楕円曲線を通じた Brumer と Lecacheux の 5 次多項式族の研究

小柴将和

自然科学研究科数理物質科学専攻
博士前期課程 2 年

2019 年 2 月 8 日

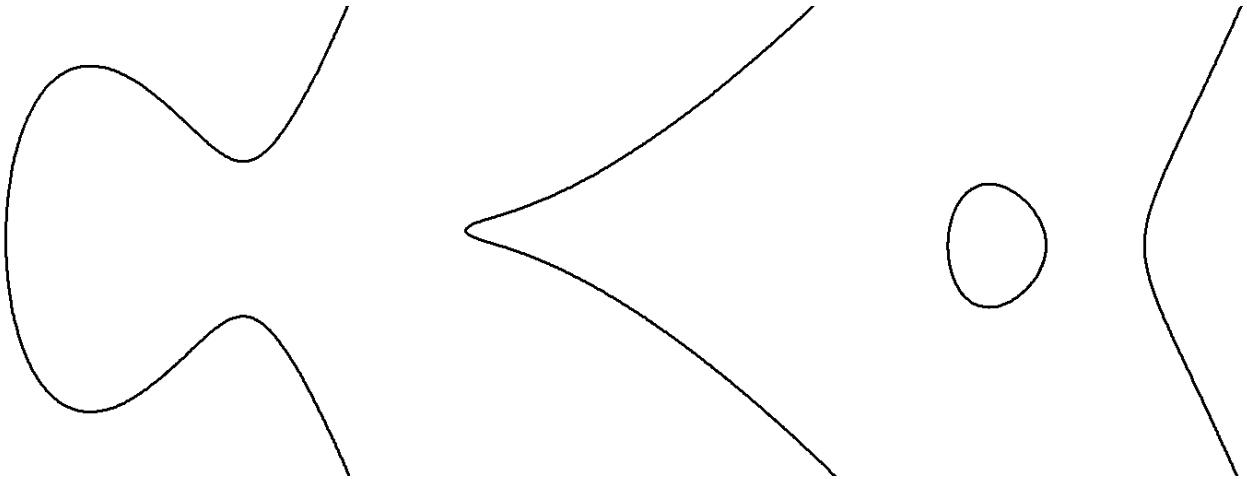
§1. Introduction

楕円曲線とは 3 次式

$$y^2 = x^3 + ax^2 + bx + c \quad (D \neq 0)$$

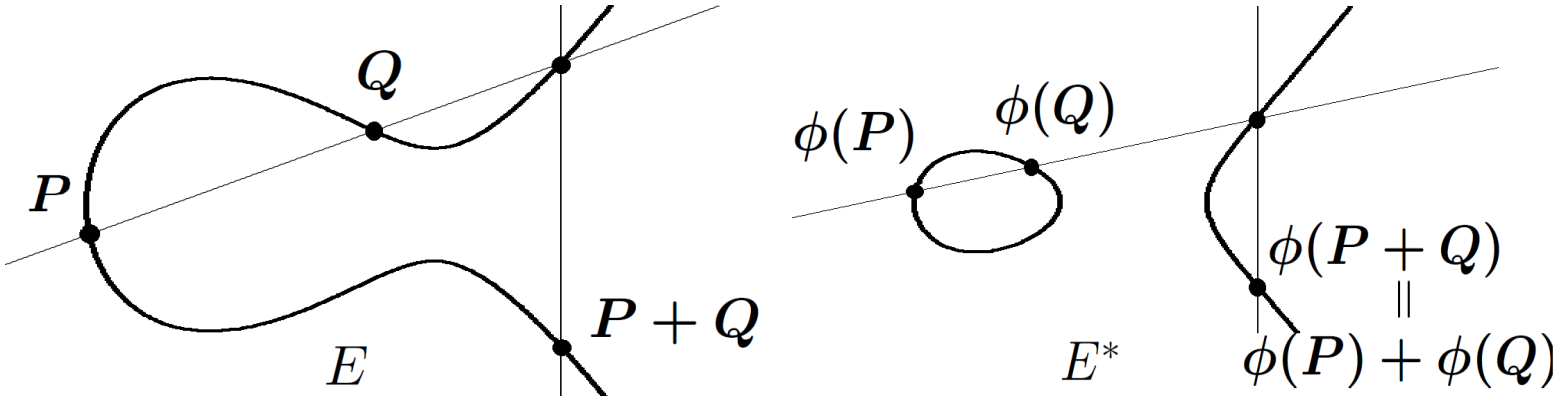
で定義された代数多様体のこと.

楕円曲線のグラフ



$y^2 = x^3 - 3x + 3$　　$y^2 = x^3 + x$　　$y^2 = x^3 - x$

有理点の和と同種写像



同種写像 $\phi : E \to E^*$ は楕円曲線の群構造を保存するような写像. すなわち, $P, Q \in E$ に対して,

$$\phi(P+Q) = \phi(P) + \phi(Q)$$

が成り立つ.

ガロアの逆問題

体 K と可移部分群 $G \subset \mathrm{S}_n$ に対し, $\mathrm{Gal}(f/K) = G$ となるような $f(X) \in K[X]$ は存在するか.

$$\begin{array}{ccc} \mathrm{Spl}_{\mathbb{Q}}(f) & \longrightarrow & \{1\} \\ | & & | \\ \mathbb{Q} & \longrightarrow & \mathrm{Gal}(f/\mathbb{Q}) = G\ ? \end{array}$$

5 次方程式	ガロア群
$f_1 = x^5 - x^3 - x^2 + x + 1 = 0$	S_5
$f_2 = x^5 + x^4 - 2x^2 - 2x - 2 = 0$	A_5
$f_3 = x^5 + x^4 + 2x^3 + 4x^2 + x + 1 = 0$	F_{20}
$f_4 = x^5 - x^3 - 2x^2 - 2x - 1 = 0$	D_5
$f_5 = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0$	C_5

例 $G = \underline{D_5}$ (A. Brumer 1995 年)

次の多項式は $\mathbb{Q}$ 上 D_5 生成的多項式である:

$$X^5+(t-3)X^4+(s-t+3)X^3+(t^2-t-2s-1)X^2+sX+t.$$

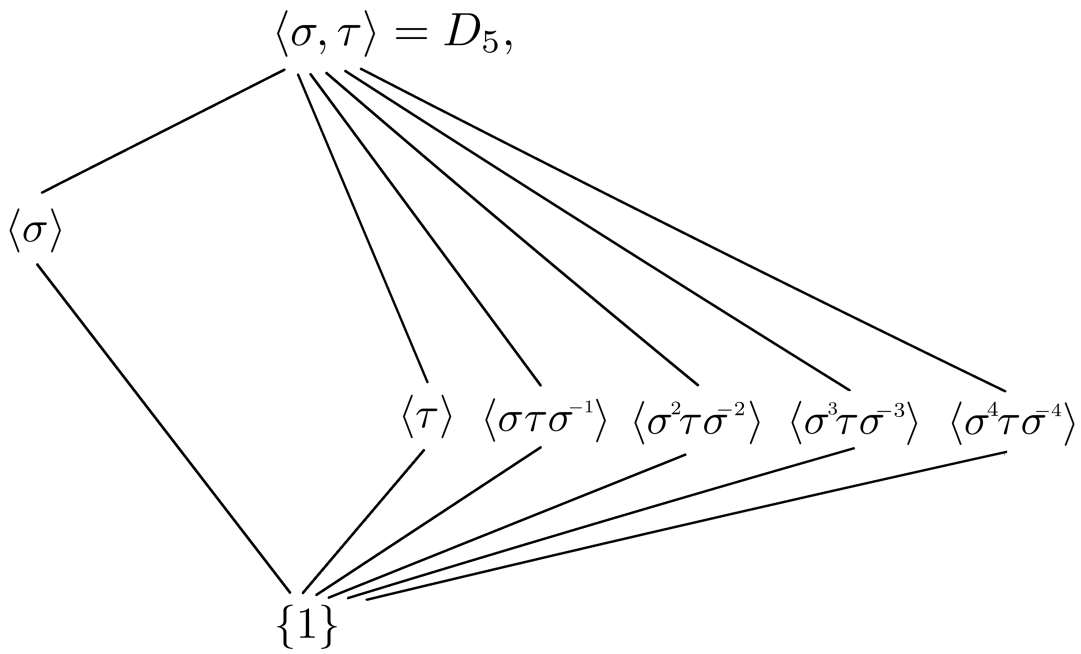
例 $G = \underline{F_{20}}$ (O. Lecacheux 1998 年)

次の多項式は $\mathbb{Q}$ 上 F_{20} 生成的多項式である:

$$X^5 + (r^2d + 2p + \tfrac{17}{4})X^4 + ((3r+1)d + \tfrac{13p}{2} + 1)X^3 + (rd + \tfrac{11p}{2} - 8)X^2 + (p-6)X - 1.$$

ここで $d = p^2 + 4$

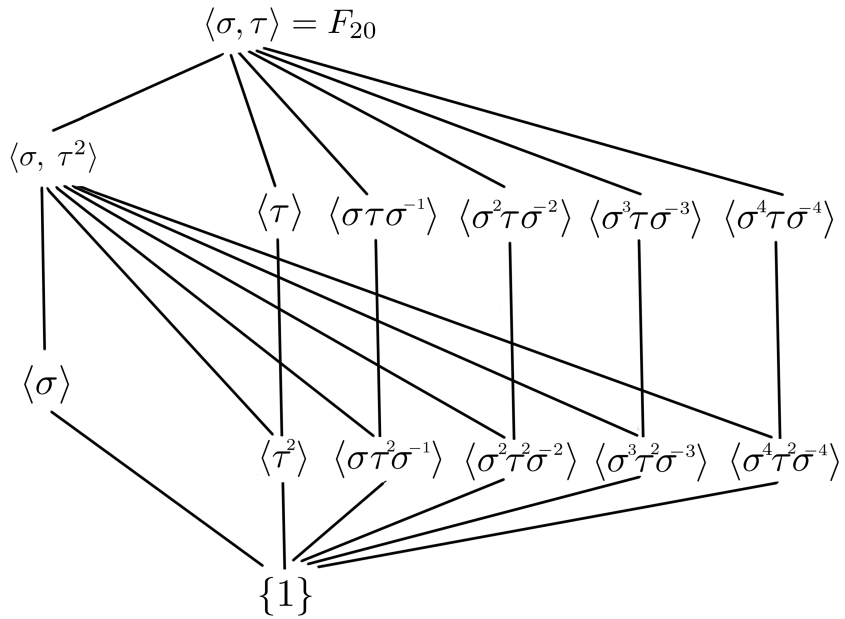
$$D_5 = \langle \sigma, \tau | \sigma^5 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$$



Brumer 多項式 $f_{s,t}^{D_5}$:

$$X^5+(t-3)X^4+(s-t+3)X^3+(t^2-t-2s-1)X^2+sX+t.$$

$$F_{20} = \langle \sigma, \tau | \sigma^5 = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^2 \rangle$$



Lecacheux 多項式 $g_{p,r}^{F_{20}}$:

$$X^5 + (r^2d + 2p + \tfrac{17}{4})X^4 + ((3r+1)d + \tfrac{13p}{2} + 1)X^3 + (rd + \tfrac{11p}{2} - 8)X^2 + (p-6)X - 1 \ (d = p^2 + 4).$$

$f_{s,t}^{D_5}$: Brumer 多項式, $K_{s,t} := \mathrm{Spl}_{\mathbb{Q}}\left(f_{s,t}^{D_5}\right)$

$g_{p,r}^{F_{20}}$: Lecacheux 多項式, $L_{p,r} := \mathrm{Spl}_{\mathbb{Q}}\left(g_{p,r}^{F_{20}}\right)$

Question

- $K_{s,t} \cong K_{s',t'}$? $L_{p,r} \cong L_{p',r'}$? (同型問題)

Brumer 多項式と Lecacheux 多項式について

	Brumer 多項式	Lecacheux 多項式
個別	星, 三宅 (2010 年)	
無限	木田, 陸名, 佐藤 (2010 年)	?

- (星, 三宅 2010 年) (s,t), $(p,r) \in \mathbb{Z}^2$ での同型の組.
  $K_{s,t}$: $-400 \leq s,t \leq 400$ 25 組
  $L_{p,r}$: $-100 \leq p,r \leq 100$ 11 組

- (木田, 陸名, 佐藤 2010 年)
  楕円曲線を用いて同型族を考察.

定理 (主結果 別バージョン)

$g_{p,r}^{F_{20}}$: Lecacheux 多項式,

$L_{p,r} := \mathrm{Spl}_{\mathbb{Q}}\left(g_{p,r}^{F_{20}}\right)$.

$P \in E_{p,r}(\mathbb{Q})$ に対して,

$$L_{p,\frac{x(P)}{4dW}} \cong L_{p,\frac{x([2]P)}{4dW}}.$$

ここで,

$d := p^2 + 4$,

$W := 16dr^3 + 4dr^2 - 4(19p + 41)r - (16p + 199)$.

§2. 主結果と証明

先行研究

$$\begin{array}{c} K_{s,t} \\ 5 \Big| \\ \mathbb{Q}(\sqrt{d_{s,t}}) \\ 2 \Big| \\ \mathbb{Q} \end{array}$$

1. $s, t \in \mathbb{Q}$ を固定する.
2. $d_{s,t} = -4s^3 + (t^2 - 30t + 1)s^2 + 2t(3t + 1)(4t - 7)s - t(4t^4 - 4t^3 - 40t^2 + 91t - 4).$
3. $d_{s,t}u^2 = d_{s',t'}.$
4. $t' = t,\ (X, Y) := (-4d_{s,t}s', 4d_{s,t}^2 u).$

$$E_{s,t} : Y^2 = X^3 + d_{s,t}(t^2 - 30t + 1)X^2 - 8d_{s,t}^2 t(3t+1)(4t-7)X - 16d_{s,t}^3 t(4t^4 - 4t^3 - 40t^2 + 91t - 4).$$

このとき,

$$^{\exists}\phi : E_{s,t} \xrightarrow{5} E_{s,t}^*,$$

$$\phi^* : E_{s,t}^* \xrightarrow{5} E_{s,t}.$$

定理 (木田, 陸名, 佐藤 2010 年)

前の記号のもと, $f_P^{D_5} := f^{D_5}_{x(P)/(-4d),t}$ $(P \in E_{s,t}(\mathbb{Q}))$ とすれば,
次が成り立つ:

1. 有理点 $P \in E_{s,t}(\mathbb{Q})$ に対して,
   $f_P^{D_5}$ が $\mathbb{Q}$ 上可約 $\iff$ $P \in \phi^*(E^*_{s,t}(\mathbb{Q}))$.

2. 集合

$$\{\mathrm{Spl}_{\mathbb{Q}}(f_P^{D_5}(X)) | P \in E_{s,t}(\mathbb{Q}) \setminus \phi^*(E^*_{s,t}(\mathbb{Q}))\}$$
$$\updownarrow 1:1$$
$$\{E_{s,t}(\mathbb{Q})/\phi^*(E^*_{s,t}) \text{ の位数 } 5 \text{ である部分群 }\},$$

   が $E_{s,t}(\mathbb{Q}) \ni P \mapsto f_P^{D_5}$ によって引き起される.

主結果

$$
\begin{array}{c}
L_{p,r} \\
5 \Big| \\
\mathbb{Q}(\sqrt{d_{p,r}}) \\
2 \Big| \\
\mathbb{Q}(\sqrt{p^2+4}) \\
2 \Big| \\
\mathbb{Q}
\end{array}
$$

1. $p, r \in \mathbb{Q}$ を固定する.
2. $W_{p,r} := 16(p^2+4)r^3 + 4(p^2+4)r^2 - 4(19p+41)r - 16p - 199,$
   $d_{p,r} = W_{p,r}((p^4+5p^2+4) + p(p^2+3)\sqrt{p^2+4})/8.$
3. $W_{p,r}u^2 = W_{p',r'}.$
4. $p' = p,$
   $(X, Y) := (4(p^2+4)W_{p,r}r', 2(p^2+4)W_{p,r}^2 u)$

$$E_{p,r} : Y^2 = X^3 + (p^2+4)W_{p,r}X^2 - 4(19p+41)W_{p,r}^2 X - 4(p^2+4)^2(16p+199)W_{p,r}^3$$

$P \in E_{p,r}(\mathbb{Q})$ に対し $g_P^{F_{20}} := g_{p,x(P)/(4(p^2+4)W)}^{F_{20}}$ とする.

このとき, $\mathrm{Spl}_{\mathbb{Q}}\left(g_P^{F_{20}}\right) \cong \mathrm{Spl}_{\mathbb{Q}}\left(g_{[2]P}^{F_{20}}\right)$ が成り立つ.

定理 (主結果)

$g_{p,r}^{F_{20}}$:Lecacheux 多項式,

$L_{p,r} := \mathrm{Spl}_{\mathbb{Q}(p,r)}\left(g_{p,r}^{F_{20}}\right)$.

$\psi(p,r) := a(p,r)/(4dW)$ とする.

- $d := p^2 + 4$,
- $a(p,r) := 16d^2r^4 + 8d(19p+41)r^2 + 4(32p^3 + 398p^2 + 128p + 159)r + 16p^3 + 560p^2 + 1622p + 2477$,
- $W := 16dr^3 + 4dr^2 - 4(19p+41)r - (16p+199)$.

$$L_{p,r} \cong L_{p,\psi(p,r)}$$

多重分解多項式

$F^1_{\mathbf{s},\mathbf{s}'}(X), F^2_{\mathbf{s},\mathbf{s}'}(X)$ $(S=(s,t), S'=(s',t'))$ を次で定義する.

$$F^1_{\mathbf{s},\mathbf{s}'}(X) := (G^1_{\mathbf{s},\mathbf{s}'}(X))^2 - \frac{d^2 d'^2}{4}(G^2_{\mathbf{s},\mathbf{s}'}(X))^2 \in k(s,t,s',t')[X],$$

$$F^2_{\mathbf{s},\mathbf{s}'}(X) := F^1_{(\frac{s+5t}{t^2},-\frac{1}{t}),(s',t')}(X).$$

ここで,

$$G^1_{\mathbf{s},\mathbf{s}'}(X) = X^5 - (t-3)(t'-3)X^4 + c_3X^3 + \frac{c_2}{2}X^2 + \frac{c_1}{2}X + \frac{c_0}{2},$$

$$G^2_{\mathbf{s},\mathbf{s}'}(X) = X^2 + (t+t'-1)X + s - t + s' - t' + tt' + 2.$$

$$d^2 = s^2 - 4s^3 + 4t - 14st - 30s^2t - 91t^2 - 34st^2 + s^2t^2 + 40t^3 + 24st^3 + 4t^4 - 4t^5, \quad d'^2 = \iota(d)^2.$$

$c_3,\ c_2,\ c_1,\ c_0 \in k(s,t,s',t')$ は次で与えられる:

$$
\begin{aligned}
c_3 =& [2s - 21t + 3t^2 - 2ts' + t^2s' - t^2t'] + 31 - 3ss' + 5tt',\\
c_2 =& [-20s + 112t + 8st - 32t^2 + 2t^3 + 5ts' - 13sts' - 12t^2s' + 4t^3s' - 15stt' + 14t^2t'\\
& + 2t^3t' + 8t^2s't' - 2t^3t'^2] - 102 + 27ss' - 119tt' - sts't' + 6t^2t'^2,\\
c_1 =& [32s + 2s^2 - 128t - 26st + 60t^2 + 4st^2 - 8t^3 - 6s^2s' - 7ts' + 38sts' + 9t^2s'\\
& - 5st^2s' - 12t^3s' + 2t^4s' - 20ts'^2 - 8sts'^2 + 6t^2s'^2 + 2t^3s'^2 + 2stt' - 77t^2t'\\
& + 3st^2t' + 8t^3t' - 29t^2s't' + st^2s't' + 18t^3s't' - 2st^2t'^2 + 10t^3t'^2]\\
& + 80 - 37ss' + 145tt' - 45sts't' + 24t^2t'^2 - 8t^3t'^3,\\
c_0 =& [-16s - 2s^2 + 56t + 24st + 2s^2t - 38t^2 - 8st^2 + 8t^3 + 5s^2s' - 2ts' - 38sts'\\
& - 7s^2ts' + 5t^2s' + 13st^2s' + 8t^3s' + 2st^3s' - 4t^4s' - 21ts'^2 - 11sts'^2 - 2t^2s'^2\\
& + 2st^2s'^2 + 4t^3s'^2 - 104stt' - 33s^2tt' + 105t^2t' + 35st^2t' + 4t^3t' + 16st^3t' - 2t^5t'\\
& - s^2ts't' + 36t^2s't' - 14st^2s't' - 6t^3s't' + 6t^4s't'8t^2s'^2t' - 37st^2t'^2 + 22t^3t'^2\\
& + 8t^4t'^2 + 8t^3s't'^2 - 2t^4t'^3] - 24 + 14ss' - 8s^2s'^2 - 224tt' + sts't' - 101t^2t'^2\\
& - st^2s't'^2 - 8t^3t'^3.
\end{aligned}
$$

ただし, $a \in k(s,t,s',t')$ に対して $[a] := a + \iota(a)$ としている. ι は $\iota(s,t,s',t') = (s',t',s,t)$ によって定義されるものとする.

定理 (星, 三宅 2010 年)

$f_{s,t}^{D_5}$ を, $\mathbf{a} = (a_1, a_2), \mathbf{a}' = (a_1', a_2') \in M^2$ で特殊化したときの最小分解体のガロア群をそれぞれ $G_{\mathbf{a}}$, $G_{\mathbf{a}'}$ として $G_{\mathbf{a}} \geq G_{\mathbf{a}'} \geq C_5$ を仮定する.
$f_{s,t}^{D_5}(X)$ の $\mathbf{a} = (a_1, a_2), \mathbf{a}' = (a_1', a_2') \in M^2$ による特殊化で得られる体の共通部分の様子は $F^1_{\mathbf{a},\mathbf{a}'}, F^2_{\mathbf{a},\mathbf{a}'}$ の M 上での因数分解の型により次の表のように分類される:

$G_{\mathbf{a}}$	$G'_{\mathbf{a}}$	$G_{\mathbf{a},\mathbf{a}'}$		$F^1_{\mathbf{a},\mathbf{a}'}$	$F^2_{\mathbf{a},\mathbf{a}'}$
D_5	D_5	$D_5 \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
		$(C_5 \times C_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	5^2	5^2
		D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5, 2^2, 1$	5^2
		D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	5^2	$5, 2^2, 1$
	C_5	$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
C_5	C_5	$C_5 \times C_5$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	5^2	5^2
		C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5, 1^5$	5^2
		C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	5^2	$5, 1^5$

Lecacheux 多項式の同型の判定

$f_{s,t}^{D_5}$ を $\mathbb{Q}(\sqrt{p^2+4})$ 上で $g_{p,r}^{F_{20}}$ に変換して D_5 での結果を用いる:

$$s = -\frac{1}{4}(5p + 8r + 2p^2 r + (2pr+5)\sqrt{p^2+4}),$$
$$t = \frac{1}{2}(p + \sqrt{p^2+4}).$$

主結果の証明

上の判定法を利用する.

$F_{\mathbf{s},\mathbf{s}'}^1(X), F_{\mathbf{s},\mathbf{s}'}^2(X)$ に (p,r) と $(p,\psi(p,r))$ を変換した後, 代入し因数分解すると, $F_{\mathbf{s},\mathbf{s}'}^2(X)$ が次の一次因子を持つことがわかる:

$$\left(X + \frac{1+2r}{2}\sqrt{p^2+4} + \frac{p-1}{2}\right).$$

□

今後の課題

- 木田, 陸名, 佐藤の定理の Lecacheux 多項式の場合の証明を付ける.
- p が異なる場合に同型になるときを考察する.

	Brumer 多項式	Lecacheux 多項式
個別	星, 三宅 (2010 年)	
無限	木田, 陸名, 佐藤 (2010 年)	?

定理 (主結果)

$g_{p,r}^{F_{20}}$:Lecacheux 多項式,

$$L_{p,r} := \mathrm{Spl}_{\mathbb{Q}(p,r)}\left(g_{p,r}^{F_{20}}\right).$$

$\psi(p,r) := a(p,r)/(4dW)$ とする.

- $d := p^2 + 4$,
- $a(p,r) := 16d^2r^4 + 8d(19p+41)r^2 + 4(32p^3 + 398p^2 + 128p + 159)r + 16p^3 + 560p^2 + 1622p + 2477$,
- $W := 16dr^3 + 4dr^2 - 4(19p+41)r - (16p+199)$.

$$L_{p,r} \cong L_{p,\psi(p,r)}$$