.

b は p を因数に持たない自然数とし $a = p^{d-1}b$ とおく. さらに, a は ${}^pM_n$ 完全数とする. このとき (3) より,

$$p^d b = (p-1)S(p^{d-1})S(b) - (p-2) {}^pM_n$$

が成り立つ. $S(p^{d-1}) = \frac{p^d-1}{p-1}$ より,

$$S(b) = \frac{p^d b + (p-2) {}^pM_n}{p^d - 1} = b + \frac{b + (p-2) {}^pM_n}{p^d - 1}$$

である. $\tau(b)$ は b を除く約数の和であるから,

$$\tau(b) = \frac{b + (p-2) {}^pM_n}{p^d - 1} = \frac{b + (p-2) {}^pM_n}{(p-1) {}^pM_d}$$

であることが分かる. よって,

$$b = (p-1)\tau(b) {}^pM_d - (p-2) {}^pM_n \quad (4)$$

を得る. 特に, b が素数のとき, $b = {}^pK_{d,n}$ であるので,

$${}^pK_{d,n} = (p-1) {}^pM_d - (p-2) {}^pM_n$$

となる.

(4) から得られる b は ${}^pM_n$ 完全数 a の定義によく似ており, 得られた結果を命題としておく.

命題 2. b は p を因数に持たない自然数とし, $a = p^{d-1}b$ とする. このとき, a が ${}^pM_n$ 完全数であるならば,

$$b = (p-1)\tau(b) {}^pM_d - (p-2) {}^pM_n$$

が成り立つ.

問題 1 が正しいとするならば, b が素数であることを示せばよい. そのためには, b が合成数であると仮定して矛盾をだせばよい.

命題 3. b は p を因数に持たないとし, $a = p^{d-1}b$ とする. さらに, a は ${}^pM_n$ 完全数であるとする. このとき, もし $d \geq n$ ならば, b の任意の素因数 q は

$$(p-1) {}^pM_d < q$$

を満たす.

(証明) a は ${}^pM_n$ 完全数であるので, b は命題 2 の等式を満たす. その等式において $b = qb'$

とすると,

$$qb' = (p-1)\tau(b) {}^pM_d - (p-2) {}^pM_n \quad (5)$$

となる. (5)は $\tau(b) = 1 + q + b' + C$ と置くと,

$$qb' = (p-1)(q + b' + C) {}^pM_d - (p-2) {}^pM_n$$

となる. ${}^pK_{d,n} = (p-1)M_d - (p-2)M_n$ より,

$$qb' = {}^pK_{d,n} + (p-1)(q + b' + C) {}^pM_d \quad (6)$$

である. $d \geq n$ より ${}^pK_{d,n} > 0$ であり, さらに(6)より

$$(q - (p-1) {}^pM_d)b' = {}^pK_{d,n} + (p-1)(q + C) {}^pM_d > 0$$

となる. したがって, $(p-1) {}^pM_d < q$ である. (証明終)

命題 3 を使って, 特に $n = d$ の場合において, 問題 1 を解決することができた.

定理 2. $p \geq 3$ のとき $n = d$ を仮定すると, 問題 1 は正しい.

(証明) b は p を因数に持たないとし, $a = p^{d-1}b$ とする. そして, $a = p^{d-1}b$ は ${}^pM_n$ 完全数であると仮定し矛盾を導く. $n = d$ より ${}^pM_d = {}^pM_n$ で, これは素数である. そして b は命題 2 の等式を満たす. すなわち

$$b = \{(p-1)\tau(b) - (p-2)\} {}^pM_d$$

である. よって, ${}^pM_d$ は b の素因数である. したがって, 命題 3 において $q = {}^pM_d$ としてもよい. しかし $(p-1) {}^pM_d < {}^pM_d$ となり矛盾する. (証明終)

定理 2 が証明できたので, 問題 1 は, 『 $p \geq 3$, $n \neq d$ で, b は素数でない』場合に, $a = p^{d-1}b$ が ${}^pM_n$ 完全数でないことを示す場合が残された. しかし, この場合を示すことはとても難しく, 今のところ私はその証明を示すことができない.

8. p の倍数でない ${}^pM_n$ 完全数

これまで, p の倍数である ${}^pM_n$ 完全数について説明してきたが, p の倍数でない ${}^pM_n$ 完全数について触れておく. これまでの調査により, 私は以下の 4 つの p の倍数でない ${}^pM_n$ 完全数を見つけている.

- (1) ${}^5M_7$ 完全数 : $a = 3^2 \times 8363$, ここで ${}^5M_7 = 19531$ である.
- (2) ${}^{31}M_{17}$ 完全数 : $a = 13 \times 1282261542060234416042729$, ここで ${}^{31}M_{17} = 568972471024107865287021434301977158534824481$ である.
- (3) ${}^{127}M_5$ 完全数 : $a = 107 \times 1725060343$, ここで ${}^{127}M_5 = 262209281$ である.
- (4) ${}^{193}M_5$ 完全数 : $a = 191 \times 266390432827$, ここで ${}^{193}M_5 = 1394714501$ である.

これらの ${}^pM_n$ 完全数はどれも $a = q^j \times r$ で q, r は素数で $q < p$ となっている. さらに, その特徴を調べるために, 素数 r は p 進表示でどのような数になるのかを考えてみた. その結果, (1)において $r = 8363$ は5進表示で6桁, (2)において $r = 1282261542060234416042729$ は31進表示で 17 桁, (3)において $r = 1725060343$ は127進表示で5桁, (4)において $r = 266390432827$ は193進表示で5桁であることがわかった. (2)から(4)について r の p 進表示での桁数は ${}^pM_n$ 完全数における n と一致する. しかし, (1)においては一致しない. そこで, (1)を ${}^5M_7$ 完全数: $a = 3 \times (3 \times 8363)$ と考え, 3×8363 の5進表示での桁数を求めると7桁となった.

p の倍数でない ${}^pM_n$ 完全数について, 現在, 私は以下の問題をたてている.

問題 2. q を p とは異なる素数とし, p の倍数でない ${}^pM_n$ 完全数 a を $a = qb$ と置く. このとき $q < p$ であり, b を p 進表示で考えたとき b の桁数は n であることは, 正しいか.

9. おわりに

昨年の JSEC2016 の後, それまでの研究を論文[K2]にまとめた. そしてまとめた論文を数学クラブの顧問の先生の勧めで日本教育学会会高専・大学部会論文誌に投稿し, 掲載された. この論文[K2]を見て, 学習院大学名誉教授の飯高茂先生が, 雑誌「現代数学」に「高校生の定義した新しい完全数」というサブタイトルで, 私の研究を紹介して評価してくださり(参考[K1], [K2]), とてもうれしく, 感謝した. 今年は定理(ユークリッドオイラー)の ${}^pM_n$ 完全数版を証明することに挑んだが, これまで述べたように, 問題 1 は条件付きではあるが定理 2 という形で証明することまではできた. また, p の倍数でない ${}^pM_n$ 完全数に関しても自らたてた問題 2 にとても関心をもっている. しかし今のところそれを証明する手立てがない.

参考文献

- [I1] 飯高茂, 数学の研究をはじめよう／高校生の定義した新しい完全数, その衝撃一前編, 現代数学 2017 年 5 月号, 現代数学社, pp. 79-85
- [I2] 飯高茂, 数学の研究をはじめよう／高校生の定義した新しい完全数, その衝撃一後編, 現代数学 2017 年 6 月号, 現代数学社, pp. 82-87
- [K1] 桐山翔伍, メルセンヌ素数とその派生数に関する研究, JSEC2016, 優等賞, 2016
- [K2] 桐山翔伍, メルセンヌ素数とその派生数の一般化に関する研究, 日本数学教育学会高専・大学部会論文誌 VOL23 No1(2017), pp. 181-190
- [Ta] 高木貞治, 初等整数論講義第 2 版, 共立出版, (1971)

正多角形から得られるルーロー図形の研究

津山工業高等専門学校 総合理工学科 2 年
加田 紘大

1. はじめに

よく知られているルーローの三角形は、正三角形の各頂点を中心に、半径がその正三角形の一辺となる円弧でできたものである（参照[1], [2]）。また、幅 s のルーローの三角形は、どの方向にも幅 s であるという特徴をもつため、辺の長さ s の正方形の中で内接しながら回転することができる。ロータリーエンジンはルーローの三角形のこの性質を利用している。またパナソニックの掃除用ロボットも部屋の隅をスムーズに掃除するために、ルーローの三角形の形状をとって主張している[3]。また、論文[4]に見られるように、ドリルの形状に関する工学的な研究も多くある。しかし、私は工学ではなく、このような不思議な形をした三角形の数学的性質に興味を覚え、普通の三角形とは違う、正三角形を対称的に膨らませた三角形にはどのような性質があるのかを研究することにした。

私は、ルーローの三角形の頂点で接線を2本引いてできた間の角が 120° である点に着目した。この理由は、ルーローの三角形を作るときの3つの円を見たとき、どの円も他の円の中心を通るからである。そしてこのとき、3つの円の中心を直線で結ぶと正三角形になる。それならば、3つの円を考え、どの円も他の円の中心を通らなくて、3つの円の中心を結んだとき正三角形となる状況から得られる対称的に膨らんだ三角形については、どんな性質があるのだろうかという疑問が沸いた。つまり、正三角形を対称的に膨らませた三角形で、頂点の角が 120° でないものについて研究したいと考えた。その後、研究は正多角形を対称的に膨らませた多角形の研究へと進んでいった。本論文では、正三角形を対称的に膨らませた三角形の研究から発見した定理と、正多角形を対称的に膨らませた多角形の研究から発見した定理を示し、これらを証明する。

2. 正三角形から得られるルーロー図形と反転図形

正三角形を対称的に膨らませた三角形を正確に定義する。

定義1（正三角形から作られるルーロー図形）.

正三角形 $A_1A_2A_3$ を考え、それを正三角形 A と呼ぶ。また、正三角形 A の重心を G とする。さらに $j = 1, 2, 3$ に対して、 A_j を中心とする半径1の円 A_j を考え、これらの隣り合う2つの円は交わっているものとする。円 A_1 と円 A_2 の交点で重心 G に近い方の点を R_1 とする。同様に円 A_2 と円 A_3 の交点で G に近い方の点を R_2 とし、さらに、円 A_3 と円 A_1 の交点で G に近い方の点を R_3 とする。このとき、3点 R_1, R_2, R_3 とその間の3つの弧 R_1R_2 , R_2R_3 , R_3R_1 で作られる図形を、正三角形 A から得られるルーロー図形と呼び、 $R[A]$ と書く。そして、3点 R_1, R_2, R_3 を $R[A]$ の頂点という。また、 $R[A]$ の1つの頂点における2つの弧の接線の間の角を、 $R[A]$ の角と呼ぶ。

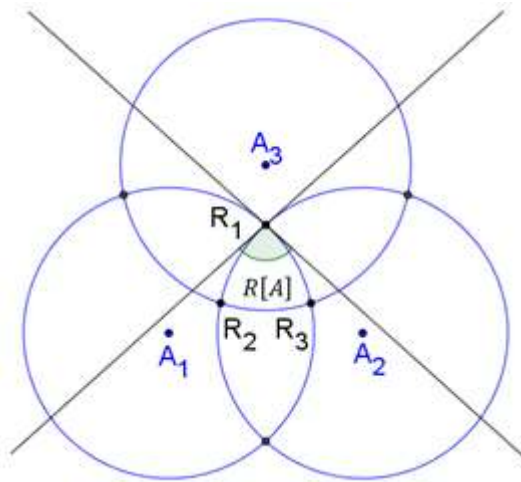


図1 ($R[A]$ と, $R[A]$ の角)

正三角形 A から得られるルーロー図形 $R[A]$ をより詳細に調べるために, フリーソフト GeoGebra を使って研究した. まず, 一般的には, $R[A]$ は凸型になるものと, 凹型になるものがあることがわかった.

(一般タイプ1) $\text{円}A_1 \cap \text{円}A_2 \cap \text{円}A_3 \neq \emptyset$ の場合, $R[A]$ は凸型である.

(一般タイプ2) $\text{円}A_1 \cap \text{円}A_2 \cap \text{円}A_3 = \emptyset$ の場合, $R[A]$ は凹型である.

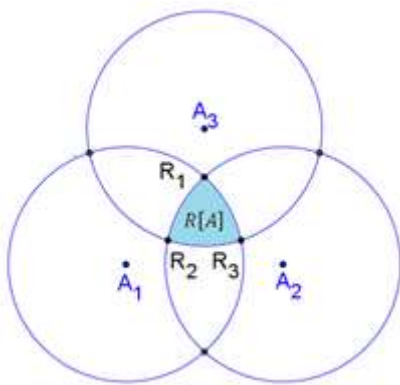


図2 (一般タイプ1)

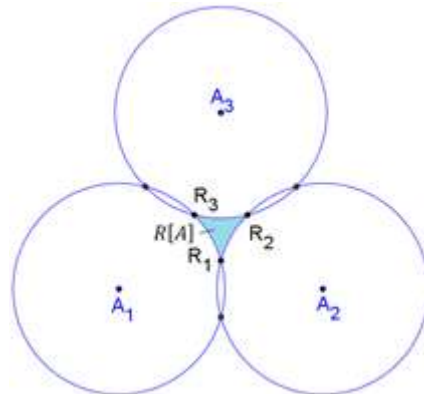


図3 (一般タイプ2)

しかし, それ以外にも, 特殊なタイプが2つ存在した. それは以下である.

(特殊タイプ1) 3点 A_1, A_2, A_3 が同じ点である場合, $R[A]$ は円である.

(特殊タイプ2) $R[A]$ が点となる場合がある.

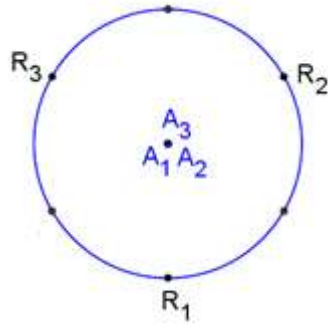


図4 (特殊タイプ1)

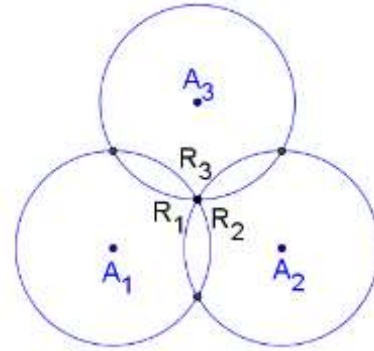


図5 (特殊タイプ2)

$R[A]$ に関係しない3点を B_1, B_2, B_3 とし、それらに着目した。ここで、円 A_1 と円 A_2 の交点で R_1 でない点を B_1 、同様に円 A_2 と円 A_3 の交点で R_2 でない点を B_2 、円 A_3 と円 A_1 の交点で R_3 でない点を B_3 としている。明らかに3点を B_1, B_2, B_3 は正三角形である。そして $j = 1, 2, 3$ に対して、 B_j を中心とする半径1の円 B_j を考え、正三角形 B から得られるルーロー図形を考えた。ここで、正三角形 B から得られるルーロー図形の頂点を R'_1, R'_2, R'_3 として、正三角形 B から得られるルーロー図形を記号で、 $R'[B]$ と表すことにする。そして次の命題を証明した。

命題1. $R'[B]$ の頂点は $R[A]$ の頂点と一致する。

(証明) 図6において、 $|B_3R_1| = |B_3A_3|$ であることを示せばよい。つまり、線分 A_3R_1 が線分 B_3B_2 の垂直二等分線であればよい。線分 A_3R_1 と線分 B_3B_2 が直交することは明らかである。したがって、 $|A_3D| = |DR_1|$ を示せばよい。

点 C を線分 A_3B_1 と A_1A_2 の交点とし、点 D を B_3 から線分 A_3R_1 へ垂線を下ろした点とする。 $\theta = \angle B_3A_3A_1 = \angle R_1A_1C$ と置く。 $\angle A_1A_3C = 30^\circ$ に注意すると、円の半径は全て1より、

$$|A_3D| = \cos(\theta + 30^\circ),$$

$$|R_1C| = \sin \theta, \quad |A_1C| = \cos \theta,$$

$$|A_3C| = \sqrt{3} \cos \theta$$

である。これより、

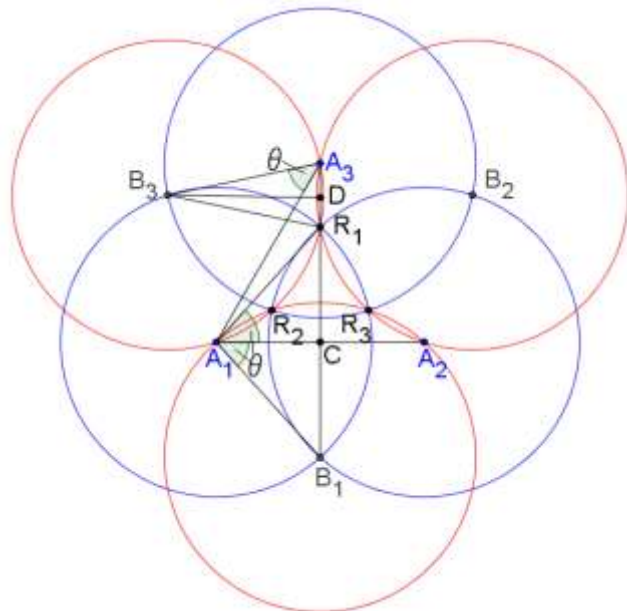


図6

$$|DR_1| = |A_3C| - |R_1C| - |A_3D| = \cos(\theta + 30^\circ) = |A_3D|$$

が得られる．すなわち，線分 A_3R_1 は線分 B_3B_2 の垂直二等分線であることが示された．

(証明終)

命題 1 より， $R'[B]$ は $R[A]$ を正三角形 $R_1 R_2 R_3$ の辺に関して反転させたものとみることができる．したがって， $R'[B]$ を改めて $R[B]$ と書く．

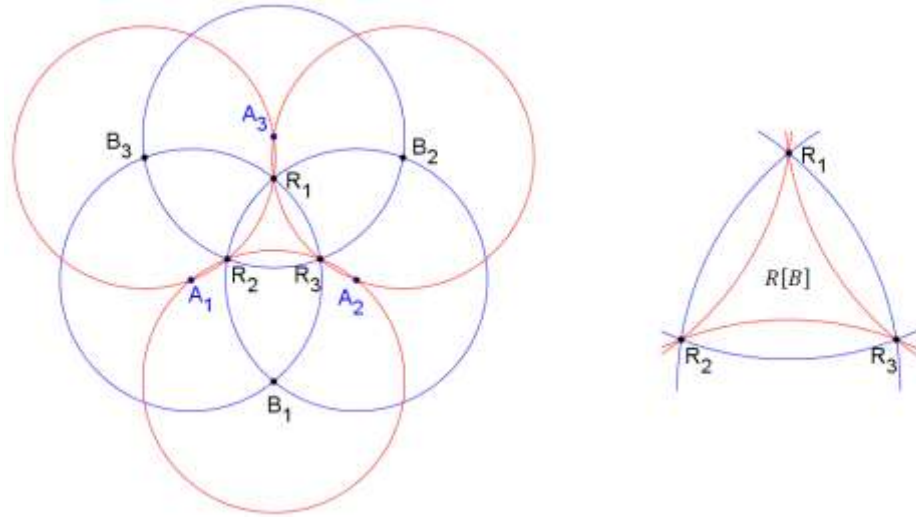


図 7 ($R[A]$ と $R[B]$)

定義 2 (反転図形). $R[B]$ を $R[A]$ の反転図形と呼ぶ．

2. 正三角形から得られるルーロー図形と反転図形の考察

$R[A]$ を正三角形 A から得られるルーロー図形， $R[B]$ を $R[A]$ の反転図形として， $R[A]$ と $R[B]$ を，(一般タイプ 1)，(一般タイプ 2)，(特殊タイプ 1)，(特殊タイプ 2) でそれぞれ考察した．

(一般タイプ 1) $R[A]$ が凸型で， $R[B]$ は凹型である．

(一般タイプ 2) $R[A]$ が凹型で， $R[B]$ は凸型である．

(特殊タイプ 1) $R[A]$ は円で， $R[B]$ は点である．

(特殊タイプ 2) $R[A]$ と $R[B]$ は同じ点である．

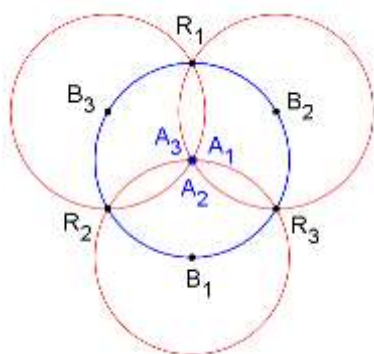


図 8 (特殊タイプ 1 の $R[A]$ と $R[B]$)

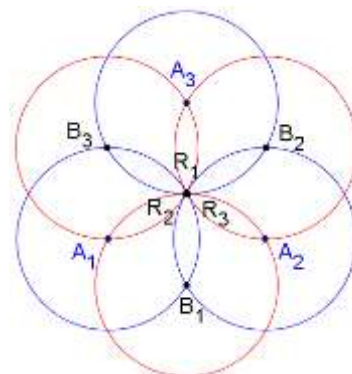


図 9 (特殊タイプ 2 の $R[A]$ と $R[B]$)

正三角形 A から得られるルーロー図形 $R[A]$ とその反転図形 $R[B]$ の角に関する研究を, GeoGebra を使って行った. そして, 一般タイプにおいて, $R[A]$ の角を α , $R[B]$ の角を β としたとき, 次の関係式を発見した.

- (1) $\alpha \leq 120^\circ$ のとき, $\alpha + \beta = 120^\circ$, (2) $\alpha > 120^\circ$ のとき, $\alpha - \beta = 120^\circ$

上の結果を特殊タイプにも対応できるようにするために, 特殊タイプ 1 と 2 の $R[A]$ の角 α と $R[B]$ の角 β については, 以下のように定義すると良いことが分かった.

- (1) $R[A]$ または $R[B]$ が点であるときのそれらの角は 60° と定義する.
 (2) $R[A]$ または $R[B]$ が円であるときのそれらの角は 180° と定義する.

3. 正三角形から作られるルーロー図形に関する定理

以下に, 正三角形 A から得られるルーロー図形 $R[A]$ とその反転図形 $R[B]$ の角に関する定理について述べ, それを証明する.

定理 1. $R[A]$ の角を α , $R[B]$ の角を β とすると, 以下が成り立つ.

- (1) $\alpha \leq 120^\circ$ のとき, $\alpha + \beta = 120^\circ$, (2) $\alpha > 120^\circ$ のとき, $\alpha - \beta = 120^\circ$

定理 1 を証明するには, 次の命題が必要となるので, まずこれを示す.

命題 2. $R[A]$ の頂点 R_j について, R_j を通る 2 つの円 A_i と円 B_k の R_j の 2 つの接線の間の角は 60° である. 例えば図 10 でいえば, 点 R_2 における円 A_2 の接線 HI と, 点 R_2 における円 B_1 の接線 JK との間の角 $\gamma = \angle HR_2J$ は 60° である.

(証明) 図 1 0 において, 三角形 $R_2B_1A_2$ は正三角形であるので, $\angle B_1R_2A_2 = 60^\circ$ である. このことと, 円 A_2 の接線 HI と円 B_1 の接線 JK から,

$$\angle JR_2I = 2 \times 90^\circ - 60^\circ = 120^\circ$$

したがって, 角 $\gamma = \angle HR_2J = 60^\circ$

(証明終)

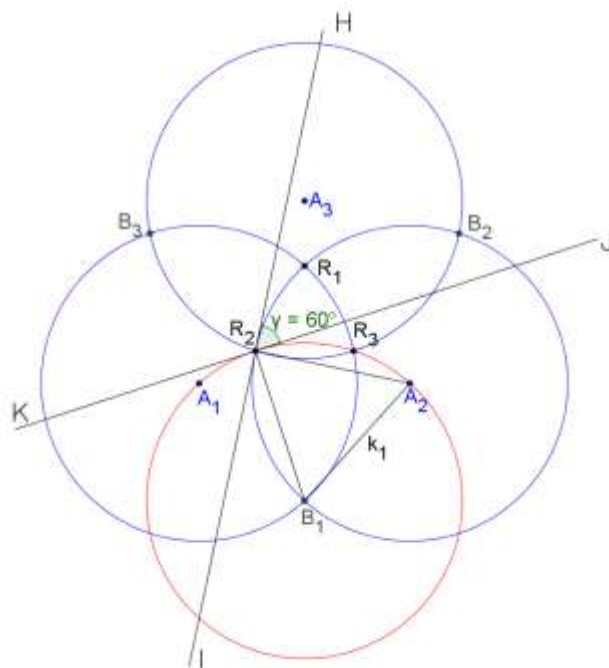


図 1 0 (角 $\gamma = \angle HR_2J$)

(定理 1 の証明) (1) の場合, すなわち $\alpha + \beta = 120^\circ$ であることを, 図 1 1 を用いて示す.

点 R_2 において図 1 1 では $\alpha = \angle HR_2P = \angle QR_2I$ である. また $\beta = \angle LR_2J$ である. $\gamma' = \angle JR_2I$ と置くと, 命題 2 より $\gamma' = 120^\circ$ である. そして $\gamma' = \angle QR_2L$ である. したがって, 点 R_2 の周りの角から,

$$\alpha + \beta + 2\gamma' = 360^\circ$$

が成り立つ. よって

$$\alpha + \beta = 120^\circ$$

である. (2) の場合も同様に示される. (証明終)

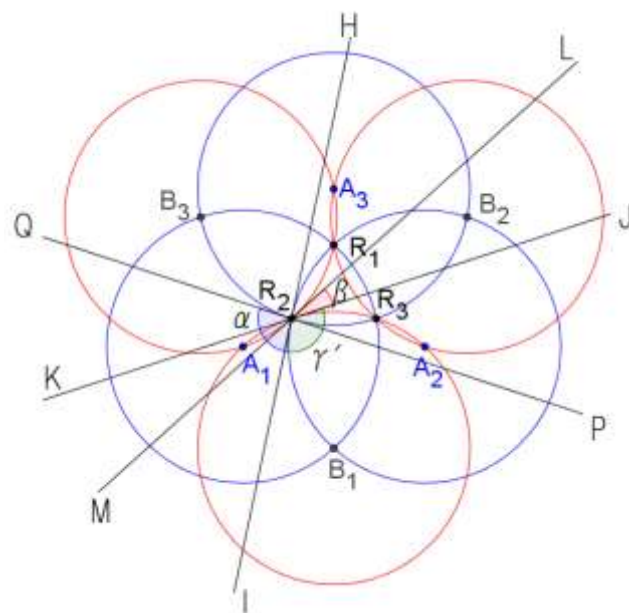


図 1 1

4. 正 n 角形から得られるルーロー図形

正三角形 A から得られるルーロー図形 $R[A]$ を一般化するために、正 n 角形での研究を行うことにした.

定義 3 (正 n 角形から得られるルーロー図形).

$n \geq 3$ とし、正 n 角形 $A_1A_2 \cdots A_n$ を考え、それを正 n 角形 A と呼ぶ. そしてその重心を G とする. さらに $j = 1, 2, \dots, n$ に対して、 A_j を中心とする半径 1 の円 A_j を考え、これらの隣り合う 2 つの円は交わっているものとする. 円 A_j と円 A_{j+1} の交点で重心 G に近い方の点を R_j とする (ただし、 $j = n$ のとき $j + 1$ は 1 とする). このとき、 n 個の点 $R_1, R_2, \dots, R_n$ とその間の n 個の弧 $R_1R_2, R_2R_3, \dots, R_nR_1$ から作られる図形を、正 n 角形 A から得られるルーロー図形と呼び、 $R_n[A]$ と書く. そして、点 R_j を $R_n[A]$ の頂点という. また、 $R_n[A]$ の 1 つの頂点における 2 つの弧の接線の間の角を、 $R_n[A]$ の角と呼ぶ.

定義 4 ($R_n[A]$ に付随する図形).

$R_n[A]$ について円 A_1 と円 A_2 の交点で R_1 でない点を B_1 、同様に円 A_2 と円 A_3 の交点で R_2 でない点を B_2 というように、 n 個の点 $B_1, B_2, \dots, B_n$ を考える. そして $j = 1, 2, \dots, n$ に対して、 B_j を中心とする半径 1 の円 B_j を考える. このとき円 B_j と円 B_{j+1} の交点で R_{j+1} でない点を R'_{j+1} とする. ただし、 $j = n$ のときは、円 B_n と円 B_1 の交点で R_1 でない点を R'_1 とする. このとき、 n 個の点 $R'_1, R'_2, \dots, R'_n$ とその間の n 個の弧 $R'_1R'_2, R'_2R'_3, \dots, R'_nR'_1$ で作られる図形を $R'_n[B]$ と書き、 $R'_n[B]$ を $R_n[A]$ に付随する図形と呼ぶ.

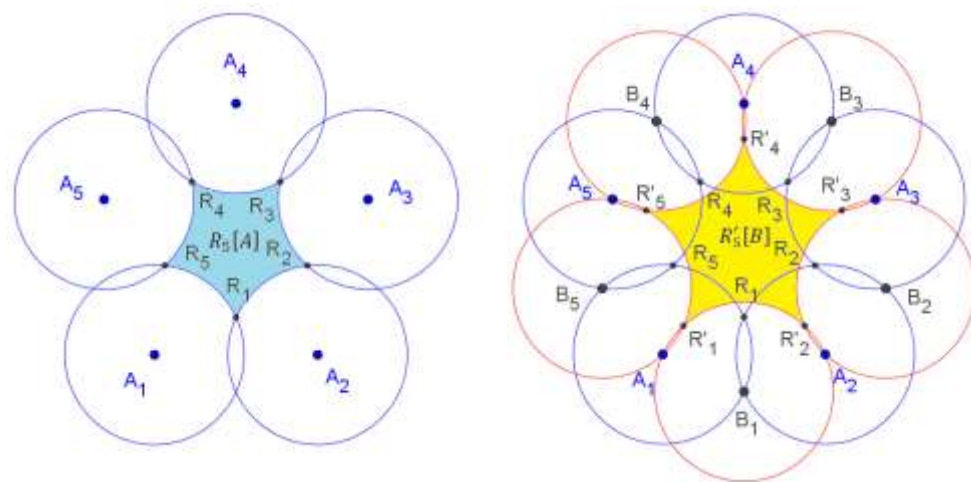


図 1.2 ($R_5[A]$ と $R_5[A]$ に付随する図形 $R'_5[B]$)

(注意) $n = 3$ のとき、命題 1 と定義 2 により、 $R_3[A]$ に付随する図形 $R'_3[B]$ は、 $R_3[A]$ の反転図形である.

$R_n[A]$ についても特殊タイプが2つあり、それらの場合の角を、以下のように定義しておく必要がある。

(特殊タイプ1) n 個の点 A_j が同じ点 G である場合、その反転図形 $R_n[B]$ は円となるが、この場合の円 $R_n[B]$ の角は 180° と定義する。

(特殊タイプ2) $R_n[A] = R_n[B]$ で点となる場合、その角は $\frac{180^\circ(n-2)}{n}$ と定義する。

5. 正 n 角形から得られるルーロー図形に関する定理

正三角形 A から得られるルーロー図形に関する定理1を一般化した次の定理を発見し、証明することができた。

定理2. 正 n 角形 A から作られるルーロー図形 $R_n[A]$ の角を α , $R_n[A]$ に付随する図形 $R_n[B]$ の角を β とすると、以下が成り立つ。

$$(1) \alpha \leq \frac{360^\circ}{n} \text{ のとき, } \alpha + \beta = \frac{360^\circ}{n}, \quad (2) \alpha > \frac{360^\circ}{n} \text{ のとき, } \alpha - \beta = \frac{360^\circ}{n}$$

証明には以下の2つの命題を使う。まずこれらを証明する。

命題3. $R_n[A]$ と $R_n[B]$ の中の角 $\angle R'_j B_j A_{j+1}$ について、

$$\angle R'_j B_j A_{j+1} = \frac{180^\circ(n-2)}{n}$$

が成り立つ。

(証明) 図13を用いて示す。

$|A_j B_{j-1}| = |A_j B_j| = |R'_j B_j| = |R'_j B_{j-1}| = 1$ より、四角形 $A_j B_{j-1} R'_j B_j$ は菱形である。同様に、四角形 $A_{j+1} B_j R'_{j+1} B_{j+1}$ も菱形である。よって、

$$\angle R'_j B_j B_{j-1} = \angle A_{j+1} B_j B_{j+1}$$

である。正 n 角形の1つの角 $\angle B_{j-1} B_j B_{j+1}$ は

$$\angle B_{j-1} B_j B_{j+1} = \frac{180^\circ(n-2)}{n}$$

であるので、命題が成り立つ。(証明終)

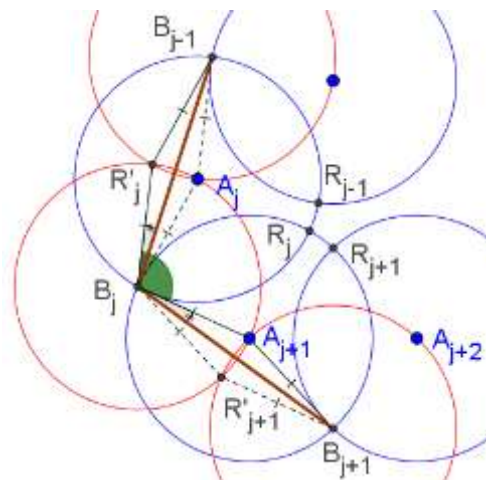


図13

命題 4. $R_n[A]$ と $R_n[B]$ を考える. このとき, 円 A_j の点 B_{j-1} における接線と, 円 B_j の点 R'_j における接線は平行である.

(証明) 図 1 4 を用いて示す.

$$|A_j B_{j-1}| = |B_{j-1} R'_j| = |R'_j B_j| = |A_j B_j| = 1$$

より, 四角形 $A_j B_{j-1} R'_j B_j$ は菱形である.

また, $\angle A_j B_{j-1} E = \angle B_j R'_j D = 90^\circ$ である. したがって, 接線 $B_{j-1} E$ と接線 $R'_j D$ は平行である. (証明終)

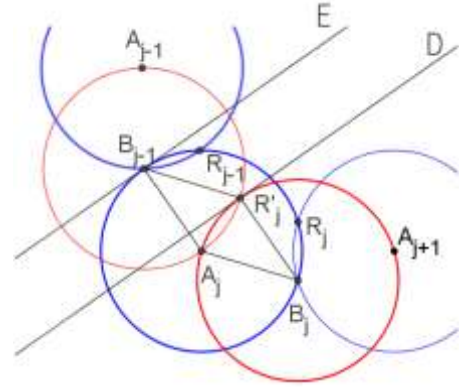


図 1 4

(定理 2 の証明) 図 1 5 を用いて(1)の場合を示す.

先ず対称性から, $\alpha = \angle P B_j Q$ としてよい.

命題 5 より, 直線 TQ と VW は平行なので

$\angle B_j D R'_{j+1} = \alpha$ である. 命題 3 より,

$$\gamma = \frac{180^\circ(n-2)}{n}$$

である. また,

$$\angle R'_{j+1} B_j D = \gamma - 90^\circ, \angle B_j R'_{j+1} D = \beta + 90^\circ$$

である. よって三角形 $B_j R'_{j+1} D$ より,

$$(\gamma - 90^\circ) + (\beta + 90^\circ) + \alpha = 180^\circ$$

である. したがって,

$$\alpha + \beta = \frac{360^\circ}{n}$$

が成り立つ. (2)も同様に示される. (証明終)

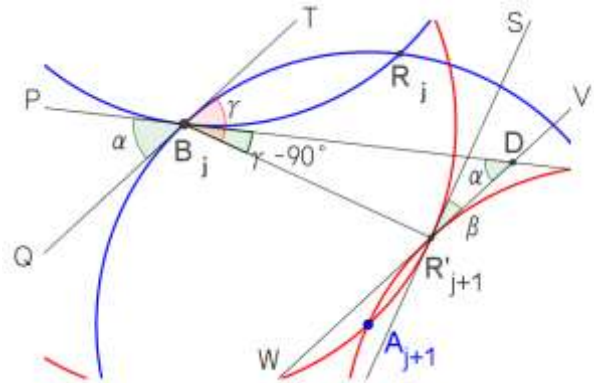


図 1 5

6. まとめと今後の研究方針

以上が, 今年度の研究成果である. 研究をスタートした頃は, いろいろな正三角形 A から得られるルーロー図形 $R[A]$ を描くために, GeoGebra の使い方をマスターすることに明け暮れた. そして, GeoGebra の使い方がある程度理解でき, $R[A]$ をスムーズに描き, 多くのデータをとれるようになったと同時に, $R[A]$ の反転図形を発見し, それにより定理 1 を発見することができた. 研究対象を正面からだけ見てはダメで, 他の側面を見ることで, その研究対象の性質が見えてくるという体験ができたことはとてもうれしかった. その後, 定理

2を発見するのに時間はかからなかった．しかしそれを証明するまでにはかなりの時間がかかった．命題5の平行線を発見したことが大きな手掛かりとなり，それが定理2の証明に繋がった．

さて，これからの研究方針であるが，今年度取り組んできたルーロー図形を振り返ると，これらはすべて同半径の円を基礎として扱った曲線図形の研究である．円は離心率0の2次曲線であることを考えると，この視点から離心率1の放物線，離心率が0から1の間にある楕円，そして離心率が1より大きくなる双曲線を基礎として，ルーロー図形のような曲線で囲まれた図形を定義できるのではないだろうかと考えている．それは，任意の2次曲線を基礎とした曲線図形で不変な性質を研究することを意味するものである．現在，GeoGebraで離心率が0から1まで変化させてできる3つ合同な2次曲線から曲線図形を作って，それらを自由に動かすプログラムまでは完成させている．そして，それを使っていくつかの実験と観察をおこなっているが，まだ面白い現象を捉えてはいない．

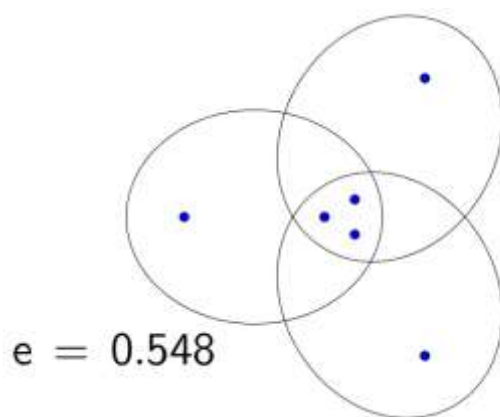


図16 (楕円によるルーロー図形)

参考文献

- [1] ルーローの三角形, Wikipedia,
<https://ja.wikipedia.org/wiki/%E3%83%AB%E3%83%BC%E3%83%AD%E3%83%BC%E3%81%AE%E4%B8%89%E8%A7%92%E5%BD%A2>
- [2] ルーローの多角形, Wikipedia,
<https://ja.wikipedia.org/wiki/%E3%83%AB%E3%83%BC%E3%83%AD%E3%83%BC%E3%81%AE%E5%A4%9A%E8%A7%92%E5%BD%A2>
- [3] ルーローの三角形と図形問題,
http://www.fumiononaka.com/Sample/Creators_MeetUp/Creators_MeetUp_161124.html
- [4] W.Gleiftner, H.Zeitler, The Reuleaux Triangle and its Center of Mass, Results in Mathematics, May 2000, Volume 37, Issue 3-4, pp 335-344

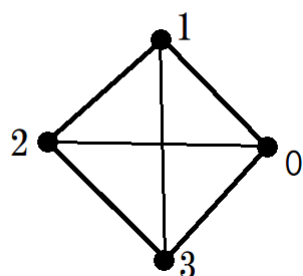
$\mathbb{Z}/m\mathbb{Z}$ からつくるグラフの曲面への 埋め込みについて

圓山 夏生

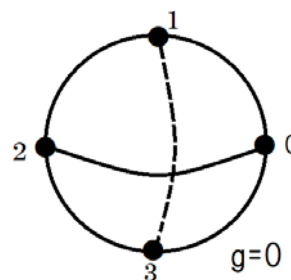
津山高専・総合理工学科・先進科学系2年

完全グラフとは、任意の二点の間に必ず枝(線分)があるものを指す。

完全グラフ K_4



K_4 は球に埋め込むことができる。



<定理>

完全グラフ K_n は, genus

$$g = \left\lceil \frac{(n-3)(n-4)}{12} \right\rceil$$

の曲面に埋め込まれる。

研究の方法

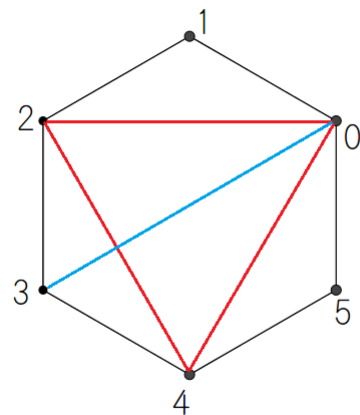
完全グラフでないものはあまり分かっていない。

そこで今回は、 $\mathbb{Z}/m\mathbb{Z}$ のルールを、グラフと考えて、
どのgenusの曲面に埋め込まれるのか研究した。

$\mathbb{Z}/6\mathbb{Z}$ について

$\times$	1	2	3	4	5	0
1	1	2	3	4	5	0
2	2	4	0	2	4	0
3	3	0	3	0	3	0
4	4	2	0	4	2	0
5	5	4	3	2	1	0

$\mathbb{Z}/6\mathbb{Z}$ のグラフ

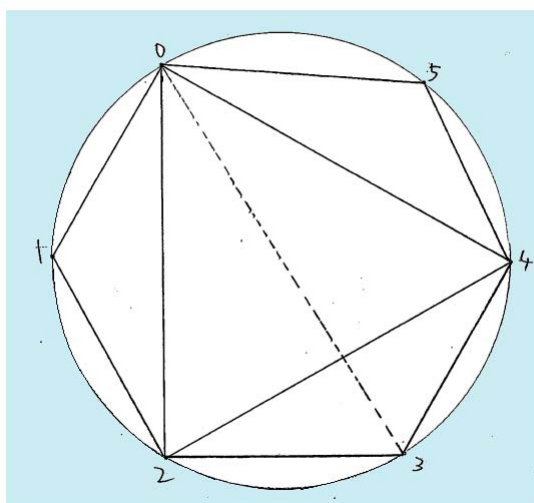


$0 \leq g \leq 1$ である。

完全グラフではない。

【問題】 g はいくつか？

$\mathbb{Z}/6\mathbb{Z}$ のグラフの $g=0$ 曲面への埋め込み

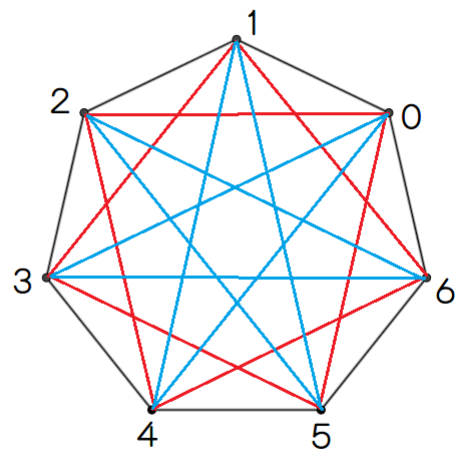


$\mathbb{Z}/7\mathbb{Z}$ について

$\times$	1	2	3	4	5	6	0
1	1	2	3	4	5	6	0
2	2	4	6	1	3	5	0
3	3	6	2	5	1	4	0
4	4	1	5	2	6	3	0
5	5	3	1	6	4	2	0
6	6	5	4	3	2	1	0

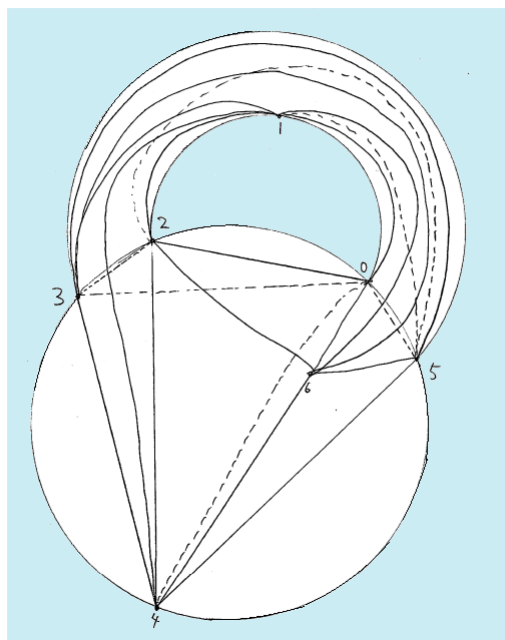
$g=1$ である。

$\mathbb{Z}/7\mathbb{Z}$ のグラフ



完全グラフ

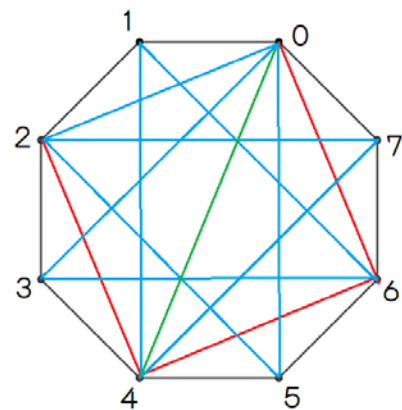
$\mathbb{Z}/7\mathbb{Z}$ のグラフの $g=0$ 曲面への埋め込み



$\mathbb{Z}/8\mathbb{Z}$ について

$\times$	1	2	3	4	5	6	7	0
1	1	2	3	4	5	6	7	0
2	2	4	6	0	2	4	6	0
3	3	6	1	4	7	2	5	0
4	4	0	4	0	4	0	4	0
5	5	2	7	4	1	6	3	0
6	6	4	2	0	6	4	3	0
7	7	6	5	4	3	2	1	0

$\mathbb{Z}/8\mathbb{Z}$ のグラフ

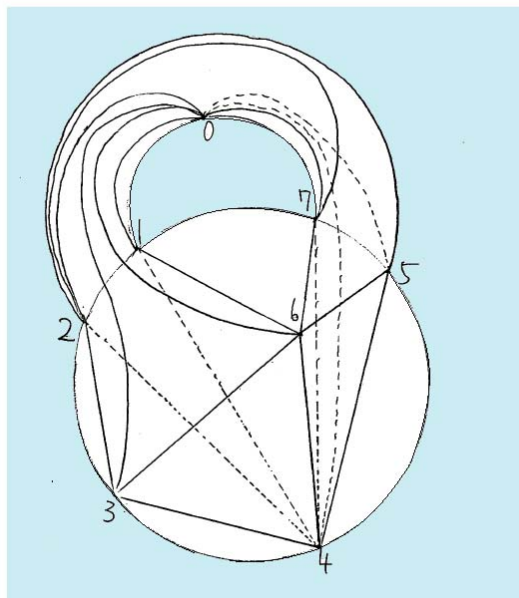


完全グラフではない。

$0 \leq g \leq 2$ である。

【問題】 g はいくつか？

$\mathbb{Z}/8\mathbb{Z}$ のグラフの $g=1$ 曲面への埋め込み



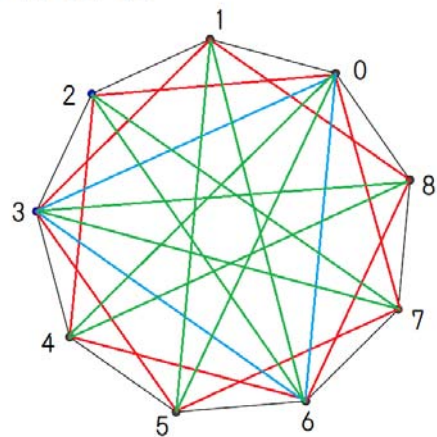
$\mathbb{Z}/9\mathbb{Z}$ について

$\times$	1	2	3	4	5	6	7	8	0
1	1	2	3	4	5	6	7	8	0
2	2	4	6	8	1	3	5	7	0
3	3	6	0	3	6	0	3	6	0
4	4	8	3	7	2	6	1	5	0
5	5	1	6	2	7	3	8	4	0
6	6	3	0	6	3	0	6	3	0
7	7	5	3	1	8	6	4	2	0
8	8	7	6	5	4	3	2	1	0

$0 \leq g \leq 3$ である。

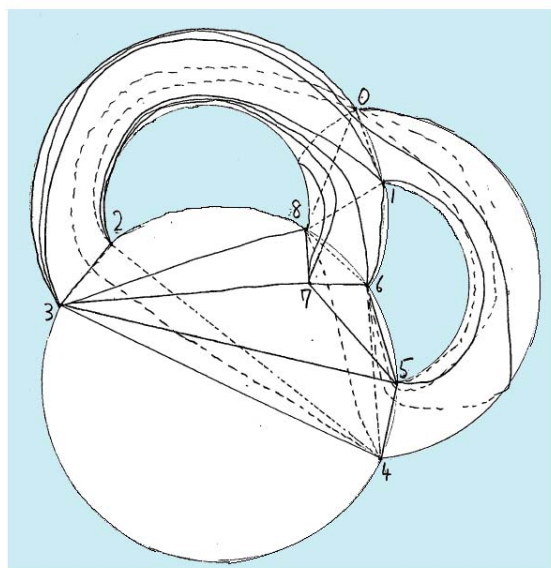
【問題】 g はいくつか？

$\mathbb{Z}/9\mathbb{Z}$ のグラフ



完全グラフではない。

$\mathbb{Z}/9\mathbb{Z}$ のグラフの $g=2$ 曲面への埋め込み



まとめ

	作れた曲面
$\mathbb{Z}/6\mathbb{Z} \quad 0 \leq g \leq 1$	$g=0$
$\mathbb{Z}/7\mathbb{Z} \quad g=1$ (完全グラフ)	$g=1$
$\mathbb{Z}/8\mathbb{Z} \quad 0 \leq g \leq 2$	$g=2$
$\mathbb{Z}/9\mathbb{Z} \quad 0 \leq g \leq 3$	$g=2$

Rational unicuspidal curves on $\mathbb{Q}$ -homology projective planes whose complements have logarithmic Kodaira dimension $-\infty$

Hideo Kojima (Niigata University)

§1. Introduction

$/\mathbb{C}$

· A cuspidal curve means a projective curve whose singular points are locally irreducible.

Definition. Let S be a normal algebraic surface.

- (1) S is called a $\mathbb{Q}$ -homology projective plane if it has only quotient singular points (i.e., klt singular points) and $H_i(S; \mathbb{Q}) \cong H_i(\mathbb{P}^2; \mathbb{Q})$ for all $i \geq 0$.
- (2) S is called a log $\mathbb{Q}$ -homology plane if it has only quotient singular points and $H_i(S; \mathbb{Q}) \cong H_i(\mathbb{C}^2; \mathbb{Q})$ for all $i \geq 0$.

§2. Results of Gurjar–Hwang–Kolté

Theorem 1. ([1]) *Let S be a $\mathbb{Q}$ -homology projective plane and set $S^0 = S - \text{Sing } S$. Let C be a rational cuspidal curve in S^0 . Then the following assertions hold true.*

- (1) *If the logarithmic Kodaira dimension of a resolution of $S - C$ is $-\infty$, then $\bar{\kappa}(S^0 - C) = -\infty$ and $\# \text{Sing } C \leq 1$.*
- (2) *If $\bar{\kappa}(S^0 - C) \leq 1$, then $\# \text{Sing } C \leq 2$.*
- (3) *$\bar{\kappa}(S^0 - C) \neq 0$.*

The assertions (1) and (2) of Theorem 1 generalize results of Wakabayashi [7, Theorem], and the assertion (3) generalizes Orevkov [6, Theorem B(c)]. (See also Yoshihara [8] and the author [3] for results related to them.)

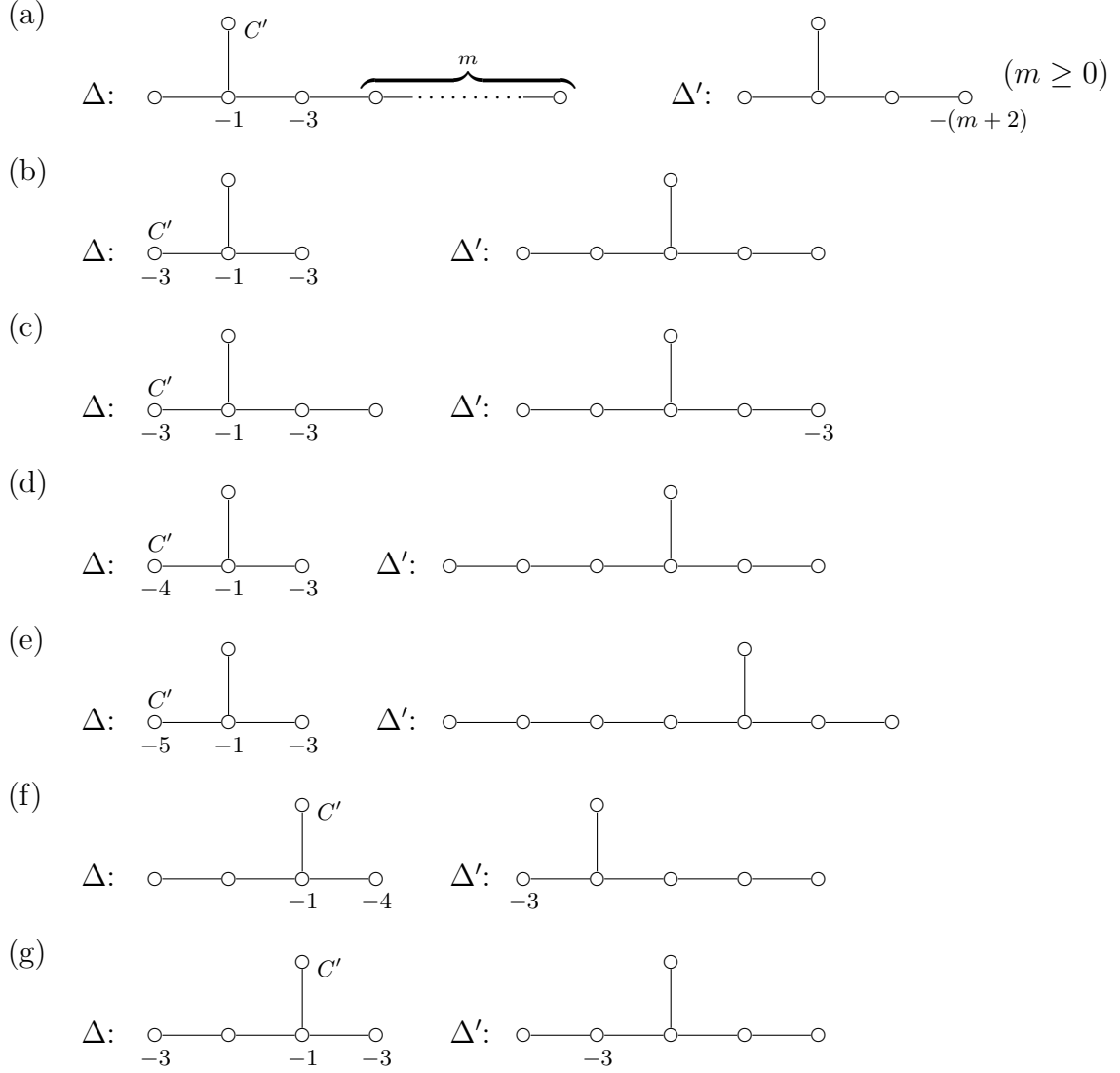
§3. Results of this talk

Let S be a $\mathbb{Q}$ -homology projective plane and set $S^0 = S - \text{Sing } S$. Let C be a rational cuspidal curve in S^0 . Let $\pi : V \rightarrow S$ be a resolution of singularities of both S and C such that $\pi^{-1}(C)$ is a simple normal crossing divisor. Here $\Delta' = \pi^{-1}(\text{Sing } S)$ is a simple normal crossing divisor since S has at worst quotient singular points. Set $D = \Delta + \Delta'$. We assume further that the map π is minimal, that is, the Picard number of V is the least possible. Then such a map π is determined uniquely. We call the map π the minimal SNC-map for (S, C) .

The main result of this talk is the following.

Theorem 2. ([4]) *Let S be a $\mathbb{Q}$ -homology projective plane and C a rational cuspidal curve with $\# \text{Sing } C \leq 1$ in $S^0 = S - \text{Sing } S$. Let $\pi : V \rightarrow S$ be the minimal SNC-map for the pair (S, C) and set $\Delta = \pi^{-1}(C)$, $\Delta' = \pi^{-1}(\text{Sing } S)$ and $D = \Delta + \Delta'$. Let C' be the proper transform of C on V . Then the following assertions hold.*

- (1) *$S^0 - C$ is affine ruled if and only if $C'^2 \geq -1$.*
- (2) *Assume that $C'^2 \leq -2$ and $\bar{\kappa}(S^0 - C) = -\infty$. Then $-5 \leq C'^2 \leq -2$ and the weighted dual graph of $D = \Delta + \Delta'$ is one of (a)–(g), where we omit the weight corresponding to a (-2) -curve. All the cases (a)–(g) can be realized.*



REFERENCES

- [1] R. V. Gurjar, D.-S. Hwang and S. Kolte, *A note on rational cuspidal curves on $\mathbb{Q}$ -homology projective planes*, J. Ramanujan Math. Soc. **32** (2017), 135–146.
- [2] S. Iitaka, *The virtual singularity theorem and the logarithmic bigenus theorem*, Tohoku Math. J. **32** (1980), 337–351.
- [3] H. Kojima, *Complements of plane curves with logarithmic Kodaira dimension zero*, J. Math. Soc. Japan **52** (2000), 793–806.
- [4] H. Kojima, *Rational unicuspidal curves on $\mathbb{Q}$ -homology projective planes whose complements have logarithmic Kodaira dimension $-\infty$* , Nihonkai Math. J., to appear.
- [5] M. Miyanishi and S. Tsunoda, *Logarithmic del Pezzo surfaces of rank one with non-connected boundaries at infinity*, Japan. J. Math. **10** (1984), 271–319.
- [6] S. Yu Orevkov, *On rational cuspidal curves I. Sharp estimate for degree via multiplicities*, Math. Ann. **324** (2002), 657–673.
- [7] I. Wakabayashi, *On the logarithmic Kodaira dimension of the complement of a curve in $\mathbb{P}^2$* , Proc. Japan Acad. **54** (1978), 157–162.
- [8] H. Yoshihara, *On plane rational curves*, Proc. Japan Acad. **55** (1979), 152–155.
- [9] H. Yoshihara, *Rational curves with one cusp*, Sugaku **40** (1988), 269–271 (in Japanese).

偏極多様体の随伴束の大域切断の なす次元に関する話題

高知大学 理工学部 福間 慶明

設定

X : 複素数体上定義された n 次元非特異射影多様体

L : X 上の因子

L : 豊富な因子 $\Rightarrow (X, L)$: 偏極多様体

L : nefかつbigな因子 $\Rightarrow (X, L)$: 準偏極多様体

今日考えること

随伴束の大域切断の次元に関する考察

⇒ (準)偏極多様体の不変量を用いた立場から見てみる.

今日考えること

今日は主に L が豊富な場合について考える.

⇒ 随伴束の大域切断の次元についての問題とそれに関連する話をする.

話の構成

1. 断面幾何種数と随伴束の大域切断の次元との関係について.
2. BS予想に関する話について.
3. 随伴束の大域切断の次元に関する予想・問題とわかっていることについて.

Beltramette-Sommese 予想について

(Conjecture 1) [Beltrametti-Sommese (1995)]

$(X, L): n$ 次元非特異偏極多様体

$K_X + (n - 1)L$ が nef.

$\implies h^0(K_X + (n - 1)L) > 0.$

以下, この予想を **BS 予想** と呼ぶ.

Beltramette-Sommese予想について

(BS予想についてわかっていること)

- (i) $\dim X \leq 2$ の場合は知られていた.
- (ii) $\dim X = 3$ の場合 (2006).
- (iii) $\dim X = n$ かつ $h^0(L) > 0$ の場合
Höring (2012).
- (iv) $\dim X = 4$ の場合 (2016).

1. 断面幾何種数について

この考察に必要な偏極多様体の不変量

⇒ 断面幾何種数

以下でこれについて解説する.

1. 断面幾何種数について

Notation 1

X : n 次元射影多様体 L : X 上の直線束

$\Rightarrow \chi(L^{\otimes t})$: t に関する多項式で次数が高々 n .

$\Rightarrow \chi(L^{\otimes t}) = \sum_{k=0}^n \chi_k(X, L) \binom{t+k-1}{k}$
という形に一意的に書ける.

1. 断面幾何種数について

Definition 2 (断面幾何種数)

(X, L) : n 次元準偏極多様体

i : $0 \leq i \leq n$ なる任意の整数

$\Rightarrow (X, L)$ の第 i 断面幾何種数 $g_i(X, L)$

$$g_i(X, L) := (-1)^i (\chi_{n-i}(X, L) - \chi(\mathcal{O}_X)) \\ + \sum_{j=0}^{n-i} (-1)^{n-i-j} h^{n-j}(\mathcal{O}_X)$$

1. 断面幾何種数について

Remark 3.

(i) $g_i(X, L) \in \mathbb{Z}$.

(ii) $\cdot i = 0 \Rightarrow g_0(X, L) = L^n$: 次数.

$\cdot i = 1 \Rightarrow g_1(X, L) = g(X, L)$: 断面種数.

$\cdot i = n \Rightarrow g_n(X, L) = h^n(\mathcal{O}_X)$.

断面幾何種数の幾何的意味

X を非特異, L を nef かつ big で **基点自由**

i を $1 \leq i \leq n - 1$ をみたす整数

$\Rightarrow |L|$ の $n - i$ 個の一般の元の intersection Z_{n-i} は i 次元非特異射影多様体

$\Rightarrow g_i(X, L) = h^i(\mathcal{O}_{Z_{n-i}})$

断面幾何種数の幾何的意味

$\Rightarrow g_i(X, L)$ は一般に (X, L) が n 次元準偏極多様体のとき i 次元非特異射影多様体の幾何種数の持つ性質と類似の性質を持つのではないか? という期待が生じる.

断面幾何種数の幾何的意味

i 次元非特異射影多様体の幾何種数に関する結果

$\Rightarrow$ 第 i 断面幾何種数などを使って
 n 次元準偏極多様体の問題へ言い換え可能!

曲面論から準偏極多様体論への言い換え

Theorem 4.

S : 一般型曲面 $\Rightarrow h^2(\mathcal{O}_S) \geq h^1(\mathcal{O}_S)$.

$\Rightarrow$ この準偏極多様体版は以下の通り

Conjecture A.

(X, L) : n 次元非特異準偏極多様体で

$\kappa(K_X + (n - 2)L) \geq 2$

$\Rightarrow g_2(X, L) \geq h^1(\mathcal{O}_X)$.

Conjecture Aについて

Conjecture Aについてわかっていること.

(i) $n = 3$ の時は正しい.

(ii) $n \geq 4$ かつ $\kappa(X) \geq 0$ の時も正しい.

断面幾何種数に関する不等式

Proposition 5.

X を非特異, L を nef かつ big で **基点自由**
 i を $0 \leq i \leq n$ をみたす整数

$$\Rightarrow g_i(X, L) \geq h^i(\mathcal{O}_X).$$

↓ 一般にも成立するのでは?

断面幾何種数に関する不等式

Conjecture B.

X を非特異, L を nef かつ big
 i を $0 \leq i \leq n$ をみたす整数
 $\Rightarrow g_i(X, L) \geq h^i(\mathcal{O}_X).$

Conjecture Bについて

Remark 6.

$$\cdot i = 0 \Rightarrow g_0(X, L) = L^n \geq 1 = h^0(\mathcal{O}_X).$$

$$\cdot i = 1 \Rightarrow \text{藤田氏による予想.}$$

$$\cdot i = n \Rightarrow g_n(X, L) = h^n(\mathcal{O}_X).$$

後で述べるように

上記Conjecture AとBは, BS予想と関係がある.

断面幾何種数と随伴束の大域切断の次元 との関係

$(X, L) : n$ 次元偏極多様体

(Definition) 任意の正整数 t と $1 \leq i \leq n$ なる任意の整数 i に対して

$$F_0(t) := h^0(K_X + tL)$$

$$F_i(t) := F_{i-1}(t+1) - F_{i-1}(t).$$

断面幾何種数と随伴束の大域切断の次元 との関係

(Definition)

$0 \leq i \leq n$ なる任意の整数 i に対して
 $A_i(X, L) := F_{n-i}(1)$ と定義する.

断面幾何種数と随伴束の大域切断の次元 との関係

(Proposition)

$1 \leq i \leq n$ なる任意の整数 i に対して
 $A_i(X, L) = g_i(X, L) + g_{i-1}(X, L) - h^{i-1}(\mathcal{O}_X)$
が成り立つ.

断面幾何種数と随伴束の大域切断の次元 との関係

(Theorem) 任意の正整数 t と $1 \leq i \leq n$ なる任意の整数 i に対して $F_{n-i}(t) = \sum_{j=0}^i \binom{t-1}{i-j} A_j(X, L)$ が成り立つ.

断面幾何種数と随伴束の大域切断の次元 との関係

とくに $i = n$ とおくと,

$$h^0(K_X + tL) = \sum_{j=0}^n \binom{t-1}{n-j} A_j(X, L)$$

BS予想との関連

上記2つの結果を用いると次が言える.

Conjecture A + Conjecture B $\implies$ BS予想

$A_i(X, L)$ の性質

(Remark) ・ $i = 0$ のとき, $A_0(X, L) = L^n > 0$

・ $i = 1$ のとき, $A_1(X, L) \geq 0$

$A_1(X, L) = 0 \Leftrightarrow (X, L) \cong (\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$

・ $i = n$ のとき, $A_n(X, L) = h^0(K_X + L) \geq 0$

$A_i(X, L)$ の性質

・ $i = 2$ のとき,

$$\dim X \leq 4 \text{ なら } A_2(X, L) \geq 0$$

$$\kappa(X) \geq 0 \text{ なら } A_2(X, L) \geq 2$$

・ $i = 3$ のとき,

$$\kappa(X) \geq 0 \text{ なら } A_3(X, L) \geq 0$$

$A_i(X, L)$ の性質

(Conjecture)

$1 \leq i \leq n$ なる任意の整数 i に対して $A_i(X, L) \geq 0$ が成り立つ.

2. BS予想について

(BS予想)

$(X, L): n$ 次元非特異偏極多様体

$K_X + (n - 1)L$ がnef.

$$\implies h^0(K_X + (n - 1)L) > 0.$$

2. BS予想について

$n = 4$ の場合のBS予想の証明の流れを簡単に見る.

まず $h^1(\mathcal{O}_X) > 0$ となる場合について考える.

$\implies$

このときは, Albanese写像をとることができる. すると $h^0(K_X + 3L) > 0 \Leftrightarrow h^0((K_X + 3L)_F) > 0$ となることがわかる. (ただし F は Albanese 写像の一般ファイバー)

2. BS予想について

F の次元は3以下となるので、低次元における結果を用いてやると $h^0(K_X + 3L) > 0$ がいえる。
したがって今後 $h^1(\mathcal{O}_X) = 0$ とする。

2. BS予想について

もし $\kappa(K_X + 2L) = -\infty$ なら、 $t = 1, 2$ に対して $h^0(K_X + tL) = 0$ 。

$\implies$ Höring の定理より $h^0(K_X + 3L) > 0$ 。

2. BS予想について

Höringの定理

(X, L) を n 次元偏極多様体で $K_X + (n - 1)L$ は nef とする. このとき, $1 \leq t \leq n - 1$ なるある整数 t に対して $h^0(K_X + tL) > 0$ となる.

2. BS予想について

$\kappa(K_X + 2L) \geq 0$ と仮定してよい

$\implies$ 随伴束の理論より $K_X + 2L$ は nef としてよい.

$\Omega_X \langle L \rangle$ が generically nef であるとき,

$$A_2(X, L) + 2A_3(X, L) > 0$$

を証明することができる.

$\implies$

$$h^0(K_X + 3L)$$

$$= A_4(X, L) + 2A_3(X, L) + A_2(X, L) > 0.$$

2. BS予想について

$\Omega_X \langle L \rangle$ が generically nef でないとき,
ある4次元非特異射影多様体 X' と Y , 双有理写像 $\mu : X' \rightarrow X$ そしてあるファイバー空間 $\lambda : X' \rightarrow Y$ が存在して $m := \dim Y < 4$ となり,
 λ の一般ファイバー F_λ は rationally connected となり,
さらに $j \in [0, 4 - m] \cap \mathbb{Q}$ なる任意の j と $D \sim_{\mathbb{Q}} K_{F_\lambda} + j(\mu^*(L))_{F_\lambda}$ をみたす F_λ 上の任意のカルティエ因子 D に対して $h^0(D) = 0$ となるものが存在する.

2. BS予想について

$\dim Y$ による場合分けを行って, 議論をする.

・ $\dim Y = 0$ もしくは 1 の場合. このとき,
 $t = 1, 2, 3$ に対して, $h^0(K_X + tL) = h^0(K_{X'} + \mu^*(tL)) = 0$ となることがわかる.

しかしこれは Höring の定理に矛盾する.

2. BS予想について

・ $\dim Y = 2$ の場合.

$h^0(K_{F_\lambda} + \mu^*(2L)_{F_\lambda}) = 0$ が成り立つ. 一方 $\kappa(K_X + 2L) \geq 0$ より, $\kappa(K_{F_\lambda} + \mu^*(2L)_{F_\lambda}) \geq 0$ が言える.

今 $\dim F_\lambda = 2$ より, $h^0(K_{F_\lambda} + \mu^*(2L)_{F_\lambda}) > 0$ がいえ, 矛盾となる.

2. BS予想について

・ $\dim Y \geq 3$ の場合.

$h^1(\mathcal{O}_X) = 0$ などを用いると $A_2(X, L) < 0$ を示すことができるが, 一方で今の状況の下では $A_2(X, L) \geq 0$ となることを示すことができるので矛盾を示せる.

2. BS予想について

$n = 3, 4$ の時, 以下がいえる.

$$h^0(K_X + (n - 1)L) = 0$$

$\implies (X, L)$ は次のいずれか

- ・ $(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$
- ・ $(\mathbb{Q}^n, \mathcal{O}_{\mathbb{Q}^n}(1))$
- ・ 非特異曲線上のscroll

$h^0(K_X + (n - 1)L) = 1$ なる (X, L) の分類も可能.

3. 随伴束の大域切断の次元に関する 予想・問題

(Conjecture 2) [Ionescu (1990)]

(X, L) : 非特異準偏極多様体で $K_X + L$ が nef.

$$\implies h^0(K_X + L) > 0.$$

3. 随伴束の大域切断の次元に関する 予想・問題

(Conjecture 3)

$(X, L) : n$ 次元偏極多様体 ($n \geq 3$)

もし $\kappa(K_X + (n-2)L) \geq 0$ なら, $h^0(K_X + (n-2)L) > 0$ が成り立つ.

わかっていること

(Conjecture 2, 3)

・ $n = 3$ のときは正しい.

Conjecture 3 を示すには, $K_X + (n-2)L$ は nef と仮定してよいことが随伴束の理論からわかる.

3. 随伴束の大域切断の次元に関する 予想・問題

(Conjecture 4)

(X, L) : n 次元偏極多様体

このとき、次が成り立つ.

- (1) $h^0(K_X + mL) \geq \binom{m-1}{n}$
for every integer $m \geq n + 1$
- (2) $h^0(K_X + nL) > 0$
unless $(X, L) \cong (\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$

わかっていること

(Conjecture 4)

- ・ (1)については $n \leq 4$ では成立.
また $\dim \text{Bs}|L| \leq 1$ なら任意次元で成立.
- ・ (2)については $n \leq 4$ では成立.
 $n \geq 5$ では $h^0(L) > 0$ という条件下では成立.

わかっていること

(Conjecture 4)

- ・ (2) に関して, 上と同じ条件の下で $h^0(K_X + nL) = 1$ なる (X, L) の分類もわかっている.
- ・ (2) の $n = 4$ については最近 Andreatta-Fontanari も示している。arXiv:1703.00758 を参照

3. 随伴束の大域切断の次元に関する 予想・問題

(Conjecture 5)

$(X, L) : n$ 次元偏極多様体 ($n \geq 3$)

$S(X, L) := \{m \in \mathbb{N} \mid h^0(K_X + mL) = 0\}$

このとき, 次が成り立つ.

- (1) If $\#S(X, L) = n$,
then $(X, L) \cong (\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$

3. 随伴束の大域切断の次元に関する 予想・問題

- (2) If $\#S(X, L) = n - 1$,
then $(X, L) \cong (\mathbb{Q}^n, \mathcal{O}_{\mathbb{Q}^n}(1))$ or
a scroll over a smooth projective curve.

わかっていること

(Conjecture 5)

- ・ $n \leq 5$ で成立
- ・ Conjecture 4 が正しいなら, Conjecture 5 も正しい
- ・ $h^0(L) > 0$ なら Conjecture 5 は正しい
- ・ $\forall t \geq n + 1$ に対して $h^0(K_X + tL) > 0$ なら Conjecture 5 は正しい

3. 随伴束の大域切断の次元に関する 予想・問題

(Conjecture 5)に関連して次の問題が考えられる:

(問題1)

$$q(n) := \min\{m \in \mathbb{N} \mid h^0(K_X + pL) > 0 \\ \text{for } \forall p \geq m \text{ and } \forall (X, L)\}$$

とおいたとき, $q(n)$ の値を求めよ.

わかってること

(問題1)に関してわかっていること.

- ・ $n \leq 5$ では $q(n) = n + 1$ が成立.
- ・ 一般次元では $q(n) \leq \frac{n(n+1)}{2} + 1$ がわかっている.

3. 随伴束の大域切断の次元に関する 予想・問題

(Conjecture 6)

$(X, L) : n$ 次元偏極多様体

$0 \leq i \leq n - 1$ なる任意の整数 i に対して,

$$h^0(K_X + (n - i)L) \geq g_i(X, L) - h^i(\mathcal{O}_X)$$

わかっていること

(Conjecture 6)

- ・ $n \leq 3$ のときは $0 \leq i \leq n$ なる任意の i で正しい
- ・ $i = 0$ の時は, $n \leq 4$ で成立
- ・ $i = n - 1$ の時は, 正しい.

わかっていること

(Conjecture 6)

・ $i = 1$ の時は, 論文 (Canad. Math. Bull. 41 (1998), 267–278, Conjecture 3.8) で述べられた予想.

3. 随伴束の大域切断の次元に関する 予想・問題

問題 2 (Tsuji)

任意の正整数 m に対して

$$h^0(K_X + (m + 1)L) \geq h^0(K_X + mL)$$

が成り立つか?

わかっていること

(1) $\dim X \leq 4$ に対しては成立する.

(2) $\dim X \geq 5$ のとき

Conjecture Bが正しければ, 問題の不等式は成立.

環拡大の森田同値

山中 聡

津山工業高等専門学校総合理工学科

2017 年 9 月 22 日

諸定義と導入
主結果

自己紹介

- ▶ 山中聡
- ▶ 津山高専 総合理工学科 先進科学系 助教
- ▶ 専門：数学 $\supset$ 代数学 $\supset$ 環論 $\supset$ 環拡大, 歪多項式環
- ▶ 略歴：
 - ▶ 平成 18 年 3 月：鳥取県立米子西高等学校 卒業
 - ▶ 平成 18～22 年：岡山大学環境理工学部 環境数理学科
 - ▶ 平成 22～24 年：岡山大学大学院自然科学研究科 博士前期課程
 - ▶ 平成 24～27 年：岡山大学大学院自然科学研究科 博士後期課程
 - ▶ 平成 27～29 年：岡山大学大学院自然科学研究科 博士研究員
 - ▶ 平成 29 年 4 月：津山高専総合理工学部先進科学系 助教

Introduction

環拡大の森田同値は宮下庸一により導入され, G -ガロア拡大とフロベニウス拡大は森田不変であることが示された.

その後, 池畑秀一により, 分離拡大, 平田分離拡大, symmetric 拡大, QF-拡大も森田不変であることが示された.

この発表では環拡大の森田同値の理論を解説するとともに, 上記以外の森田不変な環拡大を紹介する.

発表の流れ

- ① 諸定義と導入
 - 環拡大の森田同値の定義と性質
 - 環拡大の森田同値に関する既知の結果
- ② 主結果
 - 森田不変な環拡大
 - 森田不変でない環拡大

1. 諸定義と導入

環の森田同値

環 A, A' について, 左 A -加群の圏 ${}_A\mathcal{M}$ と左 A' -加群の圏 ${}_{A'}\mathcal{M}'$ が圏同値となるとき, A と A' は **森田同値** (Morita equivalence) であるという.

定理 1.1 (Morita)

環 A, A' について, 次は同値.

1. A と A' は森田同値.
2. 射影生成加群 ${}_AM$ (有限生成射影的かつ生成加群) が存在して, $\text{End}^r({}_AM) \cong A'$ が成り立つ.
この ${}_AM_{A'}$ を **森田加群** (Morita module) という.

森田同値によって不変な環に関する性質は **森田不変** (Morita invariant) であると言われる. 例えば, 単純環, 半単純環, 左 (または右) ネーター環, 左 (または右) アルティン環, 有限次元多元環は森田不変な性質である. 一方, 整域, 可換環のどは森田不変でない.

環拡大の森田同値

環 A が環 B の拡大環 (B が A の部分環) となるとき, A/B と表す.

定義 1.2 (Miyashita, 1970)

2つの環拡大 $A/B, A'/B'$ について, 2つの森田加群 ${}_A M_{A'}, {}_{B'} N_{B'}$ が存在して, ${}_A A \otimes_B N_{B'} \cong {}_A M_{B'}$ が成り立つとき, A/B と A'/B' は **森田同値** (Morita equivalence) であるという.

例 1.3

環拡大 A/B について, A/B と $\mathbb{M}_n(A)/\mathbb{M}_n(B)$ ($n > 1$) は森田同値である. 実際,

$$M := \overbrace{A \oplus A \oplus \cdots \oplus A}^n, N := \overbrace{B \oplus B \oplus \cdots \oplus B}^n$$

と定めれば, ${}_A A \otimes_B N_{\mathbb{M}_n(B)} \cong {}_A M_{\mathbb{M}_n(B)}$ が成り立つ.

環拡大の森田同値の基本事項 (1/2)

以降, 本発表では A/B と A'/B' は森田同値であるとし, ${}_A M_{A'}$ と ${}_{B'} N_{B'}$ をそれに関する森田加群とする (すなわち, ${}_A A \otimes_B N_{B'} \cong {}_A M_{B'}$).

また, $N^* := \text{Hom}^r({}_B N, {}_B B)$ と定め, $\rho \in N^*$ による $u \in N$ の像を $u\rho$ で表す.

ここで ${}_B N$ が射影生成加群であることより, 有限個の元の組 $\{f_j, m_j\}$ と $\{g_k, n_k\}$ ($g_k, f_j \in N^*, n_k, m_j \in N$) が存在して, 以下が成り立つことに注意しておく.

1. 任意の $n \in N$ について, $n = \sum_j n f_j \cdot m_j$ が成り立つ.
(この $\{f_j, m_j\}$ を ${}_B N$ の双対基底 (dual basis) という.)
2. $\sum_k n_k g_k = 1$.

環拡大の森田同値の基本事項 (2/2)

ここで以下の写像 α を考える.

$$\begin{aligned}\alpha : N^* \otimes_B A \otimes_B N &\longrightarrow A' \cong \text{End}^r({}_A M) \cong \text{End}^r({}_A A \otimes_B N) \\ \rho \otimes x \otimes u &\longmapsto [y \otimes v \mapsto y \cdot v \rho \cdot x \otimes u]\end{aligned}$$

このとき, α は $B'-B'$ -同型である (逆写像は $h \mapsto \sum_j f_j \otimes (1 \otimes m_j)h$ で与えられる). さらに, α は $N^* \otimes_B B \otimes_B N \cong B'$ を誘導する.

ここで $N^* \otimes_B A \otimes_B N$ における積を以下のように定めることが出来る.

$$(\rho \otimes x \otimes u)(\sigma \otimes y \otimes v) := \rho \otimes x \cdot u \sigma \cdot y \otimes v.$$

これにより $N^* \otimes_B A \otimes_B N$ は環をなす (単位元は $\sum_j f_j \otimes 1 \otimes m_j$).

A/B と A'/B' が森田同値ならば,

$$A' = N^* \otimes_B A \otimes_B N \text{ かつ } B' = N^* \otimes_B B \otimes_B N \text{ (環として同一視)}.$$

既知の結果 (1/4)

補題 1.4 (Ikehata, 1975)

森田同値な環拡大 A/B , A'/B' について,

1. ${}_B A$ が有限生成射影的ならば, ${}_{B'} A'$ も有限生成射影的である.
2. ${}_B A$ が生成加群ならば, ${}_{B'} A'$ も生成加群である.

既知の結果 (2/4)

環 A の部分集合 X について, 以下のように定める.

$$V_A(X) := \{\alpha \in A \mid \alpha x = x\alpha \ (\forall x \in X)\}$$

とくに, 環拡大 A/B について, $V_A(B)$ は A における B の中心化環 (centralizer) であり, $V_A(A)$ および $V_B(B)$ はそれぞれ A および B の中心 (center) である.

補題 1.5 (Ikehata, 1975)

森田同値な環拡大 $A/B, A'/B'$ について, 森田加群 ${}_B N$ の双対基底を $\{f_j, m_j\}$ とするとき, 写像

$$\varphi : A \longrightarrow A', a \longmapsto \sum_j f_j \otimes a \otimes m_j$$

環同型 $V_A(B) \cong V_{A'}(B'), V_A(A) \cong V_{A'}(A'), V_B(B) \cong V_{B'}(B')$ を誘導する.

既知の結果 (3/4)

補題 1.6 (Ikehata 1975)

森田同値な環拡大 $A/B, A'/B'$ について, 写像

$$\begin{aligned} \rho : \text{End}^\ell({}_B A_B) &\longrightarrow \text{End}^\ell({}_{B'} A'_{B'}) = \text{End}^\ell({}_{B'} N^* \otimes A \otimes N_{B'}) \\ \eta &\longmapsto 1 \otimes \eta \otimes 1 \end{aligned}$$

について, 以下が成り立つ.

1. ρ は環同型である.
2. ρ は加法群の同型 $\text{Hom}^\ell({}_B A_B, {}_B B_B) \cong \text{Hom}^\ell({}_{B'} A'_{B'}, {}_{B'} B'_{B'})$ を誘導する.
3. ρ は加法群の同型 $\text{Aut}^\ell(A/B) \cong \text{Aut}^\ell(A'/B')$ を誘導する.
4. H が $\text{Aut}^\ell(A/B)$ の部分群で, $A^H = B$ のとき, $A'^{\rho(H)} = B'$ が成り立つ.

既知の結果 (4/4)

環拡大 A/B について, 以下のように定める.

$$(A \otimes_B A)^A := \{\mu \in A \otimes_B A \mid \mu\alpha = \alpha\mu \ (\forall \alpha \in A)\}$$

補題 1.7 (Ikehata 1975)

森田同値な環拡大 $A/B, A'/B'$ について, $\{f_j, m_j\}$ および $\{g_k, n_k\}$ を射影生成加群 ${}_B N$ の2つの元の組とする. このとき, 写像

$$\begin{aligned} \psi : A \otimes_B A &\longrightarrow A' \otimes_{B'} A' \\ x \otimes y &\longmapsto \sum_{j,k} (f_j \otimes x \otimes n_k) \otimes (g_k \otimes y \otimes m_j) \end{aligned}$$

は加法群の同型 $(A \otimes_B A)^A \cong (A' \otimes_{B'} A')^{A'}$ を誘導する.

森田不変な環拡大 (既知の結果)

森田同値で不変な環拡大は**森田不変** (Morita invariant) であると言われる.

定理 1.8 (Miyashita, 1970)

以下の環拡大は森田不変である.

1. G -ガロア拡大
2. フロベニウス拡大

定理 1.9 (Ikehata, 1975)

以下の環拡大は森田不変である.

1. 分離拡大
2. 平田分離拡大 (H -分離拡大)
3. symmetric 拡大
4. QF-拡大

2. 主結果

強分離拡大 (strongly separable extension)

定義 2.1 (Mewborn - McMahon, 1984)

環拡大 A/B について, $V = V_A(B)$, $C = V_A(A)$ とおく. このとき, A/B が **強分離拡大** (strongly separable extension) であるとは, ${}_C V$ が 有限生成射影的であり, A - A -準同型

$$\begin{aligned}\alpha : A \otimes_B A &\longrightarrow \operatorname{Hom}^\ell(V_C, A_C) \\ x \otimes y &\longmapsto [v \mapsto xvy]\end{aligned}$$

が分裂全射 (split epimorphism) になるときにいう.

定理 2.2 (Y, 2016)

強分離拡大は森田不変である.

定理 2.2 の証明の概略 (1/2)

補題 2.3 (Sugano, 1996)

環拡大 A/B が強分離的であるための必要十分条件は, 有限個の $v_i \in V_A(B)$ と $\sum_r x_{ir} \otimes y_{ir} \in (A \otimes_B A)^A$ が存在して, 任意の $u \in V_A(B)$ について $u = \sum_{i,r} v_i x_{ir} u y_{ir}$ が成り立つことである.

[証明] A/B と A'/B' は森田同値で, A/B が強分離的であるとし, $v_i \in V_A(B)$ および $\sum_r x_{ir} \otimes y_{ir} \in (A \otimes_B A)^A$ を上の補題の条件をみたす元の組とする.

$$\begin{aligned} \sum_r x'_{ir} \otimes y'_{ir} &:= \sum_{r,j,k} (f_j \otimes x_{ir} \otimes n_k) \otimes (g_k \otimes y_{ir} \otimes m_j), \\ v'_i &:= \sum_{\lambda} f_{\lambda} \otimes v_i \otimes m_{\lambda} \end{aligned}$$

と定めると, $v'_i \in V_{A'}(B')$ かつ $\sum_r x'_{ir} \otimes y'_{ir} \in (A' \otimes_{B'} A')^{A'}$ となる.

定理 2.2 の証明の概略 (2/2)

任意の $u' = \sum_{\ell} f_{\ell} \otimes u \otimes m_{\ell} \in V_{A'}(B')$ ($u \in V_A(B)$) について,

$$\begin{aligned} \sum_{i,r} v'_i x'_{ir} u' y'_{ir} &= \sum_{i,r,\lambda,j,k,\ell} (f_{\lambda} \otimes v_i \cdot m_{\lambda} f_j \cdot x_{ir} \otimes n_k) (f_{\ell} \otimes u \cdot m_{\ell} g_k \cdot y_{ir} \otimes m_j) \\ &= \sum_{i,r,\lambda,j,k,\ell} (f_{\lambda} \cdot m_{\lambda} f_j \otimes v_i \cdot x_{ir} \otimes n_k) (f_{\ell} \cdot m_{\ell} g_k \otimes u \cdot y_{ir} \otimes m_j) \\ &= \sum_{i,r,j,k} (f_j \otimes v_i \cdot x_{ir} \otimes n_k) (g_k \otimes u \cdot y_{ir} \otimes m_j) \\ &= \sum_j f_j \otimes \left(\sum_{i,r} v_i \cdot x_{ir} \cdot u \cdot y_{ir} \right) \otimes m_j \\ &= \sum_j f_j \otimes u \otimes m_j \\ &= u'. \end{aligned}$$

したがって, A'/B' も強分離的である. □

depth two 拡大

定義 2.4 (Kadison - Szlachányi, 2003)

環拡大 A/B が左 (または右) **depth two 拡大** (depth two extension) であるとは, $A \otimes_B A$ が A の有限個の直和の直和因子に B - A -同型 (または A - B -同型) になるときにいう.

定理 2.5 (Y, 2016)

左 (または右) depth two 拡大は森田不変である.

証明に関する Key lemmas

補題 2.6 (Y, 2016)

森田同値な環拡大 $A/B, A'/B'$ について, 補題 1.7 にける写像 ψ は加法群の同型 $(A \otimes_B A)^B \cong (A' \otimes_{B'} A')^{B'}$ を誘導する.

補題 2.7 (Kadison - Szlachányi, 2003)

環拡大 A/B が 左 (または右) depth two 拡大であるための必要十分条件は, 有限個の $t_i \in (A \otimes_B A)^B$ と $\beta_i \in \text{End}^\ell({}_B A_B)$ が存在して, 任意の $z, w \in A$ に対し, $\sum_i t_i \cdot \beta_i z \cdot w = z \otimes w$ (または $\sum_i z \cdot \beta_i w \cdot t_i = z \otimes w$) が成り立つことである.

定理 2.5 の証明の概略 (1/2)

[証明] A/B と A'/B' は森田同値で, A/B は左 depth two 拡大であるとし, $t_i = \sum_r x_{ir} \otimes y_{ir} \in (A \otimes_B A)^B$ および $\beta_i \in \text{End}^\ell({}_B A_B)$ を先の補題の条件を満たす元の組とする.

$$t'_i := \sum_{r,j,k} (f_j \otimes x_{ir} \otimes n_k) \otimes (g_k \otimes y_{ir} \otimes m_j) \quad \text{および} \quad \beta'_i := 1 \otimes \beta_i \otimes 1$$

と定めれば, $t'_i \in (A' \otimes_{B'} A')^{B'}$ かつ $\beta'_i \in \text{End}^\ell({}_{B'} A'_{B'})$ となる.
ここで, 以下の $B'-B'$ -同型 θ を考える.

$$\begin{aligned} \theta : A' \otimes_{B'} A' &\longrightarrow N^* \otimes_B A \otimes_B A \otimes_B N \\ (\rho \otimes x \otimes u) \otimes (\sigma \otimes y \otimes v) &\longmapsto \rho \otimes x \cdot u \sigma \otimes y \otimes v \end{aligned}$$

(θ^{-1} は $\rho \otimes x \otimes y \otimes u \mapsto \sum_k (\rho \otimes x \otimes n_k) \otimes (g_k \otimes y \otimes u)$ で与えられる)

定理 2.5 の証明の概略 (2/2)

任意の $z' = \sum_\lambda \rho_\lambda \otimes z_\lambda \otimes u_\lambda$, $w' = \sum_\mu \sigma_\mu \otimes w_\mu \otimes v_\mu \in A'$ について,
 $\theta(z' \otimes w') = \sum_{\lambda,\mu} \rho_\lambda \otimes z_\lambda \otimes u_\lambda \sigma_\mu \cdot w_\mu \otimes v_\mu$, であり,

$$\begin{aligned} &\theta\left(\sum_i t'_i \beta'_i(z') w'\right) \\ &= \theta\left(\sum_{i,r,\lambda,\mu,j,k} (f_j \otimes x_{ir} \otimes n_k) \otimes (g_k \otimes y_{ir} \cdot m_j \rho_\lambda \cdot \beta_i z_\lambda \cdot u_\lambda \sigma_\mu \cdot w_\mu \otimes v_\mu)\right) \\ &= \sum_{\lambda,\mu,j} f_j \cdot m_j \rho_\lambda \otimes \left(\sum_i t_i \cdot \beta_i z_\lambda \cdot u_\lambda \sigma_\mu \cdot w_\mu\right) \otimes v_\mu \\ &= \sum_{\lambda,\mu} \rho_\lambda \otimes z_\lambda \otimes u_\lambda \sigma_\mu \cdot w_\mu \otimes v_\mu. \end{aligned}$$

これより $\sum_i t'_i \beta'_i(z') w' = z' \otimes w'$ を得るので, A'/B' は左 depth two 拡大である. $\square$

弱分離拡大

環拡大 A/B と両側 A - A -加群 S について, 加法的な写像 $D : A \rightarrow S$ が **B -微分** (B -derivation) であるとは, $D(xy) = D(x)y + xD(y)$ ($\forall x, y \in A$) かつ $D(\beta) = 0$ ($\forall \beta \in B$) が成り立つときにいう.

定義 2.8 (Hamaguchi - Nakajima, 2013)

環拡大 A/B が**弱分離拡大** (weakly separable extension) であるとは, 任意の B -微分 $D : A \rightarrow A$ が内部的 (inner), すなわち, 適当な $u \in A$ が存在して $D(x) = ux - xu$ となるときにいう.

定理 2.9 (Y, 2016)

弱分離拡大は森田不変である.

証明に関する Key Lemma

補題 2.10

A/B と A'/B' は森田同値とする. 両側 A - A -加群 S に対し, $S' := N^* \otimes_B S \otimes_B N$ とおき, 以下のように定める.

$$\begin{aligned} \text{Der}_B(A, S) &:= \{D \mid D : A \rightarrow S \text{ は } B\text{-微分} \} \\ \text{Der}_{B'}(A', S') &:= \{D' \mid D' : A' \rightarrow S' \text{ は } B'\text{-微分} \} \end{aligned}$$

このとき,

$$\begin{aligned} \tau : \text{Der}_B(A, S) &\longrightarrow \text{Der}_{B'}(A', S') \\ D &\longmapsto 1 \otimes D \otimes 1 \end{aligned}$$

は加法群の同型である.

定理 2.9 の証明の概略 (1/2)

[証明] A/B と A'/B' は森田同値で, A/B は弱分離的とする.

任意の B' -微分 D' について, 先の補題より適当な B -微分 D が存在して $D' = 1 \otimes D \otimes 1$ が成り立つ.

A/B は弱分離的だから, 適当な $v \in A$ が存在して $D(x) = vx - xv$ ($x \in A$) と表される. とくに, $v \in V_A(B)$ に注意しておく.

また, $v' = \sum_j f_j \otimes v \otimes m_j$ とおく.

定理 2.9 の証明の概略 (2/2)

このとき, 任意の $x' = \sum_r \rho_r \otimes x_r \otimes u_r \in A'$ について,

$$\begin{aligned}
 D'(x') &= \sum_r \rho_r \otimes D(x_r) \otimes u_r \\
 &= \sum_r \rho_r \otimes (vx_r - x_r v) \otimes u_r \\
 &= \sum_r \left\{ \left(\sum_i f_i \cdot m_i \rho_r \right) \otimes vx_r \otimes u_r - \rho_r \otimes x_r v \otimes \left(\sum_j u_r f_j \cdot m_j \right) \right\} \\
 &= \sum_{r,i,j} (f_i \otimes v \cdot m_i \rho_r \cdot x_r \otimes u_r - \rho_r \otimes x_r \cdot u_r f_j \cdot v \otimes m_j) \\
 &= \sum_{r,i,j} \{ (f_i \otimes v \otimes m_i)(\rho_r \otimes x_r \otimes u_r) - (\rho_r \otimes x_r \otimes u_r)(f_j \otimes v \otimes m_j) \} \\
 &= v'x' - x'v'.
 \end{aligned}$$

したがって, D' は内部的である. □

その他の環拡大について

- ▶ 環拡大 A/B が **自明な拡大** (trivial extension) であるとは、適当な両側 B - B -加群 S が存在して、 $A = B \oplus S$ かつ A における積が $(b, s)(c, t) = (bc, bt + sc)$ ($b, c \in B, s, t \in S$) で与えられるときにいう。
- ▶ 環拡大 A/B が **centralizing 拡大** (centralizing extension) であるとは、 $A = V_A(B)B := \{\sum_i v_i b_i \mid v_i \in V_A(B), b_i \in B\}$ が成り立つときにいう。

命題 2.11 (Y, 2016)

自明な拡大は森田不変である。

命題 2.12 (Y, 2016)

centralizing 拡大は森田不変である。

森田不変でない環拡大の例 (1/2)

k を素数標数 p の体とし、 $A = k[t]$, $B = k[t^p]$ とおき、環拡大 A/B を考える。このとき、 $\{x^p \mid x \in A\} \subseteq B$ となる。

先の例 1.3 より、 A/B と $M_2(A)/M_2(B)$ は森田同値である。

一方、 $X := \begin{bmatrix} 1 & t \\ 0 & 0 \end{bmatrix} \in M_2(A)$ を考えると、任意の自然数 n について $X^n = X \notin M_2(B)$ であるから、以下のような環拡大の性質は森田不変でない。

環拡大 A/B について、適当な自然数 $n > 1$ が存在して $\{x^n \mid x \in A\} \subseteq B$ が成り立つ。

森田不変でない環拡大の例 (2/2)

定義 2.13

環拡大 A/B が**擬似分離拡大** (quasi-separable extension) であるとは, 任意の両側 A - A -加群 S について, A から S への中心的 B -微分がすべて 0 であるときにいう.

ここで B -微分 D が**中心的** (central) であるとは, $yD(x) = D(x)y$ ($\forall x, y \in A$) が成り立つことを意味する.

補題 2.14 (Komatsu, 2001)

任意の環拡大 A/B について, $M_n(A)/M_n(B)$ ($n > 1$) は擬似分離拡大である.

系 2.15

擬似分離拡大は森田不変でない.

参考文献

1. S. Ikehata, *On Morita equivalence in ring extensions*, Math. J. Okayama Univ. **18** (1975), 73–79.
2. Y. Miyashita, *On Galois extensions and crossed products*, J. Fac. Sci. Hokkaido Univ., Ser.I **21** (1970), 97–121.
3. S. Yamanaka, *Note on Morita equivalence in ring extensions*, Comm. in Algebra **44** (2016), no.9, 4121–4131.

Thank you for your attention!!

二次方程式の実数解の個数の割合

海城中学三年 *島倫太郎 **清水琢也

1 本研究の概要

本研究は、昨年8月に京都大学で開催されたマifestaにおいて清心女子高校(倉敷市)二年の坪倉、前田両女史が発表された内容を拡張すべく、共同で研究したものである。

本研究の目的は以下の通りである。

目的

$f(x) = ax^2 + bx + c = 0$ ($a \neq 0$) の定数 a, b, c が独立して、閉区間 $[-r, r]$ ($r \geq 0$) の値を同様に確からしくとるとする。
このとき、 r の値を変動させると、 $f(x) = 0$ の実数解の個数の割合がどのように変化するかを調べる。

2 主結果

2.1 $r = 10$ で、 a, b, c が区間内の整数値のみをとるとき

実数解の個数ごとの確率は次の通り

相異なる二実数解を持つ	: 63.1%
重解を持つ	: 0.9%
実数解を持たない	: 36.0%

2.2 $r \rightarrow \infty$ としたとき

a, b, c が整数値のみをとるとしたとき、範囲内の実数を全てとりうるとしたときの確率は、いずれも次の通り

相異なる二実数解を持つ	: $41/72 + \log 2/12 \approx 62.7\%$
重解を持つ	: 限りなく 0 に近い
実数解を持たない	: $31/72 - \log 2/12 \approx 37.3\%$

特に、 a, b, c が範囲内の実数を全てとりうるとしたときは、 r の値に関わらず、解の個数の割合は上の通りになる。

3 証明のアイデア

a, b, c が整数値のみをとるとしたときは、一辺 $2r$ で中心が O の立方体と、 $z^2 = 4xy$ の交点のうち、格子点であるものの個数を数えて割合を導出した。 $r \rightarrow \infty$ の場合は、解の個数の割合を r のみで表す式を導出し、離散モデルを不等式評価してから、はさみうちの原理を適用することで連続関数の極限を計算して導出した。

a, b, c が範囲内の実数を全てとりうるとしたときは、上で述べた立方体の、曲線 $z^2 = 4xy$ で分けられた部分ごとに積分して体積を計算することで割合を導出した。

なお、本発表の内容に関する論文を準備中である。

連絡先

島 : shima.rin1206@ezweb.ne.jp 清水 : shimizu24862@gmail.com